Institute of Mathematics

Factorization of Natural Numbers based on Quaternion Algebra using Lipschitz Integers

Master thesis of
Milan Markovic

Written under supervision of
Prof. Dr. Joachim Rosenthal and Dr. Felix Fontein

2014

Preface

Factorization of integers is still a very difficult task. And there are only few sub-exponential algorithms for factoring integers.

In 1770, Lagrange proved the Bachet de Méziriac conjecture, that every positive integer can be written as a sum of four squares. And by the Theorem of Jacobi, for an odd natural number $n \in \mathbb{N}$, there exist

$$8 \sum_{d|n} d$$

different tuples (a_1, a_2, a_3, a_4) with $a_l \in \mathbb{Z}$ for all $l \in \{1, \ldots, 4\}$ such that the sum $a_1^2 + a_2^2 + a_3^2 + a_4^2 = n$. By using the quaternion algebra, we can construct $8 \sum_{d|n} d$ different integral quaternions $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ such that the norm of those quaternions is $N(\alpha) = \alpha\overline{\alpha} = a_1^2 + a_2^2 + a_3^2 + a_4^2 = n$.

On the other hand, Lipschitz has proven a fundamental theorem in the arithmetics of quaternions which states that a quaternion $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ with norm $N(\alpha) = n$ has a unique right divisor up to its left-associates of the norm p if $\gcd(a_1, a_2, a_3, a_4, p) = 1$ and $p|n$.

Even though the Lipschitz ring is not an Euclidean domain, with some small restrictions we can show the existence of the greatest common right divisor of two Lipschitz integers.

So we can pose the question "Can we find two Lipschitz integers of the same norm n having a greatest common right divisor, which is a non-trivial factor?" And since we can compute the greatest common right divisor of two Lipschitz integers with the norm n in polynomial time, there is the question "How difficult is it to find such two Lipschitz integers?" But unfortunately, there is still no sub-exponential factorization algorithm using Lipschitz integers.

In this thesis we will prove that every natural number n is a sum of four squares, we will show the arithmetics of quaternion algebra and Lipschitz ring, and we will see the algorithm that constructs a Lipschitz integer with norm n in polynomial time. At the end of this thesis, we will present a factorization algorithm using the Lipschitz integers. But unfortunately, this algorithm returns a result in exponential time.

This thesis is split into six chapters:

Chapter 1 introduces the idea and motivation of this thesis. In the second part, there is also an introduction to some basic notations used throughout this thesis.

Chapter 2 is about presenting the numbers as a sum of two squares. Since the ring of Gaussian integers appears to be very practical for this subject, there is a short discussion of the Gaussian integers and their properties. In the second section, there is the theory on numbers as a sum of two squares.

Chapter 3 goes in to the discussions of the quaternion algebras. In this chapter we will present some general properties of the quaternions in quaternion algebras over the field or ring of the characteristic different 2. There will also be presentations of the Lipschitz and Hurwitz ring, which are sub-rings of the Hamiltonian division ring. The main focus of this chapter lies on the Lipschitz ring.

Chapter 4 presents the formulas for computing exact number of two and four square presentations of a natural number n. In the first part of this chapter, we will discuss the formula for two square presentation of n, and in the second part, we will see the formula of Jacobi, which computes the number of different four square presentations of n.

Chapter 5 presents two randomly probabilistic algorithms published by Michael O. Rabin and Jeffery O. Shallit [3], in which you find a solution for a two square problem respectively four square presentation in polynomial time.

Chapter 6 presents a factorization algorithm using the Lipschitz integers. The theory supporting this algorithm will be presented at the beginning of this chapter. There you will see that this algorithm finds a solution, but unfortunately in exponential time.

Contents

Chapter 1

Introduction

1.1 Motivation

The factorization problem has been challenging generations over the centuries. Since we still do not know if there exists a deterministic algorithm that computes a factor of a positive integer n in polynomial time, there is lot of research into the question "Is factorization NP-complete?" And because the factorization is of great importance for cryptography, lot of research has been done to find out "How fast we can find a non-trivial factor of a given integer that is a product of two large primes" so that we can prove or disprove if security communication protocols based on factorization of such numbers as RSA, are indeed secure.

This thesis will concentrate on constructing a factorization algorithm using the Lipschitz integers. The ideas of this thesis are based on the paper [1] of Professors António Machiavelo and Luís Roçadas. They suggested that some properties of Lipschitz and Hurwitz integers can be used to compute factors of any composed natural number. They also pointed out that there might exist some interesting results, since there is no known sub-exponential factorization algorithm based on Lipschitz or Hurwitz integers.

It is known that we can compute a presentation as a sum of two squares for some positive integers $n \in \mathbb{N}$. So we can find a Gaussian integer $\alpha = a + bi \in \mathbb{Z}[i]$ which has a norm $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$. If we find another Gaussian integer β with $N(\beta) = N(\alpha)$, we can compute the greatest common divisor (g.c.d.) of α and β, whose norm must divide n. And therefore, for some β, the norm of g.c.d. can be a non-trivial factor of n.

In paper [1], they use a similar idea to compute factors for some number n by looking for Lipschitz integers that have the same norm. As we will see in the Section 3.3 (we can also see it in Appendix Chapter C), we can present any positive integer as a sum of four squares, i.e. we can find a Lipschitz integer of the form $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ that has a norm $N(\alpha) = \alpha\overline{\alpha} = a_1^2 + a_2^2 + a_3^2 + a_4^2 = n$ for any $n \in \mathbb{N}$. And from the Jacobi Theorem 4.2.6 we see that there are $8\sum_{d|n} d$ different presentations for an odd integer $n \in \mathbb{N}$. So by computing such two different integral quaternions α and β, we can compute the greatest common right divisor (g.c.r.d.) of α and β, which norm must divide n. But not any pair of two Lipschitz integers will have g.c.r.d. with a norm equal to the non-trivial factor of n.

In paper [2], Gordon Pall has proven, that for two given integral quaternions α and β of the same norm, they have the same left or right divisor or they have the same both divisors if they are orthogonal and their integral coordinates are pairwise co-prime. This led António Machiavelo and Luís Roçadas to look for the orthogonal quaternions to the given quaternion. If we found such an orthogonal quaternion to a given one, we would be able to compute the non-trivial factors of an composed integer n. As it seams, the results in [1] did not lead to the solution of the method described above.

In this thesis, we will try to construct an algorithm that finds factors of a given composed integer, using the Lipschitz integers and the non-commutativity of quaternions.

Since there are no known factorization algorithms based on quaternion algebra, we will try to find any such algorithm that is better than computing a set of $8(p+1)+1$ different presentations of n, for smallest prime p dividing n, where this set has to have two quaternions with g.c.r.d., which norm is a non-trivial factor of n.

Of course, this algorithm should be able to compute a four square presentation for an integer in polynomial time. Therefore, we will present a probabilistic algorithm stated in [3], that give us the four square presentation of an integer in polynomial time. Since this algorithm uses properties of presenting the numbers as a sum of two squares, we will present the properties of Gaussian integers and also algorithms for computing two square presentations.

1.2 Notations

In this thesis we will use the following notations: the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ which stand as usual for additive group, algebraic rings, algebraic fields and division ring. The set $\mathbb{K}$ will denote an arbitrary ring or field.

The letters a, $b, \ldots, h$, $l, \ldots, x$, y, z are integers or rational numbers. x can also stand for the variable in polynomials. Since we are working mainly with complex numbers and quaternions, the letters i, j, k stand for imaginary numbers, where $i^2 = j^2 = k^2 = -1$.

The Greek letters α, $\beta, \ldots$ stand for complex numbers respectively for quaternions of the form $\alpha = a_1 + a_2 i$ or $\alpha = a_1 + a_2 i + a_3 j + a_4 k$. We will define the norm of a complex number α respectively quaternion α as $N(\alpha) = a_1^2 + a_2^2$ or $N(\alpha) = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

Let be $\alpha_l = a_1 + a_2 i + a_3 j + a_4 k$ an integral quaternions, i.e. $a_s \in \mathbb{Z}$ for $s \in \{1, \ldots, 4\}$. Then we will denote any left-associate of α_l with $\alpha^{(l)}$, i.e. $\alpha^{(l)} = \varepsilon \alpha_l$ for some integral quaternion ε with $N(\varepsilon) = 1$.

Let be $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ and $\beta = b_1 + b_2 i + b_3 j + b_4 k$ two integral quaternions such that $a_s \equiv b_s \bmod n$ for all $s \in \{1, \ldots, 4\}$, where $n \in \mathbb{N}$. Then we can write the following: $\alpha \equiv \beta \bmod n$.

In this thesis we will use some more notations for the sets or elements with some specific properties or forms. For those notations, see the index at the end of this thesis.

Chapter 2

Gaussian integers and the sum of two squares

In this chapter, we are going to show some arithmetics of Gaussian integers and later use them to present the numbers as a sum of two squares.

Note that some integers are not a sum of two squares. Consider an integer $a \in \mathbb{N}$, then $a^2 \equiv 0$ or $1 \bmod 4$. This means that any number $n \in \mathbb{N}$, which is a sum of two squares, can only be congruent 0, 1 or 2 modulo 4, i.e. if $n \equiv 3 \bmod 4$, then n cannot be presented as a sum of two squares.

So in the first section, we will present Gaussian integers and some properties, we will later use to present a number as a sum of two squares.

In the second section, we will prove that all primes $p \equiv 1 \bmod 4$ can be presented as a sum of two squares, which is stated in Theorem 2.2.1. Later on, we will show the main result Corollary 2.2.2, that specifies which positive numbers are a sum of two squares.

2.1 Gaussian integers

In this section, we will introduce the Gaussian integers and the some properties of the ring of the Gaussian integers.

Definition 2.1.1. Gaussian integers are complex numbers that are in the set

$$\mathbb{Z}[i] = \left\{a + bi \mid a, b \in \mathbb{Z},\, i^2 = -1\right\}.$$

Consider that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

We will now list some usual definitions for Gaussian integers:

Definition 2.1.2. Let be $\alpha = a + bi \in \mathbb{Z}[i]$, then

1. we call $a - bi$ the *conjugate* of α and denote it with $\overline{\alpha}$.
2. we define the *norm* of α as
$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 = |\alpha|^2. \tag{2.1}$$
3. we call β an *inverse* of α for $\alpha \neq 0$, if $\alpha\beta = 1$. If such β exists in $\mathbb{Z}[i]$, we denote it with α^{-1} and we say that α is *invertible*.

Let be $\alpha \in \mathbb{Z}[i]$, with $N(\alpha) = a_1^2 + a_2^2 = a \in \mathbb{N}$. Then is a integer a a sum of two squares and it is always a positive integer.

Proposition 2.1.3. This norm $N(\cdot)$ is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. Let be $\alpha = a_1 + a_2 i$ and $\beta = b_1 + b_2 i$ two Gaussian integers, then we can compute the product $\alpha\beta = (a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1)\, i$. Using this multiplication, we get

$$\begin{aligned} N(\alpha\beta) &= (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_1 b_2)^2 \\ &= (a_1 b_1)^2 + (a_2 b_2)^2 - 2a_1 a_2 b_1 b_2 + (a_1 b_2)^2 + (a_2 b_1)^2 + 2a_1 a_2 b_1 b_2 \\ &= (a_1 b_1)^2 + (a_2 b_2)^2 + (a_1 b_2)^2 + (a_2 b_1)^2 \\ &= \left(a_1^2 + a_2^2\right)\left(b_1^2 + b_2^2\right) \\ &= N(\alpha)N(\beta). \end{aligned} \tag{2.2}$$

□

Proposition 2.1.3 implicates that two integers $N(\alpha) = a$ and $N(\beta) = b$ are the sums of two squares, then the product $n = ab$ is a sum of two squares too. Later we will use this to simplify the problem of presenting a number as a sum of two squares.

Now consider an arbitrary $\alpha \in \mathbb{Z}[i]$. Then α has an inverse in $\mathbb{Z}[i]$, if

$$\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)} = \frac{a_1}{N(\alpha)} - \frac{a_2}{N(\alpha)} i \in \mathbb{Z}[i].$$

Definition 2.1.4. We say that $\varepsilon \in \mathbb{Z}[i]\backslash\{0\}$ is a *unit* if ε is invertible in $\mathbb{Z}[i]$, i.e. ε^{-1} exists in $\mathbb{Z}[i]$.

Lemma 2.1.5. An element $\varepsilon \in \mathbb{Z}[i]\backslash\{0\}$ is a unit if and only if $N(\varepsilon) = 1$.

Proof. If ε is a unit, then there exists ε^{-1} in $\mathbb{Z}[i]$ such that $\varepsilon\varepsilon^{-1} = 1$ and following holds:

$$1 = N(1) = N(\varepsilon\varepsilon^{-1}) = N(\varepsilon)N(\varepsilon^{-1}). \tag{2.3}$$

Since the norm of a Gaussian integer is always a positive integer, from the equation above we can follow that $N(\varepsilon) = N(\varepsilon^{-1}) = 1$.

If $N(\varepsilon) = 1$ for some $\varepsilon \in \mathbb{Z}[i]$, then ε can only be the element from the set $\{\pm 1, \pm i\}$. But then there exists such $\varepsilon^{-1} \in \{\pm 1, \pm i\}$ such that $\varepsilon\varepsilon^{-1} = 1$. □

As we already saw in the proof above all units $\varepsilon \in \mathbb{Z}[i]$ are $\{1, -1, i, -i\} \subset \mathbb{Z}[i]$. From this we can also easily follow that by multiplying any Gaussian integer α by a unit ε we do not change the value of the norm.

Definition 2.1.6. The Gaussian integers α and β are called *associates* if there exists a unit $\varepsilon \in \mathbb{Z}[i]$ such that $\alpha = \varepsilon\beta$.

In the next part, we want to show that $\mathbb{Z}[i]$ is an Euclidean domain and that any Gaussian integer has a unique factorization.

Proposition 2.1.7. Let α, $\beta \in \mathbb{Z}[i]$, where $\beta \neq 0$. There exists γ, $\delta \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \delta$ and $N(\delta) < N(\beta)$.

Proof. Consider the complex number

$$\frac{\alpha}{\beta} = \alpha\frac{\overline{\beta}}{N(\beta)} = x + yi \in \mathbb{C} \qquad x, y \in \mathbb{R}. \tag{2.4}$$

Then choose m,$n \in \mathbb{Z}$ such that $|x - m| \leq \frac{1}{2}$ and $|y - n| \leq \frac{1}{2}$. Set $\gamma = m + ni \in \mathbb{Z}[i]$ and $\delta = \beta[(x - m) + i(y - n)]$. Consider $\frac{\alpha}{\beta} = \gamma + \frac{\delta}{\beta}$. Clearly $\alpha = \gamma\beta + \delta$ and $\delta = \alpha - \beta\gamma \in \mathbb{Z}[i]$, i.e. δ is a Gaussian integer. Now we can compute

$$N\left(\frac{\delta}{\beta}\right) = (x - m)^2 + (y - n)^2 \leq \frac{1}{2} \tag{2.5}$$

and from this follows $N(\delta) \leq 1/2N(\beta) < N(\beta)$. □

Definition 2.1.8. Let be α,$\beta \in \mathbb{Z}[i]$, then

1. we say α *divides* β if there exists $\gamma \in \mathbb{Z}[i]$ such that $\beta = \gamma\alpha$.
2. we say $\delta \in \mathbb{Z}[i]$ is a *greatest common divisor* (short g.c.d.) of α and β if δ divides α and β, and whenever γ divides α and β, it also divides δ. We will denote it by $\gcd(\alpha, \beta) = \delta$.

Proposition 2.1.9. For any $\alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$, there exists a unique greatest common divisor $\gcd(\alpha, \beta) \in \mathbb{Z}[i]$ up to its associates. Moreover, there exist $\gamma, \delta \in \mathbb{Z}[i]$ such that $\gcd(\alpha, \beta) = \alpha\gamma + \beta\delta$.

Proof. Let be $I = (\alpha, \beta)$ an ideal generated by α and β. We can find

$$\mu = \alpha\gamma + \beta\delta \in I, \tag{2.6}$$

with the smallest norm different from zero, where γ, $\delta \in \mathbb{Z}[i]$.

Consider that $N(\alpha) \geq N(\mu)$. By Proposition 2.1.7, we can find σ_1 and τ_1 such that $\alpha = \sigma_1\mu + \tau_1$ and $N(\tau_1) < N(\mu)$. This means that $\tau_1 = \alpha - \sigma_1\mu$, which implies that τ is an element of I. Since μ is the element with the smallest norm different from zero in I and $N(\tau_1) < N(\mu)$, then τ_1 has to be zero. So we have that $\alpha = \sigma_1\mu + 0 = \sigma_1\mu$, and by Definition 2.1.8 point 1, μ divides α. In the same way, we can show that μ also has to divide β.

Now we know that μ is one common divisor of α and β, and we want to show that μ has to be the greatest common divisor of α and β.

Let be ρ any common divisor of α and β. Then write the equation $\mu = \rho(\sigma_1\gamma + \sigma_2\delta)$, where $\alpha = \rho\sigma_1$ and $\beta = \rho\sigma_2$. Here we see that any such common divisor ρ has to divide μ, and by Definition 2.1.8 point 2, μ is the greatest common divisor of α and β.

From equation (2.6), we see that there exist γ and δ, such that $\gcd(\alpha, \beta) = \alpha\gamma + \beta\delta$.

Now assume μ_1 and μ_2 are two greatest common divisors. Then by the definition we know that $\mu_1|\mu_2$ and $\mu_2|\mu_1$. Meaning that we can find $\tilde{\mu}_1$ and $\tilde{\mu}_2$ such that

$$\mu_2 = \mu_1\tilde{\mu}_2 \text{ and } \mu_1 = \mu_2\tilde{\mu}_1,$$

and following holds:

$$N(\mu_2) = N(\mu_1)N(\tilde{\mu}_2) \text{ and } N(\mu_1) = N(\mu_2)N(\tilde{\mu}_1).$$

By substituting this two equations we get that

$$\frac{N(\mu_1)}{N(\tilde{\mu}_1)} = N(\mu_1)N(\tilde{\mu}_2) \quad \Rightarrow \quad N(\tilde{\mu}_1)N(\tilde{\mu}_2) = 1.$$

And from the last equation we see that $\tilde{\mu}_1$ and $\tilde{\mu}_2$ are units, meaning that μ_1 and μ_2 are associated. □

Note that if $\gcd(\alpha, \beta) \in \{\pm 1, \pm i\}$, then we call α and β *relatively prime* or *co-prime*. Since ± 1 and $\pm i$ are pairwise associated, we can simply write $\gcd(\alpha, \beta) = 1$.

In the next proposition we want to show that any Gaussian integer, with a norm bigger than one, can be written as the product of prime Gaussian integers and that there is a unique factorization up to their associates.

Definition 2.1.10. A Gaussian integer $\pi \in \mathbb{Z}[i]$ is *prime* if π is not a unit in $\mathbb{Z}[i]$ and for any α,$\beta \in \mathbb{Z}[i]$, such that $\pi = \alpha\beta$, then either α or β is a unit in $\mathbb{Z}[i]$.

Proposition 2.1.11. $\pi \in \mathbb{Z}[i]$ is a prime if and only if, whenever π divides a product $\alpha\beta$, for some α, $\beta \in \mathbb{Z}[i]$, then π divides at least α or β.

Proof. ($\Rightarrow$) First we assume that π is a prime that divides the product $\alpha\beta$. Now we want to show that if π does not divide one of the factors, then it has to divide another one.

So assume that $\pi|\alpha\beta$ and π do not divide one of factors. Without loss of generality we can say that $\pi \nmid \alpha$. Then $\gcd(\pi, \alpha) = 1$ and by Proposition 2.1.9 we can find $\gamma, \delta \in \mathbb{Z}[i]$ such that

$$\pi\gamma + \alpha\delta = 1. \tag{2.7}$$

By multiplying the equation (2.7) with β, we get $\beta = \pi\gamma\beta + \alpha\beta\delta$. Since $\pi|\alpha\beta$, we can write $\alpha\beta = \pi\sigma_1$ for some $\sigma_1 \in \mathbb{Z}[i]$ and we have the equation

$$\beta = \pi\gamma\beta + \pi\sigma_1\delta = \pi(\gamma\beta + \sigma_1\delta), \tag{2.8}$$

which proves that π has to divide β.

($\Leftarrow$) We will prove this direction by constructing the contra-position.

Claim 2.1.12. If π is not a prime, then there exist α and β such that $\pi|\alpha\beta$ and π do not divide neither α nor β.

Assuming π is not a prime, we can find α and β such that $\pi = \alpha\beta$ and neither α nor β are units. Considering that π does not divide both α and β, proves the claim above.

And from the contraposition of Claim 2.1.12 follows: whenever $\pi|\alpha\beta$ and π divides either α or β, then π has to be a prime.

□

Proposition 2.1.13. Every non-zero element in $\mathbb{Z}[i]$, which is not a unit and not in $\mathbb{Z}$, it is in a unique way a product of primes in $\mathbb{Z}[i]$. More precisely, if $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ with $N(\alpha) > 1$, then $\alpha = \pi_1\pi_2\cdots\pi_r$ for some primes $\pi_1, \pi_2, \ldots, \pi_r$ in $\mathbb{Z}[i]$. And if $\alpha = \pi_1\pi_2\cdots\pi_r = \sigma_1\sigma_2\cdots\sigma_l$ are two factorizations of α into primes, then $r = l$ and, after permuting the induces, π_h is associated to σ_h, for all $h \in \{1, 2, \ldots, r\}$.

Proof. First, we will give a short idea how to prove the existence of such factorization by using the induction steps over the norm of Gaussian integers.

Let be $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) > 1$. If α is a prime Gaussian integer, we have a trivial case and the proposition holds.

So assume that $\alpha \in \mathbb{Z}[i]$ is not a prime. By Definition 2.1.10, we can find γ_1 and δ_1 such that $\alpha = \gamma_1\delta_1$, where neither of the factors is a unit. By multiplicity of the norm, we know that $N(\alpha) = N(\gamma_1)N(\delta_1)$. Since γ_1 and δ_1 are not units, $N(\gamma_1), N(\delta_1) > 1$, which implies

$$N(\alpha) > N(\gamma_1), N(\delta_1) > 1. \tag{2.9}$$

Considering that a norm of Gaussian integers is always a natural number, the following inequality holds:

$$N(\gamma_1),\ N(\delta_1) \leq \frac{N(\alpha)}{2}. \tag{2.10}$$

If both factors are primes, the proposition holds. If at least one of the factors is not a prime, by Definition 2.1.10 we can find two new factors with smaller norm. We can do this until all factors are primes and we are not able to factor them further in non-invertible elements. From the inequality (2.10), we can easily see that we need at most $\log_2(N(\alpha))$ steps, till we have found one factorization.

At the end we get that $\alpha = \pi_1\pi_2\cdots\pi_r$ for some $r \leq \log_2(N(\alpha))$, $r \in \mathbb{N}$, where π_s is a prime for all $s \in \{1, \ldots, r\}$.

In the second part, we want to show the uniqueness of the prime factorization. So let be

$$\alpha = \pi_1\pi_2\cdots\pi_r = \sigma_1\sigma_2\cdots\sigma_l \tag{2.11}$$

two different prime factorizations for some $\alpha \in \mathbb{Z}[i]$ and $r, l \in \mathbb{N}$. Consider that all π_s's for $s \in \{1,\dots,r\}$ and all σ_m's for $m \in \{1,\dots,l\}$ are prime Gaussian integers.

First, we want to show that for any π_s , there exists σ_m such that $\pi_s = \varepsilon\sigma_m$, where ε is a unit. From the equation (2.11) follows that any π_s for $s \in \{1,\dots,l\}$ divides α and $\sigma_1\sigma_2\cdots\sigma_r$. And Proposition 2.1.11 implies that for any $s \in \{1,\dots,r\}$, we can find $m \in \{1,\dots,r\}$, such that $\pi_s = \varepsilon\sigma_m$, since π_s and σ_m are primes. But then ε has to be a unit. Analogous, we can show that for any σ_m , there exists π_s such that $\sigma_m = \varepsilon\pi_s$, where ε is a unit.

In the next part, we want to show that r and l have to be equal. So assume that $r \leq l$. From above, we know that π_1 is a prime that divides α and $\sigma_1\sigma_2\cdots\sigma_l$. Meaning that there exists a σ_s such that $\pi_1|\sigma_s$ and $\sigma_s = \varepsilon_1\pi_1$ for some $s \in \{1,\dots,l\}$. Without loss of generality, take $\pi_1|\sigma_1$ and $\sigma_1 = \varepsilon_1\pi_1$. Recall that ε_1 has to be a unit. So we can write the equation (2.11) as follows:

$$\varepsilon_1\sigma_1\pi_2\cdots\pi_r = \sigma_1\sigma_2\cdots\sigma_l \Rightarrow \varepsilon_1\pi_2\cdots\pi_r = \sigma_2\cdots\sigma_l. \tag{2.12}$$

Now we can construct the induction steps. Assume that for some $t \in \mathbb{N}$ and $t < r$ the following holds:

$$\pi_o|\sigma_o \quad \forall o \in \{1,\dots,t\} \quad \text{and} \quad \varepsilon_1\cdots\varepsilon_t\pi_{t+1}\cdots\pi_r = \sigma_{t+1}\cdots\sigma_l.$$

Then for $t+1$ we know that $\pi_{t+1}|\varepsilon_1\cdots\varepsilon_t\pi_{t+1}\cdots\pi_r = \sigma_{t+1}\cdots\sigma_l$. Without loss of generality, take that $\pi_{t+1}|\sigma_{t+1}$ and $\sigma_{t+1} = \varepsilon_{t+1}\pi_{t+1}$. And we can write:

$$\varepsilon_1\cdots\varepsilon_{t+1}\pi_{t+2}\cdots\pi_r = \sigma_{t+2}\cdots\sigma_l.$$

By this induction we see that last equation holds for all $t \leq r$.

On the other hand, assuming that $l \leq r$ we can show the following:

$$\pi_{t+2}\cdots\pi_r = \varepsilon_1\cdots\varepsilon_{t+1}\sigma_{t+2}\cdots\sigma_l \quad \forall t \leq l,$$

by constructing the correspondent induction steps for some $t < l$.

Using the two inductions above, it follows that $r \leq l$ and $r \geq l$ and $r = l$, which proves the proposition. □

2.2 Two square presentation

In this section, we will state and prove in Corollary 2.2.2 which numbers are a sum of two squares. The idea of this proof is to show that a positive integer n is a sum of two squares, if and only if, there exists a factorization of $n = f_1 f_2 \dots f_w$ (f_t's not necessarily primes) such that f_t is a sum of two squares for all $t \in \{1,\dots,w\}$. Then we can find a Gaussian integer $\phi_t \in \mathbb{Z}[i]$, with $N(\phi_t) = f_t$ for all $t \in \{1,\dots,w\}$. And from the multiplicity of the norm, we can build a Gaussian integer $\alpha = a + bi = \prod_t \phi_t$, where

$$a^2 + b^2 = N(\alpha) = \prod_t N(\phi_t) = \prod_t f_t = n. \tag{2.13}$$

So in the first part, we will discuss which prime integers are a sum of two squares.

As we already mentioned, all positive integers n, which are congruent to 3 modulo 4, cannot be presented as a sum of two squares since the sum of any two squares can only give the congruence to 0,1 or 2 modulo 4.

So we see that 2 is a sum of two squares, namely $1^2 + 1^2 = 2$, and it can be presented by four Gaussian integers $(\pm 1 \pm i)$.

The next theorem is famous result stated by Fermat around 1640, and first proved by Euler in 1793, which states that every prime integer $p \equiv 1 \bmod 4$ is a sum of two squares.

Theorem 2.2.1. Let be p an odd prime in $\mathbb{N}$. The following are equivalent:

1. $p \equiv 1 \bmod 4$.
2. -1 is a quadratic residue in $\mathbb{F}_p$, i.e. there exits $x \in \mathbb{F}_p$ such that $x^2 \equiv -1 \bmod p$.
3. p is a sum of two squares.

Proof. (1. $\Leftrightarrow$ 2.) We will prove this equivalence by splitting the set $\mathbb{F}_p^*$ in small distinct sets P_x, where

$$P_x = \left\{x, -x, x^{-1}, -x^{-1}\right\}. \tag{2.14}$$

By the construction of those sets, we will see that most of them have four elements apart from two possible exceptions with only two elements. One of them will always exist, and the other one will only exist if $x^2 \equiv -1 \bmod p$ has a solution. This will create equivalence between points 1. and 2.

First define the set

$$P_x = \left\{x, -x, x^{-1}, -x^{-1}\right\}, \tag{2.15}$$

where $x \in \mathbb{F}_p^*$. Consider that for all x_1, $x_2 \in \mathbb{F}_p^*$, where $x_1 \neq x_2$, the sets P_{x_1} and P_{x_2} are equal or distinct sets.

In general, set P_x has four elements, except if there exist $x \in \mathbb{F}_p$, such that one of the following holds: $x \equiv -x \bmod p$, $x \equiv x^{-1} \bmod p$ or $x \equiv -x^{-1} \bmod p$.

The first case $x \equiv -x \bmod p$ cannot happen since p is an odd prime. The second case $x \equiv x^{-1} \bmod p$ can only happen if $x = \pm 1$. Then the set $P_1 = \{1, -1\}$ has two elements. Note that P_1 always exists in any $\mathbb{F}_p^*$. The last case $x \equiv -x^{-1} \bmod p$ can only happen if there exits $x \in \mathbb{F}_p^*$, such that $x^2 \equiv -1 \bmod p$. In this case, we have another set P_x with two elements.

So we see that we always have one set P_x with two elements, namely P_1. And if there exists $x \in \mathbb{F}_p$, such that $x \equiv -x^{-1} \bmod p$, then there are two sets P_x's with two elements.

This means that if $p \equiv 3 \bmod 4$, then there is only one set P_x with two elements, namely P_1. And there is no element $x \in \mathbb{Z}_p^*$, such that $x \equiv -x^{-1} \bmod p$. On the other hand, if $p \equiv 1 \bmod 4$, there must be two sets P_x with two elements. One of them is P_1 and the other has to be P_x, where $x \equiv -x^{-1} \bmod p$.

In the same way we can show the other direction.

(2. $\Rightarrow$ 3.) Supposing that -1 is a quadratic residue in $\mathbb{F}_p$, then there is an element $x \in \mathbb{F}_p^*$, such that $x^2 = -1 \bmod p$, meaning that p divides $x^2 + 1$ in $\mathbb{Z}[i]$. Since $x^2 + 1 = (x + i)(x - i)$, where $p \mid \left(x^2 + 1\right)$ but $p \nmid (x + i), (x - i)$ in $\mathbb{Z}[i]$, we see that p is not a prime in $\mathbb{Z}[i]$. In other words, we can find Gaussian integers α and β, such that $p = \alpha\beta$, where $N(p) > N(\alpha), N(\beta) > 1$. Consider $N(p) = N(\alpha)N(\beta) = p^2$. This means that $N(\alpha), N(\beta) | p^2$, and from this follows that $N(\alpha) = N(\beta) = p$, which implies that we can write p as a sum of two squares.

(2. $\Leftarrow$ 3.) Suppose that

$$p = a^2 + b^2. \tag{2.16}$$

Since $a, b \in \mathbb{F}_p^*$, we know that a and b are invertible. But this implies that we can find $c \in \mathbb{F}_p^*$ such that $bc \equiv 1 \bmod p$. From the equation (2.16) we get that

$$pc^2 = (ac)^2 + (bc)^2 \tag{2.17}$$

and when we compute the equation (2.17) by modulo p, we get that $(ac)^2 + 1 \equiv 0 \bmod p$. □

Using the theorem above and the multiplicity of the norm, we can give the characterization of all integers that can be presented as a sum of two squares.

Corollary 2.2.2. An integer $n \geq 2$ is a sum of two squares if and only if every prime number $p \equiv 3 \bmod 4$ appears with an even exponent in the factorization of n into primes.

Proof. ($\Leftarrow$) Let be $n \in \mathbb{N}$ a positive integer, then we can write n as

$$n = 2^r \prod_{s=1}^{l} p_s^{o_s} \prod_{t=1}^{m} q_t^{e_t}, \tag{2.18}$$

where p_s's are odd primes such that $p_s \equiv 1 \bmod 4$ for all s, q_t's are odd primes such that $q_t \equiv 3 \bmod 4$ for all t and all e_t's are even. By Theorem 2.2.1, p_s is a sum of two squares for all s, and integer $2 = 1^2 + 1^2$ is also a sum of two squares. This means that we can find Gaussian integers π_s such that $N(\pi_s) = p_s$ for all s's and $\mu = 1 + i$ such that $N(\mu) = 2$.

Now we only have to show that $q_t^{e_t}$ can be written as a sum of two squares for all t's. But since e_t is even for all t's, we have $e_t = 2w_t$ for some $w_t \in \mathbb{N}$. And we see that

$$q_t^{e_t} = q_t^{2w_t} = (q_t^{w_t})^2 = (q_t^{w_t})^2 + 0^2 \tag{2.19}$$

is already a sum of two squares. So we can construct a Gaussian integer $\rho \in \{\pm q^{w_t}, \pm q^{w_t} i\}$ such that $N(\rho) = q^{e_t}$.

Now we can built a Gaussian integer $\alpha = a + bi$ as follows:

$$\alpha = a + bi = \mu^r \prod_{s=1}^{l} \pi_s^{o_s} \prod_{t=1}^{m} \rho_t. \tag{2.20}$$

By the multiplicity of the norm, we can compute that

$$a^2 + b^2 = N(\alpha) = N(\mu)^r \prod_{s=1}^{l} N(\pi_s)^{o_s} \prod_{t=1}^{m} N(\rho_t) = 2^r \prod_{s=1}^{l} p_s^{o_s} \prod_{t=1}^{m} q_t^{e_t} = n, \tag{2.21}$$

meaning that $n = a^2 + b^2$ is a sum of two squares.

($\Rightarrow$) Let be n an integer, which is a sum of two squares. Then we can find $a, b \in \mathbb{N}$, such that

$$n = a^2 + b^2. \tag{2.22}$$

And let be $p, w \in \mathbb{N}$, where p is an odd prime that divides n, and w is the highest power of p, such that p^w divides a and b. Then we can compute $x = \frac{a}{p^w}$ and $y = \frac{b}{p^w}$, where the following holds:

$$\frac{n}{p^{2w}} = x^2 + y^2. \tag{2.23}$$

Note that for any such p and $w > 0$, p^{2w} has to divide n since $n = a^2 + b^2$.

By using the same idea as in Theorem 2.2.1, in the next part, we will show, that p has to be congruent to 1 modulo 4 if p can still divide $\frac{n}{p^{2w}}$.

Suppose $p | \frac{n}{p^{2w}} = x^2 + y^2$. Since $x^2 + y^2 = (x + yi)(x - yi)$ in $\mathbb{Z}[i]$ and p does not divide neither x nor y, we see that p does not divide any of factors $(x + yi)$ and $(x - yi)$. With the same argument from the proof in Theorem 2.2.1, we see that p can be written as a sum of two squares and we know that $p \equiv 1 \bmod 4$.

The contra-position shows if $p \equiv 3 \bmod 4$, then p cannot divide n/p^{2w}. From this contra-position and the equation (2.23), we see that any $p \equiv 3 \bmod 4$ that divides n, can appear only with even exponent in the factorization of n.

□

Remark 2.2.3. From the proof above, we can easily notice that any number $n = q^{2w}$, where $q \equiv 3 \bmod 4$ is an odd prime, it can only be presented as a Gaussian integer $\rho \in \{\pm q^w, \pm q^w i\}$, where ρ has the norm equal n.

In the next part, we will state a interesting result of the primes in the Gaussian integer ring $\mathbb{Z}[i]$ without proving it. The proof of this proposition can be seen in [4].

Proposition 2.2.4. A Gaussian integer $\pi \in \mathbb{Z}[i]$ is a prime if and only if one of the following three cases holds

1. $N(\pi) = 2$ (in this case π is an associate of $1+i$, that is , $\pi \in \{1 \pm i, -1 \pm i\}$).
2. $N(\pi) = p$, where p is a prime in $\mathbb{Z}$ and $p \equiv 1 \bmod 4$.
3. π is an associate to q, where q is a prime in $\mathbb{Z}$, and $q \equiv 3 \bmod 4$.

Chapter 3

Quaternions and the sum of four squares

When we talk about quaternions, we usually mean the Hamilton quaternions over reals. But there is a more general definition of Quaternion Algebra over arbitrary field or ring, then the Algebra of Hamilton quaternions.

Depending on what subject and for what purpose we want to use the quaternions, there can be a slight difference in the definition of Quaternion Algebra. In general, a Quaternion Algebra $\mathbb{H}(\mathbb{K})$ over the field or ring $\mathbb{K}$, where $\mathbb{K}$ is not of characteristic 2, is the free $\mathbb{K}$-module of rank 4 with basis $\{1, i_1, i_2, i_1 i_2\}$, where the following holds:

$$\begin{aligned} i_1^2 &= a \\ i_2^2 &= b \\ i_1 i_2 &= -i_2 i_1, \end{aligned} \tag{3.1}$$

and where a, $b \in \mathbb{K}$ are not zero-elements. From equations in (3.1), we can easily compute that $(i_1 i_2)^2 = -ab$. The Quaternion Algebra over field or ring $\mathbb{K}$ with characteristic 2 can also be presented with a different presentation of a 4-dimensional vector space, but we will go no further into the details since we are mainly interested in the Hamilton quaternions $\mathbb{H}(\mathbb{R})$ and in their sub-rings Lipschitz ring $\mathcal{L}$ and Hurwitz ring $\mathcal{H}$, where in neither case $\mathbb{K}$ has characteristic 2. For that matter, from now on we will use the traditional notations used for Hamilton quaternions, since Hamilton carved them in stone.

3.1 Quaternions and Hamilton Quaternions

In this chapter, we will present some of the basic definitions and notations and take a look at some arithmetic properties of quaternions. So we start with the standard definition of the quaternions:

Definition 3.1.1. The *Quaternion Algebra* over a field or ring $\mathbb{K}$, where $\mathbb{K}$ is not of characteristic 2, is the associative unital algebra, denoted by $\mathbb{H}(\mathbb{K})$ and by the form

$$\mathbb{H}(\mathbb{K}) = \mathbb{K} + \mathbb{K}i + \mathbb{K}j + \mathbb{K}k, \tag{3.2}$$

where the following holds:

1. 1 is the multiplicative unit.
2. $i^2 = j^2 = k^2 = ijk = -1$.

Quaternion Algebra over reals $\mathbb{H}(\mathbb{R})$ is called Hamilton Quaternion Algebra and we will denote it short with $\mathbb{H}$.

The Definition 3.1.1 is similar to the definition we gave at the beginning of this chapter. Only the notations in (3.1) are now denoted with $i_1 = i$, $i_2 = j$, $i_1 i_2 = k$ and the values a and b are now $a = b = -1$.

The addition of two quaternions $\alpha, \beta \in \mathbb{H}(\mathbb{K})$, where $\alpha = (a_1 + a_2 i + a_3 j + a_4 k)$ and $\beta = (b_1 + b_2 i + b_3 j + b_4 k)$, is defined as

$$\begin{aligned} \alpha + \beta &= (a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) \\ &= (a_1 + b_1) + (a_2 + b_2) i + (a_3 + b_3) j + (a_4 + b_4) k. \end{aligned} \tag{3.3}$$

On the other hand, the multiplication of two quaternions is not that straightforward. First we have to terminate the pairwise multiplications of i, j and k. From the equation in Definition 3.1.1 point 2, we can easily compute that $ij = k$, $ji = -k$, $ik = -j$, $ki = j$, $jk = i$ and $kj = -i$. So we can also compute the multiplication of two quaternions α and β.

$$\begin{aligned} \alpha\beta &= (a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k) \\ &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) \\ &+ (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i \\ &+ (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) j \\ &+ (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) k \end{aligned} \tag{3.4}$$

and that

$$\begin{aligned} \beta\alpha &= (b_1 + b_2 i + b_3 j + b_4 k)(a_1 + a_2 i + a_3 j + a_4 k) \\ &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) \\ &+ (a_1 b_2 + a_2 b_1 - a_3 b_4 + a_4 b_3) i \\ &+ (a_1 b_3 + a_2 b_4 + a_3 b_1 - a_4 b_2) j \\ &+ (a_1 b_4 - a_2 b_3 + a_3 b_2 + a_4 b_1) k. \end{aligned} \tag{3.5}$$

Consider that in general $\alpha\beta \neq \beta\alpha$, i.e. the multiplication on $\mathbb{H}(\mathbb{K})$ is not commutative. Using this addition and multiplication, it is clear that $(\mathbb{H}(\mathbb{K}), +)$ is an abelian group, and since $\mathbb{K}$ is at least a ring, we can see that the distributivity low and associativity over the multiplication are also provided.

Definition 3.1.2. Let be $\alpha \in \mathbb{H}(\mathbb{K})$ a quaternion, then the *conjugate* of α is defined as

$$\overline{\alpha} := a_1 - a_2 i - a_3 j - a_4 k.$$

Definition 3.1.3. Let be $\alpha \in \mathbb{H}(\mathbb{K})$ a quaternion, then the *norm* of α is defined as

$$N(\alpha) := \alpha\overline{\alpha} = \overline{\alpha}\alpha = a_1^2 + a_2^2 + a_3^2 + a_4^2 \in \mathbb{K}.$$

The definition of the norm of quaternions is similar to the definition of the norm of Gaussian integers. And from Euler's identity

$$\begin{aligned} &\left(a_1^2 + a_2^2 + a_3^2 + a_4^2\right)\left(b_1^2 + b_2^2 + b_3^2 + b_4^2\right) = \\ &= (a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4)^2 + (a_1 b_2 - a_2 b_1 + a_3 b_4 - a_4 b_3)^2 \\ &+ (a_1 b_3 - a_3 b_1 + a_4 b_2 - a_2 b_4)^2 + (a_1 b_4 - a_4 b_1 + a_2 b_3 - a_3 b_2)^2 \end{aligned} \tag{3.6}$$

follows that the norm of quaternions is multiplicative too, i.e. for two quaternions α and β, then $N(\alpha\beta) = N(\alpha)N(\beta)$.

Definition 3.1.4. Let be $\alpha \in \mathbb{H}(\mathbb{K})$. We say that $\beta \in \mathbb{H}(\mathbb{K})$ is *multiplicative inverse* (or short *inverse*) of α if $\alpha\beta = 1$. If such β exists in $\mathbb{H}(\mathbb{K})$, we denote it with α^{-1} and we say that α is *invertible*.

Remark 3.1.5. Note that in general $\alpha\beta \neq \beta\alpha$. So if α is invertible, the multiplicative inverse on left does not have to be the same as he multiplicative inverse on tight. But following equation shows that those two inverses of α has to be the same, i.e. α and α^{-1} commute.

$$\alpha\alpha^{-1} = 1 \Leftrightarrow \overline{\alpha}\alpha\alpha^{-1} = N(\alpha)\alpha^{-1} = \overline{\alpha} = \alpha^{-1}N(\alpha) = \alpha^{-1}\alpha\overline{\alpha} \Leftrightarrow \alpha^{-1}\alpha = 1$$

In general not every element in $\mathbb{H}(\mathbb{K})$ has a multiplicative inverse. For example, if $\mathbb{K} = \mathbb{Z}$, only the elements $\{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}(\mathbb{Z})$ have a multiplicative inverse. But if there is any, we can compute it with

$$\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)} = \frac{a_1}{N(\alpha)} - \frac{a_2}{N(\alpha)}i - \frac{a_3}{N(\alpha)}j - \frac{a_4}{N(\alpha)}k, \tag{3.7}$$

where $\alpha = a_1 + a_2 i + a_3 j + a_4 k$.

Consider that $N(\alpha)$, where $a_l \in \mathbb{K}$ for all $l \in \{1, 2, 3, 4\}$. Then from the equation (3.7), we can see that α has a multiplicative inverse if and only if $a_l/N(\alpha) \in \mathbb{K}$ for all $l \in \{1, 2, 3, 4\}$. This means that every Hamilton quaternion $\alpha \in \mathbb{H}$ has a multiplicative inverse.

Definition 3.1.6. Let be $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in \mathbb{H}(\mathbb{K})$, then

1. we call $\mathscr{R}(\alpha) := \frac{1}{2}(\alpha + \overline{\alpha}) = a_1$ the *real part* of α.
2. we call $\hat{\alpha} := \frac{1}{2}(\alpha - \overline{\alpha}) = a_2 i + a_3 j + a_4 k$ the *vector part* of α.
3. we say, α is *pure*, if $\mathscr{R}(\alpha) = 0$.

Remark 3.1.7. A set of all pure quaternions can be presented as a three-dimensional vector space $\mathbb{K}^3$. But the multiplication of two pure quaternions is not a pure quaternion in general.

In the next part, we will give a matrix presentation of quaternions and briefly discuss their matrix algebra. As we already pointed out at the beginning of this chapter, Quaternion Algebra can be described as four-dimensional vector space $\mathbb{K}^4$, where $\mathrm{char}(\mathbb{K}) \neq 2$. According to the Definition 3.1.1, we will take $i_1 = i$, $i_2 = j$, $i_1 i_2 = k$ and $a = b = -1$. Then we can write quaternions as matrices, so that the quaternion addition and multiplication correspond to the matrix addition and multiplication by taking e_1 as the multiplicative unit and

$$e_2^2 = e_3^2 = e_4^2 = e_2 e_3 e_4 = -e_1,$$

where $\{e_1, e_2, e_3, e_4\}$ is the standard basis of $\mathbb{K}^4$. By setting $e_1 = 1$, $e_2 = i$, $e_3 = j$ and $e_4 = k$, we get the same definition as above. This implies that the quaternions 1, i, j, k are orthonormal to each other as vectors.

From the equation (3.4) and the definitions above, we can see that the multiplication on $\mathbb{H}(\mathbb{K})$ with $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ on the left respectively on the right corresponds to the endomorphism on $\mathbb{R}^4$ given by the matrices

$$\begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{bmatrix} \quad \text{resp.} \quad \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ -a_2 & a_1 & -a_4 & a_3 \\ -a_3 & a_4 & a_1 & -a_2 \\ -a_4 & -a_3 & a_2 & a_1 \end{bmatrix}. \tag{3.8}$$

Consider that every column in the first matrix is a presentation of a quaternion of the form α, αi, αj and αk, and every row in the second matrix is a presentation of a quaternion of the form α, $i\alpha$, $j\alpha$ and $k\alpha$.

Now we have given a presentation of quaternions with 4×4-matrices with real entries. But there is also another way to present quaternions as matrices, where quaternion addition and multiplication correspond to matrix addition and multiplication, namely by presenting the quaternions with 2×2-matrices with complex entries.

Consider a quaternion of the form $a_1 + a_2 i + a_3 j + a_4 k \in \mathbb{H}(\mathbb{K})$. Then we can write $a_1 + a_2 i + a_3 j + a_4 k = (a_1 + a_2 i) + (a_3 + a_4 i) j = \alpha + \beta j$, where α, $\beta \in \mathbb{C}$. Then note that for any $\alpha \in \mathbb{C}$, $j\alpha = \overline{\alpha} j$. So we can compute that

$$\begin{aligned} &(\gamma + \delta j)(\alpha + \beta j) = \gamma\alpha + \gamma\beta j + \delta j\alpha + \delta j\beta j = \\ &= \gamma\alpha + \gamma\beta j + \delta\overline{\alpha} j + \delta\overline{\beta} jj = \left(\gamma\alpha - \delta\overline{\beta}\right) + (\gamma\beta + \delta\overline{\alpha})\, j. \end{aligned} \tag{3.9}$$

This shows that the action on $\mathbb{C} \oplus \mathbb{C}j$ given by the multiplication on the right by $\alpha + \beta j$ has the matrix representation

$$\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} \tag{3.10}$$

In the same way we can show that the multiplication on the left by $\alpha + \beta j$ is given by the matrix representation

$$\begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix} \tag{3.11}$$

Furthermore, we are going to present some interesting results that are rather easy to terminate if we look at the quaternions as vectors.

By using the vector presentation of quaternions and by the multiplication listed in the equation (3.4), we can compute that

$$\mathscr{R}(\alpha\beta) = \alpha \cdot \overline{\beta} \quad \text{and} \tag{3.12}$$

$$\hat{\alpha}\hat{\beta} = -\hat{\alpha} \cdot \hat{\beta} + \hat{\alpha} \times \hat{\beta}, \tag{3.13}$$

where '$\cdot$' stands for dot product, i.e. $\alpha \cdot \beta = (a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4) \in \mathbb{K}$ and '$\times$' stands for cross or vector product in $\mathbb{K}^3$. Consider that the product of two quaternions can also be written as

$$\alpha\beta = \mathscr{R}(\alpha)\beta + \mathscr{R}(\beta)\alpha - \alpha \cdot \beta + \hat{\alpha} \times \hat{\beta}. \tag{3.14}$$

Remark 3.1.8. From the given definitions and equations above, the following is easy to elaborate:

- $\mathscr{R}(\alpha) = \mathscr{R}(\overline{\alpha})$
- $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$
- $\alpha \cdot \beta = \beta \cdot \alpha$
- $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta} = \alpha \cdot \beta$
- From the equation (B.7), it is simple to compute that

$$\overline{\hat{\alpha} \times \hat{\beta}} = -\overline{\hat{\alpha}} \times \overline{\hat{\beta}} = -\hat{\overline{\alpha}} \times \hat{\overline{\beta}} = -\hat{\alpha} \times \hat{\beta}$$

- For a quaternion $\varepsilon \in \{\pm i, \pm j, \pm k\}$, $\overline{\varepsilon} = -\varepsilon = \varepsilon^{-1}$

So, using the Remark 3.1.8 and the equations above, it is also easy to compute the following:

$$\begin{aligned} \overline{\alpha\beta} &= \overline{\mathscr{R}(\alpha)\beta + \mathscr{R}(\beta)\alpha - \alpha \cdot \beta + \hat{\alpha} \times \hat{\beta}} \\ &= \mathscr{R}(\overline{\beta})\overline{\alpha} + \mathscr{R}(\overline{\alpha})\overline{\beta} - \overline{\beta} \cdot \overline{\alpha} + \hat{\overline{\beta}} \times \hat{\overline{\alpha}} \\ &= \overline{\beta}\overline{\alpha} \end{aligned} \tag{3.15}$$

and

$$\alpha \cdot \beta = \mathscr{R}(\alpha\overline{\beta}) = \frac{1}{2}\left(\alpha\overline{\beta} + \beta\overline{\alpha}\right). \tag{3.16}$$

From the equation (3.14) and the Remark 3.1.8 follows:

$$\begin{aligned}
\alpha\beta &= \mathscr{R}(\alpha)\beta + \mathscr{R}(\beta)\alpha - \alpha\cdot\beta + \hat{\alpha}\times\hat{\beta} \\
&= \tfrac{1}{2}\left(\alpha+\overline{\alpha}\right)\beta + \tfrac{1}{2}\left(\beta+\overline{\beta}\right)\alpha - \mathscr{R}(\alpha\overline{\beta}) + \hat{\alpha}\times\hat{\beta} \\
&= \tfrac{1}{2}\alpha\beta + \tfrac{1}{2}\beta\alpha + \tfrac{1}{2}\left(\overline{\alpha}\beta + \overline{\beta}\alpha\right) - \mathscr{R}(\alpha\overline{\beta}) + \left(\hat{\alpha}\times\hat{\beta}\right) \\
&= \tfrac{1}{2}\alpha\beta + \tfrac{1}{2}\beta\alpha + \mathscr{R}(\overline{\alpha}\beta) - \mathscr{R}(\alpha\overline{\beta}) + \left(\hat{\alpha}\times\hat{\beta}\right) \\
&= \tfrac{1}{2}\alpha\beta + \tfrac{1}{2}\beta\alpha + \mathscr{R}(\overline{\alpha\overline{\beta}}) - \mathscr{R}(\alpha\overline{\beta}) + \left(\hat{\alpha}\times\hat{\beta}\right) \\
&= \tfrac{1}{2}\alpha\beta + \tfrac{1}{2}\beta\alpha + \left(\hat{\alpha}\times\hat{\beta}\right)
\end{aligned} \tag{3.17}$$

and from that we can get

$$\alpha\beta - \beta\alpha = 2\left(\hat{\alpha}\times\hat{\beta}\right). \tag{3.18}$$

This is interesting because it shows us that two quaternions commute if and only if their vector parts are collinear.

3.2 Lipschitz integers and arithmetic of $\mathbb{H}(\mathbb{Z})$

In this section, we will present the ring of integral quaternions and some arithmetical properties. Integral quaternions, also called Lipschitz integers, are very interesting since the norm of all Lipschitz integers is a natural number, and because for every natural number n, there are Lipschitz integers α's such that $N(\alpha) = n$. Unfortunately, the Lipschitz integers do not have a unique factorization, and the ring of Lipschitz integers is not an euclidean domain. But still, with a small redaction, we will give a functional euclidean algorithm.

So, as by Gaussian integers, we will discuss the properties of integral quaternions and give some characterization of their factors.

Definition 3.2.1. The set of integral quaternions, also called Lipschitz integers, is

$$\{a_1 + a_2 i + a_3 j + a_4 k \mid a_1, a_2, a_3, a_4 \in \mathbb{Z}\}.$$

We will denote this set with $\mathcal{L}$.

According to Definition 3.1.1 about the set $\mathcal{L} = \mathbb{H}(\mathbb{Z})$, it is easy to check that the set of Lipschitz integers $\mathcal{L}$ together with addition and multiplication is a ring. We call this ring $(\mathcal{L}, +, \cdot)$, the Lipschitz ring.

Proposition 3.2.2. For every $\alpha \in \mathcal{L}$, $N(\alpha) \in \mathbb{N}$.

Proof. For every $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in \mathcal{L}$ we know that $a_l \in \mathbb{Z}$, $\forall l \in \{1, 2, 3, 4\}$. Then $N(\alpha) = a_1^2 + a_2^2 + a_3^2 + a_4^2 \in \mathbb{N}$, since all a_l^2 are positive. □

Definition 3.2.3. A Lipschitz integer $\varepsilon \in \mathcal{L}$ is a *unit* if ε is invertible in $\mathcal{L}$, i.e. there exists ε^{-1} in $\mathcal{L}$ such that $\varepsilon\varepsilon^{-1} = 1$.

As we already saw with the Gaussian integers, if a Lipschitz integer is a unit, then it has a norm equal to 1.

Lemma 3.2.4. An element $\varepsilon \in \mathcal{L}$ is a unit if and only if $N(\varepsilon) = 1$.

Proof. If ε is a unit, then there exists ε^{-1} in $\mathcal{L}$ such that $\varepsilon\varepsilon^{-1} = 1$ and following holds:

$$1 = N(1) = N(\varepsilon\varepsilon^{-1}) = N(\varepsilon)N(\varepsilon^{-1}). \tag{3.19}$$

Since the norm of a Lipschitz integer $\varepsilon = e_1 + e_2 i + e_3 j + e_4 k$ is $N(\varepsilon) = e_1^2 + e_2^2 + e_3^2 + e_4^2 \in \mathbb{N}$, from the equation above we can follow that $N(\varepsilon) = N(\varepsilon^{-1}) = 1$.

If $N(\varepsilon) = 1$ for some $\varepsilon \in \mathcal{L}$, then ε can only be the element from the set $\{\pm 1, \pm i, \pm j, \pm k\}$. But then there exists such $\varepsilon^{-1} \in \{\pm 1, \pm i, \pm j, \pm k\}$ such that $\varepsilon\varepsilon^{-1} = 1$. □

From last lemma, it is clear that there are exactly 8 units $\{\pm 1, \pm i, \pm j, \pm k\} \subset \mathcal{L}$ in a Lipschitz ring.

Definition 3.2.5. Let be $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in \mathcal{L}$ and $m \in \mathbb{N}_{>0}$ a positive integer, then

1. α is *odd* (resp. *even*) if $N(\alpha)$ is an odd (resp. even) positive integer.

2. α is *periodical* if there exist an $e \in \mathbb{N}$, such that $\alpha^e \in \mathbb{Z}$. We also say that α has the *period* $\tilde{e}$, where $\tilde{e} = \min\{e \mid \alpha^e \in \mathbb{Z},\, e \in \mathbb{N}\}$.

3. α is a *prime* if it is not a unit, and for every $\beta, \gamma \in \mathcal{L}$, where $\alpha = \beta\gamma$, either β or γ is a unit. They are called prime quaternions.

4. α is *associated* with $\beta \in \mathcal{L}$ if there exist units $\varepsilon_1, \varepsilon_2 \in \mathcal{L}$, such that $\alpha = \varepsilon_1 \beta \varepsilon_2$. Similarly, α and β are *left-associated* (resp. *right-associated*) if there exists a unit $\varepsilon \in \mathcal{L}$, such that $\alpha = \varepsilon\beta$ (resp. $\alpha = \beta\varepsilon$).

5. $\delta \in \mathcal{L}$ is a *left divisor* (resp. *right divisor*) of α if there exists a quaternion $\beta \in \mathcal{L}$, such that $\alpha = \delta\beta$ (resp. $\alpha = \beta\delta$).

6. we call α *pure* $\bmod m$ if m divides a_1.

7. we call α *proper* $\bmod m$ if the g.c.d. of $a_1, \ldots, a_4$ and m is 1.

8. we call α *proper* if the g.c.d. of $a_1, \ldots, a_4$ is 1.

Next, we will define some sets of Lipschitz integers that have some properties common.

Definition 3.2.6. Let be $\alpha \in \mathcal{L}\backslash\{0\}$, then

1. $\mathfrak{DL}_\alpha$ (resp. $\mathfrak{DR}_\alpha$) is the set of eight left-associates (resp. right-associates) proper quaternions $\{\pm\alpha, \pm i\alpha, \pm j\alpha, \pm k\alpha\}$ (resp. $\{\pm\alpha, \pm\alpha i, \pm\alpha j, \pm\alpha k\}$).

2. $\mathfrak{E}_\alpha$ is the set obtained from a given proper quaternion α by an even number of sign-changes or interchanges of the coordinates a_l for $l \in \{1, \ldots, 4\}$. We call two quaternions α and β of the *same structure* if $\beta \in \mathfrak{E}_\alpha$.

3. $\mathfrak{S}_\alpha \subset \mathfrak{E}_\alpha$ is the smallest set of quaternions $\tilde{\alpha} \in \mathfrak{E}_\alpha$ such that for every $\beta \in \mathfrak{E}_\alpha$, there exist $\tilde{\alpha} \in \mathfrak{S}_\alpha$ such that $\beta = \varepsilon_1 \tilde{\alpha} \varepsilon_2$, where ε_1 and ε_2 are units.

Proposition 3.2.7. If $\alpha = \tau\gamma$ and $\beta = \tau\delta$ (resp. $\alpha = \gamma\tau$ and $\beta = \delta\tau$), where $\tau, \gamma, \delta \in \mathcal{L}$, then $\alpha \cdot \beta = N(\tau)\,(\gamma \cdot \delta)$. In particular, if τ is a left (resp. right) divisor of α and β, then $N(\tau) | \alpha \cdot \beta$.

Proof. Consider the equation (3.16). Then we get

$$\begin{array}{rclcll} 2\,(\alpha\cdot\beta) & = & \alpha\overline{\beta}+\beta\overline{\alpha} & = & \tau\gamma\overline{\delta}\overline{\tau}+\tau\delta\overline{\gamma}\overline{\tau} & = \\ & = & \tau\left(\gamma\overline{\delta}+\delta\overline{\gamma}\right)\overline{\tau} & = & \tau 2\,(\gamma\cdot\delta)\,\overline{\tau} & = \\ & = & 2\tau\overline{\tau}\,(\gamma\cdot\delta) & = & 2N(\tau)\,(\gamma\cdot\delta)\,, & \end{array} \tag{3.20}$$

and from this equation we see that $N(\tau)|\alpha\cdot\beta$. An entirely analogue equation is valid for right divisor. □

For γ and δ that are orthogonal we know that $(\gamma\cdot\delta)=0$. But then by the proposition above $(\alpha\cdot\beta)=N(\tau)\,(\gamma\cdot\delta)=0$, i.e. α and β are also orthogonal. In this case, we see that $2\,(\alpha\cdot\beta)=\alpha\overline{\beta}+\beta\overline{\alpha}=0$ and also $\alpha\overline{\beta}=-\beta\overline{\alpha}$.

Proposition 3.2.8. Let be $\varepsilon_1,\varepsilon_2\in\{1,i,j,k\}$ with $\varepsilon_1\neq\varepsilon_2$. Then $\forall\alpha\in\mathbb{H}\backslash\{0\}$, $\alpha\varepsilon_1$ and $\alpha\varepsilon_2$ (resp. $\varepsilon_1\alpha$ and $\varepsilon_2\alpha$) are orthogonal.

Proof. From Proposition 3.2.7, the equation $2\,(\alpha\varepsilon_1\cdot\alpha\varepsilon_2)=2N(\alpha)\,(\varepsilon_1\cdot\varepsilon_2)=0$ holds, since ε_1 and ε_2 are orthogonal, i.e. $(\epsilon\cdot\delta)=0$. and this implies that $\alpha\varepsilon_1$ and $\alpha\varepsilon_2$ are orthogonal.

Consequently, we can show that $\varepsilon_1\alpha$ and $\varepsilon_2\alpha$ are orthogonal too. □

Lemma 3.2.9. Let be $\alpha\in\mathcal{L}\backslash\{0\}$, then $|\mathfrak{DL}_\alpha|=8$ (resp. $|\mathfrak{DR}_\alpha|=8$).

In particular, this lemma tells us that $\alpha\varepsilon_1\neq\alpha\varepsilon_2$ (resp. $\varepsilon_1\alpha\neq\varepsilon_2\alpha$) for all units ε_1 and ε_2, where $\varepsilon_1\neq\varepsilon_2$, and that this set will always have eight elements.

Proof. Let be $\alpha\in\mathcal{L}\backslash\{0\}$ and $\varepsilon_1,\varepsilon_2\in\{\pm1,\pm i,\pm j,\pm k\}$.

If $\varepsilon_1=-\varepsilon_2$, then it is clear that $\alpha\varepsilon_1\neq\alpha\varepsilon_2$ (resp. $\varepsilon_1\alpha\neq\varepsilon_2\alpha$).

If $|\varepsilon_1|\neq|\varepsilon_2|$, then by Proposition 3.2.8 we know that scalar product $(\alpha\varepsilon_1\cdot\alpha\varepsilon_2)=0$ (resp. $(\varepsilon_1\alpha\cdot\varepsilon_2\alpha)=0$). Note that if $\alpha\varepsilon_1=\alpha\varepsilon_2$ (resp. $\varepsilon_1\alpha=\varepsilon_2\alpha$), the scalar product $(\alpha\varepsilon_1\cdot\alpha\varepsilon_2)=N(\alpha\varepsilon_1)\neq0$ (resp. $(\varepsilon_1\alpha\cdot\varepsilon_2\alpha)=N(\varepsilon_1\alpha)\neq0$). From this scalar product, we see that $\alpha\varepsilon_1\neq\alpha\varepsilon_2$ (resp. $\varepsilon_1\alpha\neq\varepsilon_2\alpha$).

□

Lemma 3.2.10. Let be $\alpha,\beta\in\mathcal{L}$ not left-associates (resp. right-associates). Then $\mathfrak{DL}_\alpha$ and $\mathfrak{DL}_\beta$ (resp. $\mathfrak{DR}_\alpha$ and $\mathfrak{DR}_\beta$) are disjoint sets. Otherwise those sets are equal, i.e. $\mathfrak{DL}_\alpha=\mathfrak{DL}_\beta$ (resp. $\mathfrak{DR}_\alpha=\mathfrak{DR}_\beta$).

Proof. If α and β are left-associates, then there exists a unit ε such that $\alpha=\varepsilon\beta$, and this implies that $\beta\in\mathfrak{DL}_\alpha$ and vice versa. And by definition of the sets $\mathfrak{DL}_\alpha$ and $\mathfrak{DL}_\beta$, we see that $\mathfrak{DL}_\alpha\subseteq\mathfrak{DL}_\beta$ and $\mathfrak{DL}_\alpha\supseteq\mathfrak{DL}_\beta$. In the same way we can show for right-associates that $\mathfrak{DR}_\alpha=\mathfrak{DR}_\beta$.

If α and β are not left-associates, then there is not a unit ε such that $\alpha=\varepsilon\beta$. But assume that there exists a unit ε_1 such that $\varepsilon_1\beta\in\mathfrak{DL}_\alpha$, i.e. $\mathfrak{DL}_\alpha$ and $\mathfrak{DL}_\beta$ are not disjoint sets and that there exists another unit ε_2 such that $\varepsilon_1\beta=\varepsilon_2\alpha$. Note that units are invertible in $\mathcal{L}$ by definition. But then we can see that

$$\varepsilon_2^{-1}\varepsilon_1\beta=\varepsilon_2^{-1}\varepsilon_2\alpha=\alpha. \tag{3.21}$$

This means that there exists a unit $\varepsilon=\varepsilon_2^{-1}\varepsilon_1$ such that $\alpha=\varepsilon\beta$. Note that ε is a unite since $N(\varepsilon_2^{-1}\varepsilon_1)=N(\varepsilon_2^{-1})N(\varepsilon_1)=1$. And this is the contradiction to the assumption that α and β are not left-associates, which implies that $\mathfrak{DL}_\alpha$ and $\mathfrak{DL}_\beta$ are disjoint sets. In the same way we can show that $\mathfrak{DR}_\alpha$ and $\mathfrak{DR}_\beta$ are disjoint sets. □

In Chapter 4, we will present a resalt of Jacobi's Theorem which states an exact formula for computing number of distinct tuples $(a_1,\,a_2,\,a_3,\,a_4)$ such that $a_1^2+a_2^2+a_3^2+a_4^2=n$ for some fixed $n\in\mathbb{N}$. And from this we see that this is also the number of different quaternions with the same norm. So using Jacob's Theorem 4.2.6 and last two lemmas, we can present the next result.

Lemma 3.2.11. Let be $\mathcal{A}_n$ any set of quaternions of the odd norm n which are pairwise not left-associates. Then $\mathcal{A}_n$ can have cardinality at most $\sum_{d|n} d$.

Proof. Let be n an odd integer. Then by Jacobi's Theorem 4.2.6 there are $8\sum_{d|n} d$ different Lipschitz integers of the norm n. And by last two lemmas, we know that there are distinct sets of left-associates, where each set has exactly eight elements. So we have $\sum_{d|n} d$ distinct sets, where each element of one set is not left-associate with any other quaternion of any other set. So we can have at most $\sum_{d|n} d$ quaternions in the set $\mathcal{A}_n$. □

Theorem 3.2.12. Let be $\alpha \in \mathcal{L}\backslash\{0\}$ and $m \in \mathbb{N}_{>1}$ an odd integer, where α is proper modulo m and $m|N(\alpha)$. Then there is only one left (resp. right) divisor of α of the norm m, up to right-associates (resp. left-associates).

In general, this theorem tells us that if $\delta \in \mathcal{L}$ divides α on right (resp. left), where $N(\delta) = m$ is an odd integer and $m|N(\alpha)$, then $\mathfrak{DL}_\alpha$ (resp. $\mathfrak{DR}_\alpha$) are all divisors from right (resp. left) of α, with the norm m.

This is a fundamental theorem in the arithmetic of quaternions, and it was first proved by Lipschitz in the case of a prime m. Here we will line out the proof listed in [2]. The variations or extensions of this proof are also listed in [11] and [12].

As usual, before we present the proof of this theorem, we will first prove some lemmas.

Lemma 3.2.13. Let be α, $\beta \in \mathcal{L}$ and $m \in \mathbb{N}$ an odd integer. If $\alpha \equiv \beta \bmod m$, than α and β have the same right divisors of the norm m.

Proof. Let be $\alpha = \gamma\delta$ and $N(\delta) = m$ an odd integer. Than for any $\beta = \alpha + \sigma m$ with some $\sigma \in \mathcal{L}$. And we have that

$$\beta = \gamma\delta + \sigma\overline{\delta}\delta = \left(\gamma + \sigma\overline{\delta}\right)\delta.$$

□

Lemma 3.2.14. Let be $\alpha = \gamma\delta$ and $N(\delta) = m$ an odd integer. If $N(\beta)$ and m are co-prime, α and $\beta\alpha$ have the same right divisors of norm m.

Proof. if δ is a right divisor of α, i.e. $\alpha = \gamma\delta$, than we can write $\beta\alpha = \beta\gamma\delta$, i.e. δ is a right divisor of $\beta\alpha$.

Conversely, let be δ a right divisor of $\beta\alpha$, i.e. $\beta\alpha = \gamma\delta$. And let be $n \in \mathbb{N}$, such that $nN(\beta) \equiv 1 \bmod m$. (Recall that $N(\beta)$ and m are co-prime, meaning such n exists.) Than

$$\alpha = \overline{\beta}\beta\alpha = \overline{\beta}\gamma\delta \quad \Rightarrow \quad \alpha \equiv \left(n\overline{\beta}\gamma\right)\delta \bmod m.$$

And by Lemma 3.2.13, $\beta\alpha$ and α have the same right divisors. □

As next we will state two lemmas without proving them. The proves of this two lemmas is listed in the paper [11]

Lemma 3.2.15. If Theorem 3.2.12 holds for every product m of $r-1$ odd primes or less ($r > 1$), it holds for products m of r odd primes.

Lemma 3.2.16. If α is proper $\bmod p$ for same odd prime p. We can find a pure quaternion β, where $N(\beta)$ and p are co-prime, such that $\beta\alpha$ is pure $\bmod p$.

And now we can start with the proof of the Theorem 3.2.12.

Proof of Theorem 3.2.12. By the last four lemmas the proof of this theorem reduces to the case where m is an odd prime p, and $\alpha \in \mathcal{L}$ is a pure quaternion of the form $\alpha = i + a_3 j + a_4 k$ and $N(\alpha) = qp$ for some integer q.

Recall that for any quaternion $\tilde{\tilde{\alpha}} \in \mathcal{L}$,where $\tilde{\tilde{\alpha}}$ is proper $\bmod p$ and has a right divisor $\delta = d_1 + d_2 i + d_3 j + d_4 k \in \mathcal{L}$ with $N(\delta) = p$, there exists a pure quaternion $\beta \in \mathcal{L}$, where

$N(\beta)$ and p are co-prime, such that $\beta\tilde{\bar{\alpha}} = \tilde{\alpha}$ has the same right divisors of the norm equal to p and $\tilde{\alpha}$ is a pure $\bmod p$.

Consider that $\tilde{\alpha}$ is proper $\bmod p$ and in this case there exist at least two coefficients that are co-prime with p. Without loss of generality, let be $\tilde{a_2} \not\equiv 0 \bmod p$.

So we can find an integer n such that $n\tilde{a_2} \equiv 1 \bmod p$ and we can construct the quaternion $\alpha \in \mathcal{L}$ such that

$$n\tilde{\alpha} \equiv \alpha \bmod p \quad \Rightarrow \quad \alpha = i + a_3 j + a_4 k,$$

and it has all the same right divisors as the quaternion $\tilde{\bar{\alpha}}$.

Now we want to know how many quaternions δ satisfy the equations $\alpha = \gamma\delta$ and $N(\delta) = p$? This equations are also equivalent to $\alpha\bar{\delta} \equiv 0 \bmod p$ and $N(\delta) = p$.

Consider the product

$$\begin{aligned} \alpha\bar{\delta} &= (i + a_3 j + a_4 k)(d_1 + d_2 i + d_3 j + d_4 k) \\ &= (d_2 + a_3 d_3 + a_4 d_4) + (d_1 - a_3 d_4 + a_4 d_3) i + \\ &+ (d_4 + a_3 d_1 - a_4 d_2) j + (-d_3 + a_3 d_4 + a_4 d_3) k, \end{aligned}$$

and

$$\begin{aligned} d_2 + a_3 d_3 + a_4 d_4 &\equiv 0 \bmod p \\ d_1 - a_3 d_4 + a_4 d_3 &\equiv 0 \bmod p \\ d_4 + a_3 d_1 - a_4 d_2 &\equiv 0 \bmod p \\ -d_3 + a_3 d_4 + a_4 d_3 &\equiv 0 \bmod p. \end{aligned}$$

From the last equivalences we can construct two congruences $d_1 \equiv a_3 d_4 - a_4 d_3 \bmod p$ and $d_2 \equiv -a_3 d_3 - a_4 d_4 \bmod p$. Than set $d_3 = x_3$ and $d_4 = x_4$ and from this

$$d_1 = p x_1 + a_3 x_4 - a_4 x_3 \bmod p \text{ and } d_2 = p x_2 - a_3 x_3 - a_4 x_4 \bmod p, \tag{3.22}$$

where $x_1, \ldots, x_4$ are integers.

If we substitute it in $\sum_l d_l = p$, we compute

$$\begin{aligned} p^2\left(x_1^2 + x_2^2\right) + 2pa_3\left(x_1 x_4 - x_2 x_3\right) - 2pa_4\left(x_1 x_3 - x_2 x_4\right) + pq\left(x_3^2 + x_4^2\right) &= p \text{ or} \\ p\left(x_1^2 + x_2^2\right) + 2a_3\left(x_1 x_4 - x_2 x_3\right) - 2a_4\left(x_1 x_3 - x_2 x_4\right) + q\left(x_3^2 + x_4^2\right) &= 1. \end{aligned}$$

Consider that the number of solutions $(x_1, \ldots, x_4)$ of the last equation is the number of divisors.

In the paper [11] is shown that this last equation hast exactly eight solutions by using the theory of quadratic forms. And it is also shown that if δ is any of the corresponding solution defined in equation (3.22), its left-associates exhaust the other seven possibilities.

In this proof, we will go no further in the details of showing that last equation has eight solutions, but the exact proof is listed in the [11]. □

There is even a generalization of the last theorem that shows that this theorem holds with m even, provided α is actually proper and $N(\alpha)/m$ is odd. Anyway we will go no further in this discussion, since we will work later only with odd factors in presented algorithms in last chapter.

Proposition 3.2.17. Every quaternion $\alpha \in \mathcal{L}$ with $N(\alpha) > 1$ is a product of prime quaternions.

This proposition was already proven by Lipschitz. But today the most common proof is by using Hurwitz integers and the units in the Hurwitz ring. Anyway, we are going to demonstrate how to prove this proposition with the Lipschitz integers as well.

Proof. Let be $\alpha \in \mathcal{L}$ with $N(\alpha) > 1$. If α is a prime, it is already the prime factorization and we are done.

But assume that α is not a prime. Then by Definition 3.2.5 point 3, there exist $\beta, \gamma \in \mathcal{L}$, such that $\alpha = \beta\gamma$ and β and γ are not units. Consider $\frac{N(\alpha)}{2} \geq N(\beta), N(\gamma) > 1$, meaning that both quaternions have a norm smaller at least by the factor two. If β and γ are primes, we are done. And if at least one is not a prime, then by Definition 3.2.5, we can find two new factors with a smaller norm.

We can do this as long as not all factors are primes and we are not able to factor them any further in not invertible elements. At each step, the new quaternions have a norm smaller at least by factor two. From this we see that we need at most $\log_2(N(\alpha))$ steps, till we have found one prime factorization.

□

Consider that this factorization is not unique. Since the quaternion algebra is not commutative, the order of the factors in a composed quaternions becomes important. For example the quaternion $(1+2i+2j+2k)(1-2i-2j-2k) = 13 = (2+3i)(1-3i)$ or for example a proper quaternion $(3+2i)(4+k) = 12+8i+3j+2k = (2+2i-3k)(2-i+2j+2k)$.

Lemma 3.2.18. Let $\alpha, \beta \in \mathcal{L}$, with β odd. There exists $\gamma, \tau \in \mathcal{L}$ such that

$$\alpha = \gamma\beta + \tau \quad \text{and} \quad N(\tau) < N(\beta). \tag{3.23}$$

Lipschitz ring $\mathcal{L}$ is no euclidean domain. The problem appears if α and β are both even, then we cannot assure that $N(\tau) < N(\beta)$ holds. Anyway, assuming that at least one of the quaternions is odd, we can show that $N(\tau)$ is always smaller than $N(\beta)$.

Proof. We start this proof with a claim.

Claim 3.2.19. For a given $\delta = d_1 + d_2 i + d_3 j + d_4 k \in \mathcal{L}$ and $m \in \mathbb{N}$ odd, there exists $\gamma \in \mathcal{L}$, such that $N(\delta - \gamma m) < m^2$.

First find $c_i \in \mathbb{Z}$ for each d_i, such that c_i's satisfy

$$mc_i - \frac{m}{2} < d_i < mc_i + \frac{m}{2}. \tag{3.24}$$

There is strict inequality because m is odd. Set $t_i = d_i - mc_i$ and $\gamma = c_1 + c_2 j + c_3 j + c_4 k$. Then $|t_i| < \frac{m}{2}$, and $N(\delta - \gamma m) = t_1^2 + t_2^2 + t_3^2 + t_4^2 < 4\left(\frac{m}{2}\right)^2 = m^2$. This proves the claim.

Now set $m = N(\beta)$ and $\delta = \alpha\overline{\beta}$. By the claim we get

$$N(\beta)N(\overline{\beta}) = N(\beta) = m^2 > N(\delta - \gamma m) = N(\alpha\overline{\beta} - \gamma\beta\overline{\beta}) = N(\alpha - \gamma\beta)N(\overline{\beta}). \tag{3.25}$$

Set $\tau = \alpha - \gamma\beta$, then we see from the inequality above that $N(\beta) > N(\tau)$. □

Definition 3.2.20. Let be α, $\beta \in \mathcal{L}$. We say that $\delta \in \mathcal{L}$ is the greatest common right divisor (g.c.r.d.) of α and β

1. if δ is a right divisor of α and β, and
2. if $\delta_0 \in \mathcal{L}$ is any right divisor of α and β, then δ_0 is a right divisor of δ.

We will denote this δ with $\text{gcrd}(\alpha, \beta)$.

The existence of the greatest common divisor in Lipschitz ring is not trivial since it is not an euclidean domain. But we can show it in the following way:

Definition 3.2.21. Let be $\mathbb{Z}\left[\frac{1}{2}\right]$ the subset of rational numbers defined as

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{z}{2^n} : z \in \mathbb{Z}, n \in \mathbb{N}\right\}. \tag{3.26}$$

Lemma 3.2.22. Let be $\alpha \in \mathcal{L}$. Then α has a unique factorization

$$\alpha = 2^l \pi \alpha_0 \tag{3.27}$$

where $l \in \mathbb{N}$, $\pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ and $\alpha_0 \in \mathbb{H}(\mathbb{Z})$ is odd.

The proof of this lemma is stated in [4], but since we are only interested in the existence of the greatest common divisor, we will go straight to the next theorem.

Theorem 3.2.23. Let α, $\beta \in \mathcal{L}$, with β odd. Then $\operatorname{gcrd}(\alpha, \beta)$ exists. Moreover, there exists γ, $\delta \in \mathbb{H}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ such that $\operatorname{gcrd}(\alpha, \beta) = \gamma\alpha + \delta\beta$.

Proof. The steps of proof for this theorem are similar to the Euclidean Algorithm for computing the greatest common divisor of integers.

By Lemma 3.2.18, we get γ_0, $\tau_0 \in \mathcal{L}$, such that $\alpha = \gamma_0\beta + \tau_0$. For the next step of Euclidean Algorithm, τ_0 has to be odd. But this is not given by the Lemma 3.2.18, whereas from Lemma 3.2.22, $\tau_0 \in \mathcal{L}$ has a unique factorization $\tau_0 = 2^{l_0}\pi_0\tau_0'$, where τ_0' is odd. Then we can write

$$\alpha = \gamma_0\beta + 2^{l_0}\pi_0\tau_0'. \tag{3.28}$$

In the next step using Lemmas 3.2.18 and 3.2.22, we have

$$\beta = \gamma_1\tau_0' + \tau_1 = \gamma_1\tau_0' + 2^{l_1}\pi_1\tau_1'. \tag{3.29}$$

And then we get in s-the step of Euclidean Algorithm

$$\tau_{s-1}' = \gamma_{s+1}\tau_s' + 2^{l_{s+1}}\pi_{s+1}\tau_{s+1}' \tag{3.30}$$

for all $s \in \{0, \ldots, h+1\}$, where $h+1$ is the last step with $\tau_{h+1} = 0$, meaning that

$$\tau_{h-1}' = \gamma_{h+1}\tau_h'. \tag{3.31}$$

Consider that this iteration steps have to terminate since $N(\tau_s') > N(\tau_{h+1}) \geq N(\tau_{h+1}')$ for all $s \leq h$. Now we are coming to the last part where we want to show that the greatest common right divisor of α and β is τ_h'.

Claim 3.2.24. $\operatorname{gcrd}(\alpha, \beta) = \tau_h'$.

It is easy to check that τ_h' is a right divisor of τ_{h-1}', τ_{h-2}', $\ldots$, τ_0', β and α. So assume δ is any right divisor of α and β. Consider that τ_h' is odd, and also δ has to be odd since β is odd as well. From $\alpha = \gamma_0\beta + 2^{l_0}\pi_0\tau_0'$, we see that δ has to divide τ_0'. By going through all steps of Euclidean Algorithm with the same argument, we see that δ has to divide all τ_s' for all $s \in \{0, \ldots h\}$, i.e. δ divides τ_h'. And from the definition of g.c.r.d., τ_h is the greatest common right divisor of α and β, which proves the claim.

Now we are coming to the last point of the theorem. Consider that we can rewrite all the steps of computing τ_s' as follows:

$$\begin{array}{rcl} \tau_0' & = & 2^{-l_0}\pi_0^{-1}(\alpha - \gamma_0\beta) \\ \tau_1' & = & 2^{-l_1}\pi_1^{-1}(\beta - \gamma_1\tau_0') \\ \vdots & & \\ \tau_h' & = & 2^{-l_h}\pi_h^{-1}\left(\tau_{h-2}' - \gamma_h\tau_{h-1}'\right). \end{array} \tag{3.32}$$

Note that π_s is invertible in $\mathbb{H}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. By substitution of all of those equations, we can express $\tau_h' = \gamma\alpha + \delta\beta$, where $\gamma, \delta \in \mathbb{H}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. □

Lemma 3.2.25. For $\alpha \in \mathcal{L}$ and $m \in \mathbb{Z}$ odd:

$$\operatorname{gcrd}(m, \alpha) = 1 \quad \text{if and only if} \quad \gcd(m, N(\alpha)) = 1. \tag{3.33}$$

Proof. ($\Rightarrow$) We assume that $\gcrd(m, \alpha) = 1$. From the Theorem 3.2.23, we know that we can find γ and δ such that $\gamma, \delta \in \mathbb{H}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ and $1 = \gamma m + \delta\alpha$. Then it is clear that we can write the following:

$$\begin{aligned} 1 = N(1) &= N(\gamma m + \delta\alpha) \\ &= (\gamma m + \delta\alpha)\,\overline{(\gamma m + \delta\alpha)} \\ &= (\gamma m + \delta\alpha)\left(\overline{\gamma} m + \overline{\delta\alpha}\right) \\ &= \gamma m\overline{\gamma} m + \gamma m\overline{\delta\alpha} + \delta\alpha\overline{\gamma} m + \delta\alpha\overline{\delta\alpha} \\ &= N(\gamma)m^2 + 2\,(\gamma \cdot \delta\alpha)\,m + N(\delta\alpha) \\ &= (N(\gamma)m + 2\,(\gamma \cdot \delta\alpha))\,m + N(\delta)N(\alpha). \end{aligned} \tag{3.34}$$

It is also clear that $N(\gamma)$, $(\gamma \cdot \delta\alpha)$ and $N(\delta)$ are in $\mathbb{Z}\left[\frac{1}{2}\right]$ and therefore also elements of $\mathbb{H}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. This means that we can find $\gamma_2 = (N(\gamma)m + 2\,(\gamma \cdot \delta\alpha))$ and $\delta_2 = N(\delta)$ such that

$$\gamma_2 m + \delta_2 N(\alpha) = 1 = \gcrd\,(m, N(\alpha)) \tag{3.35}$$

and $\gamma_2, \delta_2 \in \mathbb{H}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$.

($\Leftarrow$) Now, $\gcrd(m, N(\alpha)) = 1$. So let δ be any common right divisor of m and α. This implies that δ is also a right divisor of $\overline{\alpha}\alpha = N(\alpha)$. And since $\gcrd(m, N(\alpha)) = 1$, δ is a right divisor of 1. From this we see that any common right divisor of m and α has to be a unit, i.e. $\gcrd(m, \alpha) = 1$. □

3.3 Prime quaternions and four square presentation

In the next part, we want to present the prime quaternions in Lipschitz ring and some of their properties. Adjacent to it, we will use the theory of the primes to prove that any natural number $n \in \mathbb{N}$ can be presented as a sum of four squares. On the end, we will also take a look at the prime quaternions that are periodical.

Lemma 3.3.1. Let be $p \in \mathbb{N}$ an odd prime. Assume that there exists $\alpha \in \mathcal{L}$, such that α is proper $\bmod p$, but $N(\alpha)$ is divisible by p. Set $\gcrd(\alpha, p) = \delta$. Then δ is a prime in $\mathcal{L}$ and $N(\delta) = p$.

Proof. Let be p an odd prime and $\alpha \in \mathcal{L}$ such that α is proper $\bmod p$, but $p|N(\alpha)$. Then set $\delta = \gcrd\,(\alpha,\, p)$. By Lemma 3.2.25, we know that δ is not a unit since $\gcd\,(N(\alpha),\, p) \neq 1$.

So let be $\gamma_1,\, \gamma_2 \in \mathcal{L}$ such that $p = \gamma_1\delta$ and $\alpha = \gamma_2\delta$. Then consider that γ_1 is not a unit. If it were, then p and δ would be left-associates, and this would imply that p also divides α, which is in contradiction to the condition from the settings of the lemma.

Then we can write

$$N(p) = N(\gamma_1)N(\delta) = p^2. \tag{3.36}$$

And since $N(\gamma_1),\, N(\delta) \neq 1$, it follows that $N(\gamma_1) = N(\delta) = p$.

Now assume that δ is not a prime quaternion. Then by Definition 3.2.5 point 3, there exist $\delta_1,\, \delta_2 \in \mathcal{L}$ such that $\delta = \delta_1\delta_2$, where δ_1 and δ_2 are not units, i.e. $N(\delta_1),\, N(\delta_2) \neq 1$. But then $N(\delta) = N(\delta_1)N(\delta_2) = p$, which implies that one of norms has to be equal to 1. And this is a contradiction since δ_1 and δ_2 are not units.

So we see that δ has to be a prime quaternion. □

Theorem 3.3.2. For every $p \in \mathbb{N}$ odd prime, there exists a prime $\delta \in \mathcal{L}$ such that $N(\delta) = p = \delta\overline{\delta}$. In particular, p is not a prime in $\mathcal{L}$.

To prove this theorem, we will use a lemma which is listed and proved in Appendix C.

Proof. Let be $p \in \mathbb{N}$ an odd prime. Then consider Lemma C.0.6 from Appendix C. By this lemma, we can find $x,\, y \in \mathbb{Z}_p$ such that $x^2 + y^2 + 1 \equiv 0 \bmod p$. Then we can build the

quaternion $\alpha = x + yi + j$. Note that α is a proper quaternion and therefore not divisible by p. But p divides $N(\alpha) = x^2 + y^2 + 1$.

By Lemma 3.2.25, the quaternion $\delta = \text{gcrd}(\alpha, p)$ is not a unit. And by Lemma 3.3.1 δ is a prime. □

Corollary 3.3.3. A quaternion $\delta \in \mathcal{L}$ is a prime in $\mathcal{L}$ if and only if $N(\delta)$ is a prime in $\mathbb{N}$.

Proof. ($\Leftarrow$) Note that this direction is proven by Lemma 3.3.1.

($\Rightarrow$) Let be $\delta \in \mathcal{L}$ a prime quaternion, i.e. for any two quaternions α, $\beta \in \mathcal{L}$ such that $\delta = \alpha\beta$, then either α or β is a unit.

First we assume that δ is even, i.e. δ has an even norm. By Lemma 3.2.22, we can write $\delta = 2^l \pi \delta_0$, where $l \in \mathbb{N}$, $\pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ and δ_0 is odd. We already know that the integer 2 is not a prime, so l must be zero. Then π must be different from 1 since δ_0 is odd. But then δ_0 must be equal to 1, since we would already have a factorization of δ. And this implies that $\delta = \pi$, where $\pi \in \{1+i, 1+j, 1+k\}$ and $N(\pi) = 2$.

Now assume that δ is odd. And let be $p \in \mathbb{N}$ an odd prime, where $p | N(\delta)$. Note that there exists such a prime p since δ is odd. So set $\alpha = \text{gcrd}(\delta, p)$. Recall that α is not a unit by Lemma 3.2.25. Then we can find a quaternion $\gamma \in \mathcal{L}$ such that $\delta = \gamma\alpha$. But since δ is a prime, it follows that γ must be a unit.

Now we see that α and δ are left-associates and this means that δ is also a right divisor of p. Then we can write $p = \beta\delta$ and $N(p) = N(\alpha)N(\beta) = p^2$. If we divide this equation by p we get

$$N(\beta)\frac{N(\delta)}{p} = p. \tag{3.37}$$

Here we can have $N(\beta) = 1$ or $\frac{N(\delta)}{p} = 1$. If $N(\beta) = 1$, then β is a unit and δ and p are left-associates. But since δ is a prime, p must also be a prime in $\mathcal{L}$, which is the contradiction to Theorem 3.3.2. So $\frac{N(\delta)}{p} = 1$ and $N(\delta) = p$, where p is a prime in $\mathbb{N}$. □

Note that this already proves, that any natural number $n \in \mathbb{N}$ is a sum of four squares.

Corollary 3.3.4. Every natural number $n \in \mathbb{N}$ is a sum of four squares.

Proof. Let be $n \in \mathbb{N}$ an arbitrary positive integer. Then we can write n as a product of its factors $n = \prod_l p^{e_l}$, where p_l's are prims and $e_l \in \mathbb{N}$.

But then by Theorem 3.3.2 and Corollary 3.3.3 we can find prime quaternions $\pi_l \in \mathcal{L}$ such that $N(\pi_l) = p_l$ for all l. This means that the quaternion $\alpha = \prod_l \pi_l^{e_l}$ has the norm

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = N(\alpha) = N(\prod_l \pi_l^{e_l}) = \prod_l N(\pi_l)^{e_l} = \prod_l p_l^{e_l} = n.$$

And this proves the corollary. □

In Appendix C, we have also listed the proof of Lagrange's Theorem which proves the same.

Proposition 3.3.5. Every prime quaternion $\pi \in \mathcal{L}$ with $N(\pi) = p \in \mathbb{N}$ is always proper and has at least two coefficients different from zero.

Proof. Let be $\pi = p_1 + p_2 i + p_3 j + p_4 k \in \mathcal{L}\backslash\{0\}$ a prime quaternion. First assume that π has exactly one coefficient $p_s \neq 0$ for any $s \in \{1, \ldots, 4\}$. Then we know that the norm $N(\pi) = p_s^2$ is not a prime. But this is then the contradiction to the Corollary 3.3.3.

Now assume that π is not proper, i.e. $\gcd(p_1, p_2, p_3, p_4) = d \neq 1$, where $d \in \mathbb{N}$. Then we can write $\pi = d\left(\frac{p_1}{d} + \frac{p_2}{d}i + \frac{p_3}{d}j + \frac{p_3}{d}k\right)$, where d, $\left(\frac{p_1}{d} + \frac{p_2}{d}i + \frac{p_3}{d}j + \frac{p_3}{d}k\right) \in \mathcal{L}$ are not units. And this is the contradiction to the definition of the prime quaternion. □

Lemma 3.3.6. Let be $\alpha \in \mathbb{H}$. Then α is left-associated to $\overline{\alpha}$ if and only if α is right-associated to $\overline{\alpha}$.

Proof. Assume that α and $\overline{\alpha}$ are left-associated, i.e. $\alpha = \varepsilon\overline{\alpha}$, where $\varepsilon \in \mathcal{L}$ is a unit. Then we can compute that

$$\alpha^2 = \varepsilon\overline{\alpha}\alpha = N(\alpha)\varepsilon = \alpha\overline{\alpha}\varepsilon \quad \Rightarrow \quad \alpha = \overline{\alpha}\varepsilon. \tag{3.38}$$

Analogically, we can show that if α and $\overline{\alpha}$ are right-associated, i.e. $\alpha = \overline{\alpha}\varepsilon$, where $\varepsilon \in \mathcal{L}$ is a unit, then $\alpha = \varepsilon\overline{\alpha}$. □

Proposition 3.3.7. Let be $\pi \in \mathcal{L}$ a prime quaternion. Then π is periodical if and only if π and $\overline{\pi}$ are left-associates (resp. right-associates).

Proof. ($\Rightarrow$) Let be $\pi \in \mathcal{L}$ periodical and prime, with $N(\pi) = p$ prime and period $e_1 \in \mathbb{N}$, i.e.

$$\pi^{e_1} = z \in \mathbb{Z}. \tag{3.39}$$

Note that z has to be a power of p and that $p = \overline{\pi}\pi$. This means that there exists $e \in \mathbb{N}$ and $e \leq e_1$ such that π^e is not proper mod p anymore. So let be

$$\tilde{e_1} = \min\{e \leq e_1 \mid \pi^e \text{ is not proper } \bmod p\}.$$

Then we can write the following equation

$$\left(\pi^{\tilde{e_1}}\right) = \varphi p^{e_2} = \varphi\left(\overline{\pi}^{e_2}\right)\left(\pi^{e_2}\right) \quad \Rightarrow \quad \pi^{\tilde{e_1}-e_2} = \varphi\overline{\pi}^{e_2}, \tag{3.40}$$

where φ is quaternion proper mod p and $e_2 \in \mathbb{N}$. Note that $\varphi\overline{\pi}^{e_2}$ has to be proper mod p, since $\pi^{\tilde{e_1}-e_2}$ is proper mod p. And this implies that π and $\overline{\pi}$ are two right divisors of the same norm that divides both quaternions $\pi^{\tilde{e_1}-e_2}$ and $\varphi\overline{\pi}^{e_2}$. And by the Theorem 3.2.12 π, $\overline{\pi} \in \mathfrak{DL}$. That they are also right-associates follows directly from Lemma 3.3.6.

($\Leftarrow$) Assume that π is left-associated to $\overline{\pi}$, i.e. $\pi = \varepsilon\overline{\pi}$ for some $\varepsilon \in \mathcal{L}$, ε being a unit. Then

$$\pi^2 = \varepsilon\overline{\pi}\pi = N(\pi)\varepsilon. \tag{3.41}$$

If $\varepsilon = \pm 1$, then π^2 is already in $\mathbb{Z}$. If $\varepsilon \in \{\pm i, \pm j, \pm k\}$ then $\varepsilon^2 = -1$ and

$$\pi^4 = \left(\pi^2\right)^2 = (N(\pi)\varepsilon)^2 = -N(\pi)^2 \in \mathbb{Z}. \tag{3.42}$$

We can show that this is also true for right-associates. □

This proposition implies that all prime quaternions that are periodical must have a period equal to 2 or 4. They always have the period 2 if $\pi = -1\overline{\pi}$, i.e $\varepsilon = -1$. This is only the case if π is a pure quaternion. In general, we can easily show that the direction ($\Leftarrow$) of Corollary 3.3.7 is true for all quaternions $\alpha \in \mathcal{L}$, such that α and $\overline{\alpha}$ are left-associates resp. right-associates. This means that every pure quaternion $\alpha \in \mathcal{L}$ different from zero is periodical and has a period $e = 2$.

Lemma 3.3.8. Let be π a prime periodical quaternion. Then π has a period $e \in \{2, 4\}$, i.e. $\pi^e \in \mathbb{Z}$ for $e \in \{2, 4\}$.

Proof. As we already discussed it above, this is a direct consequence of Proposition 3.3.7.

Since π is periodical and prime, it follows that $\pi = \varepsilon\overline{\pi}$ for some unit ε. Then

$$\pi^2 = \varepsilon\overline{\pi}\pi = \varepsilon N(\pi). \tag{3.43}$$

If $\varepsilon = -1$, then $\pi^2 \in \mathbb{Z}$ and π has the period $e = 2$. If $\varepsilon \neq \pm 1$, then

$$\pi^4 = (\varepsilon N(\pi))^2 = -1N(\pi)^2 \in \mathbb{Z}, \tag{3.44}$$

and π has the period $e = 4$. □

Now consider any quaternion of the form $\beta = z\alpha$, where $\alpha \in \mathcal{L}$ is periodical and $z \in \mathbb{Z}$. Then β is also periodical. But if $\beta = \alpha_1\alpha_2$ is product of two quaternions, where $\alpha_1,\ \alpha_2 \in \mathcal{L}$ are both periodical, it seams that β does not have a period related to periods of α_1 and α_2 or is not periodical at all. For example, if $\alpha_1 = i + j$ and $\alpha_2 = i + j + k$, both are pure quaternions and have the period 2. But $\beta = \alpha_1\alpha_2 = -2 + i - j$ appears to have no period at all. And quaternion $\beta = 1 + i + j + k = (1 + i)(1 + j) = \alpha_1\alpha_2$, where α_1 and α_2 have both period 4, is periodical and has a period 3.

Proposition 3.3.9. Every quaternion $\pi \in \mathcal{L}$ of norm $N(\pi) = 2$ is periodical and has a period $e \in \{2, 4\}$.

Proof. All prime quaternions of norm equal to 2 are of the form $\pi = \varepsilon_1 + \varepsilon_2$, where $\varepsilon_1,\ \varepsilon_2 \in \{\pm 1, \pm i, \pm j, \pm k\}$ and $\varepsilon_1 \neq \pm\varepsilon_2$.

Since every such π, π and $\overline{\pi}$ are left-associates, we know from Corollary 3.3.7 that π is periodical.

To show that π has the period $e \in \{2, 4\}$, we will present two cases.

First, assume that $\varepsilon_1,\ \varepsilon_2 \neq \pm 1$, meaning that $\varepsilon_1^2 = -1$, $\varepsilon_2^2 = -1$ and $\varepsilon_1\varepsilon_2 = -\varepsilon_2\varepsilon_1$, since $\varepsilon_1,\ \varepsilon_2 \in \{\pm i, \pm j, \pm k\}$ and $\varepsilon_1 \neq \pm\varepsilon_2$. So we can compute

$$(\varepsilon_1 + \varepsilon_2)(\varepsilon_1 + \varepsilon_2) = \varepsilon_1^2 + \varepsilon_1\varepsilon_2 + \varepsilon_2\varepsilon_1 + \varepsilon_2^2 = -1 + \varepsilon_1\varepsilon_2 - \varepsilon_1\varepsilon_2 - 1 = -2 \in \mathbb{Z} \tag{3.45}$$

and π has the period equal 2.

In the second case, let be $\varepsilon_1 = \pm 1$ and $\varepsilon_2 \in \{\pm i, \pm j, \pm k\}$, then $\varepsilon_1^2 = 1$, $\varepsilon_2^2 = -1$ and $\varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_1$. So we can compute

$$(\varepsilon_1 + \varepsilon_2)(\varepsilon_1 + \varepsilon_2) = \varepsilon_1^2 + \varepsilon_1\varepsilon_2 + \varepsilon_2\varepsilon_1 + \varepsilon_2^2 = 1 + \varepsilon_1\varepsilon_2 + \varepsilon_1\varepsilon_2 - 1 = 2\varepsilon_1\varepsilon_2, \tag{3.46}$$

and therefore $\pi^4 = (2\varepsilon_1\varepsilon_2)^2 = -4$. So all π's of the form $\pm 1 + \varepsilon$, where $\varepsilon \in \{\pm i, \pm j, \pm k\}$, have the period equal 4. □

At this point, we still have open questions: "What do all periodical quaternions look like?" and "Are there any quaternions with large period?" In Chapter 6, we will briefly discuss how the answers to those questions can be relevant for the factorization of integers.

3.4 Hurwitz integers

In this section, we will shortly discuss a small extension of the Lipschitz ring $\mathcal{L}$ that will give us advantage over some problems in Lipschitz ring.

As we already saw, a Lipschitz ring is not an euclidean domain, and since there always exists a greatest common right (resp. left) divisor, we cannot always compute its value. A Hurwitz ring that is an extension of $\mathcal{L}$, but still analogue to a Lipschitz ring, is an euclidean domain. Also some proofs that we did in Lipschitz ring become simpler by using the Hurwitz ring.

Anyway, since the theory we use for describing the factorization algorithm of integers in this thesis is already provided by the Lipschitz ring, we do not need this extension. Anyway, we will shortly present the Hurwitz ring.

Definition 3.4.1. The set of *Hurwitz integers* is the set $\mathcal{L} \cup (\omega + \mathcal{L})$, where quaternion $\omega = \frac{1}{2}(1 + i + j + k)$, i.e.

$$\{a_1 + a_2 i + a_3 j + a_4 k \mid a_1, a_2, a_3, a_4 \in \mathbb{Z} \text{ or } a_1, a_2, a_3, a_4 \in \mathbb{Z} + 1/2\}.$$

This set is denoted by $\mathcal{H}$.

Note that Hurwitz integers are the quaternions whose coefficients a_i's are all either integers or half of an odd integer. And so the norm of a Hurwitz integer is always a positive integer, i.e. $\forall \alpha \in \mathcal{H}$, $N(\alpha) \in \mathbb{N}$.

Also consider that for two Hurwitz integers $\alpha, \beta \in \mathcal{H}$, the addition and the multiplication are well defined. And since $\mathcal{H} \subset \mathbb{H}$, it is easy to see that associativity and distributivity lows are provided and that $(\mathcal{H}, +, \cdot)$ is a ring.

Now we are going to give some definitions that we already saw with Lipschitz integers.

Definition 3.4.2. We say $\varepsilon \in \mathcal{H}$ is a *unit* if ε is invertible, i.e. there exists ε^{-1} in $\mathcal{H}$ such that $\varepsilon\varepsilon^{-1} = 1$.

With the same argument as with Lipschitz integers, we can show that for any $\alpha \in \mathcal{H}$, where α is a unit, the norm of α must be 1. But now there are 24 quaternions with the norm 1, namely $\left\{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\right\}$.

Definition 3.4.3. Let be $\alpha, \beta \in \mathcal{H}$. Then we say that α is *associated* with β if there exist units $\varepsilon_1, \varepsilon_2 \in \mathcal{H}$, such that $\alpha = \varepsilon_1 \beta \varepsilon_2$. Similarly, we say that α and β are *left-associated* (resp. *right-associated*) if there exists a unit $\varepsilon \in \mathcal{L}$, such that $\alpha = \varepsilon\beta$ (resp. $\alpha = \beta\varepsilon$).

Definition 3.4.4. Let be $\alpha, \beta \in \mathcal{H}$. We say that β is a left (resp. right) divisor of α if there exists $\delta \in \mathcal{H}$ such that $\alpha = \beta\delta$ (resp. $\alpha = \delta\beta$).

In the next part, we will show in which way the Hurwitz ring is an approval according to the Lipschitz ring.

Proposition 3.4.5. The ring $\mathcal{H}$ is a left (and right) euclidean.

Proof. Let be $\alpha, \beta \in \mathcal{H}$ with $N(\alpha) > N(\beta)$. Define

$$\delta = \beta^{-1}\alpha = \frac{\overline{\beta}\alpha}{N(\beta)} \in \mathbb{H}. \tag{3.47}$$

If $\delta = (d_1 + d_2 i + d_3 j + d_4 k) \in \mathcal{H}$, then α divides β in $\mathcal{H}$ since $\alpha = \beta\delta + 0$. So we assume that $\delta \notin \mathcal{H}$. Then we can construct $\gamma = (c_1 + c_2 i + c_3 j + c_4 k) \in \mathcal{L}$ such that every coordinate c_i for $i \in \{1, 2, 3, 4\}$ of γ is the closest integer of the corresponding coordinate d_i of δ. Now we can compute $\varepsilon = (e_1 + e_2 i + e_3 j + e_4 k) = \delta - \gamma$, where at least one of $|e_i| < 1/2$ because $\delta \notin \mathcal{H}$, and then $\tau = \beta\varepsilon = \beta(\delta - \gamma) = \alpha - \beta\gamma \in \mathcal{H}$. And we have an equation $\alpha = \beta\gamma + \tau$, where $\alpha, \beta, \gamma, \tau \in \mathcal{H}$.
Now we only have to prove that $N(\tau) < N(\beta)$. Consider that $N(\varepsilon) < 4\left(\frac{1}{2}\right)^2 = 1$ and that $\tau = \beta\varepsilon$. So we see that $N(\tau) = N(\beta\varepsilon) = N(\beta)N(\varepsilon) < N(\beta) \cdot 1$. And this proves the proposition.
Similarly, we can show that $\mathcal{H}$ is a right euclidean. □

By proving the Proposition 3.4.5, we see that we can use the Euclidean Algorithm to compute the greatest common right (resp. left) divisor of any two Hurwitz integers. But this also means that we can compute the greatest common right (resp. left) divisor of any two quaternions $\alpha, \beta \in \mathcal{L} \subset \mathcal{H}$ without any restrictions on the quaternion norm.

But since all computations are done in the Hurwitz ring, the result can still be a Hurwitz integer with half integer coefficients, which is then not a solution in the Lipschitz ring. Anyway, in the next lemma we will show that any Hurwitz integer with half-integer coefficients has a associate that is a quaternion with all integer coefficients, i.e. a Lipschitz integer.

Lemma 3.4.6. Let be $\alpha \in \mathbb{H}$ a Hurwitz integer with half-integer coefficients. Then there exists an associate $\varepsilon \in \mathcal{H}$, where $\varepsilon\alpha$ is a Lipschitz integer.

The proof of this lemma is very technical; it is given in [3] and presented in the form of the algorithm that from the given Hurwitz integer with half-integer coefficients returns the wanted Lipschitz integer.

Chapter 4

Number of two and four square presentations of a positive integer

In this chapter, we will prove the formulas to compute the number of two and four square presentations.

In the first section, we will proof the Theorem 4.1.4 that discuss the formula for two square presentations.

And in the second section, we will present the Jacobi Theorem that states a formula to compute the number of four square presentations for a given natural number n.

4.1 Number of two square presentations

In this section, we will present the formula of Legendre that computes the exact number of tuples (a, b) with $a, b \in \mathbb{Z}$, such that $n = a^2 + b^2$. So we start with the following definitions.

Definition 4.1.1. For $h \geq 2$ and $n \in \mathbb{N}$, we denote by $r_h(n)$ the number of representations of n as a sum of h-squares,

$$r_h(n) = \left| \left\{ (x_1, x_2, \ldots, x_h) \in \mathbb{Z}^h \middle| \sum_{s=1}^{h} x_s^2 = n \right\} \right|.$$

Remark 4.1.2. Consider any tuple $(x_1, \ldots, x_s, \ldots, x_t, \ldots, x_h)$, which is a solution for $\sum_{s=1}^{h} x_s^2 = n$, then all other tuples, that are permutation and sing changes of a solution $(x_1, \ldots, x_s, \ldots, x_t, \ldots, x_h)$ are also solutions for $\sum_{s=1}^{h} x_s^2 = n$, and all such pairwise distinct tuples are also counted in $r_h(n)$ too.

Definition 4.1.3. Let be

1. $d_1(n)$, the number of divisors of $n \in \mathbb{N}$ which are congruent to 1 mod 4.
2. $d_3(n)$, the number of divisors of $n \in \mathbb{N}$ which are congruent to 3 mod 4.
3. $d(n)$, the number of divisors of $n \in \mathbb{N}$.

From this definition we see right away that for an odd number n, we have that $d(n) = d_1(n) + d_3(n)$.

Theorem 4.1.4. For $n \in \mathbb{N}$, $n > 0$: $r_2(n) = 4\,(d_1(n) - d_3(n))$.

Proof. Let us define $\delta(n) = d_1(n) - d_3(n)$, and consider that n can be represented as $n = 2^r pq$ with $r \in \mathbb{N}$ and

$$p = \prod_{s=1}^{l} p_s^{o_s} \qquad p_s \equiv 1 \bmod 4 \quad \forall s \tag{4.1}$$

$$q = \prod_{t=1}^{m} q_t^{e_t} \qquad q_t \equiv 3 \bmod 4 \quad \forall t. \tag{4.2}$$

First let be n an odd number, i.e. $r = 0$ and $n = pq$.

Claim 4.1.5. $\delta(n) = d(p)\delta(q)$ for $n \in \mathbb{N}$ odd.

By definition of δ, we know that $\delta(n) = d_1(n) - d_3(n)$. Consider that all prime factors of p are congruent to 1 modulo 4. Then all factors of p have to be congruent to 1 modulo 4, meaning that $d(p) = d_1(p)$. Also consider that $\tilde{q}^2 \equiv 1 \bmod 4$, where $\tilde{q} \equiv 3 \bmod 4$ is an odd prime. Now we can easily estimate that $d_1(n) = d_1(p)d_1(q)$ and that all other divisors of n are $d_3(n) = d_1(p)d_3(q)$. Then we can show the claim

$$\begin{aligned} \delta(n) = d_1(n) - d_3(n) &= d_1(p)d_1(q) - d_1(p)d_3(q) &= \\ &= d_1(p)\,(d_1(q) - d_3(q)) &= d(p)\delta(q). \end{aligned} \tag{4.3}$$

Next we are interested in the value of $\delta(q)$.

Claim 4.1.6.

$$\delta(q) = \begin{cases} 0 & \text{if } \exists\ t \text{ such that } e_t \text{ is odd.} \\ 1 & \text{otherwise, meaning that } q \text{ is a square.} \end{cases}$$

Consider the notation from equation (4.2) and that $\delta(1) = 1$.

Now we define $q' = \frac{q}{q_1^{e_1}}$. From the discussion above, we saw that the divisors of $q_1^{e_1}$ can only be congruent to 1 modulo 4 if they are squares. To be precise, we have $\lfloor e_1/2 \rfloor + 1$ factors of q that are congruent to 1 modulo 4 and $\lceil e_1/2 \rceil$ factors of q that are congruent to 3 modulo 4. This means if e_1 is even, then we get

$$d_1(q) = \left(\frac{e_1}{2} + 1\right) d_1(q') + \frac{e_1}{2} d_3(q') \tag{4.4}$$

$$d_3(q) = \frac{e_1}{2} d_1(q') + \left(\frac{e_1}{2} + 1\right) d_3(q') \tag{4.5}$$

From equations above, we can compute $\delta(q) = d_1(q) - d_3(q) = d_1(q') - d_3(q') = \delta(q')$. In the case where all exponents e_t's are even (i.e. q is a square), using induction steps, we can take out all other factors $q_t^{e_t}$, and we get $\delta(q) = \delta(q') = \ldots = \delta(1) = 1$.

Next, we want to estimate the value of $\delta(q)$, it there is one t, such that e_t is an odd number, i.e. q is not a square. So, without loss of generality, we assume that e_1 is odd. Then we can use the same arguments about the number of divisors $d_1(q)$ and $d_3(q)$ as above, and compute the following equations:

$$d_1(q) = \left(\frac{e_1 - 1}{2} + 1\right) d_1(q') + \frac{e_1 + 1}{2} d_3(q') = \frac{e_1 + 1}{2} d_1(q') + \frac{e_1 + 1}{2} d_3(q') \tag{4.6}$$

$$d_3(q) = \frac{e_1 + 1}{2} d_1(q') + \left(\frac{e_1 - 1}{2} + 1\right) d_3(q') = \frac{e_1 + 1}{2} d_1(q') + \frac{e_1 + 1}{2} d_3(q') \tag{4.7}$$

As we can see from these equations, $d_1(q) = d_3(q)$ and $\delta(q) = d_1(q) - d_3(q) = 0$, which proves the claim.

The Claims 4.1.5 and 4.1.6 imply that

$$\delta(n) = \begin{cases} 0 & \text{if } \exists\ t \text{ such that } e_t \text{ is odd.} \\ d(p) & \text{otherwise, i.e. } q \text{ is a square.} \end{cases} \tag{4.8}$$

Consider that the equation (4.8) above also holds for n even since $\delta(n) = d_1(n) - d_3(n)$ and even divisors of n are not counted in the values $d_1(n)$ and $d_3(n)$.

Now we want to give a formula for computing a value $r_2(n)$ for any arbitrary $n \in \mathbb{N}$. Let be $n \in \mathbb{N}$ a sum of two squares. Then there exists a, $b \in \mathbb{Z}$, such that $a^2 + b^2 = n$, and we can find a Gaussian integer $\alpha = a + bi$ with $N(\alpha) = n$. From Proposition 2.1.9, α has a unique factorization

$$\alpha = a + bi = \mu^r \prod_{s=1}^{l} \pi_s^{o_s} \prod_{t=1}^{m} \rho_t^{h_t}, \tag{4.9}$$

where $N(\mu) = 2$, $N(\pi_s) = p_s$, $N(\rho_t) = q_t^2$, $2h_t = e_t$ and p, q, p_s, q_t, r, and e_t are defined as in equations (4.1) and (4.2), and we see that the norm of α is

$$n = a^2 + b^2 = N(\mu)^r \prod_{s=1}^{l} N(\pi_s)^{o_s} \prod_{t=1}^{m} q_t^{e_t} = 2^r pq. \tag{4.10}$$

Considering that for any Gaussian integer γ, $N(\gamma) = \gamma\overline{\gamma}$, the equation (4.10) can be remodeled in:

$$n = (a + bi)(a - bi) = (-i)^r (1 + i)^{2r} \prod_{s=1}^{l} \pi_s^{o_s} \overline{\pi}_s{}^{o_s} \prod_{t=1}^{m} q_t^{e_t}. \tag{4.11}$$

Since $N((a + bi)) = N((a - bi))$, we can split the equation (4.11) in

$$(a + bi) = \varepsilon (1 + i)^r \prod_{s=1}^{l} \pi_s^{u_s} \overline{\pi}_s{}^{w_s} \prod_{t=1}^{m} q_t^{e_t/2} \text{ and} \tag{4.12}$$

$$(a - bi) = \varepsilon' (1 + i)^r \prod_{s=1}^{l} \pi_s^{w_s} \overline{\pi}_s{}^{u_s} \prod_{t=1}^{m} q_t^{e_t/2}, \tag{4.13}$$

where $\varepsilon, \varepsilon'$ with $\varepsilon\varepsilon' = (-i)^r$ and $u_s + w_s = o_s$ for all $s \in \{1, 2, \ldots, l\}$. Now we only have to terminate the number of all possible different presentations of $(a + bi)$, which only depend on different choices of ε and u_i's in the equation above. So there are

$$4 \prod_{s=1}^{l} (o_s + 1) = 4d(p) = 4\delta(n) = 4 (d_1(n) - d_3(n)) \tag{4.14}$$

different choices, and this proves the theorem.

□

Remark 4.1.7. Recall Corollary 2.2.2. It states that any $n = 2pq \in \mathbb{N}$ is a sum of two squares if and only if q is a square.

From the last theorem, if q is not a square, then $\delta(n) = \delta(q) = 0$. And we can compute $r_2(n) = 4\delta(n) = 0$. And if q is a square, then $\delta(q) = 1$ and $\delta(n) = d(p) > 0$. So from theorem above follows, $r_2(n) = 4\delta(n) > 0$.

As we can see, that last theorem also proves the statement of Corollary 2.2.2.

4.2 Jacobi's Theorem

In this section, we will prove Jacobi's Theorem which states an exact formula to compute the number of four squares presentations $a_1^2 + a_2^2 + a_3^2 + a_4^2 = n$ for a given $n \in \mathbb{N}$.

First recall the Definition 4.1 of the number $r_h(n)$, which is the number of h squares presentations for a given number n.

Lemma 4.2.1. For every $n \in \mathbb{N} : r_4(4n) = r_4(2n)$.

Proof. Let be $(a_1, a_2, a_3, a_4) \in \mathbb{Z}^4$ a solution for $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 4n$. Note that $a^2 \equiv 0 \bmod 4$ for an even integer $a \in \mathbb{N}$ and $a^2 \equiv 1 \bmod 4$ for an odd integer a. Then it is clear that all a_l's have to be even or odd, since $4n \equiv 0 \bmod 4$.

Consider now the change of variables

$$b_1 = \frac{a_1 - a_2}{2}, \quad b_2 = \frac{a_1 + a_2}{2}, \quad b_3 = \frac{a_3 - a_4}{2}, \quad b_4 = \frac{a_3 + a_4}{2}, \tag{4.15}$$

where $b_1, b_2, b_3, b_4 \in \mathbb{Z}$. Then from the equations (4.15) follows:

$$a_1 = b_1 + b_2, \quad a_2 = b_2 - b_1, \quad a_3 = b_3 + b_4 \text{ and } a_4 = b_4 - b_3. \tag{4.16}$$

So substitute a_1, a_2, a_3 and a_4 with the equalities in (4.16).

$$\begin{aligned} (b_1 + b_2)^2 + (b_2 - b_1)^2 + (b_3 + b_4)^2 + (b_4 - b_3)^2 &= 4n \\ 2b_1^2 + 2b_2^2 + 2b_3^2 + 2b_4^2 &= 4n \\ b_1^2 + b_2^2 + b_3^2 + b_4^2 &= 2n \end{aligned} \tag{4.17}$$

The change of variables (4.15) maps a solution of $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 4n$ into a solution of $b_1^2 + b_2^2 + b_3^2 + b_4^2 = 2n$, and establishes a bijection between the two sets of solutions, where the mapping (4.16) is inverse. □

Lemma 4.2.2. For odd $n \in \mathbb{N} : r_4(2n) = 3r_4(n)$.

Proof. Let be $(a_1, a_2, a_3, a_4) \in \mathbb{Z}^4$ a solution for $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 2n$, and note that if an integer a is even (resp. odd), then $a^2 \equiv 0 \bmod 4$ (resp. $a^2 \equiv 1 \bmod 4$).

Consider that for n odd, there exists $t \in \mathbb{N}$ such that $n = 2t + 1$. And in this case $2n = 2(2t + 1) \equiv 2 \bmod 4$. This implies that two of the a_l's must be even and the other two must be odd, otherwise the sum of the four squares would not be equal to $2n$ where n is odd.

So there are three different cases that can be constructed by pairing two even and two odd numbers:

$$\text{Case 1 :} \quad \left\{ \begin{array}{l} a_1 \equiv a_2 \bmod 2 \\ a_3 \equiv a_4 \bmod 2 \end{array} \right\}$$

$$\text{Case 2 :} \quad \left\{ \begin{array}{l} a_1 \equiv a_3 \bmod 2 \\ a_2 \equiv a_4 \bmod 2 \end{array} \right\}$$

$$\text{Case 3 :} \quad \left\{ \begin{array}{l} a_1 \equiv a_4 \bmod 2 \\ a_2 \equiv a_3 \bmod 2 \end{array} \right\}$$

In all three cases there exist variables change similar as in the equation (4.15), where b_1, $b_2\, b_3$ and b_4 are computed by adding and subtracting the paired values.

In other words, in the first case, we can construct the variable change:

$$b_1 = \frac{a_1 - a_2}{2}, \quad b_2 = \frac{a_1 + a_2}{2}, \quad b_3 = \frac{a_3 - a_4}{2}, \quad b_4 = \frac{a_3 + a_4}{2}, \tag{4.18}$$

where $b_1^2+b_2^2+b_3^2+b_4^2=n$. And with the same argument as in the proof of Lemma 4.2.1, we see that there is bijection between the set of solutions in case 1 and set of values $(b_1,\, b_2,\, b_3,\, b_4)$.

So we can show the same bijection for the second case, where

$$b_1=\frac{a_1-a_3}{2},\quad b_2=\frac{a_1+a_3}{2},\quad b_3=\frac{a_2-a_4}{2},\quad b_4=\frac{a_2+a_4}{2}, \tag{4.19}$$

and as well for the third case with

$$b_1=\frac{a_1-a_4}{2},\quad b_2=\frac{a_1+a_4}{2},\quad b_3=\frac{a_2-a_3}{2},\quad b_4=\frac{a_2+a_3}{2}. \tag{4.20}$$

Note that the number of solutions in all three cases is the same, since for every tuple $(a_1,\, a_2,\, a_3,\, a_4)$, with a sum of squares equal to $2n$ and counted in one of the cases, there is a corresponding permutation that is counted in the other cases. For example, assume that $a_1 \equiv a_2 \bmod 2$, then for a fixed value a_1,

$$\begin{aligned}(a_1,\, a_2,\, a_3,\, a_4)\,,\,(a_1,\, a_2,\, a_4,\, a_3)&\ \text{ are in case 1}\\ (a_1,\, a_3,\, a_2,\, a_4)\,,\,(a_1,\, a_4,\, a_2,\, a_3)&\ \text{ are in case 2}\\ (a_1,\, a_4,\, a_3,\, a_2)\,,\,(a_1,\, a_3,\, a_4,\, a_2)&\ \text{ are in case 3.}\end{aligned}$$

So the set of solutions for $a_1^2+a_2^2+a_3^2+a_4^2=2n$ has three times more solutions than the set of solutions for $b_1^2+b_2^2+b_3^2+b_4^2=n$, and this proofs the lemma.

□

Definition 4.2.3. For $h \geq 2$ and $n \in \mathbb{N}$, we denote by $\mathcal{N}_h(n)$ the number of representations of n as a sum of h-squares of positive odd integers:

$$\mathcal{N}_h(n)=\left|\left\{(x_1,x_2,\ldots,x_h)\in\mathbb{N}^h \mid \sum_{l=1}^{h} x_l^2=n,\ x_l\equiv 1 \bmod 2,\ 1\leq l\leq h\right\}\right| \tag{4.21}$$

Lemma 4.2.4. For an odd $n \in \mathbb{N} : \mathcal{N}_4(4n)=\sum_{d|n} d$.

The proof of this lemma is rather long and mostly considering sums transformations and variable changing. Therefore, we will only give a short sketch of the proof, which is stated in [4].

Proof. Let be $n,\, x_1,\, x_2,\, x_3,\, x_4 \in \mathbb{N}$ such that $x_1^2+x_2^2+x_3^2+x_4^2=4n$ and n odd. Recall from the Corollary 3.3.4 there exist such x_1, x_2, x_3 and x_4.

Note that

$$4n=\left(x_1^2+x_2^2\right)+\left(x_3^2+x_4^2\right)=r+s. \tag{4.22}$$

is also a sum of two sums of two squares. Since all x_l's are odd, r and s must be congruent to 2 modulo 4. From the equation (4.22), it is clear that the number of solutions $\mathcal{N}_4(4n)$ is then given by

$$\mathcal{N}_4(4n)=\sum_{\substack{(r,s>0):r+s=4n\\ r\equiv s\equiv 2 \bmod 4}} \mathcal{N}_2(r)\mathcal{N}_2(s). \tag{4.23}$$

Next, we are interested how big the number $\mathcal{N}_2(t)$ for $t \in \{r,s\}$ is. Consider that $t/2$ is odd, since $t \equiv 2 \bmod 4$ for $t \in \{r,s\}$. And recall the Theorem 4.1.4 and that all x_l's are odd. Then we can write that

$$\mathcal{N}_2(t)=\frac{1}{4}r_2(t)=d_1(t)-d_3(t). \tag{4.24}$$

Remark 4.2.5. The best way to see that the equation (4.24) holds, is that we do again the whole proof of the Theorem 4.1.4 by setting $n=t=2pg$, meaning that factor 2 appears only once. Then at the end of the proof, considering that we only look for solutions of the equation (4.11) where a and b are both positive, we get the equation above.

From the equation (4.24), we see that for every divisor f of $t/2$ such that $f \equiv 1 \bmod 4$, we count $+1 = (-1)^{\frac{f-1}{2}}$, and for every divisor f of $t/2$ such that $f \equiv 3 \bmod 4$, we count $-1 = (-1)^{\frac{f-1}{2}}$. So we can rewrite the equation (4.24)

$$\mathcal{N}_2(t) = \sum_{\substack{(a,b>0)\\ t=2ab}} (-1)^{\frac{a-1}{2}} = \sum_{\substack{(a,b>0)\\ t=2ab}} (-1)^{\frac{1-a}{2}}, \tag{4.25}$$

and the equations (4.23) becomes

$$\mathcal{N}_4(4n) = \sum_{\substack{(a,b,c,d>0) \text{ odd}\\ 4n=2ab+2cd}} (-1)^{\frac{a-c}{2}}. \tag{4.26}$$

Now consider the change of variables.

$$a = x + y,\ c = x - y,\ b = z - t,\ d = z + t, \tag{4.27}$$

with the inverse

$$x = \frac{a+c}{2},\ y = \frac{a-c}{2},\ z = \frac{d+b}{2},\ t = \frac{d-b}{2}. \tag{4.28}$$

Then $4n = 2ab + 2cd = 4(xz - yt) \Rightarrow n = xz - yt$, and the equation (4.26) becomes

$$\mathcal{N}_4(4n) = \sum_{\substack{(x,y,z,t) \text{ such that } n=xz-yt\\ |y|<x, |t|<z, x\not\equiv y \bmod 2, z\not\equiv t \bmod 2}} (-1)^y \tag{4.29}$$

Note that $|y| < x$, $|t| < z$, $x \not\equiv y \bmod 2$ and $z \not\equiv t \bmod 2$ can be shown from the change of variables. So depending on y, we count $+1$ or -1.

Then we can split this sum into three different sums

$$\mathcal{N}_4(4n) = \mathcal{N}_{y<0}(4n) + \mathcal{N}_{y=0}(4n) + \mathcal{N}_{y>0}(4n). \tag{4.30}$$

The equality $\mathcal{N}_{y<0}(4n) = \mathcal{N}_{y>0}(4n)$ can be shown by the change of variables.

$$x' = x, \quad y' = -y \quad z' = z \quad \text{and} \quad t' = -t. \tag{4.31}$$

The equality $\mathcal{N}_{y<0}(4n) = 0$ can also be shown by the change of variables

$$x' = 2v(x,y)z - t \quad y' = -z \quad z' = y \quad \text{and} \quad t' = 2v(x,y)y - x, \tag{4.32}$$

where $v(x, y)$ is the unique positive integer v such that

$$2v - 1 < \frac{x}{y} < 2v + 1. \tag{4.33}$$

The proofs that those two changes of variables give those results are exactly shown in [4]. So we have that

$$\mathcal{N}_4(4n) = 0 + \mathcal{N}_{y=0} + 0 = \mathcal{N}_{y=0}. \tag{4.34}$$

Note once more that $n = xz - yt$, $|t| < z$ and $z \not\equiv t \bmod 2$ and that all counted results are only with $y = 0$. Then

$$\mathcal{N}_{y=0} = |\{(x,\, 0,\, z,\, t) \mid n = xz,\ |t| < z,\ z \not\equiv t \bmod 2\}| \tag{4.35}$$

Since $n = xz$ is odd, z must be odd too. And for such fixed z, we can find z different values t such that $|t| < z$, where $z \not\equiv t \bmod 2$. So for all such z, there iare

$$\mathcal{N}_4(4n) = \mathcal{N}_{y=0} = \sum_{z|n} z \tag{4.36}$$

different possible solutions. And this proves the lemma.

□

Theorem 4.2.6. Let be $n \in \mathbb{N}$ a positive integer and $n = 2^r m$, where r, $m \in \mathbb{N}$ and m an odd integer. Then $r_4(n) = 3^e 8 \sum_{d|m} d$, where $e = (n+1) \bmod 2$.

Proof. First we will prove this this theorem for n odd, i.e. $n = m$ and $r_4(n) = 8 \sum_{d|m} d$, since $e = (n+1) \bmod 2 = 0$.

Claim 4.2.7. For n odd, we have $r_4(4m) = 16\mathcal{N}(4m) + r_4(m)$

Remember that we have already shown, if $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4m$, that either all x_l's are even or odd.

First assume that all x_l's are even. Then the change of variables $y_l = \frac{x_l}{2}$ for all $l \in \{1, \ldots, 4\}$ provide a bijection between the sets of solutions of $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4m$ and solutions of $y_1^2 + y_2^2 + y_3^2 + y_4^2 = m$. This means that there are $r_4(m)$ solutions in $r_4(4m)$, where all x_l's are even.

And now assume that all x_l's are odd. Recall that all counted solutions in $\mathcal{N}(4m)$ are tuples, where all x_l's are positive and odd. For each such tuple, we can create $2^4 = 16$ different tuples by signs changing that are all counted in $r_4(m)$. This means that there are $16\mathcal{N}(4m)$ solutions in $r_4(4m)$, where all x_l's are even.

So there are $r_4(4m) = 16\mathcal{N}(4m) + r_4(m)$ solutions altogether. And this proves the claim.

Using the claim above, we can compute

$$\begin{aligned} 3r_4(m) &= r_4(2m) && \text{(by Lemma 4.2.2)} \\ &= r_4(4m) && \text{(by Lemma 4.2.1)} \\ &= 16\mathcal{N}(4m) + r_4(m) && \text{(by the above claim)} \\ &= 16\left(\textstyle\sum_{d|m} d\right) + r_4(m) && \text{(by Theorem 4.2.6)} \end{aligned}$$

And this shows that for odd n, i.e. $n = m$, the following holds.

$$2r_4(m) = 16 \sum_{d|m} d \quad \Rightarrow \quad r_4(m) = 8 \sum_{d|m} d. \tag{4.37}$$

Now assume that n is a even number, i.e. $n = 2^r m$, with $r > 0$. Then we can write $r_4(n) = r_4(2^r m) = r_4(2^{r-1} m)$ for all $r > 1$, which we know from the Lemma 4.2.1. This means that for any even n, $r_4(n) = r_4(2^r m) = r_4(2^{r-1} m) = \ldots = r_4(2^2 m) = r_4(2m)$, and from Lemma 4.2.2, we know that $r_4(2m) = 3r_4(m)$, for m odd.

So all this together gives us that for any n even, there are

$$r_4(n) = r_4(2m) = 3r_4(m) = 3 \cdot 8 \sum_{d|m} d \tag{4.38}$$

solutions.

As we can see that for every n odd there are $r_4(n) = r_4(m) = 8 \sum_{d|m} d$ solutions and for n even there are $r_4(n) = r_4(2^r m) = 3 \cdot 8 \sum_{d|m} d$ solutions, which proves the theorem. □

Chapter 5

Constructions algorithms

In this chapter, we will present two random probabilistic algorithms stated in [3], where both work in polynomial time.

In the first section, we will see an algorithm that computes a two square presentation for an odd prime p, where $p \equiv 1 \bmod 4$, in $\mathcal{O}(\log_2 p)$ steps.

In the second section, we will see an algorithm that computes a four square presentation for any natural number $M \in \mathbb{N}$ in $\mathcal{O}(\log_2 p)$ steps.

5.1 Primes as sums of two squares

In this section, we will describe a random probabilistic algorithm published by Michael O. Rabin and Jeffery O. Shallit in [3]. In this paper, they have presented an algorithm that computes a two square presentation for an odd prime p in polynomial time, where $p \equiv 1 \bmod 4$.

Recall the Fermat-Lagrange Theorem 2.2.1 which states that every prime $p \equiv 1 \bmod 4$ is a sum of two squares. From this follows that $x^2 + 1$ has a solution in $\mathbb{Z}_p$. And this implies that there exits an integer $u < 1/2p$ such that $u^2 + 1 \equiv 0 \bmod p$.

Let be u_1 and $u_2 = p - u_1$ two roots of the polynomial $x^2 + 1 = 0$ in $\mathbb{Z}_p$. Note that $u_1 \neq u_2$ since p is an odd prime. Then for any residue $0 \leq b < p$ consider the polynomial

$$f_b(x) = (x - b)^2 + 1 = x^2 - 2xb + b^2 + 1, \tag{5.1}$$

where $u_1 + b$ and $u_2 + b$ are roots of $f_b(x)$.

Then consider the equation $x^k - 1 = 0$ with $k = (p - 1)/2$. The equation $x^k - 1 = 0$ is satisfied by exactly k quadratic residues in $\mathbb{Z}_p$. So if we have b such that, for example $u_1 + b$ is a quadratic residue and $u_2 + b$ is not, then we can compute

$$\gcd\Big(f_b(x) + 1, x^k - 1\Big) = x - u_1 - b. \tag{5.2}$$

So, if we find such b, where $u_1 + b$ is a quadratic residue and $u_2 + b$ is not, we can compute u_1 from the equation (5.2).

But for this algorithm to be efficient, we should be able to find such b and to compute the greatest common divisor (5.2) in some reasonable time. First, we will show that we can compute the equation (5.2) in polynomial time.

Let be $k = 2^{d_1} + \ldots + 2^{d_m}$ binary representation of k, where $d_1 < \ldots < d_m \leq \log_2 p$ and $m \leq \log_2 p$. And let be $r_i = 2^{d_i}$ for $1 \leq i \leq m$. Then we can write every x^{r_i} by computing the sequence

$$g_1 \equiv x^2 \bmod f_b(x), \quad g_2 \equiv g_1^2 \bmod f_b(x), \ldots, g_{d_m} \equiv g_{d_m - 1}^2 \bmod f_b(x). \tag{5.3}$$

Note that each $g_j(x)$ is a linear polynomial of the form $cx + e$, where $c, e \in \mathbb{Z}_p$ and $1 \leq j \leq d_m$.

So computing g_{j+1} from g_j requires a fixed number of operations. And computing all powers $x^{r_i} \bmod f_b(x)$ for all $1 \leq i \leq \log_2 p$ requires $\mathcal{O}(\log_2 p)$ steps. Now we only have to do m multiplications $\bmod f_b(x)$ of linear polynomials to compute

$$h(x) = x^k = \prod_i x^{r_i}. \tag{5.4}$$

Once we have presented x^k as such a product in $h(x)$, we see that we need only a fixed number of operations to compute the greatest common divisor (5.2), since

$$\gcd\Big(f_b(x), x^k - 1\Big) = \gcd\left(f_b(x), h(x) - 1\right)$$

.

In the next part, we will show that by randomly choosing an element from $\mathbb{Z}_p$, we have high probability to find an integer $b \in \mathbb{Z}_p$ such that $u_1 + b$ or $u_2 + b$ is a quadratic residue and another is not, i.e. equation (5.2) holds.

Definition 5.1.1. We say that $a_1, a_2 \in \mathbb{Z}_p$, where a_1, $a_2 \neq 0$, are of a different type if one of them is a quadratic residue and another is not.

Remark 5.1.2. Recall, if an element $a \in \mathbb{Z}_p$ is a quadratic residue then, $a^{(p-1)/2} \equiv 1 \bmod p$. Otherwise $a^{(p-1)/2} \equiv -1 \bmod p$. This means that two elements $a_1, a_2 \in \mathbb{Z}_p$ are of a different type if $a_1^{(p-1)/2} \not\equiv a_2^{(p-1)/2} \bmod p$.

Theorem 5.1.3. Let be $a_1, a_2 \in \mathbb{Z}_p$, $a_1 \neq a_2$. Then

$$|\{b | b \in \mathbb{Z}_p, a_1 + b \text{ and } a_2 + b \text{ are of a different type}\}| = 1/2(p-1) \tag{5.5}$$

This theorem is stated for any arbitrary finite field and is mostly used for solving equations in any finite field. In our case, this theorem states that for $u_1, u_2 \in \mathbb{Z}_p$, where $u_1 \neq u_2$, there are about half elements b in $\mathbb{Z}_p$ such that $u_1 + b$ and $u_2 + b$ are of a different type. And we have about fifty percent chance of choosing such b.

The proof of this theorem is stated in [6] and it can be seen in Appendix D.

Now we can present a random probabilistic algorithm for solving the equation $x^2 + 1 = 0$ in $\mathbb{Z}_p$.

First choose randomly $b \in \mathbb{Z}_p$ and compute $\gcd\big((x-b)^2, b^k - 1\big)$. By the Theorem 5.1.3, we will need about two tries on average to find an integer $b \in \mathbb{Z}_p$ such that $u_1 + b$ and $u_2 + b$ are of a different type. Without loss of generality, we can say that u_1 is a solution we are looking for. Then we can compute the solution u_1, where $u_1^2 + 1 = 0 \bmod p$. Recall that we can compute this solution in $\mathcal{O}(\log_2 p)$ steps.

Since we found u_1 such that $u_1^2 + 1 = 0 \bmod p$, we can write $u_1^2 + 1 = mp$ for some $m \in \mathbb{N}$, where $1 \leq m < p$.

If $m = 1$, we can write $p = u_1^2 + 1^2$ and we are done. But in general, there is a small probability that this happens, and we will mostly have the case where $u_1^2 + 1 = mp$ and $1 < m < p$.

Recall the theory of Gaussian integers from Chapter 2. The norm of a Gaussian integer $\alpha = a_1 + a_2 i$ is defined as $N(\alpha) = \alpha\overline{\alpha} = a_1^2 + a_2^2$. And by the Theorem 2.1.13, if $\alpha \notin \mathbb{Z}$, there exists a unique factorization of α.

So assume that $u_1^2 + 1 = mp$ and $1 < m < p$. Then we can construct two Gaussian integers $\alpha_1 = u_1 + i$ and $\alpha_2 = p + 0i$, where $N(\alpha_1) = u_1^2 + 1 = mp$ and $N(\alpha_2) = p^2$. By the Theorem 2.1.13, there exists a divisor π of α_1 such that $N(\pi) = p$. And since $\alpha_2 = \pi\overline{\pi}$, α_1 and α_2 have a common divisor π.

This means that now, we can compute $\pi = p_1 + p_2 i = \gcd(u_1 + i, p)$ such that $N(\pi) = p_1^2 + p_2^2 = p$. Note that computing gcd in Gaussian integers is a common Euclidean

algorithm, so we need $\mathcal{O}\left(\log_2(p^2)\right) = \mathcal{O}\left(\log_2(p)\right)$ steps to compute. And we have two square presentation of an odd prime p, where $p \equiv 1 \bmod 4$.

From the whole discussion above follows the next theorem.

Theorem 5.1.4. For a prime $p = 4k + 1$, we can find the representation of $p = x^2 + y^2$ by an $\mathcal{O}(\log p)$ expected number of arithmetical operations with integers smaller than p.

5.2 Sums of four squares through integral quaternions

In this section, we will discuss a random probabilistic algorithm that computes four square presentation for any positive integer $M \in \mathbb{N}$ in polynomial time. This algorithm was presented by Michael O. Rabin and Jeffery O. Shallit in [3].

Note that the algorithm presented here is for finding a four square presentation for any positive integer M. But in this thesis, we are mainly interested in finding factors of a positive integer n that is a product of two odd primes, i.e. $n = q_1 q_2$ is an odd integer, where q_1 and q_2 are odd primes. Therefore the algorithms used for factoring are variation of algorithm presented below.

Let be $M \in \mathbb{N}$ a positive integer. First, we are going to write an outline of algorithm how to compute a four square presentation of integer M.

1. First, write $M = 2^e n$ where n odd. Then we can easily obtain a four square presentation for 2^e.

   Now we only have to find a four square presentation for n.

2. We are looking for a,b such that $a^2 + b^2 \equiv -1 \bmod n$.

3. Replace a (respectively b) by $n - a$ (respectively $n - b$) if necessary to ensure that $a, b < \frac{1}{2}n$. Then construct quaternion $\alpha = a + bi + j$ and compute $\delta = \operatorname{gcrd}(\alpha, n)$ in $\mathbb{H}$.

4. If $N(\delta) = n$, then any associate of δ is a four square presentation for n. Otherwise, $N(\delta) = fn$, where $f|n$, i.e. we have found a divisor of n. Apply the algorithm recursively to f and n/f to obtain a four square presentation.

5. Multiply all computed quaternions and we obtain the quaternion presentation η, where $N(\eta) = n$, i.e. we have four square presentation for n.

Now we want to show that this algorithm is correct and can be made to run in polynomial time.

Consider the outline of this algorithm listed above and let be $M \in \mathbb{N}$ a positive integer for which we want to find a four square presentation.

First, we compute the values e and n such that $M = 2^e n$ and n is odd. Note that we can find those elements fast. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we can present 2 as a sum of four squares. Recall Euler's identity which states that a product of two sums of four squares is again a sum of four squares. Using Euler's identity, we can easily obtain a four square presentation for 2^e.

Now we have to find a four square presentation for n and we come to the second point of this algorithm.

Theorem 5.2.1. Suppose that n is odd and $\gcd(f, n) = 1$. Then we can find a solution to $x^2 + y^2 \equiv f \bmod n$ in a random polynomial time.

Proof. Choose w, $z \in \mathbb{Z}_n$ at random. Let be $w^2 + z^2 = r$. Then

$$\left(x^2 + y^2\right)\left(w^2 + z^2\right) \equiv fr \bmod n \tag{5.6}$$

where x and y are the values we want to find. Now we will claim that $fr \bmod n$ will essentially be "randomly" distributed mod n. So there will be "frequently" a number $fr \equiv p^a \bmod n$ with $p^a \equiv 1 \bmod 4$ odd prime and $a \in \mathbb{N}$ for which we can quickly find a two square representation.

So we can write $p^a = u^2 + v^2$. From equation (5.6) we get

$$\left(x^2 + y^2\right)\left(w^2 + z^2\right) \equiv u^2 + v^2 \bmod n. \tag{5.7}$$

Then we can compute x and y as follows:

$$\begin{aligned} x &\equiv (uw + vz)\left(w^2 + z^2\right)^{-1} \\ y &\equiv (vw - uz)\left(w^2 + z^2\right)^{-1} \end{aligned} \tag{5.8}$$

□

Recall that we are looking for x and y such that $x^2 + y^2 \equiv -1 \bmod n$. This means that f from this proof is equal to -1. And by choosing w and z randomly such that $w^2 + z^2 = r$, we hope that $\left(x^2 + y^2\right)\left(w^2 + z^2\right) \equiv fr \equiv -r \bmod n$ is the value we can present as a sum of two squares, i.e. that $n - r$ is of the form we look for.

So in this proof, we have claimed that finding such $fr \bmod n$ will essentially be randomly distributed by choosing w and z randomly. But first, note that by equations (5.8), the sum $w^2 + z^2 = r$ has to be invertible, so that we can compute the wanted values x and y.

Lemma 5.2.2. Let $n = \prod_{l=1}^{h} p_l^{e_l}$, n odd. Let D be a relatively prime to n. Then the number of distinct pairs $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$ that satisfy

$$x^2 - Dy^2 \equiv a \bmod n \tag{5.9}$$

for $a \in \mathbb{Z}_n^*$ is

$$\prod_{l=1}^{k} p_l^{e_l - 1}\left(p_l - \left(\frac{D}{p_l}\right)\right) \tag{5.10}$$

where $\left(\frac{D}{p}\right)$ is the Legendre symbol.

Proof. First we show the result in the case where $n = p$, p is an odd prime.
Let be X an indeterminate. Consider the ring

$$R = \mathbb{Z}[X] / \left(X^2 - D, p\right). \tag{5.11}$$

The form $x + y\sqrt{D}$ is a representation of elements in R, where $x, y \in \mathbb{Z}_p$. Now we will denote with R^* the set of elements of R, where $x^2 - Dy^2 \not\equiv 0 \bmod p$. Then we define the map $N : R^* \to \mathbb{Z}_p^*$ by

$$N(x + y\sqrt{D}) = x^2 - Dy^2. \tag{5.12}$$

Consider that for any $a, b \in R^*$, where $a = x_1 + y_1\sqrt{D}$ and $b = x_2 + y_2\sqrt{D}$. Then

$$\begin{aligned} N(ab) = N(\left(x_1 + y_1\sqrt{D}\right)\left(x_2 + y_2\sqrt{D}\right)) = \\ = N(x_1x_2 + x_1y_2\sqrt{D} + x_2y_1\sqrt{D} + y_1y_2D) = \\ = N(x_1x_2 + y_1y_2D + (x_1y_2 + x_2y_1)\sqrt{D}) = \\ = (x_1x_2 + y_1y_2D)^2 - (x_1y_2 + x_2y_1)^2 D = \\ = x_1^2x_2^2 + 2x_1^2x_2^2y_1^2y_2^2D + y_1^2y_2^2D^2 - x_1^2y_2^2D - 2x_1^2x_2^2y_1^2y_2^2D - x_2y_1D = \\ = x_1^2x_2^2 + y_1^2y_2^2D^2 - x_1^2y_2^2D - x_2y_1D = \\ = \left(x_1^2 - y_1^2D\right)\left(x_2^2 - y_2^2D\right) = \\ = N(\left(x_1 + y_1\sqrt{D}\right))N(\left(x_2 + y_2\sqrt{D}\right)) = N(a)N(b) \end{aligned} \tag{5.13}$$

So from equation (5.13), we see that N is multiplicative. Now we also see that N is a group homomorphism and that N maps R^* into $\mathbb{Z}_p^*$. Therefore, $x^2 - y^2 D$ takes on each value of $\mathbb{Z}_p^*$ equally often.

Next, we want to see the structure of R^*. If $X^2 - D$ is irreducible modulo p, this means $\left(\frac{D}{p}\right) = -1$, then R^* is isomorphic to F_{p^2}. So we have $|R^*| = p^2 - 1$ and then there are $\left(p^2 - 1\right) / (p - 1) = p + 1$ solutions for each a in the equation (5.9).

And if $X^2 - D$ is reducible, then R^* is isomorphic to $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$. This means that we have $|R^*| = (p-1)^2$ and so there are $(p-1)^2 / (p-1) = p - 1$ solutions for each a in the equation (5.9). Consider that for $X^2 - D$ reducible and while D is a relative prime to p, then we have that $\left(\frac{D}{p}\right) = 1$.

This shows that the Lemma 5.2.2 holds for each $n = p$. Now using Hensel lifting[1], we can show that for each solution mod p^k, there are p solutions mod p^{k+1}. And finally, by using the Chinese remainder theorem, it shows that Lemma 5.2.2 holds for each odd n. □

The next corollary will give us the probabilistic chance to find such a pair (w, z).

Corollary 5.2.3. If w and z are chosen randomly from $\mathbb{Z}_n$, then $w^2 + z^2$ is invertible mod n with the probability at least $\varphi(n)^2/n^2 > 1/\left(5 \log\log n\right)^2$.

For the proof of this Corollary 5.2.3 we will use an estimate of Rosser and Schönfeld shown in [7] which we will not present it in this proof.

Proof. Use the Lemma 5.2.2 with $D = -1$, (i.e. we are mapping $x + y\sqrt{-1}$ to $x^2 + y^2$). Then from (5.10), we get that there are

$$\prod_{i=1}^{k} p_i^{e_i - 1} (p_i - 1) \tag{5.14}$$

solutions for each $a \in \mathbb{Z}_n^*$ such that $w^2 + zr \equiv \bmod n$. And there is a total of

$$\varphi(n) \prod_{i=1}^{k} p_i^{e_i - 1} (p_i - 1) = \varphi(n)^2 \tag{5.15}$$

solutions. Using the estimate of Rosser and Schönfeld shown in [7], the last inequality follows. □

The last Corollary 5.2.3 shows that we need at most $\left(5 \log\log n\right)^2$ pairs (w, z) to try on average until we find a pair (w, z) where $w^2 + z^2$ is invertible mod n. And since $w^2 + z^2$ is a random element, $fr \bmod n$ will also be a random element from $\mathbb{Z}_n^*$.

To complete the proof of Theorem 5.2.1, i.e. that we can find x and y such that $x^2 + y^2 \equiv -1 \bmod n$, we still have to show that we can find a random element $fr \in \mathbb{Z}_n^*$, which is also a prime power $p^a \equiv 1 \bmod 4$.

Lemma 5.2.4. Let be

$$B_n = \{1 \leqq y \leqq n : y = p^a, p \text{ prime}, y \equiv 1 \bmod 4, \text{ and } \gcd(y, n) = 1\} \tag{5.16}$$

and let $A(n) = |B_n|$, the number of elements in B_n.
Then

$$A(n) > \frac{1}{10} \frac{n}{\log n} \quad \forall n \geqq 2. \tag{5.17}$$

To prove this lemma, we will use some results of Livingston presented in [8].

[1] The exact lemma and discussion of Hensel lifting can be looked up in [13].

Proof. Let be

$$\psi(x;k,l) = \sum_{\substack{p^a \le x \\ p \text{ prime} \\ p^a \equiv l \bmod k}} \log p \tag{5.18}$$

Livingston showed in [8] that

$$\psi(n;4,1) > \frac{2n}{5} \quad \forall n \ge 37 \tag{5.19}$$

So it follows that for all $n \ge 37$, there are at least

$$\frac{2}{5}\frac{n}{\log n} \tag{5.20}$$

terms in the sum (5.18), i.e. prime powers $p^a \le n$ with $p^a \equiv 1 \bmod 4$. Since there are at most $\log_2 n$ prime smaller or equal n which are not relatively prime to n, we see that

$$A(n) > \frac{2}{5}\frac{n}{\log n} - \log n. \tag{5.21}$$

Now it can be easily verified that

$$\frac{2}{5}\frac{n}{\log n} - \log n > \frac{2}{10}\frac{n}{\log n} \quad \forall n \ge 104, \tag{5.22}$$

and by explicit computation that

$$A(n) > \frac{2}{10}\frac{n}{\log n} \quad \text{for } 2 \le n \le 103. \tag{5.23}$$

This implies that by choosing w and z randomly, we will find an integer $fr \bmod n$ of the required form, with a probability of at least 1 in $10 \log_2 n$. And this completes the proof for the Theorem 5.2.1. □

So now, we come to the third step of this algorithm. We have to show that we can compute the right greatest common divisor in $\mathcal{H}$ in polynomial time.

The existence of such a common divisor is basically shown in Propositions 3.4.5 and 3.2.23. Therefore, we will only present the algorithm that computes g.c.r.d. in polynomial time.

Lemma 5.2.5 (Euclidean Algorithm for $\mathcal{H}$)**.** Given $\alpha, \beta \in \mathcal{H}$, we can find a greatest common right divisor δ in time, which is polynomial in $2\log_2 \min\{N(\alpha), N(\beta)\}$.

Proof. Recall the Proposition 3.4.5. Before we compute the greatest common right divisor, we have to find the quaternion $\gamma\tau \in \mathcal{H}$ such that $\alpha = \beta\gamma + \tau$. So to compute such γ that is in $\mathcal{H}$, we will need the following algorithm that returns us the quaternions that are Hurwitz integers:

function Nearest-Integral-Quaternion(α)
  for $n := 1$ **to 4 do** $h_n := \frac{1}{2}\lfloor 2a_n + 1 \rfloor$
  for $n := 1$ **to 4 do**
    if $a_n \ge h_n$ **then** $r_n := h_n + \frac{1}{2}$
      else $r_n := h_n - \frac{1}{2}$
  if $N(\alpha - \chi) \le N(\alpha - \rho)$ **then return**(χ)
  else return(ρ)

And then we can compute the g.c.r.d. using usual Euclidean algorithm.

function gcrd(α, β)
while $\beta \neq 0$ **do begin**
  $\gamma =$ Nearest-Integral-Quaternion($\beta^{-1}\alpha$)
  $\tau = \alpha - \beta\gamma$
  $\alpha = \beta$
  $\beta = \tau$
  end
return(α)

It is clear that this algorithm returns the greatest common right divisor of α and β. Note that the norm of β is reduced by at least a half in every loop, since $N(\beta) \leq \frac{1}{2}N(\tau)$. So this means, that we need at most $2\log_2 \min\{N(\alpha), N(\gamma)\}$ steps for rest to vanish and finish the algorithm. □

Since all computations have been done in $\mathcal{H}$, the greatest common right divisor δ is also a Hurwitz integer, meaning that its coordinates do not have to be integers. Anyway, the next lemma shows that every Hurwitz integer with half integer coefficients has a left (resp. right) associate that has all integer coefficients.

From the presented algorithms, we see that we can compute the greatest common right divisor $\delta \in \mathcal{L}$ in polynomial time.

Now we will summarize the points 1 to 3 of this algorithm. Recall that we start with an integer M that we present in the form $M = 2^e n$ with n odd. By taking a quaternion $\pi = 1 + i$, where $N(\pi) = 2$ we can construct the quaternion $\varphi = \pi^e$, where $N(\varphi) = 2^e$. Then we compute a and b such that $a^2 + b^2 \equiv -1 \bmod n$ by choosing the pair of integers $w, z \in \mathbb{Z}_n$ such that $w^2 + z^2 = r$ is invertible and $-r \bmod n$ is a prime power, where $p^a \equiv 1 \bmod 4$. Afterwards, we find two square presentation for this prime power. Recall that we need about $(5\log\log n)^2$ tries on average to find such an invertible r and about $10\log_2 n$ tries that $-r \bmod n$ is a prime power, i.e. we need $(5\log\log n)^2\, 10\log_2 n = 250\,(\log_2\log_2 n)^2 \log_2 n$ tries to find such a sum $w^2 + z^2$. And then to compute the two square presentation of the prime power $p^a \equiv -r \bmod n$ we need $\mathcal{O}(\log_2 p)$ steps as we saw it in the previous section.

Now we can construct the equation $a^2 + b^2 + 1 \equiv 0 \bmod n$, where $a^2 + b^2 + 1 = fn$ for some $f \in \mathbb{Z}_n$. If $f = 1$, then $a^2 + b^2 + 1 = n$ and we are done. So assume that $f \neq 1$, then we can construct a quaternion $\alpha = a + bi + j$ with $N(\alpha) = a^2 + b^2 + 1 = fn$. Note that $n|N(\alpha)$ and $N(\alpha) < n^2$. Consider another quaternion $\beta = n + 0i + 0j + 0k$ with $N(\beta) = n^2$. From Lemma 3.2.25 we see that $\mathrm{gcrd}(\alpha, n) \neq 1$, since $\mathrm{gcrd}(N(\alpha), n) \neq 1$. So we can compute the greatest common divisor $\delta = \mathrm{gcrd}\,(\alpha, \beta)$ in polynomial time with $2\log_2 \min\{N(\alpha), N(\beta)\} = 2\log_2(fn)$ steps.

Now we come to the last two points 4 and 5 of this algorithm, where we have computed the greatest common right divisor δ. Since $N(\delta)|N(\alpha)$ and $N(\delta)|n^2$, it means that $N(\delta) \in \{n, fn\}$. If $N(\delta) = n$, then $N(\delta)$ is a four square presentation of n and we are done. But if $N(\delta) = fn$, then consider that $f|n$, since $N(\delta) = fn|n^2$, i.e. we have a non-trivial factor $f = fn/n$ of n. In this case, we just repeat the algorithm for all factors until we do not have constructed Lipschitz quaternions for each factor with the norm of the factor.

At the end, we multiply all constructed quaternions and get the wanted quaternion η such that $N(\eta) = M$, where $N(\eta)$ is a four square presentation of M.

So now we have presented one algorithm for computing a four square presentation for a positive integer $M \in \mathbb{N}$, where all computations are done in polynomial time.

Chapter 6

Factorization algorithm

In this chapter, we will present the factorization algorithm and the theory around it. The main idea of the factorization algorithm was to use the non-commutative property of quaternions to create a sequence of new quaternions that would hopefully give us a pair of quaternions that will have a non-trivial common right (resp. left) divisor. Unfortunately, the length of the created sequence is growing proportionally with the size of the smallest factor.

In the first section, we will present the theory we use to describe the property of such sequences of quaternions. In this part, we will only concentrate on the sequences that are created by non-commutative property of prime quaternion α_0 with another prime quaternion π.

In the second section, we will see the property of those sequences, only this time we will take a look at sequences where α_0 is not a prime quaternion. And we will analyze how the factors of α_0 are changing. At the end of this section, we will give some interesting results according to the sequences of α_0 by choosing specific quaternion π.

And in the last section, we will present the factorization algorithm using the theory from the first two sections. And we will also discuss the complexity of the given algorithm.

First, we will give some definitions and notations we will need in all three parts. Let be $\alpha_0 \in \mathcal{L}$ a randomly chosen proper quaternion of an odd norm $n \in \mathbb{N}$, where n is the integer that we would like to factor. In this theory, we will consider only quaternions α_0 which are odd and proper, since even integers are divisible by 2 and if all coefficients has the same divisor, then we have already found a factor. And Let be $\pi \in \mathcal{L}$ a prime quaternion such that $\alpha_0\pi$ (resp. $\pi\alpha_0$) is proper. Then we can define the following operation:

Definition 6.0.6. Let be $\alpha_0, \pi \in \mathcal{L}\backslash\{0\}$ two Lipschitz integers, where α_0 has an odd norm. Then we say for the following computation

$$\alpha_1 = \operatorname{gcrd}(\alpha_0\pi,\, N(\alpha_0))\,, \tag{6.1}$$

we say, we *commutate* α_0 *with* π *from right*. The definition of *commutating* α_0 *with* π *from left* corresponds to the definition above, i.e.

$$\alpha_1 = \operatorname{gcld}(\pi\alpha_0,\, N(\alpha_0))\,. \tag{6.2}$$

Recall that we proved in Theorem 3.2.23 that such greatest common right (resp. left) divisor α_1 exists. And since $\alpha_0\pi$ (resp. $\pi\alpha_0$) is proper quaternion, quaternion α_1 has to be unique up to eight left-associates (resp. right-associates).

Lemma 6.0.7. Let be $\alpha_l \in \mathcal{L}$ a proper quaternion, $\pi \in \mathcal{L}$ a prime quaternion such that the product $\alpha_l\pi$ is proper too, and $\alpha_{l+1} = \operatorname{gcrd}(\alpha_l\pi, N(\alpha_l))$. Then for any quaternion $\alpha^{(l)} \in \mathfrak{D}\mathfrak{L}_{\alpha_l}$ the new quaternion $\alpha^{(l+1)} = \operatorname{gcrd}\left(\alpha^{(l)}\pi, N(\alpha_l)\right)$ is a left-associate to α_{l+1}.

Analogically, $\alpha^{(l+1)} = \operatorname{gcld}\left(\pi\alpha^{(l)}, N(\alpha_l)\right)$ and $\alpha_{l+1} = \operatorname{gcld}(\pi\alpha_l, N(\alpha_l))$ are right-associates, where $\alpha^{(l)} \in \mathfrak{D}\mathfrak{R}_{\alpha_l}$.

Proof. Consider that the quaternion α_{l+1} is one of eight right divisors in $\mathfrak{D}\mathfrak{L}_{\alpha_{l+1}}$ of the norm $N(\alpha_{l+1})$ which divides the product $\alpha_l\pi$. Then the product $\alpha^{(l)}\pi$ can be written as:

$$\alpha^{(l)}\pi = \varepsilon\alpha_l\pi = \varepsilon\left(\alpha_l\pi\right) = \varepsilon\left(\tilde{\pi}\alpha_{l+1}\right) = \varepsilon\tilde{\pi}\alpha_{l+1},$$

where ε is a unit such that $\varepsilon\alpha_l = \alpha^{(l)}$. Recall such ε exists since $\alpha^{(l)} \in \mathfrak{D}\mathfrak{L}_{\alpha_l}$.

By the Theorem 3.2.12, we see that there are eight right divisors in the set $\mathfrak{D}\mathfrak{L}_{\alpha_{l+1}}$ of the norm $N(\alpha_{l+1})$ which divides the product $\alpha^{(l)}\pi$. Meaning $\alpha^{(l+1)} = \operatorname{gcrd}\left(\alpha^{(l)}\pi, N(\alpha_l)\right)$ is a left-associate to α_{l+1}.

Analogically, $\alpha^{(l+1)} = \operatorname{gcld}\left(\pi\alpha^{(l)}, N(\alpha_l)\right)$ and $\alpha_{l+1} = \operatorname{gcld}\left(\pi\alpha_l, N(\alpha_l)\right)$ are right-associates, where $\alpha^{(l)} \in \mathfrak{D}\mathfrak{R}_{\alpha_l}$. □

In particular this lemma shows that any left-associate of $\alpha_{l+1} = \operatorname{gcrd}\left(\alpha_l\pi, N(\alpha_l)\right)$ is also the right divisor of the product $\varepsilon\alpha_l\pi$ of the norm $N(\alpha_{l+1})$, where ε is any unit.

Since the theory about arithmetics of commutating α_0 with π from right is equivalent to the one of commutating α_0 with π from left, we will concentrate only on the arithmetics of commutating α_0 with π from right. And therefore, we will say in short that we commutate α_0 with π.

And now consider the following notations we will use in all three sections below. Recall Definition 6.0.6 and Lemma 6.0.7, and consider the sequence $\alpha^{(0)}$, $\alpha^{(1)}, \ldots,$ $\alpha^{(l)}$, $\alpha^{(l+1)} \ldots$, where $\alpha^{(l)} \in \mathfrak{D}\mathfrak{L}_{\alpha_l}$ is any left-associate to α_l and $\alpha^{(l+1)} = \operatorname{gcrd}\left(\alpha^{(l)}\pi,\, N(\alpha_0)\right) \in \mathfrak{D}\mathfrak{L}_{\alpha_{l+1}}$ for all $l \in \mathbb{N}$. This means that for a fixed Lipschitz integers α_l for any $l \in \mathbb{N}$, we write the product

$$\alpha^{(l)}\pi = \pi^{(l+1)}\alpha^{(l+1)}, \tag{6.3}$$

where $\alpha^{(l)}$ is any left-associate of α_l, i.e. $\alpha^{(l)} \in \mathfrak{D}\mathfrak{L}_{\alpha_l}$, and $\alpha^{(l+1)}$ one of eight right divisors of $\alpha^{(l)}\pi$ with a norm equal to $N(\alpha^{(l)})$. The prime quaternion $\pi^{(l+1)}$ corresponds to prime quaternion with $N(\pi) = N(\pi^{(l+1)})$, such that the equation (6.3) holds. Note that this notation holds from the theory in Section 3.2.

Remark 6.0.8. In this chapter, we will concentrate only on the theory of commuting a odd and proper quaternion α_0 with π, where π is a prime quaternion and $\alpha_0\pi$ is proper. Actually, the following theory holds also for π not prime quaternion. But for the sake of this thesis, we will only discuss the theory where π is a prime, since otherwise we would have much more things to consider.

6.1 Commutation of two prime quaternions

In this section, we will take a closer look at commutating $\alpha^{(0)}$ with π, where $\alpha^{(0)} \in \mathcal{L}$ is an odd prime with $N(\alpha^{(0)}) = q$ and $\pi \in \mathcal{L}$ is any prime with $N(\pi) = p$. And then we will discuss some experimental results that are relevant for the factorization algorithm in the last section. Note that since $\alpha^{(0)}$ and π are prime quaternions, q and p must be prime integers by Corollary 3.3.3.

In the first lemma, we want to show what happens if $N(\alpha^{(0)}) = q = p = N(\pi)$.

Lemma 6.1.1. Let be $\alpha^{(0)}$, π, $\pi^{(1)}$, $\alpha^{(1)} \in \mathcal{L}$ with the same norm equal to q such that $\alpha^{(0)}\pi = \pi^{(1)}\alpha^{(1)}$ and $\alpha^{(0)}\pi$ is proper $\bmod q$. Then $\alpha^{(0)}$ and $\pi^{(1)}$ are right-associated and π and $\alpha^{(1)}$ left-associated.

Proof. From the Theorem 3.2.12, the product $\alpha^{(0)}\pi$ has exactly eight right divisors of the norm q, since $q|N(\alpha^{(0)}\pi) = q^2$. But from the equation $\alpha^{(0)}\pi = \pi^{(1)}\alpha^{(1)}$, we can find two sets $\mathfrak{D}\mathfrak{L}_{\pi}$ and $\mathfrak{D}\mathfrak{L}_{\alpha^{(1)}}$, where each has eight elements. Note that each quaternion in those two sets has the norm equal to q. Since there are altogether at most eight right divisors of the norm q, it implies that for every quaternion $\beta \in \mathfrak{D}\mathfrak{L}_{\pi}$, β is also an element in $\mathfrak{D}\mathfrak{L}_{\alpha^{(1)}}$, and so π and $\alpha^{(1)}$ are left-associated. In the same way, we can show that $\alpha^{(0)}$ and π must be right-associated. □

With this lemma, we have only proven the obvious conclusion that by commutating two quaternions $\alpha^{(0)}$ and π with the same norms, we will get $\alpha^{(1)} = \text{gcrd}\left(\alpha^{(0)}\pi,\, N(\alpha^{(0)})\right)$, which is a right-associate of π. Since this case is not interested for us, we will from now on assume that the quaternions $\alpha^{(0)}$ and π have the different norms, meaning that $N(\alpha^{(0)}) = q \neq p = N(\pi)$.

Of course, there is also the case where $\alpha^{(0)}$ and π commute, i.e. $\alpha^{(0)}\pi = \pi\alpha^{(0)}$. This means that $\alpha^{(0)}$ is left and right divisor of $\alpha^{(0)}\pi$, i.e. $\alpha^{(1)} = \alpha^{(0)}$. This is of no interest for us, either.

Lemma 6.1.2. For any prime quaternion $\alpha^{(0)} \in \mathcal{L}$, there exists a prime quaternion $\pi \in \mathcal{L}$ such that $\alpha^{(0)}$ and π do not commute.

Proof. In general, quaternion algebra is not commutative, but we will give a small arithmetic proof that this lemma holds.

Recall Proposition 3.3.5, since $\alpha^{(0)} = a_1^{(0)} + a_2^{(0)}i + a_3^{(0)}j + a_4^{(0)}k$ is a prime quaternion, it must be proper and it has at least two coefficients $a_l^{(0)}$'s different from zero, where $l \in \{1, \ldots, 4\}$.

Assume that $\alpha^{(0)}$ and π are two any arbitrary prime quaternions of a different norm such that they do commute. Then we can construct three other quaternions $\beta_l \in \mathcal{L}$, where $l \in \{2, 3, 4\}$ such that $\beta_2 = \pi + i$, $\beta_3 = \pi + j$ and $\beta_4 = \pi + k$. From the theory in Section 3.1, we can easily compute that for one β_l, $\alpha^{(0)}$ and β_l do not commute.

But still β_l does not have to be the prime quaternion. So by Proposition 3.2.17, β_l can be written as a product of prime quaternions. If all prime factors of β_l commute with $\alpha^{(0)}$, then β_l would also commute $\alpha^{(0)}$, which is a contradiction, since β_l does not commute with $\alpha^{(0)}$. And this means that there exists a prime quaternion π, which is in prime factorization of β_l and does not commute with $\alpha^{(0)}$. □

In the next proposition, we will differ a bit with our notations. The indexes below the Greek letters are not meant in connotation with indexes in the braces above. But afterwards we will continue with the above definitions.

Proposition 6.1.3. Let be $\alpha^{(0)}$ defined as above, and let be π_1 and π_2 two prime quaternions of not necessarily the same norm, and the norm of $\alpha^{(0)}$ is different from the norms of π_1 and π_2. Let be $\alpha_1^{(1)}$, $\alpha_1^{(2)}$ and $\alpha_2^{(1)}$ such that $\alpha^{(0)}\pi_1 = \pi_1^{(1)}\alpha_1^{(1)}$, $\alpha_1^{(1)}\pi_2 = \pi_2^{(1)}\alpha_1^{(2)}$ and $\alpha^{(0)}\gamma = \gamma^{(1)}\alpha_2^{(1)}$, where $\gamma = \pi_1\pi_2$. Then $\alpha_1^{(2)}$ and $\alpha_2^{(1)}$ are left-associates.

Proof. Let be all quaternions defined as in the proposition above. Then we can construct the following equation:

$$\gamma^{(1)}\alpha_2^{(1)} = \alpha^{(0)}\gamma = \alpha^{(0)}\pi_1\pi_2 = \left(\alpha^{(0)}\pi_1\right)\pi_2 =$$

$$= \left(\pi_1^{(1)}\alpha_1^{(1)}\right)\pi_2 = \pi_1^{(1)}\left(\alpha_1^{(1)}\pi_2\right) = \pi_1^{(1)}\left(\pi_2^{(1)}\alpha_1^{(2)}\right) = \pi_1^{(1)}\pi_2^{(1)}\alpha_1^{(2)}.$$

This equation implies that $\alpha_2^{(1)}$ and $\alpha_1^{(2)}$ are both right divisors of the product $\alpha^{(0)}\gamma$ of the same norm. And from the Theorem 3.2.12 follows that $\alpha_2^{(1)}$ and $\alpha_1^{(2)}$ are left-associates. Note also that $\gamma^{(1)} = \pi_1^{(1)}\pi_2^{(1)}$. □

In general, this proposition shows that for given $\alpha^{(0)}$ and π, there is no difference, if we compute $\alpha^{(2)}$ by commutating $\alpha^{(0)}$ twice with π, or if we first compute $\gamma = \pi^2$ and then commutate $\alpha^{(0)}$ with γ only once. So by using induction, we can show the following proposition:

Proposition 6.1.4. Let be $\alpha^{(0)}$ and π as usually defined. Then the following holds: $\alpha^{(0)}\pi^e = \left(\prod_{l=1}^{e}\pi^{(l)}\right)\alpha^{(e)}$.

Proof. Note that from Proposition 6.1.3, this equation holds for $e = 1$ and $e = 2$. So we are constructing the induction step by assuming that the equation is true for $e - 1$, i.e.

$$\alpha^{(0)}\pi^{e-1} = \prod_{l=1}^{e-1} \pi^{(l)}\alpha^{(e-1)}. \tag{6.4}$$

Now we will show this for e. Recall the notation from the beginning of this chapter, $\alpha^{(e-1)}\pi = \pi^{(e)}\alpha^{(e)}$ for all $e \in \mathbb{N}$. Then we can compute the following:

$$\begin{aligned} &\alpha^{(0)}\pi^{e} = \left(\alpha^{(0)}\pi^{e-1}\right)\pi = \textstyle\prod_{l=1}^{e-1} \pi^{(l)} \left(\alpha^{(e-1)}\pi\right) = \\ &= \textstyle\prod_{l=1}^{e-1} \pi^{(l)} \left(\pi^{(e)}\alpha^{(e)}\right) = \prod_{l=1}^{e} \pi^{(l)}\alpha^{(e)}. \end{aligned} \tag{6.5}$$

□

Consider the sequence $\alpha^{(0)}$, $\alpha^{(1)}, \ldots, \alpha^{(e)}, \ldots$ created by commutating $\alpha^{(e)}$ with π, for $e \in \mathbb{N}$. The last proposition implicates that $\alpha^{(e)}$ can be computed directly by commutating $\alpha^{(0)}$ with γ, where $\gamma = \pi^e$. Note that for a growing integer e, the quaternion γ grows exponentially.

Now we want to present another more interesting consequence of the Proposition 6.1.3, and this is the case if $\pi_2 = \overline{\pi}_1$.

Lemma 6.1.5. Let be $\alpha^{(0)}$, $\alpha^{(1)}$, π and $\pi^{(1)}$ defined as usual. Then $\alpha^{(1)}\overline{\pi} = \overline{\pi^{(1)}}\alpha^{(0)}$.

Proof. The proof of this lemma is a direct consequence of Proposition 6.1.3.

Note the following equation:

$$\pi^{(1)}\alpha^{(1)}\overline{\pi} = \alpha^{(0)}\pi\overline{\pi} = N(\pi)\alpha^{(0)} = \pi^{(1)}\overline{\pi^{(1)}}\alpha^{(0)}. \tag{6.6}$$

By dividing the last equation with $\pi^{(1)}$ from left, we get that $\alpha^{(1)}\overline{\pi} = \overline{\pi^{(1)}}\alpha^{(0)}$. □

This lemma is interesting because it shows us that by commutating $\alpha^{(0)}$ with π and then commutating $\alpha^{(1)}$ with $\overline{\pi}$, we get the initial prime quaternion $\alpha^{(0)}$. This result has an important consequence that we will present in the next lemma

Lemma 6.1.6. Let be $\alpha^{(0)}$, $\pi \in \mathcal{L}$ two prime quaternions, defined as usual. Recall that $N(\alpha^{(0)}) = q \neq p = N(\pi)$. And let be $\alpha^{(0)}$, $\alpha^{(1)}$, $\alpha^{(2)}, \ldots$ an infinite sequence generated by commutating $\alpha^{(l)}$ with π, where $l \in \mathbb{N}$. Then there exist integers e_1, $e_2 \in \mathbb{N}$ such that $\alpha^{(e_1)}$ and $\alpha^{(e_2)}$ are left-associates and $e_1 < e_2 \leq q + 1$. Even more, if $e_2 > 0$ is the smallest integer such that $\alpha^{(e_2)}$ is left-associate to some $\alpha^{(e_1)}$, where $e_1 < e_2$, then $e_1 = 0$.

Proof. So let be π, $\alpha^{(0)}$, $\alpha^{(1)}$, $\alpha^{(2)}, \ldots$ and e_1, $e_2 \in \mathbb{N}$ defined as in lemma.

First, if $\alpha^{(0)}$ and π are commutative, we see right away that lemma holds, since

$$\alpha^{(0)}\pi = \pi^{(1)}\alpha^{(1)} = \pi\alpha^{(0)} \quad \Rightarrow \quad \alpha^{(0)} = \alpha^{(1)}. \tag{6.7}$$

and $0 = e_1 < e_2 = 1 \leq q + 1$.

Assume now that $\alpha^{(0)}$ and π do not commute. Then define the sequence $S_e(\alpha^{(0)}, \pi)$ as follows,

$$S_e(\alpha^{(0)}, \pi) = \left(\alpha^{(0)}, \alpha^{(1)}, \ldots, \alpha^{(e)}\right). \tag{6.8}$$

This sequence has exactly $e + 1$ elements. Now consider the sequence $S_{q+1}(\alpha^{(0)}, \pi)$ with exactly $q + 2$ elements. But there are at most $q + 1$ quaternions that are pairwise not left-associated (see Lemma 3.2.11). This means that there exist e_1, $e_2 \in \mathbb{N}$, where $e_1 < e_2 \leq q + 1$ such that $\alpha^{(e_1)}$ and $\alpha^{(e_2)}$ are in $S_{q+1}(\alpha^{(0)}, \pi)$, where $\alpha^{(e_1)}$ and $\alpha^{(e_2)}$ are left-associated.

Now, let be $0 < e_1 \leq e_2$ two positive integers such that $\alpha^{(e_1)}$ and $\alpha^{(e_2)}$ are in the sequence $S_{q+1}(\alpha^{(0)}, \pi)$, and left-associates. Then there exists a unit ε, such that $\alpha^{(e_1)} = \varepsilon\alpha^{(e_2)}$. From Lemma 6.1.5, the following holds:

$$\alpha^{(e_1)}\overline{\pi} = \overline{\pi^{e_1}}\alpha^{(e_1-1)}, \tag{6.9}$$

but then also

$$\alpha^{(e_1)}\overline{\pi} = \varepsilon\alpha^{(e_2)}\overline{\pi} = \varepsilon\overline{\pi^{(e_2)}}\alpha^{(e_2-1)}. \tag{6.10}$$

In other words, $\alpha^{(e_1-1)}$ and $\alpha^{(e_2-1)}$ are two right divisors of $\alpha^{(e_1)}\overline{\pi}$ of the same norm. And by Theorem 3.2.12, $\alpha^{(e_1-1)}$ and $\alpha^{(e_2-1)}$ are left-associates.

Applying Lemma 6.1.5, we can show by induction that $\alpha^{(e_1-l)}$ and $\alpha^{(e_2-l)}$ must also be left-associates for all $l \in \{0, 1, \ldots, e_1\}$. This means that there exists $e_3 = e_2 - e_1 \leq e_2$ such that $\alpha^{(e_3)}$ from $S_{q+1}(\alpha^{(0)}, \pi)$ is left-associated to $\alpha^{(0)}$, which proves the lemma. □

From this lemma we see that the first quaternion $\alpha^{(e)}$ with $e > 0$ that is left-associate to any other quaternion in sequence, is left-associated with the starting quaternion $\alpha^{(0)}$.

Then, this sequence start to repeats it self after the quaternion $\alpha^{(e)}$, i.e. $\alpha^{(l)}$ and $\alpha^{(e+l)}$ are left-associated for all $l \in \mathbb{N}$.

And, there is no smaller sequence inside this sequence. Meaning, by taking any quaternion $\alpha^{(l)}$ from the sequence $S_{q+1}(\alpha^{(0)}, \pi)$ and commutating $\alpha^{(l)}$ with π will generate again the same elements of the sequence $S_{q+1}(\alpha^{(0)}, \pi)$.

Definition 6.1.7. Let be $S_e(\alpha^{(0)}, \pi)$ defined as in equation (6.8). Then we define the set $\langle\alpha^{(0)}, \pi\rangle = \{\alpha^{(0)}, \alpha^{(1)}, \ldots, \alpha^{(e-1)}\}$, where $\alpha^{(l)}$ are all elements from $S_{e-1}(\alpha^{(0)}, \pi)$ and $e = \min\{e_1 \mid \alpha^{(0)}$ and $\alpha^{(e_1)}$ are left-associate$\}$. We say that $\langle\alpha^{(0)}, \pi\rangle$ has an order e, and denote it by $e = \mathrm{ord}\langle\alpha^{(0)}, \pi\rangle$ which is the number of elements in set $\langle\alpha^{(0)}, \pi\rangle$.

Remark 6.1.8. Recall the notations from the beginning of this chapter. We have denoted with $\alpha^{(l)}$ any quaternion from the set $\mathfrak{DL}_{\alpha_l}$, since all used operations have a unique solution up to the left-associates. So recall the Lemma 3.2.11. We see that $\langle\alpha^{(0)}, \pi\rangle$ is one of the sets $\mathcal{A}_n$, where $N(\alpha^{(0)}) = n$. So in general, we do not care which left-associate $\alpha^{(l)}$ is, since this does not affect our computations of $\alpha^{(l+1)}$ (see Lemma 6.0.7). Therefore, when we say that $\alpha^{(l)}$ is an element of the set $\langle\alpha^{(0)}, \pi\rangle$ we mean on any left-associate of that quaternion.

Proposition 6.1.9. Let be $\alpha^{(0)}, \beta^{(0)} \in \mathcal{L}$ such that $\alpha^{(0)} \notin \langle\beta^{(0)}, \pi\rangle$, for some prime quaternion π. Then

$$\forall\gamma \in \langle\alpha^{(0)}, \pi\rangle \quad \Rightarrow \quad \gamma \notin \langle\beta^{(0)}, \pi\rangle, \tag{6.11}$$

and vice versa.

Proof. Clear. □

6.1.1 Order of the set $\langle\alpha^{(0)}, \pi\rangle$

In this part we will discuss the order of set $\langle\alpha^{(0)}, \pi\rangle$. Since we have no particular property that describes the elements in this set, we were not able to estimate the magnitude of the order. Anyway, we will present some interesting experimental results and observations using some algorithms from the algorithm tests in Appendix E.4

Let be $\alpha^{(0)}$ a Lipschitz prime quaternion with $N(\alpha^{(0)}) = q$ sufficiently large, and π a randomly chosen Lipschitz prime quaternion with $N(\pi) = p \neq q$ and $\mathrm{ord}\langle\alpha^{(0)}, \pi\rangle = e$.

First, assume that π is a periodical prime quaternion which has a period $\tilde{e}$. Then Lemma 3.3.8 states that π has a period $e \in \{2, 4\}$. Using the result from Proposition 6.1.4 for some fixed prime quaternion $\alpha^{(0)}$, the $\langle\alpha^{(0)}, \pi\rangle$ has at most the order $\tilde{e}$, since $\pi^{\tilde{e}} \in \mathbb{Z}$ and $\alpha^{(0)}\pi^{\tilde{e}} = \pi^{\tilde{e}}\alpha^{(0)}$. This means that $\mathrm{ord}\langle\alpha^{(0)}, \pi\rangle = e \in \{1, 2, 3, 4\}$ for $\alpha^{(0)}$. Note that using Lemma 6.1.6, it is simple to show the case where order $e = 3$ can never occur. So here is not much to discuss about periodical primes.

Remark 6.1.10. The interesting part happens if π has a period greater than $N(\alpha^{(0)})$. Note that π is not a prime quaternion in that case. Since we did not prove that Lemma 6.1.6 also holds with π, where π is not a prime quaternion, we won't discuss this further. Anyway, we can show that Lemma 6.1.6 also holds for π not prime and if we were able to find a π with a period $\tilde{e}$ greater than $N(\alpha^{(0)})$, the order e of the set $\langle \alpha^{(0)}, \pi \rangle$ would be equal to a factor of the period $\tilde{e}$.

Now we want to give some experimental results for the order e of the set $\langle \alpha^{(0)}, \pi \rangle$, where π is a prime and not periodical. For this, we will use the algorithm "Test1" listed in Appendix E.4 on the page XXIII.

The first interesting experimental result from this test is that every order e is the factor of $N(\alpha^{(0)}) + 1 = q + 1$ or of $N(\alpha^{(0)}) - 1 = q - 1$. But unfortunately, the order e still has a large value respectively to the norm of $\alpha^{(0)}$. Apparently, the length on the sequence $\langle \alpha^{(0)}, \pi \rangle$ does not depend of the particular prime π; it only depends on the norm of the $\alpha^{(0)}$. Anyway, it seems that by choosing one quaternion $\alpha^{(0)}$ of the norm q, the set $\langle \alpha^{(0)}, \pi \rangle$ has mostly many elements. This means that such set will contain most likely the quaternions β that are of the same structure or even associated or right-associated to $\alpha^{(0)}$. Recall that this set by Lemma 6.1.6 only has no left-associates.

From this "Test1" we have also observed that quaternions of the same norm, but are not necessarily of the same structure, have the same order with one fixed prime quaternion π. Naturally of course, since the e is relatively large, there is a great chance that we take a quaternion $\alpha^{(l)} \in \langle \alpha^{(0)}, \pi \rangle$, where $\langle \alpha^{(l)}, \pi \rangle$ is the same set, i.e. has the same order e.

So now we are raising the question, "What is the order e of $\langle \alpha^{(0)}, \pi \rangle$, where π is fixed prime and α_0 is any quaternion of the norm q". For this question, we have write the algorithm "Test2(alpha,pi)", which is listed in Appendix E.4 on the page XXVI. "Test2" creates all $q+1$ quaternions $\alpha^{(0)}$ that have the same norm and are not left-associate, and computes the order of all possible sets $\langle \alpha^{(0)}, \pi \rangle$. Recall that all those sets are disjoint.

It appears that, if there exists a quaternion $\alpha^{(0)}$ such that $e = \mathrm{ord}\langle \alpha^{(0)}, \pi \rangle$, where e divides $N(\alpha^{(0)})+1$, then all the orders of the other sets $\langle \tilde{\alpha}^{(0)}, \pi \rangle$, where $N(\tilde{\alpha}^{(0)}) = N(\alpha^{(0)})$ and $\tilde{\alpha}^{(0)} \notin \langle \alpha^{(0)}, \pi \rangle$ is also equal to e. And if the order e of one set $\langle \alpha^{(0)}, \pi \rangle$ divides $N(\alpha^{(0)}) - 1$, then all the other sets $\langle \tilde{\alpha}^{(0)}, \pi \rangle$, where $\tilde{\alpha}^{(0)} \notin \langle \alpha^{(0)}, \pi \rangle$ have the same order e, except two quaternions which have the order equal to 1 and they are right associated.

Example 6.1.11.

```
N(Alpha)=643 N(Pi)=293
ListOfOrders= [7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,
7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,
7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,
7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,
7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,
7, 7, 7, 7, 7]
```

Finding such two quaternions is in general very difficult since if they exist, we have only the chance $\frac{2}{q+1}$ of constructing them randomly, which is a very small probability for q sufficiently large.

Since we saw what happens with the order by changing the structure of $\alpha^{(0)}$ with a fixed π, we will now consider what happens if we fix $\alpha^{(0)}$ and change the prime π. As first we will take the different quaternions π with the same norm.

Example 6.1.12. This are the results of the test algorithm "Test1" (listed on the page XXIII) which creates one fixed quaternion α_0 and different quaternions π all with same norm. And it returns the following:

```
Example:1-----------------------------------------------
N(Alpha)=7877 N(Pi)=503 ord(<Alpha,Pi>)=3938
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
```

```
Answer: True ,by factor=2
Example:2------------------------------------------
N(Alpha)=7877 N(Pi)=503 ord(<Alpha,Pi>)=3938
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
Answer: True ,by factor=2
Example:3------------------------------------------
N(Alpha)=7877 N(Pi)=503 ord(<Alpha,Pi>)=3939
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
Answer: True ,by factor=2
```

As it appears, in general there is no big difference between orders if we choose different quaternion π, where the norm stays constant. But it seems that some of the forms create rather the smaller order than the others. For example the quaternions π, where $N(\pi) = 7$ and which are of the form $\pi = \pm 2 \pm i \pm j \pm k$ tend to create the sets with smaller order. This implies that the order depends on the coefficients permutation and not on the sign changing. Even more, it seems that the quaternions π (in this case π not necessarily a prime) of the form $a + bi + bj + bk$, where $a, b \in \mathbb{Z}$ have mostly some special properties. For example $3 + i + j + k$ is periodical with period 6. But in general, it appears that there is no big difference between the size of orders and no particular rule when it is so. Therefore, we will take the last test to see how the order e changes when we take primes π randomly with different norms.

Example 6.1.13. This are the results of the test algorithm "Test1" (listed on the page XXIII) which creates one fixed quaternion α_0 and different quaternions π all with different norms. And it returns the following:

```
Example:1------------------------------------------------
N(Alpha)=8609 N(Pi)=503 ord(<Alpha,Pi>)=8608
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
Answer: True ,by factor=1
Example:2------------------------------------------------
N(Alpha)=8609 N(Pi)=907 ord(<Alpha,Pi>)=2152
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
Answer: True ,by factor=4
Example:3------------------------------------------------
N(Alpha)=8609 N(Pi)=1063 ord(<Alpha,Pi>)=4305
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
Answer: True ,by factor=2
Example:4------------------------------------------------
N(Alpha)=8609 N(Pi)=509 ord(<Alpha,Pi>)=4304
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
Answer: True ,by factor=2
Example:5------------------------------------------------
N(Alpha)=8609 N(Pi)=727 ord(<Alpha,Pi>)=35
Is the order a factor of N(Alpha)+1 or N(Alpha)-1?
Answer: True ,by factor=246
```

In this case, it appears that the order e can have a rather big difference depending on the norm of quaternion π. As we estimated from the experimental results, the average order is about $\frac{N(\alpha^{(0)})}{2} = \frac{q}{2}$. But the minimal order can get rather small as in the case where for example the set $\langle -527 + 427i + 610j - 323k, -161 + 729i + 426j - 5k \rangle$ has the order 49 and $N(\alpha^{(0)}) = 936487$ and $N(\pi) = 738863$. Anyway, as it appears, the average of orders is growing with the same speed as the norm of $\alpha^{(0)}$.

6.1.2 Elements of the set $\langle \alpha^{(0)}, \pi \rangle$

In this part, we will analyze the elements in the set $\langle \alpha^{(0)}, \pi \rangle$ and how they are ordered in this set.

Let be elements $\alpha^{(l)} \in \langle \alpha^{(0)}, \pi \rangle$ ordered by theirs indexes $l \in \{0, 1 \ldots, e-1\}$. Now we will also give a definition of the expression *distance of two quaternions*.

Definition 6.1.14. We say that two quaternions $\alpha^{(l_1)}$, $\alpha^{(l_2)} \in \langle \alpha^{(0)}, \pi \rangle$ have the *distance* d, where $d = |l_1 - l_2|$.

In other words, d is the number of quaternions we have to count from the quaternion $\alpha^{(l_1)}$ till we reach the quaternion $\alpha^{(l_2)}$ in the ordered set $\langle \alpha^{(0)}, \pi \rangle$. So now we can start with the discussion about the elements in $\langle \alpha^{(0)}, \pi \rangle$.

As we have already pointed out, the elements in $\langle \alpha^{(0)}, \pi \rangle$ are pairwise not left-associated, but there can still be quaternions that are pairwise of the same structure or even associated. So consider all elements $\alpha^{(l)}$ of the set $\langle \alpha^{(0)}, \pi \rangle$ which are pairwise of the same structure (see the first table in Example 6.1.15). And consider the distances between two nearest quaternions of the same structure. Then the distance of two nearest quaternions of the same structure occur in the certain pattern (see the second table in Example 6.1.15).

Example 6.1.15. This are the results of the test algorithm "Test3" (listed on the page XXVIII) which computes all elements $\alpha^{(l)} \in \langle \alpha^{(l)}, \pi \rangle$ and sorts them in distinct sets so that in each set are only elements that are pairwise of the same structure. And it returns two tables.

In the first table, we see those distinct sets presented in rows separated by square brackets. The values l's in each brackets present the ordered element $\alpha^{(l)} \in \langle \alpha^{(l)}, \pi \rangle$ which are pairwise of the same structure.

```
a=Test3(-3 - 25*i + 18*j - 3*k,2+i+j+k)

Table 1.
-----------------------------------------
[0, 13, 27, 94, 105, 230, 241, 308, 322, 335, 349, 416, 427, ...]
[1, 12, 14, 41, 59, 60, 65, 86, 127, 208, 249, 270, 275, ...]
[2, 11, 20, 42, 53, 75, 110, 151, 155, 180, 184, 225, 260, ...]
[3, 4, 5, 8, 9, 10, 68, 70, 71, 81, 150, 185, 254, 264, ...]
[6, 7, 23, 25, 46, 113, 121, 149, 167, 168, 186, 214, 222, ...]
[15, 18, 29, 32, 58, 66, 85, 138, 197, 250, 269, 277, 303, ...]
[16, 17, 24, 103, 232, 311, 318, 319, 338, 339, 346, 425, ...]
[19, 35, 37, 79, 125, 129, 139, 154, 181, 196, 206, 210, ...]
[21, 74, 130, 132, 153, 163, 164, 165, 170, 171, 172, 182, ...]
[22, 111, 112, 152, 183, 223, 224, 313, 344, 433, 434, 474, ...]
[26, 45, 95, 157, 178, 240, 290, 309, 348, 367, 417, 479, ...]
.
.
.
[90, 245, 412, 567, 734, 889]
[96, 108, 158, 159, 176, 177, 227, 239, 418, 430, 480, 481, ...]
[98, 119, 134, 147, 188, 201, 216, 237, 420, 441, 456, 469, ...]
-----------------------------------------
```

In the second table, we see the list of the rows separated by square brackets. The first value l in each bracket stands for the smallest l were $\alpha^{(l)} \in \langle \alpha^{(l)}, \pi \rangle$ is the first quaternion of a particular structure. All other values stand for the distance between two nearest ordered quaternions of the same structure.

```
Table 2.
-----------------------------------------
[0, 13, 14, 67, 11, 125, 11, 67, 14, 13, 14, 67, 11, 125, ...]
[1, 11, 2, 27, 18, 1, 5, 21, 41, 81, 41, 21, 5, 1, ...]
[2, 9, 9, 22, 11, 22, 35, 41, 4, 25, 4, 41, 35, 22,  ...]
[3, 1, 1, 3, 1, 1, 58, 2, 1, 10, 69, 35, 69, 10, 1, 2, 58, 1, ...]
[6, 1, 16, 2, 21, 67, 8, 28, 18, 1, 18, 28, 8, 67, 21, 2, ...]
[15, 3, 11, 3, 26, 8, 19, 53, 59, 53, 19, 8, 26, 3, 11, 3,  ...]
[16, 1, 7, 79, 129, 79, 7, 1, 19, 1, 7, 79, 129, 79, 7, 1, ...]
[19, 16, 2, 42, 46, 4, 10, 15, 27, 15, 10, 4, 46, 42, 2, ...]
[21, 53, 56, 2, 21, 10, 1, 1, 5, 1, 1, 10, 21, 2, 56, 53, ...]
[22, 89, 1, 40, 31, 40, 1, 89, 31, 89, 1, 40, 31, 40, 1, 89, ...]
[26, 19, 50, 62, 21, 62, 50, 19, 39, 19, 50, 62, 21, 62, 50, ...]
.
.
.
[90, 155, 167, 155, 167, 155]
[96, 12, 50, 1, 17, 1, 50, 12, 179, 12, 50, 1, 17, 1, ...]
[98, 21, 15, 13, 41, 13, 15, 21, 183, 21, 15, 13, ...]
-----------------------------------------
```

As it appears, there are two specific ways how the elements of the same structure in the set $< \alpha^{(0)}, \pi >$ are ordered. One is given in the Example 6.1.15 in the second table. If we take a set of quaternions where all elements are of the same structure as $\alpha^{(0)}$, we see that they appear in a symmetrically sequence of the distance values. The first two quaternions of the same structure have the distance 13, then the next two 14, then 67, 11, 125, 11, 67, 14, 13, etc. Here we see that the sequence starts to repeat backwards after the distance 125. Another example is given in Example 6.1.16, where the sequence of distances just starts to repeat from the beginning. By taking the same set of elements as in Example 6.1.16, as we took in Example 6.1.15, we see that the distance between the first two is distance 1, then the next two 5, then 16, 9, 1, 3, 14, 1, 5, 16, 9, etc.

Example 6.1.16. In this example, we have the same description as in the last example.

```
a=Test3(1 + 23*i - 8*j - 17*k,1+i+j)

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

```
Table 2.
-----------------------------------------
[0, 1, 5, 16, 9, 1, 3, 14, 1, 5, 16, 9, 1, 3]
[2, 10, 1, 17, 6, 1, 14, 10, 1, 17, 6, 1]
[3, 8, 3, 38, 8, 3]
[4, 11, 38, 11]
[5, 11, 5, 12, 1, 14, 6, 11, 5, 12, 1, 14]
[7, 16, 33, 16]
[8, 2, 47, 2]
[9, 49]
[17, 2, 1, 26, 1, 19, 2, 1, 26, 1]
[18, 27, 22, 27]
[24, 16, 2, 31, 16, 2]
[25, 3, 11, 4, 31, 3, 11, 4]
[26, 1, 48, 1]
[29, 9, 6, 34, 9, 6]
[41, 49]
-----------------------------------------
```

Note that there are at most $4! \cdot 2^4 = 384$ quaternions of the same structure. And there are at most $384/8 = 48$ quaternions of the same structure in the set $\langle \alpha^{(0)}, \pi \rangle$, since there are no left-associates. So if the order of this set is sufficiently large, we can find the pairs $\left(\alpha^{(l)}, \alpha^{(l+1)}\right)$ and $\left(\alpha^{(m)}, \alpha^{(m\pm1)}\right)$, where neither $\alpha^{(l)}$ and $\alpha^{(l+1)}$ nor $\alpha^{(m)}$ and $\alpha^{(m\pm1)}$ are of the same structure. But $\alpha^{(l)}$ and $\alpha^{(m)}$ are of the same structure and $\alpha^{(l+1)}$ and $\alpha^{(m\pm1)}$ are as well.

Since we have not found any simple way of describing how the quaternions are changing in each step of computing the sequence S_{e-1}, we were not able to prove why this occurs in this such a way. However, there are some more interesting results according to the elements that are associate to each other or of a certain coefficient permutation and sign changing. But we will not pursue this any further, as we will not present a factorization algorithm that uses this as an advantage.

6.2 Commutation of quaternion η with prime quaternion π

In this section, we will take a closer look at commutating a quaternion η_0 with prime quaternion π, where $\eta_0 = \alpha_0\beta_0$ is a product of two prime quaternions α_0, $\beta_0 \in \mathcal{L}\backslash\{0\}$ with norms $N(\alpha_0) = q_1 \neq N(\beta_0) = q_2$ and $N(\pi) = p$ a prime such that $p \neq q_1, q_2$.

The more general case where η_0 is a product of many arbitrary prime quaternions is similar to our discussion in this section. Anyway, there are more special cases to be considered, especially if there are more than one prime factors with the same norm. But in this thesis, we will concentrate only on the case where η_0 is a product of two quaternions with different norms.

Now we will discuss some notions we will use in this section. Let be $\eta_0 = \alpha_0\beta_0$, where $N(\eta_0) = n = N(\alpha_0)N(\beta_0) = q_1q_2$ and $q_1 > q_2 > 1$ are prime integers. Recall that if q_1 and q_2 are prime integers, α_0 and β_0 are prime quaternions. Then we denote with $\eta^{(0)} \in \mathfrak{D}\mathfrak{L}_{\eta_0}$ any left-associate of the quaternion η_0. And $\alpha^{(0)}$ (resp. $\beta^{(0)}$) denotes an according associate of α_0 (resp. β_0) such that the equation $\eta^{(0)} = \alpha^{(0)}\beta^{(0)}$ holds. Note that by Theorem 3.2.12, there exists another factorization of $\eta^{(0)} = \gamma^{(0)}\delta^{(0)}$, where $N(\gamma^{(0)}) = q_2$ and $N(\delta^{(0)}) = q_1$, since $q_1 \neq q_2$.

And as usual we have the equation $\eta^{(l)}\pi = \tilde{\pi}^{(l+1)}\eta^{(l+1)}$ for all $l \in \mathbb{N}$, where $\eta^{(l)} = \tilde{\alpha}^{(l)}\tilde{\beta}^{(l)}$. $S(\eta^{(0)}, \pi)$ will denote the infinite sequence $(\eta^{(0)}, \eta^{(1)}, \ldots)$ generated by commutating $\eta^{(l)}$ with π over $l \in \{0, 1, 2, \ldots\}$.

Lemma 6.2.1. Let be $\eta^{(l)}$ in sequence $S(\eta^{(0)}, \pi)$, where $l \in \mathbb{N}$. Then there exists $\beta^{(r)} \in \langle \beta^{(0)}, \pi \rangle$ such that $\beta^{(r)}$ is a left-associate to $\tilde{\beta}^{(l)}$. Even more $l \equiv r \bmod e$, where $e = \mathrm{ord}\langle \beta^{(0)}, \pi \rangle$.

Proof. Recall that the set $\langle \beta^{(0)}, \pi \rangle = \{\beta^{(0)}, \beta^{(1)}, \ldots, \beta^{(e-1)}\}$ is generated by commutating $\beta^{(l)}$ with π over $l \in \{0, 1, \ldots, e-1\}$, where $e = \mathrm{ord}\langle \beta^{(0)}, \pi \rangle$ is the smallest integer such that $\beta^{(0)}$ and $\beta^{(e)}$ are left-associates.

From the definitions of $\eta^{(0)}$ and the set $\langle \beta^{(0)}, \pi \rangle$ following two equations holds:

$$\eta^{(0)}\pi = \alpha^{(0)}\beta^{(0)}\pi = \alpha^{(0)}\left(\beta^{(0)}\pi\right) = \alpha^{(0)}\pi^{(1)}\beta^{(1)} \tag{6.12}$$

and

$$\eta^{(0)}\pi = \tilde{\pi}^{(1)}\eta^{(1)} = \tilde{\pi}^{(1)}\tilde{\alpha}^{(1)}\tilde{\beta}^{(1)}. \tag{6.13}$$

By the Theorem 3.2.12, it follows that $\beta^{(1)}$ and $\tilde{\beta}^{(1)}$ are left-associated, since

$$\alpha^{(0)}\pi^{(1)}\beta^{(1)} = \tilde{\pi}^{(1)}\tilde{\alpha}^{(1)}\tilde{\beta}^{(1)}.$$

Remark 6.2.2. Recall that the Theorem 3.2.12 states that a quaternion has a unique right divisor of a norm m up to its left-associates. In this case, $\eta^{(0)}\pi$ has a unique divisor of the norm $N(\beta^{(1)}) = N(\tilde{\beta}^{(1)})$, and this implies that $\beta^{(1)}$ and $\tilde{\beta}^{(1)}$ are left-associates.

By creating an induction over l, the following equations hold:

$$\eta^{(l-1)}\pi = \tilde{\alpha}^{(l-1)}\varepsilon\beta^{(l-1)}\pi = \tilde{\alpha}^{(l-1)}\varepsilon\left(\beta^{(l-1)}\pi\right) = \tilde{\alpha}^{(l-1)}\varepsilon\pi^{(l)}\beta^{(l)} \tag{6.14}$$

where ε is a unit such that $\varepsilon\beta^{(l-1)} = \tilde{\beta}^{(l-1)}$ and

$$\eta^{(l-1)}\pi = \tilde{\pi}^{(l)}\eta^{(l)} = \tilde{\pi}^{(l)}\tilde{\alpha}^{(l)}\tilde{\beta}^{(l)}, \tag{6.15}$$

for $l \in \{1, 2, \ldots, e-1\}$, and from this follows that $\beta^{(l)}$ and $\tilde{\beta}^{(l)}$ are left-associates for all $l \in \{1, 2, \ldots, e-1\}$.

Now consider the equations (6.14) and (6.15) for $l = e$. Then

$$\eta^{(e-1)}\pi = \tilde{\alpha}^{(e-1)}\varepsilon\pi^{(e)}\beta^{(e)} = \tilde{\pi}^{(e)}\tilde{\alpha}^{(e)}\tilde{\beta}^{(e)}. \tag{6.16}$$

But since $\beta^{(0)}$ and $\beta^{(e)}$ are left-associated, $\beta^{(0)}$ and $\tilde{\beta}^{(e)}$ are also left-associated. In the same way, we can show that $\beta^{(1)}$ and $\tilde{\beta}^{(e+1)}$ are also left-associated for $l = e+1$. And therefore, $\beta^{(r)}$ and $\tilde{\beta}^{(l)}$ are also left-associated for all $l \in \mathbb{N}$ and $l \equiv r \bmod e$. □

In general, this lemma states that the right divisor of the quaternion $\eta^{(l)}$ with the norm q_2 is the left-associate to $\beta^{(r)} \in \langle \beta^{(0)}, \pi \rangle$, where $l \equiv r \bmod e$. In other words, if $\mathrm{ord}\langle \beta^{(0)}, \pi \rangle = e$, $\eta^{(0)}$ and $\eta^{(e)}$ have the same right divisor of the norm q_2.

On the other hand, this does not hold for the quaternions $\tilde{\alpha}^{(l)}$'s. Consider now the equation $\tilde{\alpha}^{(l-1)}\tilde{\beta}^{(l-1)}\pi = \alpha^{(l-1)}\pi^{(l)}\tilde{\beta}^{(l)} = \tilde{\pi}^{l}\tilde{\alpha}^{(l)}\tilde{\beta}^{(l)}$ for $l \in \mathbb{N}$. From this equality, we see that we are commutating $\alpha^{(l-1)}$ with $\pi^{(l)}$, where the $\pi^{(l)}$'s do not have to be pairwise right-associates for all $l \in \mathbb{N}$.

Consider that if all $\pi^{(l)}$'s were pairwise right-associates for all $l \in \mathbb{N}$, then we could find a unit ε_l such that $\pi^{(1)}\varepsilon_l = \pi^{(l)}$ for all $l \in \mathbb{N}$. But then

$$\tilde{\alpha}^{(l-1)}\tilde{\beta}^{(l-1)}\pi = \tilde{\alpha}^{(l-1)}\pi^{(l)}\tilde{\beta}^{(l)} = \tilde{\alpha}^{(l-1)}\pi^{(1)}\varepsilon_l\tilde{\beta}^{(l)} = \tilde{\pi}^{1}\tilde{\alpha}^{(l)}\varepsilon_l\tilde{\beta}^{(l)}. \tag{6.17}$$

In other words, then $\tilde{\alpha}^{(l)}$ is left-associated to $\alpha^{(r)}$ for $l \in \mathbb{N}$, where $\alpha^{(r)} \in \langle \alpha^{(0)}, \pi^{(1)} \rangle$, $l \equiv r \bmod \tilde{e}$ and $\mathrm{ord}\langle \alpha^{(0)}, \pi^{(1)} \rangle = \tilde{e}$.

Since in general $\pi^{(l)}$'s are not pairwise right-associates (in experimental results this never happened) we see that the sequence $\alpha^{(0)}$, $\tilde{\alpha}^{(1)}$, $\tilde{\alpha}^{(2)}\ldots$ is in general different from $S(\alpha^{(0)}, \pi^1)$. Accordingly, there is no particular way to describe the sequence $\tilde{\alpha}^{(l)}$'s.

Theoretically there is always a chance that for such $\eta^{(0)}$ and $\eta^{(e)}$, where $\beta^{(0)}$ and $\tilde{\beta}^{(e)}$ are left-associated, that $\alpha^{(0)}$ and $\tilde{\alpha}^{(e)}$ are associated. Then the following holds $\eta^{(e)} = \tilde{\alpha}^{(e)}\tilde{\beta}^{(e)} = \varepsilon_1\alpha^{(0)}\varepsilon_2\varepsilon_3\beta^{(0)}$. Only if $\varepsilon_2\varepsilon_3 = \pm 1$, we would have the case where the greatest common right divisor has the norm bigger then q_2. But this never happened in experimental results as long as π was not periodical. Since we do not know if or how we can construct periodical quaternions with large periods, the periodical quaternions are in general not interesting. Anyway, we will discuss some of the best representative of periodical primes.

Now we are going to look at the sets $\langle \eta^{(0)}, \pi \rangle$, where $N(\pi) = 2$. Since all prime quaternions of norm 2 are periodical with period $\tilde{e} \in \{2, 4\}$, we see that $\eta^{(0)}$ and $\eta^{(\tilde{e})}$ are left-associated, where $\eta^{(0)}$ and $\eta^{(\tilde{e})}$ are in $S(\eta^{(0)}, \pi)$.

Lemma 6.2.3. Let be $\eta^{(0)}$, $\pi \in \mathcal{L}$, where $N(\pi) = 2$. Then every $\eta^{(l)}$ from the sequence $S(\eta^{(0)}, \pi)$ is an element of $\mathfrak{E}$, meaning that they are all of the same structure.

This lemma states that all quaternions $\eta^{(l)}$ from the sequence $S(\eta^{(0)}, \pi)$ are pairwise coefficient permutations and sign change. And therefore also the permutation of coefficients and sign change of $\eta^{(0)}$.

Before we start proving this lemma, we first have to show a proposition.

Proposition 6.2.4. Let be $\pi = 1+\varepsilon_2$ prime quaternion with $N(\pi) = 2$, where $\varepsilon_2 \in \{i, j, k\}$ is a unit. Then the following equations hold:

$$\begin{array}{ll} \varepsilon_1 (1 + \varepsilon_2) = (1 - \varepsilon_2)\, \varepsilon_1 & \text{if } \varepsilon_1 \neq \varepsilon_2 \\ \varepsilon_1 (1 + \varepsilon_2) = -(1 - \varepsilon_2) & \text{if } \varepsilon_1 = \varepsilon_2 \end{array} \tag{6.18}$$

where $\varepsilon_1 \in \{i, j, k\}$ is a unit.

Proof. Let be π, ε_1, ε_2 defined as above and note that $\varepsilon_1\varepsilon_2 = -\varepsilon_2\varepsilon_1$ if $\varepsilon_1 \neq \varepsilon_2$ and $\varepsilon_1\varepsilon_2 = -1$ if $\varepsilon_1 = \varepsilon_2$. Then

$$\varepsilon_1 (1 + \varepsilon_2) = (\varepsilon_1 + \varepsilon_1\varepsilon_2) = (\varepsilon_1 - \varepsilon_2\varepsilon_1) = (1 - \varepsilon_2)\, \varepsilon_1 \quad \text{if } \varepsilon_1 \neq \varepsilon_2 \tag{6.19}$$

and

$$\varepsilon_1 (1 + \varepsilon_2) = (\varepsilon_1 + \varepsilon_1\varepsilon_2) = (\varepsilon_2 - 1) = -(1 - \varepsilon_2) \quad \text{if } \varepsilon_1 = \varepsilon_2 \tag{6.20}$$

□

Proof of Lemma 6.2.3. Recall the Definition 3.2.6 point 3 and consider the set for the quaternion $1+i$, $\mathfrak{S}_{1+i} = \{1 + i, 1 + j, 1 + k\} \subset \mathfrak{E}_{1+i}$. This means that we can write every $\tilde{\pi} \in \mathfrak{E}_{1+i}$ as $\tilde{\pi} = \varepsilon_1\pi\varepsilon_2$, where $\pi \in \mathfrak{S}_{1+i}$, and ε_1 and ε_2 are units. Note that all quaternions with the norm 2 are in set $\mathfrak{E}_{1+i}$.

So let be $\tilde{\pi}$ and π defined as above. And let be $\eta \in \mathcal{L}$ any quaternion. Then

$$\eta\tilde{\pi} = \eta\varepsilon_1\pi\varepsilon_2 = \eta^{(0)}\pi\varepsilon_2. \tag{6.21}$$

Note that η and $\eta^{(0)}$ are of the same structure, since they are right-associates.

Now consider the product $\eta^{(0)}\pi$. So let be $\eta^{(0)} = n_1+n_2i+n_3j+n_4k$ in $\mathcal{L}$ and $\pi = 1+\varepsilon$ for $\varepsilon \in \{i, j, k\}$. Then we can write

$$(n_1 + n_2i + n_3j + n_4k)(1 + \varepsilon) = n_1(1 + \varepsilon) + n_2i(1 + \varepsilon) + n_3j(1 + \varepsilon) + n_4k(1 + \varepsilon).$$

Assume that $\varepsilon = i$, then by Proposition 6.2.4 follows

$$n_1(1 + i) + n_2i(1 + i) + n_3j(1 + i) + n_4k(1 + i) = \tag{6.22}$$
$$n_1(1 - i)i + n_2((1 - i)) + n_3(1 - i)j + n_4(1 - i)k = \tag{6.23}$$
$$(1 - i)(-n_2 + n_1i + n_3j + n_4k) = \tag{6.24}$$
$$\overline{\pi}(-n_2 + n_1i + n_3j + n_4k) = \overline{\pi}\tilde{\eta}^{(1)}. \tag{6.25}$$

In the same way we can compute for $\varepsilon = j$

$$(n_1 + n_2 i + n_3 j + n_4 k)(1 + j) = \overline{\pi}(-n_3 + n_2 i + n_1 j + n_4 k) = \overline{\pi}\tilde{\eta}^{(1)} \tag{6.26}$$

and for $\varepsilon = k$

$$(n_1 + n_2 i + n_3 j + n_4 k)(1 + k) = \overline{\pi}(-n_4 + n_2 i + n_1 j + n_1 k) = \overline{\pi}\tilde{\eta}^{(1)}. \tag{6.27}$$

Consider that in all cases $\tilde{\eta}^{(1)}$ is of the same structure as $\eta^{(0)}$ and as η.

So if we go back to equation (6.21), then

$$\eta\tilde{\pi} = \left(\eta^{(0)}\pi\right)\varepsilon_2 = \overline{\pi}\tilde{\eta}^{(1)}\varepsilon_2 = \overline{\pi}\eta^{(1)}. \tag{6.28}$$

Note that $\tilde{\eta}^{(1)}$ and $\eta^{(1)}$ are right-associated and therefore also of the same structure. From all this follows that $\eta^{(1)}$, $\tilde{\eta}^{(1)}$, $\eta^{(0)}$ and η are all of the same structure, which proves the lemma. □

In general, $\eta^{(0)}$ and $\eta^{(1)}$ are not associated to each other, but also the factors of $\eta^{(1)}$ are of the same structure as the factors of $\eta^{(0)}$. In other words, this lemma indicates, which coefficient permutation and sign changing of $\eta^{(0)}$ are not associated to $\eta^{(0)}$, but still have factors that are of the same structure as factors of $\eta^{(0)}$. Naturally, there exist such coefficients n_1, n_2, n_3 and n_4 of $\eta^{(0)}$ such that $\eta^{(0)}$ and $\eta^{(1)}$ are associated. Even more, it can happen that one of the factors is left- or right-associated, which would give us a solution for factorization, but this happens very seldom.

Next we want to take a look at the set $\langle \eta^{(0)}, \pi \rangle$, where π is of the norm 3. At first, we see from Proposition 3.3.7 that quaternions $\pi = \pm i \pm j \pm k$ are periodical and with period 2. But there is another interesting property.

Lemma 6.2.5. Let be $\eta^{(0)}$, $\pi \in \mathcal{L}$, where $N(\pi) = 3$. Then two quaternions $\eta^{(l)}$ and $\eta^{(l+1)}$ from sequence $S(\eta^{(0)}, \pi)$ will have at least one coefficient of the same absolute value.

In particular, this lemma states that by commutating any quaternion with a prime quaternion of the norm 3, the new quaternion will have at least one coefficient of the same absolute value as one of coefficients in the previous quaternion. To show this, we need a small proposition.

Proposition 6.2.6. Every quaternion $\eta = n_1 + n_2 i + n_3 j + n_4 k \in \mathcal{L}$ has a left-associate $\tilde{\eta} = \tilde{n}_1 + \tilde{n}_2 i + \tilde{n}_3 j + \tilde{n}_4 k$, such that the following three values are divisible by 3:

$$2\tilde{n}_1 - 2\tilde{n}_2 + \tilde{n}_3, \quad -2\tilde{n}_1 - \tilde{n}_2 + 2\tilde{n}_3 \quad \text{and} \quad \tilde{n}_1 + 2\tilde{n}_2 + \tilde{n}_3. \tag{6.29}$$

Proof. Since the proof of this proposition is an arithmetic nightmare, we will give an algorithm that shows that this is true in every case. But first we have to show that there is an algorithm which can prove this proposition.

Consider that every coefficient $n_l \in \mathbb{Z}$ of $\eta^{(0)}$ can be presented as $n_l = 3b_l + r_l$, where $r_l \in \{0, 1, 2\}$ for all $l \in \{1, \ldots, 4\}$. And we can write

$$\eta^{(0)} = (3b_1 + 3b_2 i + 3b_3 j + 3b_4 k) + (r_1 + r_2 i + r_3 j + r_4 k) = \beta + \gamma.$$

Now consider that any sum is divisible by 3 if and only if it is congruent with zero modulo 3. But then the three sums listed in (6.29) are divisible by 3 if and only if the sums of r_l's are congruent with zero modulo 3, since $3b_l \equiv 0 \bmod 3$ for all l. So we see that this problem reduces only to checking if it is true for quaternions of the form $\gamma = r_1 + r_2 i + r_3 j + r_4 k$ and since $r_l \in \{0, 1, 2\}$ for all $l \in \{1, \ldots, 4\}$, there is a finite number of possible quaternions γ that we have to check.

So the small algorithm "ProofOfProposition.sage" creates all quaternions γ that are possible choices of $r_l \in \{0, 1, 2\}$ for $l \in \{1, \ldots, 4\}$ and its sign changes. Then it tests all 625 constructed quaternions, to find out if there is a left-associate to each quaternion, such that the values from (6.29) are all divisible by 3, and prints 'True' if it finds a hit for all 625 quaternions.

And here is the algorithm:

```
1
2 list1=[Q(0), Q(1), 1+i, 1+i+j, 1+i+j+k, Q(2),2+i, 2+i+j, 2+i+j+k,
    2+2*i, 2+2*i+j, 2+2*i+j+k, 2+2*i+2*j, 2+2*i+2*j+k,
    2+2*i+2*j+2*k]
3 list2=[]
4
5 for q in list1:
6     list2+=QuatPermutations(q)
7
8 print len(list2)
9 isItInGeneral=True
10 for q in list2:
11
12     isItForq=False
13     for u in [1,-1,i,-i,j,-j,k,-k]:
14
15         if isItForq:
16            break
17
18        newq=u*q
19        [a1,a2,a3,a4]=newq.coefficient_tuple()
20
21        value1=2*a1-2*a2+a3
22        value2=-2*a1-a2+2*a3
23        value3=a1+2*a2+2*a3
24
25        rest1=value1%3
26        rest2=value2%3
27        rest3=value3%3
28
29        if (rest1==0) and (rest2==0) and (rest3==0):
30            isItForq=True
31
32     isItInGeneral= isItInGeneral and isItForq
33
34 print isItInGeneral
```

Note that some methods used in this algorithm are defined and discussed in Section E.1. □

Proof of Lemma 6.2.5. The proof of this lemma is similar to the proof of Lemma 6.2.3.

Recall the Definition 3.2.6 and that the set $\mathfrak{S}_{1+i+j} = \{1+i+j\} \subset \mathfrak{E}_{1+i+1}$. This means that we can write every $\pi \in \mathfrak{E}_{1+i+j}$ as $\pi = \varepsilon_1 \tilde{\pi} \varepsilon_2$, where $\tilde{\pi} \in \mathfrak{S}_{1+i+j}$, and ε_1 and ε_2 are units. Note that all quaternions of norm 3 are in the set $\mathfrak{E}_{1+i+j}$ and since $\mathfrak{S}_{1+i+j} = \{1+i+j\}$, they are all pairwise associated.

Let be $\eta^{(0)} = n_1 + n_2 i + n_3 j + n_4 k \in \mathcal{L}$ any quaternion and $\tilde{\pi}$ and π defined as above. Then

$$\eta^{(0)}\pi = \eta^{(0)}\varepsilon_1\tilde{\pi}\varepsilon_2 = \eta\pi\varepsilon_2, \tag{6.30}$$

where $\eta^{(0)}$ and η are right-associates. So we know that there exits $\tilde{\eta} = \tilde{n}_1 + \tilde{n}_2 i + \tilde{n}_3 j + \tilde{n}_4 k$ and ε such that $\eta = \varepsilon\tilde{\eta}$ and Proposition 6.2.6 holds. Then we can write the equation (6.30)

$$\eta^{(0)}\pi = \eta\pi\varepsilon_2 = \varepsilon\tilde{\eta}\pi\varepsilon_2. \tag{6.31}$$

Now consider the product $\tilde{\eta}\pi$.

Claim 6.2.7. $\tilde{\pi}^{(1)} = -i + j + k$ is a left divisor of $\tilde{\eta}\pi$, i.e. $\left(\tilde{\pi}^{(1)}\right)^{-1}\tilde{\eta}\pi \in \mathcal{L}$, where $\left(\tilde{\pi}^{(1)}\right)^{-1} = \frac{\overline{\tilde{\pi}^{(1)}}}{N(\tilde{\pi}^{(1)})}$.

So we have to show that $\frac{\overline{\tilde{\pi}^{(1)}}\tilde{\eta}\pi}{N(\tilde{\pi}^{(1)})} \in \mathcal{L}$.

$$\begin{aligned}
&\frac{\overline{\tilde{\pi}^{(1)}}\tilde{\eta}\pi}{N(\tilde{\pi}^{(1)})} = (i-j-k)(\tilde{n}_1+\tilde{n}_2 i+\tilde{n}_3 j+\tilde{n}_4 k)(1+i+j)\tfrac{1}{3} = \\
&= (i-j-k)\left[(\tilde{n}_1-\tilde{n}_2-\tilde{n}_3)+(\tilde{n}_1+\tilde{n}_2-\tilde{n}_4)i+\right. \\
&\left.+(\tilde{n}_1+\tilde{n}_3+\tilde{n}_4)j+(\tilde{n}_2-\tilde{n}_3+\tilde{n}_4+)k\right]\tfrac{1}{3} = \\
&= [3\tilde{n}_4+(2\tilde{n}_1-2\tilde{n}_2+\tilde{n}_3)i+(-2\tilde{n}_1-\tilde{n}_2+2\tilde{n}_3)j+ \\
&+(\tilde{n}_1+2\tilde{n}_2+\tilde{n}_3)k]\tfrac{1}{3} = \tilde{\eta}^{(1)}.
\end{aligned} \tag{6.32}$$

and by Proposition 6.2.6, coefficients are divisible by 3 and $\tilde{\eta}^{(1)} \in \mathcal{L}$. Note that $\mathscr{R}(\tilde{\eta}^{(1)}) = \tilde{n}_4$, which is a coefficient that appears in $\tilde{\eta}$ and η. So we can write the following equation

$$\eta^{(0)}\pi = \varepsilon\left(\tilde{\eta}\pi\right)\varepsilon_2 = \varepsilon\tilde{\pi}^{(1)}\tilde{\eta}^{(1)}\varepsilon_2 = \pi^{(1)}\eta^{(1)}, \tag{6.33}$$

where $\varepsilon\tilde{\pi}^{(1)} = \pi^{(1)}$ and $\tilde{\eta}^{(1)}\varepsilon_2 = \eta^{(1)}$ which proves the lemma.

□

6.3 Factorization using Lipschitz integers

In this section, we will present a factorization algorithm based on the theory discussed in Sections 6.1 and 6.2. Note that all algorithms used for this factorization are implemented for the factoring problem of an odd integer $n \in \mathbb{N}$, where n is a product of two odd primes q_1 and q_2, since we concentrated on the theory of prime quaternions and quaternions that are the product of two prime quaternions. And since q_1 and q_2 are both odd, the theory of the Lipschitz ring is sufficient for all computations, and therefore all written algorithms are constructed for the Lipschitz integers in $\mathcal{L}$.

6.3.1 Factorization algorithm

The algorithm we will present in this section is based on results of Lemmas 6.1.6 and 6.2.1. So let be $n \in \mathbb{N}$ an odd integer such that $n = q_1 q_2$, where $q_1 > q_2 > 2$ odd primes.

Recall the notations from Sections 6.1 and 6.2 of quaternions $\eta^{(0)} = \alpha^{(0)}\beta^{(0)} = \gamma^{(0)}\delta^{(0)}$, where $N(\alpha^{(0)}) = N(\delta^{(0)}) = q_1$ and $N(\beta^{(0)}) = N(\gamma^{(0)}) = q_2$. Then we can describe the factorization algorithm as follows:

1. Construct a quaternion $\eta^{(0)}$, where $N(\eta^{(0)}) = n$, using the random probabilistic algorithm described in the Section 5.2.

2. Choose randomly a prime integer p such that $\gcd(n,p) = 1$ and, using the same random probabilistic algorithm described in the Section 5.2, construct a prime quaternion π, where $N(\pi) = p$. If π is periodical, then construct the new quaternion π. Otherwise go to the next point.

3. Compute a new quaternion $\eta^{(l)}$ by commutating $\eta^{(l-1)}$ with π from the right, i.e. compute $\eta^{(l)} = \operatorname{gcrd}\left(\eta^{(l-1)}\pi, N(\eta^{(0)})\right)$, for $l \in \{1, 2, \ldots\}$.
   Then compute $\phi = \operatorname{gcrd}\left(\eta^{(l)}, \eta^{(0)}\right)$. If $N(\phi)$ is a non-trivial divisor of n, then we are done. If $N(\phi) = n$, then start the algorithm from the second point.
   Otherwise, repeat the last point of this algorithm.

So let be $n \in \mathbb{N}$ a positive odd integer, where n is a product of two odd primes q_1 and q_2. Note that we want to find q_1 and q_2.

First we construct a quaternion $\eta^{(0)}$ with $N(\eta^{(0)}) = n$ using the random probabilistic algorithm described in the Section 5.2. Note that this Algorithm can already find a non-trivial factor of n, in which case we are already done. But in most cases, it returns a

quaternion $\eta^{(0)}$. And from Section 5.2 we know that this algorithm returns a solution in polynomial time. Recall that $\eta^{(0)} = \alpha^{(0)}\beta^{(0)} = \gamma^{(0)}\delta^{(0)}$ has two factorizations, where $N(\alpha^{(0)}) = N(\delta^{(0)}) = q_1$ and $N(\beta^{(0)}) = N(\gamma^{(0)}) = q_2$.

In the second point of this algorithm we choose randomly a prime integer $p \leq b$, where $b \in \mathbb{N}$ is fixed upper bound for p. In general, there is no optimal size of this bound b. In most tests of this algorithm, we set $b = n$ or $b = \sqrt{n}$.

Remark 6.3.1. Consider that finding sufficiently large prime numbers p is in general a hard task. But we can randomly generate a number we can test if it is a prime with large probability. For that, first consider the Fermat Test, which tests if p is not a prime. After s times of testing, if p is not a prime, we can say that p is a prime with a probability bigger then $1 - (1/2)^s$. And by the theorem of prime numbers, which states that

$$\lim_{x\to\infty} \frac{\Pi(x)}{x/\log x} = 1, \tag{6.34}$$

where $\Pi(x)$ is the number of primes in the interval $[1, x]$, we know that there is high probability to find a prime number p by randomly choosing integers from the interval $[1, x]$.

The exact proof of the Fermat Test and of the theory of prime numbers can be looked up in [9].

Note that it is already known that finding such a prime can be done in polynomial time. Then construct a prime quaternion π with $N(\pi) = p$ using the same random probabilistic algorithm as before. In general, we can use an already constructed quaternion π, in which case we do not need any steps for constructing such a quaternion. Anyway, we can let the algorithm construct a prime quaternion π in polynomial time.

In the next part, we are starting with factorization. Recall the Lemmas 6.1.6 and 6.2.1. We see that after exactly e times commutating $\eta^{(l)}$ with prime quaternion π, where $e = \min\{\mathrm{ord}\langle\beta^{(0)}, \pi\rangle, \mathrm{ord}\langle\delta^{(0)}, \pi\rangle\}$, we will have the greatest common right divisor of $\eta^{(0)}$ and $\eta^{(e)}$ that is different from 1. But since we do not know how big the order e is, we have to compute all quaternions $\eta^{(l)}$ and to test if $\mathrm{gcrd}\big(\eta^{(0)}, \eta^{(l)}\big)$ is not a unit for $l \in \{1, 2, \ldots, e\}$. Note that the norm of the greatest common right divisor of $\eta^{(0)}$ and $\eta^{(e)}$ can also be equal n, but there is a very small probability that this will happen. Anyway, if this is the case, generate a new prime quaternion π and repeat the third point of the algorithm again.

So we will execute the third point of this algorithm exactly e times. And each time, we have to multiply $\eta^{(l-1)}$ and π and we have to compute twice the greatest common right divisor. Recall that we can compute g.c.r.d. in polynomial time.

From the discussion above we see that all operations can be done in polynomial time. Only we do not know how often we have to execute the third point of this algorithm. So recall that Lemma 6.1.6 states that the order of $\langle\beta^{(0)}, \pi\rangle$ is at most $N(\beta^{(0)}) + 1 = q_2 + 1$, meaning that we can only make the estimation that $e \leq q_2 + 1 < \sqrt{n}$, where q_2 is the value of the smaller norm of those two prime quaternions. And recall the experimental results from the discussion of orders of $\langle\beta^{(0)}, \pi\rangle$, where $\beta^{(0)}$ is a prime factor of $\eta^{(0)}$ with a smaller norm. We have seen that for one fixed prime quaternion π, that order e is about $\frac{q_2}{2}$ on average. In the worst case, the factorization algorithm will execute the third point e times so that we can estimate only to the $\sqrt{n}$, which implies that the order $q_2 + 1$ is growing proportionally with n and this factorization algorithm does not work in polynomial time.

To improve this factorization method we should try to predict the order e for a given problem or try to find π such that the order e is smaller then $\log_2 n$. Anyway, there are still some open questions about periodical quaternions and about in which way the elements $\alpha^{(0)}$, $\alpha^{(1)}$, $\alpha^{(2)}, \ldots$ are ordered, i. e. the elements of the set $\langle\alpha^{(0)}, \pi\rangle$, for some prime $\alpha^{(0)}$.

6.3.2 Probabilistic algorithms

In Section 6.1, we discussed the order of the set $\langle \alpha^{(0)}, \pi \rangle$ and the elements of the same set. Unfortunately, we were not able to explain or prove any of the results we saw there. Anyway, there are still some interesting experimental results about the magnitude of the order by choosing different prime quaternions π or how the elements of the set $\langle \alpha^{(0)}, \pi \rangle$ were sorted. All those results are leaving questions if there are probabilistic algorithms based on this results that maybe give us the wanted quaternions in only several steps.

As we saw in the discussion about the elements in the set $\langle \alpha^{(0)}, \pi \rangle$, the elements of the same structure seem to appear in a certain order that repeats itself independently of the length of the sequence for some sufficiently large $\mathrm{ord}\langle \alpha^{(0)}, \pi \rangle = e$. This means that the right factor of the quaternion $\eta^{(l_1)}$ will behave in the same way. In other words, we could generate a small group of the sequence $\eta^{(0)}$, $\eta^{(1)}, \ldots, \eta^{(m)}$, where m is a small integer. Then, using the property of Lemma 6.2.3 and associate quaternions, we can construct a new group of quaternions of the same structure to the one of $\eta^{(0)}$, $\eta^{(1)}, \ldots, \eta^{(m)}$. Then, by commuting the new quaternions by π or $\overline{\pi}$, there exists a chance to find a quaternion $\tilde{\eta}$ such that $\tilde{\eta}$ has a non-trivial right divisor with some of the quaternions in the sequence $\eta^{(0)}$, $\eta^{(1)}, \ldots, \eta^{(m)}$.

The experimental results have shown that this method gives a solution right away for the smaller prime factors. But when the norm of the factors gets bigger than 10^5, this method does not return a solution. Anyway, we were not able to prove any of the results according to this method.

Appendix A

Quadratic reciprocity

On several occasions, we wanted to know, if an element is a quadratic residue in some field $\mathbb{F}_p$, where p is an odd prime, for example in the Theorem 2.2.1 we wanted to know, when is -1 a square residue in $\mathbb{Z}_p$. Later, in some proofs of correctness of the algorithms for computing presentations of four squares, we were asking ourselves a more general question, what elements in $\mathbb{Z}_p$ are square residues? And we were using the Legendre symbol for this problem.

Quadratic reciprocity deals with this question, and here we will mention some basic statements.

Let be p an odd prime. We say that an integer m is a quadratic residue modulo p if it is congruent to the perfect square modulo p. This means that m is a quadratic residue modulo p if there exists an integer x such that $x^2 \equiv m \bmod p$. Now we can define the Legendre symbol.

Definition A.0.2 (Legendre symbol)**.** Let be p an odd prime and m an integer. Legendre symbol is then defined as

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } m \\ 1 & \text{if } p \text{ does not divides } m \text{ and } m \text{ is a square modulo } p \\ -1 & \text{if } p \text{ does not divides } m \text{ and } m \text{ is not a square modulo } p \end{cases} \tag{A.1}$$

Now we will state some useful lemma and theorem without proving them.

Lemma A.0.3. For any $n \in \mathbb{Z}$, then is $n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \bmod p$.

Theorem A.0.4. Let be p an odd prime. Then

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. if q is an odd prime distinct from p, then $\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$.

Appendix B

Vector Product

Consider two quaternions $a = a_1 + a_2 i + a_3 j + a_4 k$ and $b = b_1 + b_2 i + b_3 j + b_4 k$ with their vector parts $\tilde{a} = a_2 i + a_3 j + a_4 k$ and $\tilde{b} = b_2 i + b_3 j + b_4 k$ or written as vectors

$$\tilde{a} = \begin{pmatrix} a_2 \\ a_3 \\ a_4 \end{pmatrix}, \quad \tilde{b} = \begin{pmatrix} b_2 \\ b_3 \\ b_4 \end{pmatrix} \tag{B.1}$$

and consider the base vectors in $\mathbb{R}^3$

$$i = e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad j = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad k = e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \tag{B.2}$$

Then we can easily determinate from the standard vector product that

$$i \times j = k \quad j \times i = -k \tag{B.3}$$
$$j \times k = i \quad k \times j = -i \tag{B.4}$$
$$k \times i = j \quad i \times k = -j, \tag{B.5}$$

where i, j, k are considered basic vectors, and we can also determinate that

$$i \times i = j \times j = k \times k = 0. \tag{B.6}$$

And then we can also compute the vector product for

$$\begin{aligned} \tilde{a} \times \tilde{b} &= \begin{vmatrix} i & j & k \\ a_2 & a_3 & a_4 \\ b_2 & b_3 & b_4 \end{vmatrix} \\ &= \begin{vmatrix} a_3 & a_4 \\ b_3 & b_4 \end{vmatrix} i - \begin{vmatrix} a_2 & a_4 \\ b_2 & b_4 \end{vmatrix} j + \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} k \\ &= (a_3 b_4 - a_4 b_3)\, i + (a_4 b_2 - a_2 b_4)\, j + (a_2 b_3 - a_3 b_2)\, k, \end{aligned} \tag{B.7}$$

where $|\cdot|$ stands for determinate of the matrix and i, j and k are the imaginary numbers as in Definition 3.1.1. Consider also that

$$\tilde{a} \times \tilde{b} = -\tilde{b} \times \tilde{a}. \tag{B.8}$$

Appendix C

Lagrange's Theorem

In this chapter we will state Lagrange's theorem and prove that every natural number $n \in \mathbb{N}$ is a sum of four squares.

In the first part, we want to prove that if we can present every prime factor of a positive integer $n \in \mathbb{N}$ as a sum of four squares, we can also present the whole number n as a sum of four squares.

In second part we want to prove that we can present every prime number p as sum of four squares.

So first consider the following Euler's identity:

$$\begin{aligned}\left(x_1^2+x_2^2+x_3^2+x_4^2\right)\left(y_1^2+y_2^2+y_3^2+y_4^2\right) = \\ &(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ &+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ &+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2 \\ &+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\end{aligned} \tag{C.1}$$

Remark C.0.5. It is easy to verify the equation C.1 by expanding both sides of the equality.

From this identity is clear that the product of two numbers that are the sum of four squares is again the sum of four squares. So now we only have to prove that prime integers are the sum of four squares.

Consider the prime integer $p = 2$. From the equation $1^2 + 1^2 + 0^2 + 0^2 = 2$, we see that 2 is a sum of four squares.

The proof that any prime integer $p > 2$ is a sum of four squares, will need a bit more work.

Lemma C.0.6. If $p \in \mathbb{N}$ is an odd prime, then we can find integers x, y and m such that

$$1 + x^2 + y^2 = mp, \quad 0 < m < p. \tag{C.2}$$

Proof. Consider the set $S = \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$, and assume that there exist x_1, $x_2 \in S$, where $x_1 \neq x_2$, such that $x_1^2 \equiv x_2^2 \bmod p$. Then the following holds:

$$p|(x_1 - x_2)(x_1 + x_2) \Rightarrow x_1 \equiv \pm x_2 \bmod p. \tag{C.3}$$

But this is a contradiction since x_1, $x_2 < \frac{p}{2}$. This means that for all $x \in S$, we will have $\frac{p+1}{2}$ different values x^2's, that are pairwise not congruent modulo p.

In the same way, we can show that for every $y \in S$, we will have $\frac{p+1}{2}$ different values $-1 - y^2$, where all of them are pairwise not congruent modulo p.

Now consider those two sets of the residues obtained by x^2 and $-1-y^2$ modulo p. Then there are all together $p+1$ residues of x^2 and $-1-y^2$ modulo p for all x, $y \in S$, but only p different possible residues. This means that there must exist at least one x and y in S such that

$$x^2 \equiv -1 - y^2 \bmod p \quad \Rightarrow \quad 1 + x^2 + y^2 \equiv 0 \bmod p. \tag{C.4}$$

And this equation implies that there exists $m \in \mathbb{N}$ such that $1 + x^2 + y^2 = mp$.

Note $x^2 < (p/2)^2$ and $y^2 < (p/2)^2$. Then follows

$$mp = 1 + x^2 + y^2 < 1 + (p/2)^2 + (p/2)^2 < p^2 \quad \Rightarrow \quad m < p. \tag{C.5}$$

and this proves the lemma. □

Now we know from Lemma C.0.6 that any odd prime p can be presented in the form $mp = 1 + x^2 + y^2$, where m,x,$y \in \mathbb{N}$. In other words, for any prime integer p, there exist m, x_1, x_2, x_3, $x_4 \in \mathbb{N}$ such that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \tag{C.6}$$

Corollary C.0.7. Consider the equation (C.6). The smallest $m > 0$, where the positive integers x_1, x_2, x_3, $x_4 \in \mathbb{N}$ exist such that $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ holds, is $m = 1$.

Proof. Let be such a smallest m denoted with m_0 and suppose that $1 < m_0 < p$.

First assume that m_0 is even. Then either all x_s's are even, or two of them are even and two are odd, or all x_s's are odd.

Without loss of generality let be x_1 and x_2 even in all first three cases. Then in all four cases $x_1 \pm x_2$ and $x_3 \pm x_4$ are always even and we can compute that

$$\frac{m_0}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2. \tag{C.7}$$

But then m_0 is not the smallest $m > 0$, which is a contradiction to the first assumption.

Now assume that m_0 is an odd number. Then we can choose $y_s \in \mathbb{Z}$ such that

$$y_s \equiv x_s \bmod m_0, \qquad |y_s| < \frac{m_0}{2} \tag{C.8}$$

There always exit such $y_1, \ldots, y_4$, since all residues of $x_s \bmod m_0$ are between the values $-\frac{m_0-1}{2} \leq y_s \leq \frac{m_0-1}{2}$. Also consider that not all x_s's are divisible by m_0, otherwise we would have

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0^2 \left(\left(\frac{x_1}{m_0}\right)^2 + \left(\frac{x_2}{m_0}\right)^2 + \left(\frac{x_3}{m_0}\right)^2 + \left(\frac{x_4}{m_0}\right)^2 \right), \tag{C.9}$$

and therefore $m_0^2 | m_0 p \Rightarrow m_0 | p$, which would be a contradiction. So we have

$$\sum_{s=1}^{4} y_s^2 < m_0^2, \quad \text{and} \quad \sum_{s=1}^{4} y_s^2 \equiv 0 \bmod m_0. \tag{C.10}$$

This means that there exists a $m_1 \in \mathbb{N}$ such that $m_1 < m_0$ and

$$\sum_{s=1}^{4} y_s^2 = m_1 m_0. \tag{C.11}$$

By multiplying the equations (C.6) and (C.11) we get

$$\sum_{s=1}^{4} y_s^2 \cdot \sum_{s=1}^{4} x_s^2 = m_1 m_0 \cdot m_0 p = m_1 m_0^2 p = \sum_{s=1}^{4} z_s^2, \tag{C.12}$$

where the z_s's correspond to the brackets of the right side of Euler's identity.

Consider the equation (C.8) and the equations z_s. Then

$$\begin{aligned}
z_1 &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \equiv (x_1x_1 + x_2x_2 + x_3x_3 + x_4x_4)^2 \equiv 0 \bmod m_0 \\
z_2 &= (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \equiv (x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3)^2 \equiv 0 \bmod m_0 \\
z_3 &= (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \equiv (x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4)^2 \equiv 0 \bmod m_0 \\
z_4 &= (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2 \equiv (x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2)^2 \equiv 0 \bmod m_0.
\end{aligned}$$

Since $z_s \equiv 0 \bmod m_0$ for all s's, we can write $z_s = m_0w_s$ and get the following

$$\sum_{s=1}^{4} z_s^2 = m_0^2 \sum_{s=1}^{4} w_s^2 = m_1 m_0^2 p \Rightarrow m_1 p = \sum_{s=1}^{4} w_s^2, \tag{C.13}$$

which is a contradiction to the assumption that m_0 is the smallest integer that satisfies the equation (C.6).

So it follows, that smallest m that satisfies equation (C.6) has to be $m_0 = 1$. □

And now we are coming to the main result of Lagrange.

Theorem C.0.8 (Lagrange's Theorem)**.** Every positive integer $n \in \mathbb{N}$ is the sum of four squares.

Proof of Lagrange's Theorem. Let be $n \in \mathbb{N}$ a positive integer with prime factorization $n = \prod_l p_l$. From the theory above, we know that any prime $p_l = 2 = 1^2 + 1^2 + 0^2 + 0^2$ is a sum of four squares and by Corollary C.0.7 every odd prime p_l is also a sum of four squares. By Euler's identity, we get that $n = \prod_l p_l$ is a sum of four squares too. □

Appendix D

Probabilistic algorithms in finite fields

This paper is about probabilistic algorithms of finding an irreducible polynomial, roots of polynomial and factoring polynomial over a finite field.

The question here is, for a given prime p and an integer n, how do we perform an arithmetic operation of $\mathbb{F}_q$ where $q = p^n$. And this paper lists a theorem [Theorem 4] that solves the root finding problem for $f \in \mathbb{F}_q$. I will use that theorem to prove the efficiency of computing a presentation as a sum of two squares for some given number. The probabilistic nature of those algorithms for finding such solutions does not detract from their practical applicability. The main idea of this probabilistic step is a random choice of an element $b \in \mathbb{F}_q$ that then splits a polynomial f in to two factors. Here it shows that for any given field and the fixed f, the probability of finding the solution is at least half.

D.1 Arithmetic of $\mathbb{F}_q$

In this section, there is one idea of representation of arithmetic in an arbitrary finite field and a random probabilistic algorithm for computing irreducible polynomial in $\mathbb{Z}_p[x]$.

Consider the usual Number Theory notations for $p, n, q, \mathbb{F}_q, \mathbb{Z}_p, g(x), (g)$ where the polynomial $g(x) \in \mathbb{Z}_p[x]$ an irreducible polynomial of degree n, (g) an ideal generated by $g(x)$. Consider that $\mathbb{F}_p = \mathbb{Z}_p$, $\mathbb{F}_q \approx \mathbb{Z}_p/(g)$.

Given such an irreducible polynomial $g(x)$, the elements in $\mathbb{F}_q$ can be written as n-tuples of elements in $\mathbb{Z}_p$. Consider two elements $b = (b_{n-1}, \ldots, b_0)$ and $c = (c_{n-1}, \ldots, c_0)$. Then the addition is component wise. For the multiplication, consider the product

$$\left(b_{n-1}x^{n-1} + \cdots + b_0\right)\left(c_{n-1}x^{n-1} + \cdots + c_0\right). \tag{D.1}$$

So find the residue $d(x) = \left(d_{n-1}x^{n-1} + \cdots + d_0\right)$ of the product (D.1) when divided by $g(x)$. Then $b \cdot c = (d_{n-1}, \ldots, d_0)$.

Now, for finding an irreducible polynomial $g(x) \in \mathbb{Z}_p[X]$ and to see how fast we can find it, we need the following two lemmas.

Lemma D.1.1. Let $l_1, \ldots, l_k$ be all prime factors of n and denote $m_i = n/l_i$. A polynomial $g(x) \in \mathbb{Z}_p[X]$ of degree n is irreducible in $\mathbb{Z}_p[X]$ if and only if

$$g(x) \mid \left(x^{p^n} - x\right), \tag{D.2}$$

$$\gcd\left(g(x), x^{p^{m_i}} - x\right) = 1, \qquad 1 \le i \le k \tag{D.3}$$

Lemma D.1.2. Denote by $m(n)$ the number of different monic polynomials in $\mathbb{Z}_p[X]$ of degree n which are irreducible. Then

$$\frac{p^n - p^{n/2}\log n}{n} \le m(n) \le \frac{p^n}{n} \tag{D.4}$$

$$\frac{1}{2n} \leq \frac{m(n)}{p^n} \sim \frac{1}{n} \tag{D.5}$$

Note that the number of all monic polynomials of degree n is p^n.

The algorithm for finding irreducible polynomials goes as follows: First we choose a polynomial $g(x)$ randomly and test it if it is irreducible. Continue so until an irreducible polynomial of degree n is found. By Lemma D.1.2 we see that we will need about n attempts to find such a polynomial. By computing exactly the number of basic operations in $\mathbb{Z}_p$ to check if the chosen polynomial is irreducible, we need $\mathcal{O}(n^2 \log nL(n) \cdot \log p)$ operations. (As it is shown in this paper, I will not go further checking if it is so. But I suppose they got better bound in last 20 years:)) And because we will probably have to check n such polynomials, we have the bound $\mathcal{O}(n^3 \log nL(n) \cdot \log p)$.

D.2 Root finding in $\mathbb{F}_q$

In this part, we are giving an algorithm that finds the roots for a given polynomial $f(x) \in \mathbb{Z}_p[X]$.

Assume in this case that $q = p$ is odd. This is enough for what we need. Consider the polynomial $f(x) \in \mathbb{Z}_p[X]$, for which we want to find one or all roots $r \in \mathbb{Z}_p$, i.e. $f(r) = 0$.

Let define $f_1(x) = \gcd\left(f(x), x^{p-1} - 1\right)$. In the first case, if $f_1(x) = 1$, we know that $f(x)$ has no roots in $\mathbb{Z}_p$ and we do not have to compute any roots. But now, we want to consider another case where $f_1(x) \neq 1$. So let be

$$f_1(x) = (x - r_1) \dots (x - r_k) \quad k \leq m \tag{D.6}$$

where the r_i's are all the pairwise different roots of the polynomial $f(x)$ in $\mathbb{Z}_p$. By computing such polynomials, we still do not have the linear polynomial $x - r_i$, i.e. computed at one root of a polynomial. But now we can write $\left(x^{q-1} - 1\right) = \left(x^{(q-1)/2} - 1\right)\left(x^{(q-1)/2} + 1\right)$ and then compute a $\gcd\left(f_1(x), \left(x^{(q-1)/2} - 1\right)\right)$. Then some of the roots could be in $\left(x^{(q-1)/2} - 1\right)$ and others in $\left(x^{(q-1)/2} + 1\right)$, and so we get closer to our solution. But still we are not sure that we will get the gcd different from 1 or $f(x)_1$. However, this situation can be simulated by a randomized algorithm. For that define, let be $a, b \in \mathbb{Z}_p$, where $a, b \neq 0$. Then we say that a and b are of a different type if $a^d \neq b^d$, where $d = (q-1)/2$.

Theorem D.2.1. Let be $a, b \in \mathbb{Z}_p$, $a \neq b$. Then

$$|\{c | c \in \mathbb{Z}_p, a + c \text{ and } b + c \text{ are of a different type}\}| = 1/2(p-1) \tag{D.7}$$

Proof. The elements $a + c$ and $b + c$ are of a different type if and only if neither of them is zero and if

$$\left(\frac{a+c}{b+c}\right)^d \neq 1, \quad \text{because } \left(\frac{a+c}{b+c}\right)^d = -1 \tag{D.8}$$

The equation (D.8) has exactly d solutions in $\mathbb{Z}_p$. Consider the isomorph mapping $\phi(c) = (a + c)/(b + c)$. As the c goes through all elements of $\mathbb{Z}_p$ except $-b$, so $\phi(c)$ goes through all values of $\mathbb{Z}_p$ except 1. So we see that $\phi(c)^d = -1$ for exactly d different values. And this proves the theorem. □

Corollary D.2.2. Consider for $c \in \mathbb{Z}_p$, $f_c(x) = \gcd\left(f_1(x), (x + c)^d - 1\right)$. We have

$$\Pr\left(c | 0 < \deg f_c(x) < \deg f_1\right) \geq \frac{1}{2} \tag{D.9}$$

Proof. The common roots of both polynomials in the gcd are r_i's such that both polynomials get zero for those values. By the Theorem D.2.1, we see that with probability 1/2 $a + c$ or $b + c$ will have that property and another will not. This proves the corollary. □

Note that apparently Michel O. Rabin has got the probability of near $1 - \frac{1}{2^k}$, where $k = \deg f_1$, but could not prove it.

Finally we are coming to the **root-finding algorithm**. For a given $f(x)$ of degree m, compute the polynomial $f_1(x)$. Choose $c \in \mathbb{Z}_p$ randomly and compute $f_c(x)$. If $0 < \deg f_c(x) < \deg f_1(x)$, then set $f_2(x) = f_c(x)$ or $f_2(x) = f_1(x)/f_c(x)$ depending on whether $\deg f_c < 1/2 \deg f_1$ or not. If $f_c \in \{1, f_1\}$ then choose another c and repeat the previous step. By the Corollary (D.2.2), we see that the expected number for choosing c is less then two. Since the degree of f_j for $j \in \{1, 2, \ldots\}$ is always at least half of the previous degree of polynomial f_{j-1}, we see that we need at most $\log m$ steps till we find a linear factor $x + r_i$ for some root r_i.

So by analyzing the algorithm, fort finding a root in a finite field $\mathbb{Z}_p$, we require

$$\mathcal{O}\left(n^2 \cdot mL(m)L(n)\log p\right) \tag{D.10}$$

basic arithmetic operations in $\mathbb{Z}_p$. The $L(n)$ stands for the number of basic operations for multiplication or division of the numbers of the size n.

Appendix E

Algorithms

In this chapter, we will present various small algorithms we used for computing four square presentation, finding the factors of an integer n and estimating some experimental results for this thesis. Each section stands for a file where all listed methods were defined.

Note that all presented algorithms in this chapter are constructed for Lipschitz integers and all computations are done in a Lipschitz ring. Recall that we have constructed all these algorithms to find the prime factors of n, where n is an odd product of two odd prime integers, i.e. $n = q_1 q_2$ for q_1 and q_2 odd primes. In other words, we will do all computations with quaternion $\eta^{(0)}$, where $N(\eta^{(0)}) = n$ is odd, i.e. $\eta^{(0)}$ is odd and we can construct an Euclidean algorithm that holds in the Lipschitz ring. And therefore the described algorithms below are enough for all computations we need, and Hurwitz integers are not needed.

E.1 All algorithms used for quaternion computations

In this section we will describe all algorithms or methods we need to construct quaternions and do all computations with them.

The first line defines the quaternion algebra over rational numbers, where the following holds: $i^2 = j^2 = -1$ and $ij = k$.

```
Q.<i,j,k>=QuaternionAlgebra(QQ,-1,-1)
```

The next method tests if two quaternions are of the same structure.

```
def isSameStructure(q1,q2):

    [q1a1,q1a2,q1a3,q1a4]=q1.coefficient_tuple()
    [q1a1,q1a2,q1a3,q1a4]=[abs(q1a1),abs(q1a2),abs(q1a3),abs(q1a4)]

    [q2a1,q2a2,q2a3,q2a4]=q2.coefficient_tuple()
    [q2a1,q2a2,q2a3,q2a4]=[abs(q2a1),abs(q2a2),abs(q2a3),abs(q2a4)]

    SameStruc=True
    for l in [q1a1,q1a2,q1a3,q1a4]:
        SameStruc = (SameStruc) and (l in [q2a1,q2a2,q2a3,q2a4])

    return SameStruc
```

The following two methods return the set of four right- respectively left-associates of a quaternion. Consider that other four right- respectively left-associates are just negative quaternions of the returned set.

```
def RightAssociates(q):
    return [q,q*i,q*j,q*k]

```

```
def LeftAssociates(q):
    return [q,i*q,j*q,k*q]
```

The next method returns the set of all coefficient permutations and sign changes of a quaternion α. This means it returns the set of all quaternions that are of the same structure to quaternion α, i.e. it returns the set $\mathfrak{E}_\alpha$.

```
def QuatPermutations(q):


    [q1a1,q1a2,q1a3,q1a4]=q.coefficient_tuple()

    listq11=Permutation([q1a1,q1a2,q1a3,q1a4],[])
    listq12=Ssigns(listq11)
    listq13=MakeQuaternions(listq12)
    return listq13
```

The next three methods return the set of all coefficient permutations and sign changes of a quaternion α, which are pairwise not left-associated, resp. not right-associated, resp. not associated at all.

```
def QuatPermutationsLeft(q):

    list=QuatPermutations(q)
    newlist=[list[0]]
    for l in list:
        InTheList=False
        for ll in newlist:
            if isLeftAssociate(l,ll):
                InTheList=True
                break
        if not InTheList:
            newlist+=[l]
    return newlist

def QuatPermutationsRight(q):

    list=QuatPermutations(q)
    newlist=[list[0]]
    for l in list:
        InTheList=False
        for ll in newlist:
            if isRightAssociate(l,ll):
                InTheList=True
                break
        if not InTheList:
            newlist+=[l]
    return newlist

def QuatPermutationsNotAssoc(q):

    list=QuatPermutations(q)
    newlist=[list[0]]
    for l in list:
        InTheList=False
        for ll in newlist:
            if isAssociate(l,ll):
                InTheList=True
                break
            if not InTheList:
                newlist+=[l]
```

```
41      return newlist
```

Consider that the last method above is equal to set $\mathfrak{S}_\alpha$. The next three methods are algorithms used by the method QuatPermutations(q).

The first method constructs all possible pairwise different permutation of coefficients of the given quaternion.

The second method constructs all possible pairwise different sign changes for given coefficients. Note that in the case of the method QuatPermutations(q), the Ssigns(list) computes such sign changes for each coefficient permutation for a given quaternion.

And the third method constructs the quaternions from the given list of coefficients.

```
1  def Permutation(a,b):
2
3      didThat=[]
4      coeff=deepcopy(a)
5      newcoeff=deepcopy(a)
6      result=deepcopy(b)
7      list=[]
8
9
10     for l in xrange(len(coeff)):
11         coeff[l]=abs(coeff[l])
12
13     if len(coeff)==1:
14         result=result+[coeff[0]]
15         list =list+[result]
16         return list
17
18     if len(coeff)>1:
19         for ll in xrange(len(coeff)):
20             result=deepcopy(b)
21
22             if not coeff[ll] in didThat:
23                 result=result+[coeff[ll]]
24                 didThat=didThat+[coeff[ll]]
25                 del newcoeff[ll]
26                 list =list+Permutation(newcoeff, result)
27                 newcoeff=deepcopy(a)
28
29         return list
30
31 def Ssigns(list):
32
33     result=[]
34     for tuple in list:
35         sum=0
36         sign=[]
37
38         for l in tuple:
39             if l!=0:
40                 sign=sign+[0]
41                 sum+=1
42             else:
43                 sign=sign+[-1]
44
45         result=result+[tuple]
46
47         for lll in xrange(1,2**sum):
48                 NotDone= True
49                 count=0
```

```
                while (NotDone):
                    if sign[count]>=0:
                        sign[count]=(sign[count]+1)%2
                        if sign[count]==1:
                            NotDone= False
                    count+=1
                newtuple=[]
                for ll in xrange(len(sign)):
                    if sign[ll]>=0:
                        newtuple = newtuple +
                           [tuple[ll]*((-1)**sign[ll])]
                    else:
                        newtuple=newtuple+[0]
                result=result+[newtuple]

    return result

def MakeQuaternions(list):

    result=[]
    for l in list:
        r=Q(l)
        result=result+[r]

    return result
```

The next method returns the scalar product of two quaternions α and β, i.e. returns $a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4$, where $\alpha = a_1 + a_2i + a_3j + a_4k$ and $\beta = b_1 + b_2i + b_3j + b_4k$.

```
def scalarProd(a,b):

    coeffa=a.coefficient_tuple()
    coeffb=b.coefficient_tuple()
    result=coeffa[0]*coeffb[0] + coeffa[1]*coeffb[1] +
       coeffa[2]*coeffb[2] + coeffa[3]*coeffb[3]
    return result
```

The next three methods test two quaternions α and β if they are respectively left-associates, right-associates or associates, and returns "True" if they are, otherwise returns "False".

```
def isLeftAssociate(a,b):


    list=[1,i,j,k]

    for l in list:
        if a==(l*b):
            return True
        if a==(-1*l*b):
            return True

    return False

def isRightAssociate(a,b):

    list=[1,i,j,k]

    for l in list:
        if a==(b*l):
            return True
        if a==(-1*b*l):
```

```
            return True

    return False

def isAssociate(a,b):

    list=[1,i,j,k]

    for l1 in list:
        for l2 in list:
            if a==(l1*b*l2):
                return True
            if a==(-1*l1*b*l2):
                return True

    return False
```

The next two methods are actually the statement of Lemma 3.2.18. So for two given quaternions α and β, where at least one of them is odd, these methods return the quaternions γ and τ such that $\alpha = \beta\gamma + \tau$ (resp. $\alpha = \gamma\beta + \tau$).

```
def EuclidianRightDom(a,b):

    a=Q(a)
    b=Q(b)
    c=a*b.conjugate()/b.reduced_norm()
    coeff=c.coefficient_tuple()
    gamma =round(coeff[0]) + round(coeff[1])*i + round(coeff[2])*j
       + round(coeff[3])*k
    tau=a-(gamma*b)
    return (gamma,tau)

def EuclidianLeftDom(a,b):

    a=Q(a)
    b=Q(b)
    c=(b.conjugate()*a)/b.reduced_norm()
    coeff=c.coefficient_tuple()
    gamma =round(coeff[0]) + round(coeff[1])*i + round(coeff[2])*j
       + round(coeff[3])*k
    tau=a-(b*gamma)
    return (gamma,tau)
```

And now we present the two methods that compute the greatest common right (resp. left) divisor of two quaternions α and β. In particular, the following methods are the statement of Theorem 3.2.23 and the usual euclidean algorithm. Note that these methods only compute the greatest common divisor and not the quaternions γ and δ such that $\text{gcrd}(\alpha, \beta) = \gamma\alpha + \delta\beta$ (resp. $\text{gcld}(\alpha, \beta) = \alpha\gamma + \beta\delta$) since we never use those values.

```
def GCRD(a,b):
    tau = 1
    while tau!=0:
        (gamma,tau)=EuclidianRightDom(a,b)
        a,b=b,tau
    return a


def GCLD(a,b):
    tau = 1
    while tau!=0:
        (gamma,tau)=EuclidianLeftDom(a,b)
```

```
13          a,b=b,tau
14      return a
```

The method "BinaryExp(x, e, m)", where x, e, $m \in \mathbb{N}$, is usual square and multiply method for computing $x^e \bmod m$ in polynomial time. We use this method only to quickly compute values in the methods below, like for example in method "isPrime(p)".

```
1  def BinaryExp(x, exp, m):
2
3      result=1
4      while exp!=0:
5          if (exp%2)!=0:
6              result=(result*x)%m
7              exp-=1
8          x=(x**2)%m
9          exp/=2
10     return result
```

As we already mentioned above, the method "isPrime(p)" tests if a randomly chosen integer p is a prime. It is well known that for very large integers it is rather difficult to show that an integer is in fact a prime. We have some methods that can show with high probability that an integer is a prime. The method "isPrime(p)" uses the Fermat-Test described in [9], which either returns that integer p is not a prime or that it is a prime with probability $1 - 2^{-s}$, where s is the number of the repeated test.

```
1  def isPrime(p):
2      if p%2==0:
3          return False
4      elif p<=100:
5          for l in xrange(3, int(p**0.5)):
6              if (p%l)==0:
7                  return False
8          return True
9      for l in xrange(3, 100, 2):
10         if (p%l)==0:
11             return False
12     e=0
13     d=p-1
14     while d%2==0:
15         e+=1
16         d/=2
17     isPrime=True
18     count=0
19     while (isPrime) and (count<30):
20         count+=1
21         isPrime=False
22         a=ZZ.random_element(2, p)
23         if (p%a)==0:
24             return isPrime
25         x=BinaryExp(a, d, p)
26         if (x==1) or (x==(p-1)):
27             isPrime=True
28         for ll in xrange(e-1):
29             if isPrime:
30                 break
31             x=x**2%p
32             if x==(p-1):
33                 isPrime=True
34     return isPrime
```

The next two methods compute the solution for the problem $x^2 + y^2 = p$ for some prime number p. This is one of the methods how to compute the two square sums for a given prime integer p. It was presented in [10], but we did not discussed this method in this thesis. Anyway, we also presented this algorithm.

```
def gcdModified(a, b):
    sqrta=a**0.5
    r0=b
    r1=a%b
    if r1==1:
        return (b, 1)
    while r1 > sqrta:
        r0, r1 = r1, r0 % r1
    return (r1, r0%r1)


def SumOf2Sqrts(p):
    if (p%4)!=1:
        print 'No solution, p%4!=1.'
        return (p**0.5, 0)
    noSolution=True
    e2=(p-1)/2
    e4=(p-1)/4
    while noSolution:
        a=ZZ.random_element(1, p)
        b=BinaryExp(a, e2, p)
        if b==(p-1):
            result1=BinaryExp(a, e4, p)
            noSolution=False
    if result1>(p/2):
        result1=p-result1
    result2=gcdModified(p, result1)
    return result2
```

The following method "TwoSquaresSum(p)" is the algorithm that also computes a solution for two square problem for a prime integer p in polynomial time. This is the method that was presented by Michael O. Rabin and Jeffery O. Shallit in [3] and that we described in this thesis in Chapter 5.

```
def TwoSquaresSum(p):

    P.<t>=PolynomialRing(GF(p))
    k=(p-1)/2
    f=t**k-1
    noSolution=True
    while noSolution:

        b=ZZ.random_element(1,p)
        fb=(t-b)**2+1
        g=fb.gcd(f)

        if g!=1:
            ub=int(g[0])-p
            u1=(ub+b)
            u2=p+u1
            r1=(u1**2+1)
            r2=(u2**2+1)

            if (r1%p)==0:
                u=u1
                noSolution=False
```

```
23
24              if (r2%p)==0:
25                  u=u2
26                  noSolution=False
27
28      alpha=CDF(u,1)
29      beta=CDF(p,0)
30      if alpha.abs2()==p:
31          return abs(int(alpha[0])), abs(int(alpha[1]))
32
33      alpha=CompGcd(alpha,beta)
34      return int(alpha[0]), int(alpha[1])
```

The two methods "CompEuAlg(α, β)" and "CompGcd(α, β)" compute the greatest common divisor of two complex numbers α and β.

```
1  def CompEuAlg(alpha, beta):
2
3      if alpha.abs2()<beta.abs2():
4
5          a=alpha
6          alpha=beta
7          beta=a
8
9      g=alpha/beta
10     gamma1=floor(g[0]+0.5)
11     gamma2=floor(g[1]+0.5)
12     gamma=CDF(gamma1,gamma2)
13
14     tau=alpha-gamma*beta
15
16     alpha=beta
17     beta=tau
18     return alpha, beta
19
20 def CompGcd(alpha,beta):
21
22     while beta.abs2()!=0:
23         alpha,beta=CompEuAlg(alpha,beta)
24
25     return alpha
```

And finally, we are coming to the last method that computes the four square presentation for an integer n. It is the algorithm that was presented by Michael O. Rabin and Jeffery O. Shallit in [3] and described in Chapter 5. Note that in this thesis, we are mainly interested in the factorization of n. Since this algorithm can compute one of the factors, it is a program to stop at that point and return the factors, and it does not compute the four square presentation in this case. Consider that if n is an even integer, we can find at once the factor $f = 2$. Then this algorithm stops right away. So only in case n is odd and it does not stumble over an factor of n, this algorithm returns the four square presentation. Note that n is odd, so the norm of the wanted quaternion is also odd. This means that we can do all the computation in the Lipschitz ring and do not need the Hurwitz integers.

```
1  def SumOf4Sqrts(n):
2
3      if n%2==0:
4          e=0
5          while n%2==0:
6              n/=2
7              e+=1
8          print 'We␣found␣a␣factor␣of␣n'
```

```
        return n

    sn=int(n**(0.5))
    noSolution=True
    while noSolution:
        w=ZZ.random_element(1,sn)
        z=ZZ.random_element(1,sn)
        r=(w**2+z**2)%n
        gcd,invertr,nothing = XGCD(r, n)
        p=n-r
        if (gcd!=1) and (gcd!=n):
            print "We found a factor of n."
            return gcd
        if (isPrime(p)) and ((p)%4==1):
            [u, v]=TwoSquaresSum(p)
            x=(u*w+v*z)*(invertr)%n
            y=(v*w-u*z)*(invertr)%n
            noSolution=False
    qq=x+y*i+j
    q=GCRD(qq, Q(n))
    if (q.reduced_norm()!=n) and (q.reduced_norm()!=1):
        print "We found a factor of n diferent from 1 and n."
        return q.reduced_norm()/n
    return q
```

E.2 Some additional algorithms

This section lists some additional methods that were programmed for analyzing the elements and the order of the set $\langle \alpha, \pi \rangle$, where $\alpha, \pi \in \mathcal{L}$ are primes.

The first method generates the set $\langle \alpha, \pi \rangle$.

```
def Se(alpha,pi):

    normAlpha=alpha.reduced_norm()
    normPi=pi.reduced_norm()
    newAlpha=Q(alpha)

    set=[]

    found = False
    while not found:

        set+=[newAlpha]

        newAlpha=GCRD(newAlpha*pi,Q(normAlpha))
        found=isLeftAssociate(alpha,newAlpha)

    return set
```

The next method computes the order of the set $\langle \alpha, \pi \rangle$.

```
def order(alpha,pi):

    normAlpha=alpha.reduced_norm()
    normPi=pi.reduced_norm()
    newAlpha=Q(alpha)
    count=0

    found = False
    while (not found):
```

```
10
11          count+=1
12
13          newAlpha=GCRD(newAlpha*pi,Q(normAlpha))
14          found=isLeftAssociate(alpha,newAlpha)
15
16      return count
```

The last method tests if the order of $\langle \alpha, \pi \rangle$ is less than a given upper bound.

```
1  def isOrderLessThen(alpha,pi,bound):
2
3      normAlpha=alpha.reduced_norm()
4      normPi=pi.reduced_norm()
5      newAlpha=Q(alpha)
6      count=0
7
8
9      found = False
10     while (not found) and (count<bound):
11
12         count+=1
13
14         newAlpha=GCRD(newAlpha*pi,Q(normAlpha))
15         found=isLeftAssociate(alpha,newAlpha)
16
17     return (count,found)
```

E.3 Factorization algorithm

In this section, we will outline only one method: the factorization algorithm described in chapter 6. All methods used in this algorithm are described in Section E.1. So the input is any positive integer n and the output is a factor f of n. Recall that this algorithm computes the factor f in non polynomial time.

```
1  def factor1(n):
2
3      eta=SumOf4Sqrts(n)
4
5      if Q(eta).reduced_norm()!=n:
6          return eta
7
8      Over=False
9
10     while not Over:
11            print 'Constructing␣a␣prime␣quaternion␣pi'
12            found=False
13
14            while not found:
15                random=ZZ.random_element(500,1000)
16                found=isPrime(random)
17
18            g=GCD(n,random)
19            if g!=1:
20                 return g
21
22            pi=SumOf4Sqrts(random)
23            print 'pi='+str(pi)+'␣constracted.'
24            newEta=Q(eta)
25            foundSolution=False
```

```
26            count=0
27
28            while not foundSolution:
29                count+=1
30                newEta=GCRD(newEta*pi,n)
31                gcrd=GCRD(newEta,eta)
32                normGcrd=gcrd.reduced_norm()
33
34                if normGcrd!=1:
35                       foundSolution=True
36
37            if normGcrd!=n:
38                Over=True
39
40    print 'Found a factor f='+str(normGcrd)+' in '+str(count)+'
          steps.'
41    return normGcrd
```

E.4 Test algorithms

In this section, we will present algorithms we used to estimate some of the experimental results with respect to the elements in the set $\langle \alpha, \pi \rangle$, where α, $\pi \in \mathcal{L}$ are prime quaternions. The last algorithm was used to see how the time of factorization algorithm grows by the growing value of integer n. Some of those results were presented in chapter 6.

Note that these algorithms use some methods described in the first three sections of this chapter.

The first method "Test1" was constructed to analyze and observe how the value of the order of the set $\langle \alpha, \pi \rangle$ behaves by choosing different α and π.

So the possible inputs are:

Input:
- count1 is the number of randomly chosen primes q in $\mathbb{Z}$
- count2 is the number of quaternions α that the algorithm randomly creates, where $N(\alpha) = q$.
- primeQuaternions is the list of prime quaternions π
- count3 is the number of prime quaternions π that the algorithm creates randomly and adds to the list primeQuaternions.

And then, for each possible pair of α and π there is the output:

Output: - $N(\alpha)$, $N(\pi)$ and ord$\langle \alpha, \pi \rangle$

```
1
2 def Test1(count1,count2,primeQuaternions,count3):
3
4     count5=0
5     count4=0
6
7     while count4<count3:
8            print 'Constructing '+str(count4+1)+'.'
9            found=False
10
11           while not found:
12               random=ZZ.random_element(5000,15000)
13               found=isPrime(random)
14
15           pi=SumOf4Sqrts(random)
16           # We do not want that Pi is periodical
```

```
17            periodical=isLeftAssociate(pi,pi.conjugate())
18
19            if not periodical:
20                primeQuaternions+=[pi]
21                count4+=1
22
23    for l in xrange(count1):
24            found=False
25
26            while not found:
27                random=ZZ.random_element(100000,1000000)
28                found=isPrime(random)
29
30            for ll in xrange(count2):
31                alpha=SumOf4Sqrts(random)
32
33                for pi in primeQuaternions:
34                        e=order(alpha,pi)
35                        Answer=False
36                        factor=0
37
38                        if ((random-1)%e)==0:
39                            Answer=True
40                            factor=(random-1)/e
41
42                        if ((random+1)%e)==0:
43                            Answer=True
44                            factor=(random+1)/e
45
46                        count5+=1
47                        print 'Example:' + str(count5) +
                              '--------------------'
48                        print 'N(Alpha)=' + str(random), 'N(Pi)=' +
                              str(pi.reduced_norm()),
                              'ord(<Alpha,Pi>)=' + str(e)
49                        print 'Is␣the␣order␣a␣factor␣of␣N(Alpha)+1␣
                              or␣N(Alpha)-1?␣Answer:', Answer,',by␣
                              factor='+str(factor)
```

The following method "Test4" is very similar to "Test1". The difference is only that this test does not print out the order of all possible paired quaternions α and π. It computes the orders of all sets $\langle \alpha, \pi \rangle$, where α is a fixed quaternion and π is changing. Then the algorithm returns the smallest order and the average of orders for all such fixed quaternions α.

So we have the following input:

Input:
- count1 is the number of randomly chosen quaternions alpha with randomly chosen prime norm q in $\mathbb{Z}$
- count2 is the number of prime quaternions π that the algorithm creates randomly and adds to the list of primeQuaternions.
- primeQuaternions is the list of prime quaternions π

and then for each possible pair of α and π there is the output:

Output:
- α, $N(\alpha)$, minimal and average order of the sets $\langle \alpha, \pi \rangle$, where α is fixed and π is changing.

```
def Test4(count1,count2,primeQuaternions):

    count11=0
    listAlphas=[]

    while count11<count1:
           found=False

           while not found:
               random=ZZ.random_element(10**(2+count11),
                  10**(3+count11))
               found=isPrime(random)

           alpha=SumOf4Sqrts(random)
           listAlphas+=[alpha]
           count11+=1

    count4=0

    while count4<count2:
           print 'Constructing '+str(count4+1)+'.'
           found=False

           while not found:
               bound=int(count4/3)
               random=ZZ.random_element(10**(2+bound),10**(3+bound))
               found=isPrime(random)

           pi=SumOf4Sqrts(random)
           # We do not want that Pi is periodical
           periodical=isLeftAssociate(pi,pi.conjugate())

           if not periodical:
               primeQuaternions+=[pi]
               count4+=1

    piNorms=[]

    for p in primeQuaternions:
           piNorms+=[p.reduced_norm()]

    print 'List of Primes is', primeQuaternions
    print 'and they have the norms', piNorms

    for alpha in listAlphas:
           normAlpha=alpha.reduced_norm()
           Orders=[]
           print '----------------------'
           print 'Alpha=' + str(alpha), 'N(Alpha)=' +
              str(normAlpha)

           for pi in primeQuaternions:
               e=order(alpha,pi)
               Orders+=[e]

           sum=0

           for o in Orders:
               sum+=o

```

```
59            average=float(sum/len(Orders))
60            minimum=min(Orders)
61            print 'Minimal Order='+str(minimum), 'Average of
                 Orders='+str(average), 'AllOrders=',Orders
```

So for this test consider two prime Lipschitz integers α and π, where $N(\alpha) = q$. Recall Lemmas 3.2.9 and 3.2.10. From those lemmas we know that there are exactly $q+1$ different quaternions with norm q such that they are not pairwise left-associated. As it turned out from the two test algorithms above, every computed order of the sets $\langle \alpha, \pi \rangle$ was dividing the number $q + 1$ or $q - 1$. Because of that and some other reasons, we wanted to see how big the order of all possible sets $\langle \alpha, \pi \rangle$ for all α's with the same norm q and the fixed quaternion π is.

So the following algorithm is constructing all possible sets $\langle \alpha, \pi \rangle$, where $N(\alpha) = q$ and π is always the same quaternion.

So the input is:

Input: - alpha: any Lipschitz integer. If $\alpha = 0$ the algorithm creates randomly a Lipschitz integer different from zero, and if $\alpha \neq 0$, the algorithm works with the given quaternion α.
- pi: same as alpha. Any Lipschitz integer. If $\pi = 0$, the algorithm creates randomly a Lipschitz integer different from zero, and if $\pi \neq 0$, the algorithm works with given quaternion π.

And the output is:

Output: - prints out the orders of all disjoint sets $\langle \alpha, \pi \rangle$, where $N(\alpha) = q$ and π is always the same quaternion.

```
1  def Test2(alpha,pi):
2
3      if alpha==0:
4
5              found=False
6
7              while not found:
8                  random=ZZ.random_element(500,1000)
9                  found=isPrime(random)
10
11             alpha=SumOf4Sqrts(random)
12
13     normAlpha=alpha.reduced_norm()
14
15     if pi==0:
16             periodical=True
17
18             while periodical:
19                 found=False
20
21                 while not found:
22                         random=ZZ.random_element(100,300)
23                         found=isPrime(random)
24
25                 pi=SumOf4Sqrts(random)
26                 # We do not want that Pi is periodical
27                 periodical=isLeftAssociate(pi,pi.conjugate())
28
29     AllSolutions=Se(alpha,pi)
30     SumOfOrders=len(AllSolutions)
31     ListOfOrders=[SumOfOrders]
```

```
32      count=0
33      Over=((normAlpha+1)==SumOfOrders)
34      print alpha.reduced_norm(),pi.reduced_norm(), SumOfOrders,
           Over, (normAlpha+1)%4
35      while not Over:
36
37              for u in [i,j,k]:
38                  newAlpha=AllSolutions[count]*u
39                  isElement=False
40
41                  for l in xrange(SumOfOrders):
42                          left=isLeftAssociate(newAlpha,
                               AllSolutions[l])
43                          if left:
44                              isElement=True
45                              break
46
47                  if not isElement:
48                          print 'Found', newAlpha
49                          set=Se(newAlpha,pi)
50                          ListOfOrders+=[len(set)]
51                          AllSolutions+=set
52                          SumOfOrders=len(AllSolutions)
53                          print SumOfOrders
54                          Over=((normAlpha+1)==SumOfOrders)
55
56              count+=1
57
58              if count==(SumOfOrders-1):
59                  print 'Creating newAlpha'
60                  isElement=False
61                  found=False
62
63                  while not found:
64                          newAlpha=SumOf4Sqrts(normAlpha)
65                          fond=True
66
67                          for s in AllSolutions:
68                              left=isLeftAssociate(newAlpha, s)
69                              if left:
70                                      isElement=True
71                                      break
72
73                          if not isElement:
74                              found=True
75                              set=Se(newAlpha,pi)
76                              ListOfOrders+=[len(set)]
77                              AllSolutions+=set
78                              SumOfOrders=len(AllSolutions)
79                              print SumOfOrders
80                              Over=((normAlpha+1)==SumOfOrders)
81
82      print 'N(Alpha)=' + str(alpha.reduced_norm()), 'N(Pi)=' +
           str(pi.reduced_norm()), SumOfOrders
83      print 'ListOfOrders=', ListOfOrders
```

The next method was programed to analyze the elements in the set $\langle \alpha, \pi \rangle$ and to see if there is any frequency between the elements.

So the next algorithm computes all elements of the set $\langle \alpha, \pi \rangle$ for some prime quaternions α and β. Then it sorts all elements after their structure in the separate sets, i.e. for

one quaternion $\alpha^{(l_1)} \in \langle \alpha, \pi \rangle$ is in the set with other quaternions $\alpha^{(l_2)}$, where $\alpha^{(l_2)} \in \langle \alpha, \pi \rangle$ and $\alpha^{(l_2)} \in \mathfrak{E}_{\alpha(l_1)}$. And the algorithm prints the set with values l out in the table.

Remark E.4.1. In other words, all quaternions $\alpha^{(l)} \in \langle \alpha, \pi \rangle$ that are of the same structure are in one group.

Then the algorithm computes the distance of two nearest quaternions in one group of quaternions and also prints the distances.

So the input is:

Input:
- alpha: any Lipschitz integer. If $\alpha = 0$, the algorithm creates randomly a Lipschitz integer different from zero, and if $\alpha \neq 0$, the algorithm works with the given quaternion α.
- pi: same as alpha. Any Lipschitz integer. If $\pi = 0$, the algorithm creates randomly a Lipschitz integer different from zero, and if $\pi \neq 0$, the algorithm works with the given quaternion π.

And the output is:

Output:
- Prints out two tables. In one table the sets of sorted quaternions that are of the same structure. In another the it prints out the distances of two nearest quaternions in one set.

```
def Test3(alpha,pi):

    if alpha==0:

        found=False
        while not found:

            random=ZZ.random_element(1000,10000)
            found=isPrime(random)

        alpha=SumOf4Sqrts(random)

    normAlpha=alpha.reduced_norm()

    if pi==0:

        periodical=True
        while periodical:

            found=False
            while not found:

                random=ZZ.random_element(100,300)
                found=isPrime(random)

            pi=SumOf4Sqrts(random)

            # We do not want that Pi is periodical
            periodical=isLeftAssociate(pi,pi.conjugate())

    set=Se(alpha,pi)

    Results=deepcopy(set)
    results=[]
    for l in xrange(len(Results)):

        results+=[(l,Results[l])]
```

```
    AllSolutions=[]
    while len(results)>0:

        print len(results)
        fix=results[0]
        SomeSolutions=[fix]
        del results[0]
        Hits=[]
        for lll in xrange(len(results)):

            SameStructure=isSameStructure(fix[1],results[lll][1])
            if SameStructure:
                SomeSolutions+=[results[lll]]
                Hits=[lll]+Hits
        print len(Hits)
        for h in Hits:
            del results[h]

        AllSolutions+=[SomeSolutions]

    OrderedValuesOfl=[]
    DifBetweenLs=[]
    for s in AllSolutions:
        valuesOfl=[]
        difOfLs=[]
        lastHit=0
        for l in s:
            valuesOfl+=[l[0]]
            difOfLs+=[l[0]-lastHit]
            lastHit=l[0]
        OrderedValuesOfl+=[valuesOfl]
        DifBetweenLs+=[difOfLs]

    print '-----------------------------------------'

    for r in OrderedValuesOfl:
        print r

    print '-----------------------------------------'
    print '-----------------------------------------'

    for r in DifBetweenLs:
        print r

    print '-----------------------------------------'
```

In the last method, we want to test how fast the time is growing to compute a factor of the growing integer n, using the method "factor1(n)". Note that with the expression "growing time" we do not mean only the particular time in seconds, but more the number of steps, i.e. the number of computed quaternions $\eta^{(l)}$ until we get the solution.

The input for the method "Test5" is the number of randomly generated integers n that the method "factor1" factors, and the outputs are the number of steps and the time until it found the solution.

```
import time

def Test5(repeat):

    for l in xrange(repeat):

            found=False
```

```
8
9             while not found:
10                random=ZZ.random_element(10000,100000)
11                found=isPrime(random)
12
13            q_1=deepcopy(random)
14
15            found=False
16
17            while not found:
18                random=ZZ.random_element(100000,1000000)
19                found=isPrime(random)
20
21            q_2=deepcopy(random)
22            n=q_1*q_2
23            print 'Computing␣factors␣of␣n='+str(n)+'.␣And␣Factors␣
                  are␣q_1='+str(q_1)+'␣and␣q_2='+str(q_2)
24            start=time.time()
25            f=factor1(n)
26            end=time.time()
27            dif=end-start
28            print 'Found␣f␣in␣'+str(dif)+'␣seconds.'
```

Bibliography

[1] António Machiavelo and Luís Roçadas, *Some connections between the arithmetic and geometry of Lipschitz integers*, 2011

[2] Gordon Pall, *On the Arithmetic of Quaternions*, Transactions of the A. M. S. 47 (1940), pp 487-500

[3] Michael O. Rabin and Jeffery O. Shallit, *Randomized Algorithms in Number Theory*, Communication on Pure and Applied Mathematics XXXIX (1986), pp 239-S256

[4] Giuliana Davodoff, Peter Sarnak and Alain Valette, *Elementary Number Theory, Group Theory and Ramanujan Graphs.*

[5] John H. Conway and Derek Smith, *On Quaternions and Octonions*, AK Peters 2003

[6] Michael O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. on Computing, 9, 1980, pp. 273-280.

[7] Bach, E., Miller, G., and Shallit, J., *Sums of divisors, perfect numbers and factoring*, Proc. 16th AMC Symposium on the Theory of Computing, 1984, pp. 183-190.

[8] Livingston, M.L., *Expicite estimates for the ψ-functions for primes in arithmetic progression*, S.I.U.E. Preprits in Mathematics #69, Southern Illinois University at Edwardsville, Edwardsville, IL, (March 1986).

[9] Joachim Rosenthal, Felix Fontein, *Cryptography*, Lecture Notes Universität Zürich, 2005, pp 11-13

[10] John Brillhart, *Note on Representing a Prime as a Sum of Two Squares*, Mathematics of Computation, vol. 26, Number 120 (October 1972), pp.1011-1013

[11] Gordon Pall, *On the factorization of generalized quaternions*, Duke Mathematical Journal, vol. 4 (1938), pp. 696-704.

[12] C. Hermite, Journal für die reine und angewandte Mathematik, vol. 47 (1854), pp.343-345.

[13] David Eisenbund, *COMMUTATIVE ALGEBRA with a View Toward Algebraic Geometry*, Springer-Verlag New York (1995)

Index