Linnæus University
Sweden

Degree project

RSA in extensions of the ring of integers

Author: Alessia Pina
Supervisor: Per-Anders Svensson
Examiner: Karl-Olof Lindahl
Date: 2017-12-22
Course Code: 5MA41E
Subject: Mathematics
Level: Master Degree

Department Of Technology

Abstract

The aim of this work is to create a variant of the RSA classical algorithm, through extensions from the ring of integers $\mathbb{Z}$ to two Euclidean domains: the domain of Gaussian integers, $\mathbb{Z}[i]$, and the domain generated by $\sqrt{2}$, $\mathbb{Z}[\sqrt{2}]$. To achieve this purpose, the study of the theory behind both these sets becomes necessary, to ensure that all the properties are preserved when moving into extensions and so that the construction of the algorithm is possible. Moreover, a description of modular arithmetic is needed, to see how modules behave inside these new sets, since they are the most important ingredient for the algorithm.

Acknowledgements

This thesis is written as a part of the Double Degree project from the Insubria and the Linnaeus Universities. I would like to thank all the people from both universities who made this project possible: being a part of it was a great opportunity for me and also a wonderful experience.

In particular, my deepest gratitude goes to my supervisor, Doctor Per-Anders Svensson, for the patience and the professionality shown during all our Skype meetings.

Finally, I thank all my family and friends for all the love and the support during all these years and for always believing in me.

Contents

Chapter 1

Introduction

The RSA algorithm, [Rivest-Shamir-Adleman], invented by Rivest, Samir and Adleman in 1977, is one of the best known and more used public-key cryptosystems, for providing security all over the network. Like every other public-key algorithm, it is based on the security of its secret key, but also on the non-easy factorization of its public key. The classical RSA was created inside the ring of rational integers through the help of modular arithmetic, as described in [Cao-Fu]. More recently, some studies have proved that and extension of such this algorithm in the domain of Gaussian integers is possible. For example, in 2005 [El-Kassar-Haraty-Awad] gave a modified version of the RSA algorithm into the domain of Gaussain integers, together with a description of the computational procedures. Almost ten years later, [Pradhan-Sharma] proposed the same extension with a deeper study of arithmetic modulo a Gaussian integer. In both cases, the aim of these works was to find a more secure and more efficient scheme.

In this thesis, beside the analysis of the RSA extended algorithm inside the domain of Gaussian integers, we are going to study the domain generates by $\sqrt{2}$, giving some detail about the choice of this particoular domain. Moreover, we would like to mimic the computational procedures needed for the creation of the algorithm and, for this reason, we will also study how modular arithmetic behaves inside the two domains. To achieve this purpose, we are going to use the support of `Matlab`.

Inside this paper, before creating the extended version of RSA algorithm, a description of RSA classical algorithm with an historical background is given in Chapter 2. Then, the ring of Gaussian integers is introduced and studied further in Chapter 3, in order to arrive at a practical application. In Chapter 4 we present a description of the domain generated by $\sqrt{2}$ trying, at the beginning, to generalize the previous description by observing the behaviour of sets generated by $\sqrt{d}$ and then, fixing d exactly equal to 2. Subsequently, the specific properties on the set chosen for the construction

of the algorithm are checked. Afterwards, Chapter 5 contains all modular aspects and the description of the two extended codes along with some examples and then we proceed with the analysis of the algorithm, in Chapter 6. Finally, Chapter 7 is a discussion about the algorithm. At the beginning of every Chapter, all the references used are shown in detail.

Chapter 2

RSA Classical Algorithm

2.1 Historical background

Over the centuries, we always wondered how it was possible to send and receive messages, by ensuring that they were being kept secret by a third party who, intercepting the message, is not supposed to understand or modify it. This aim is achieved by an obscuration of the message, called **encryption** in such a way that only the receiver of the message, knowing the **key**, is able to understand it through the **decryption**. Moreover, the original message is called **plaintext**, while the obscured message is the **ciphertext**. Together with the development of technologies, even the codes used in cryptography have become increasingly complex. The absence of geographical constraints, not only permits communication between people all over the world, but it makes a safely exchange of a key difficult. During the second world war, Germans used one of the best code known, ENIGMA. The detection of the key and the breaking of the code by the Allies was one of the crucial points which marked the end of the war and the victory of the Allied Forces. In fact, cryptography systems are mostly used in the military field. Nowadays, we have to say that keeping information secret has became more important with the arrival of internet and all its supporting technologies which uses the networks.

Public key cryptography

In general, all the classical cryptosystems are said to be **symmetric**, which means the sender and the receiver use the same key to communicate through the secret message. This implies, however, that the two must be able to safe exchange the key. In fact, it is still possible but it could be difficult to arrange it, since the sender and the receiver perhaps cannot meet personally to exchange the key. This is the reason that led to the creation of the **public key cryptography** in 1976, with the publication of *New directions in cryptography*, a project by Diffie and Hellman ([Diffie-Hellman]). The aim

of their work was to create a new way of communication which allows the exchange of information between two people who have no possibility of a safe contact. In this case, we create two different keys: the so called **public key** and **secret key**, which respectively allows to encrypt and decrypt the message. Moreover, the main concept is that both these operations must be easily computed, while decryption without the knowledge of the key must be really difficult (in a computational way) to compute. In other words, the computations will require such a long time that the final discovery of the message will no longer give any information. This new way of communication now allows the exchange of information between two people who have never had previous contact and, as the name suggests, the public key can be publicly available. Since we are using two different keys, the cryptosystem is now said to be a **asymmetric**.

The invention of RSA

Diffie and Hellman never developed a practical implementation of their method which was developed afterwards and, in 1977, Rivest, Shamir and Adleman, in [Rivest-Shamir-Adleman], proposed a new idea called **RSA algorithm**, which is based on the fact that the factorization of integers into their prime factors is complex and needs a long time to be found. Indeed, both researches mentioned above had been developed previously by the government cryptographic agencies, the United Kingdom Government Communication Headquarters, but secrecy rules prevented them from making the researches public until 1997 because they where considered classified information. Nowadays we know that James Ellis had already conceived the idea of public-key cryptography in 1970, while the description of RSA algorithm was written by Clifford Cocks in 1973. Cryptography has always tried to avoid the problem of **interceptions**, producing a message unreadable for anyone, except for the owner of the key, but through public key cryptography, we are also able to bypass the problem of **alteration**.

2.2 Theory

This section contains a brief introduction about the instruments we are going to use to develop the RSA algorithm.

2.2.1 Euler's ϕ-function

Analysing the properties of any number n, we notice that some of them depend on the number of integers less than n that do not contain any of the factors of n, i.e. the coprime numbers with n. This is the reason we now define the totient function and we describe some of its properties. In particular, here we rely on [Anderson-Bell].

Definition 2.1. If n is a positive integer, we call **Euler's ϕ-function**, or **totient function**, the function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$, the number of positive integers s such that:

- $s \leq n$,
- $(s, n) = 1$.

It is reasonable from the definition saying that $1 \leq \phi(n) \leq n$.

Theorem 2.1. *Given two coprime numbers, p and q, then the Euler's ϕ-function is multiplicative that is:*

$$\phi(pq) = \phi(p)\phi(q).$$

It is possible to find the proof in [Anderson-Bell, p. 185].

Example 1. Let $m = 8$ and $n = 9$ be two coprime numbers, since they are consecutive. We compute the two Euler's ϕ-functions $\phi(8) = 4$ and $\phi(9) = 6$ and now we can show $\phi(72) = \phi(8 \cdot 9) = \phi(8)\phi(9) = 4 \cdot 6 = 24$. In fact, counting all the coprime numbers with 72, we obtain exactly 24 (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71).

Using Theorem 2.1 we can say that the Euler's ϕ-function is multiplicative for coprime factors. Now, we would like to analyse the totient function of a prime or a power of a prime.

Proposition 2.1. *If p is a prime number,*

$$\phi(p^k) = p^k - p^{k-1}$$

Proof. Since we do not know how many numbers less than p^k are coprime with it, we proceed counting the numbers that are not coprime. They are: $0 \cdot p = 0$, $1 \cdot p = p$, $2p$, $3p$, $\cdots$, $(p^{k-1} - 1)p$, so we know that there are p^{k-1} of them. From this, we obtain that the number of the coprime numbers with p^k is $p^k - p^{k-1} = \phi(p^k)$, which is the value of the totient function. □

Proposition 2.2. *A positive integer p is prime if and only if*

$$\phi(p) = p - 1.$$

Proof. $\Rightarrow$ If p is prime, this comes immediately from Proposition 2.1.

$\Leftarrow$ Suppose p is not prime, then there exists an element q in $\mathbb{Z}$, different than 1 and p itself, such that $q \mid p$. By the definition of Euler's ϕ-function, $0 < \phi(p) \leq p - 1$, but in this case the value q must be excluded since it is not coprime with p. So $\phi(p) \neq p - 1$ which is a contradiction, so p must be prime.

□

Using a combination of Theorem 2.1 and Proposition 2.1, we can obtain an explicit formula to compute $\phi(n)$, with n any positive integer:

Theorem 2.2. *Let $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ be the decomposition into prime numbers of n, with m_i positive integers and $p_1 \neq \dots \neq p_k$. Then:*

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{m_i - 1}(p_i - 1)\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Example 2. Let $n = 20$. Using a brute force approach, we know that the coprime integers with 20 are: 1, 3, 7, 9, 11, 13, 17 and 19, so $\phi(20) = 8$. If we use the formula above,

$$\phi(20) = 20\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 8.$$

2.2.2 The Theorems of Euler and Fermat

Theorem 2.3 (Euler's Theorem)**.** *Let a be an integer and n a positive integer, with* $\gcd(a, n) = 1$*, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

In the special case when $n = p$ is a prime number, we obtain:

Theorem 2.4 (Fermat's Little Theorem)**.** *Let p be a prime number and a an integer such that $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

We can find the proofs of these Theorems in [Beachy-Blair, p. 41-42]

2.3 The RSA algorithm

The generation of the keys

Now, we see the RSA algorithm step by step to better understand the procedure. First of all, we describe the procedure the receiver needs to follow to compute the public and the secret keys:

1. Select two big prime numbers p and q such that $p \neq q$;
2. Compute the product $N = p \cdot q$;
3. Calculate $s = (p-1)(q-1) = \phi(N)$, i.e. the Euler ϕ-function of N;
4. Select a random integer e so that $0 \leq e \leq s$ and $\gcd(e, s) = 1$: e is the **encryption exponent**.

5. Compute the multiplicative inverse of e, $d \equiv e^{-1} \pmod{s}$, i.e. the element d such that $ed \equiv 1 \pmod{s}$: d is the **decryption exponent**.

6. Now, the receiver publishes the **public key** $P_k = [N, e]$ and he tries to keep the **private key** $S_k = [p, q, d]$ secret.

Remark. The two prime numbers p and q are computed only to create N and they are no longer used. Otherwise, it is necessary to keep them secret to not compromise the security of the algorithm.

Encryption and decryption

Secondly, we describe the procedure that the sender and the receiver must implement to decrypt and encrypt the message.

Before starting the encryption, the sender must convert the **message** into an integer, to compute the ciphertext using modular arithmetic; then, if it is necessary, the **plaintext** P must be divided into **blocks** such that every block P_i has a length smaller than N. For example, suppose p and q have length k: since the length of N is $2k$, every P_i must be less than or equal to $2k - 1$. Encryption and decryption are done block by block, with $1 \leq P_i \leq N - 1$ for all P_i.

E The sender encrypts the plaintext using the encryption key e:

$$C_i \equiv P_i^e \pmod{N}$$

and sends the **ciphertext** composed by the blocks C_i.

D The receiver, through the decryption exponent d, computes

$$P_i \equiv C_i^d \pmod{N},$$

re-obtaining the plaintext and finds the **message**.

2.3.1 Security

The security of the RSA algorithm is based on two different aspects: the high difficult in **factorizing** N and the so called **RSA problem**. In fact, the factorization of N give us all the informations needed, i.e. the numbers p and q, the value of the Euler's ϕ-function and also the decryption exponent, since the value of the encryption exponent is known as part of the Public key. This means the security problems of the RSA algorithm are based on "how easy" it is to find the decomposition of N. Moreover, the RSA problem consists in finding the decryption exponent given that (N, e) is a Public key. In other words, having $N = pq$, with p and q unknown primes, and also e, a rational integer such that $\gcd(e, \phi(N)) = 1$, we would like to find

$$d \equiv e^{-1} \pmod{\phi(N)}.$$

To avoid the problem of factorization, we start constructing the algorithm selecting the two primes p and q to be very large. The problem is that the value of $\phi(N)$ must be safe and so the values $p-1$ and $q-1$ must be selected carefully. We know both this values are not primes, since they are even, so we can find a decomposition of them into rational integers. Then, if all the prime factors of $p-1$ are small, but there exists a large factor of $q-1$, we are able to find p easily. This factorization method is called **Pollard's $p-1$ Method** and we remind to [Hoffstein-Pipher-Silverman], for a deeper discussion about it. This is only an example, to show that not all large prime numbers are a good choice for p and q, so we need to be careful.

Chapter 3

$\mathbb{Z}[i]$

In this chapter we will introduce the set of Gaussian integers with its properties. In order to write this chapter, and the followings, it was necessary the study of Gaussian integers, using [Aluffi] and [Artin]. Moreover, we used in particular [Stillwell] to talk about division and divisibility inside $\mathbb{Z}[i]$ and [Clark] for the factorization. In the second part of the chapter, after proving $\mathbb{Z}[i]$ is a Euclidean domain, we describe the classification of Gaussian primes, looking at [Bandyopadhyay] and [Pal]. In general, all the works just mentioned, were used for the writing.

3.1 The set of Gaussian integers

The initial purpose in introducing the set of Gaussian integers was to factorize $x^2 + y^2$, creating a set in which the decomposition of the sum of two integer squares is possible, in the following way:

$$x^2 + y^2 = (x - yi)(x + yi).$$

From this, we obtain both the factors $x - yi$ and $x + yi$ are squares of complex numbers. To let this decomposition be possible, we need to create a set containing all the rational numbers, but also the imaginary unit:

Definition 3.1. We call **Gaussian integers** the set $\mathbb{Z}[i]$ which contains the elements of the form $a + bi$, with $a, b \in \mathbb{Z}$ and i the imaginary unit $i^2 = -1$. Formally, we write this set as:

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}.$$

In other words, this is the set which contains all the complex numbers whose real and imaginary parts are integers. It follows directly from this observation that

$$\mathbb{Z}[i] \subset \mathbb{C}.$$

It is clear that the sum and the product of two Gaussian integers are a Gaussian integer. Moreover, the set of Gaussian integers, with the ordinary addition and multiplication between complex numbers, is a ring.

Proposition 3.1. $(\mathbb{Z}[i], +, \cdot)$ *is a ring.*

Proof. (i) It contains the zero element $0 = 0 + 0i$ and the unit element $1 = 1 + 0i$.

(ii) It is closed under addition: $(a+bi)+(c+di) = (a+c)+(b+d)i$, with a, b, c, d in $\mathbb{Z}$ and this implies $(a + c), (b + d)$ in $\mathbb{Z}$.

(iii) It is closed under multiplication: $(a+bi)(c+di) = ac+adi+bci+bdi = (ac-bd)+(ad+bc)i$, with a, b, c, d in $\mathbb{Z}$ and this implies $(ac-bd), (ad+bc)$ in $\mathbb{Z}$, giving the closure.

(iv) Additivity, commutativity and distributivity come directly from the fact that they holds for any complex numbers.

□

Moreover, from this fact that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, we are able to define objects we usually use with complex numbers. For example, one of the objects we will need is the **conjugate** of a number $z = a+bi$, defined as the same number, with the imaginary part changed to sign: $\overline{z} = a - bi$.

3.1.1 The norm

Again from the fact that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, we are able to define the norm on $\mathbb{Z}[i]$, in the analogous way as we do in $\mathbb{C}$:

Definition 3.2. Let $z = a + bi \in \mathbb{Z}[i]$, the **norm** of z is the function $N : \mathbb{Z}[i] \to \mathbb{N}$ defined as the product:

$$N(a + bi) = |a + bi|^2 = (a + bi)(a - bi) = a^2 + b^2.$$

Being a sum of two square integers, the norm is always non-negative. On the other hand, it is not true that every non-negative integer is a norm. In fact, from the definition, the norms are precisely all the integers of the form $a^2 + b^2$ and we cannot write every integer as the sum of two squares. Moreover, we notice that the norm is the product of a number with its conjugate.

Since the norm in $\mathbb{C}$ is multiplicative, we would like to prove the multiplicativity holds also in $\mathbb{Z}[i]$:

Proposition 3.2. *The norm is multiplicative.*

Proof. Let z and w be Gaussian integers. Then using the multiplicative property of the absolute value:

$$N(zw) = |zw|^2 = |z|^2|w|^2 = N(z)N(w)$$

and the multiplicativity in $\mathbb{Z}[i]$ is shown. □

Here, some easy consequences coming from the definition:

Proposition 3.3.
- $N(z) \geq 0$ *for all* $z \in \mathbb{Z}[i]$;
- $N(z) = 0$ *if and only if* $z = 0$;
- $N(a) = a^2$ *if* $a \in \mathbb{Z}$.

Definition 3.3. A nonzero element $z \in \mathbb{Z}[i]$ with $N(z) > 1$ is called **composite** if its decomposition contains at least one non-trivial factor. Moreover, z is called **Gaussian prime**, if it has only trivial factors.

Since these definitions are really important for our goal, we will later discuss about prime numbers in detail.

3.1.2 Divisibility

Let us start seeing some examples:

Example 3. Let $z = 11-2i$ and search the factorization. Is $11-2i$ divisible by $1+2i$?

$$\frac{11-2i}{1+2i} = \frac{(11-2i)(1-2i)}{(1+2i)(1-2i)} = \frac{7-24i}{5} = \frac{7}{5} - \frac{24}{5}i$$

and since $\frac{7}{3}$ and $-\frac{24}{5}$ are not in $\mathbb{Z}$, it is not divisible by $1+2i$ in $\mathbb{Z}[i]$. Is $11-2i$ divisible by $1-2i$? Since

$$\frac{11-2i}{1-2i} = \frac{(11-2i)(1+2i)}{(1-2i)(1+2i)} = \frac{15+20i}{5} = 3+4i$$

it is and we have also found the factorization $11-2i = (1-2i)(3+4i)$.

Example 4. We compute the norms of the numbers used in the previous example:

$$N(11-2i) = 11^2 + (-2)^2 = 125,$$
$$N(1-2i) = 5 \quad \text{and} \quad N(3+4i) = 25.$$

Resuming what we have seen from the examples, the division of two complex numbers is done by multiplying both the numerator and the denominator by the complex conjugate of the denominator.

What we are wondering now is to understand how we can use the norm to obtain information about its number. Imitating the division algorithm we have previously seen, we write:

Theorem 3.1 (Division Theorem for Gaussian integers)**.** *For any non-zero $z, w \in \mathbb{Z}[i]$, there exist $q, r \in \mathbb{Z}[i]$ such that*

$$z = wq + r \quad \textit{with} \quad N(r) < N(w).$$

In the classical division theorem, we are able to prove the uniqueness of the remainder and the quotient, while this is not possible in the case of Gaussian integers. The crucial point is the condition that the remainder must be less than the divisor, while here, the condition becomes that the norm of the remainder must be less than the norm of the divisor.

What the existence of this theorem in $\mathbb{Z}[i]$ guarantees is the validity of the **Euclidean algorithm**, which can be create, imitating the case in $\mathbb{Z}$, using the Division algorithm's theorem recursively. In the same way, we do not have the uniqueness of the greatest common divisor, but, by proving the following theorem, we obtain the relation between the greatest common divisors, i.e. all the greatest common divisors of two numbers are a linear combination, one of the other:

Proposition 3.4. *If $d \in \mathbb{Z}[i]$ is a greatest common divisor for z and w, then there exist $x, y \in \mathbb{Z}[i]$ such that*

$$zx + wy = d.$$

This proof can be found in [Beachy-Blair, p. 8].
Now, letting d be 1, we obtain:

Corollary 3.2. *Let z and w be two Gaussian integers. They are coprimes if and only if there exist $x, y \in \mathbb{Z}[i]$ such that*

$$zx + wy = 1.$$

Example 5. Let us apply the division algorithm with $65-40i$ and $31+15i$:

$$\begin{array}{rcccccc} 65-40i & = & (1-2i) & \cdot & (31+15i) & + & (4+7i) \\ 31+15i & = & (3-2i) & \cdot & (4+7i) & + & (5+2i) \\ 4+7i & = & (1+i) & \cdot & (5+2i) & + & 1. \end{array}$$

Has we have already seen, we can use the algorithm also to find a greatest common divisor:

Example 6. $(77+34i, 1+27i) = 1+2i$. In fact:

$$\begin{array}{rcccccc} 77+34i & = & (1-3i) & \cdot & (1+27i) & + & (-5+10i) \\ 1+27i & = & (2-i) & \cdot & (-5+10i) & + & (1+2i) \\ -5+10i & = & (3+4i) & \cdot & (1+2i) & + & 0 \end{array}$$

One of the reasons we introduced the notion of norm, together with its multiplicativity, is given from the fact that the norms are rational integers giving information about complex numbers. In this way, we are able to move the question about divisibility in $\mathbb{Z}[i]$ inside $\mathbb{Z}$. To do that, we use:

Proposition 3.5. *Let $z, w \in \mathbb{Z}[i]$. If $z|w$ in $\mathbb{Z}[i]$ then $N(z)|N(w)$ in $\mathbb{Z}$.*

Proof. It follows directly from the multiplicativity of the norm. In fact, since it is possible to write $N(ab) = N(a)N(b)$, writing $w = z \cdot c$ for some c, it follows $N(w) = N(cz) = N(c)N(z)$ and $N(z)$ is a divisor for $N(w)$. □

The utility of this theorem is given from the fact that we can use the value of the norm, which lies on $\mathbb{Z}$, to quickly check if a Gaussian integer does *not* divide another. Here some examples:

Example 7. If $7 + 2i \mid 5 + 4i$ in $\mathbb{Z}[i]$, then we would have

$$N(7 + 2i) = 53 \mid 41 = N(5 + 4i),$$

but the two norms are not divisible so the same happens with the two Gaussians.

However, we do not have the converse, so that the divisibility in $\mathbb{Z}[i]$ does not follow from the divisibility of the norm in $\mathbb{Z}$.

Example 8. Consider $3 + 7i$ and $5 - 2i$: the norms here are divisible, since

$$N(5 - 2i) = 29 \mid 58 = N(3 + 7i),$$

but $5 - 2i \nmid 3 + 7i$.

In conclusion, we can say that the divisibility of the norm is a necessary condition for the divisibility of the Gaussian integers, but it is not sufficient.

Remark. Even if we are not able to introduce inequalities in $\mathbb{Z}[i]$, we can talk about inequalities on the norms.

Now we wonder if it is possible to understand something more about the divisors, using Proposition 3.5. Since $w|z$ means $N(w)|N(z)$ and from the properties of the norm, we know $1 \leq N(w) \leq N(z)$ (supposing z nonzero).

Theorem 3.3. *Let $z = a + bi$ be a Gaussian integer. Then z is divisible by any rational integer $d \in \mathbb{Z}$ if and only if $d|a$ and $d|b$ in $\mathbb{Z}$.*

Proof. The divisibility of z in $\mathbb{Z}[i]$ by d can be written as: there exist two elements $e, f \in \mathbb{Z}$ such that

$$a + bi = d(e + fi)$$

and this is equivalent to say $a = de$ and $b = df$ that is $d|a$ and $d|b$. □

If we take $b = 0$ in this theorem, we obtain the divisibility of ordinary integers, so in the ring of Gaussian integers they behave as usual.

3.1.3 Units

We recall the general definition of unit, for this particular case of unit in a ring:

Definition 3.4. A Gaussian integer z is said to be **invertible** or **a unit** if there is an element w in $\mathbb{Z}[i]$ such that $zw = 1$.

Proposition 3.6. *Let z be an element of $\mathbb{Z}[i]$ and $N(z)$ its norm. Then $N(z) = 1$ if and only if z is a unit.*

This proposition came directly from the definition of norm.

Proposition 3.7. *If two elements are associates, then they have the same norm.*

Proof. Let z and w be associates, then for definition $z = wu$, with u unit. So $N(z) = N(w)N(u) = N(w)$, since the norm of a unit is 1 by Proposition 3.6. □

Example 9. Since $3 + 2i$ and $3 - 2i$ are associates, their norm is the same: $N(3 + 2i) = N(3 - 2i) = 13$.

The converse it is not always true: for example, $N(5) = 25$ and $N(3 + 4i) = 25$, but 5 and $3 + 4i$ are clearly not associates. So we need a stronger condition:

Proposition 3.8. *Let z and w be Gaussian integers such that $w|z$. If $N(w) = N(z)$ then z and w are associates.*

Proof. Since w is a divisor of z with $N(w) = N(z)$, there exists an element $x \in \mathbb{Z}[i]$ such that $z = xw$. Taking the norms, we obtain

$$N(z) = N(x)N(w) = N(x)N(z)$$

and simplifying we obtain $N(x) = 1$, providing $N(z) \neq 0$, that again means $x = \pm 1$ or $\pm i$ and consequently $w = \pm z$ or $\pm zi$. □

Proposition 3.8 does not say that the elements with norm $N(z)$ are only $\pm z$ and $\pm zi$. On the other hand, we are always sure that, given any norm $N(z) \geq 2$, we always have the following obvious elements: ± 1, $\pm i$, $\pm z$, $\pm zi$ which are called **trivial factors** of z.

Now, using Proposition 3.6, we know that all the elements with norm 1 in $\mathbb{Z}[i]$ are the units, so we can prove the following:

Proposition 3.9. *The units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.*

Proof. Let p be a unit in $\mathbb{Z}[i]$. Then by Proposition 3.6, $N(p) = 1$. The elements with norm 1 in $\mathbb{Z}[i]$ are of the form $a + bi$ such that a and b are integer solutions of the equation $a^2 + b^2 = 1$. These elements in $\mathbb{Z}[i]$ are exactly $1, -1, i$ and $-i$. □

Remark. Every number of the form $a + bi \in \mathbb{Z}[i]$ is divisible by ± 1 and $\pm i$. In fact, we can write it as

$$a + bi = -1(a + bi) = i(-ai + b) = -i(ai - b).$$

This way to write a number in $\mathbb{Z}[i]$, i.e. up to a multiplication by a unit, is the analogous way to see an integer up to its sign. According to the definition we have already given, we can say that the four elements $a+bi, a-bi, -a+bi$ and $-a-bi$ are associates.

Using the properties of the norm, we know $z = xy$ is a non-trivial factorization if and only if $N(x), N(y) > 1$. So, once again, there exists a relation between $\mathbb{Z}[i]$ and $\mathbb{Z}$.

Proposition 3.10. *Let $z, v, w \in \mathbb{Z}[i]$ such that $z = vw$, then the following statements are equivalent:*

(i) *$z = vw$ is a non-trivial factorization in $\mathbb{Z}[i]$;*

(ii) *$N(z) = N(v)N(w)$ is a non-trivial factorization in $\mathbb{Z}$;*

(iii) *$N(v), N(w) > 1$.*

Proof. This easily comes from the fact that $N(z) = 1$ if and only if z is a unit. □

3.1.4 Euclidean Domain

Now, we would like to show that the ring of Gaussian integers is a Euclidean domain, using the definition of norm:

Theorem 3.4. *The ring $\mathbb{Z}[i]$ is a Euclidean domain.*

Proof. What we are going to do is proving that the ring $\mathbb{Z}[i]$, satisfies the properties of the Euclidean domain using the norm we have previously defined. Let $z = a + bi$ and $w = c + di$ be non-zero elements of $\mathbb{Z}[i]$.

(i) From the definition of norm, $N(z) = a^2 + b^2$ and $N(zw) = (a^2 + b^2)(c^2 + d^2)$. Now, $w \neq 0$ implies $c^2 + d^2 \geq 1$ because one of c and d is at least nonzero, so the first statement follows:

$$N(zw) \geq a^2 + b^2 = N(z).$$

(ii) Given z and w in $\mathbb{Z}[i]$, we want to find two elements $q, r \in \mathbb{Z}[i]$ such that $z = qw + r$. First, we write this equation as

$$r = w\Big(\frac{z}{w} - q\Big)$$

with $\frac{z}{w}$ complex number, not necessarily Gaussian. Since we are not sure $\frac{z}{w} \in \mathbb{Z}[i]$, we cannot apply the given definition of norm to it. For this reason, after computing $\frac{z}{w}$, we round this value to the nearest integer $\tilde{z}$, so that we are sure this new value $\tilde{z}$ is in $\mathbb{Z}[i]$. What we have now are $r = w\Big(\frac{z}{w} - q\Big)$ and $r = w(\tilde{z} - q)$ with $\tilde{z} \in \mathbb{Z}[i]$ and $\frac{z}{w} \in \mathbb{C}$, but not necessarily in $\mathbb{Z}[i]$. This two different evaluations of r are not necessarily the same, since $\tilde{z}$ and $\frac{z}{w}$ are not necessarily equal. Then we write $\frac{z}{w} = x + yi$, with $x, y \in \mathbb{Q}$, and, rounding off x and y respectively to the nearest integer, we obtain $\tilde{x} + \tilde{y}i$ and we assign this value, which is a Gaussian integer, to q. Now, $r = z - qw$ turns out to be a Gaussian integer as well and we have found two Gaussian integers q and r which make the equation $z = qw + r$ true. Now we need to guarantee $N(r) < N(z)$ for every $0 \neq r \in \mathbb{Z}[i]$. We would like to compute the norm of r, but we need to use the classical definition with the absolute value since $\frac{z}{w}$ is not necessarily a Gaussian integer and we are not sure $N(\frac{z}{w})$ is defined. Then

$$N(r) = N(z - qw) = \big|z - qw\big|^2 = \big|w\big|^2\Big|\frac{z}{w} - q\Big|^2 = N(w)\big|\frac{z}{w} - q\big|^2.$$

In order to complete the proof, we need $\Big|\frac{z}{w} - q\Big|^2 < 1$, but this is easily done reminding that the notion of norm is a distance in the complex plane. In fact, $\frac{z}{w}$ was defined as $x+yi$ while $q = \tilde{x}+\tilde{y}i$ and substituting

$$\Big|\frac{z}{w} - q\Big|^2 = \big|(x+yi) - (\tilde{x}+\tilde{y}i)\big|^2 = \big|(x-\tilde{x}) + (y-\tilde{y})i\big|^2 \leq (x-\tilde{x})^2 + (y-\tilde{y})^2.$$

By the choice of $\tilde{x}$ and $\tilde{y}$, we obtain $\Big|\frac{z}{w} - q\Big|^2$ is less than one. (In particular, $|x - \tilde{x}| \leq \frac{1}{2}$ and $|y - \tilde{y}| \leq \frac{1}{2}$ since we round to the nearest integer.) So we obtain $N(r) < N(w)$ as requested.

□

Taking in mind the algebraic definitions, that we can find for example in [Beachy-Blair], now we know that the ring of Gaussian integers, being a Euclidean domain, is also a principal ideal domain, using [Beachy-Blair, p. 410]. So, being a principal ideal domain, it is a unique factorization domain, using [Beachy-Blair, p. 413]. For these reasons, starting from now we can use previously proven properties and, in particular, the uniqueness of the factorization.

3.1.5 Gaussian Primes

Now, we would like to introduce the notion of prime element inside $\mathbb{Z}[i]$, so that we are able to talk about unique factorization. The usual definition of prime number, i.e. a nonzero element that is divisible only by 1 and

itself, is not working in this case, since every number is divisible by ± 1 and $\pm i$, accordingly to Remark 3.1.3. First of all, we refer to Definition 3.3 of Gaussian prime.

Remark.

- If p is an integer, not prime, p cannot be a Gaussian prime.
- If p is a prime integer, it is not necessary a Gaussian prime.
- Every Gaussian prime of the form $a + bi$ with $b = 0$, is also a prime integer.

Example 10. The rational prime 17, is not a Gaussian prime. In fact, we can find a decomposition in $\mathbb{Z}[i]$:

$$17 = (4 + i)(4 - i).$$

Now we would like to establish a correspondence between Gaussian integers and rational primes:

Theorem 3.5. *An ordinary prime $p \in \mathbb{N}$ is a Gaussian prime if and only if $x^2 + y^2 = p$ has no solution, i.e. p is not the sum of two squares. If $p < 0$, p is Gaussian prime if and only if $-p \in \mathbb{N}$ is a Gaussian prime.*

Proof. Suppose p is an ordinary prime, not a Gaussian prime, and so it is possible to write it as a product of two Gaussian integers $p = (a+bi)(c+di)$ such that $1 < N(a+bi), N(c+di) < N(p)$. Taking the conjugate we obtain $\overline{p} = p = (a - bi)(c - di)$. Now, multiplying the two equations,

$$p^2 = (a + bi)(a - bi)(c + di)(c - di) = (a^2 + b^2)(c^2 + d^2)$$

where both these elements are different than a unit. The only factorization of p^2 is $p \cdot p$, so $p = a^2 + b^2$. On the other hand, suppose $p = a^2 + b^2$ is an ordinary prime for some $a, b \in \mathbb{Z}$. Then it has a decomposition $(a + bi)(a - bi) = p$ in $\mathbb{Z}[i]$, where

$$N(a + bi) = N(a - bi) = a^2 + b^2 = p < p^2 = N(p).$$

It follows that $p = a^2 + b^2$ has no solution if and only if p is a Gaussian prime. □

Theorem 3.6. *If $N(z)$ is a prime integer, then z is a Gaussian prime.*

Proof. Suppose z is not a Gaussian prime. Then it follows that there exist two nonzero nonunit elements v and w such that $z = vw$. Using Proposition 3.5,

$$N(z) = N(vw) = N(v)N(w).$$

Now, since $N(w)$ and $N(v)$ must be different than 1, it is possible to decompose $N(z)$. But $N(z)$, according to the hypothesis, is prime so z must be prime. □

We use this theorem to proof that the decomposition of Example 10 is a prime factorization:

Example 11. The elements $4+i$ and $4-i$ are Gaussian primes since their norms are rational primes. In fact:

$$N(4+i) = N(4-i) = 17.$$

Example 12. The converse of this theorem is false: a Gaussian prime does not necessary have a prime norm. For example, the element 3 has norm $N(3) = 9$, which is not prime, but 3 is a Gaussian prime. We show that 3 is a Gaussian prime: suppose 3 is not a Gaussian prime and try to find a decomposition, i.e. two elements such that $3 = (a+bi)(c+di)$. Since the norm is

$$9 = N(3) = N\big((a+bi)(c+di)\big) = (a^2+b^2)(c^2+d^2),$$

we are searching integer solutions of $9 = (a^2+b^2)(c^2+d^2)$, that is $a^2+b^2 = c^2+d^2 = 3$ but no such solutions exist, so the number 3 cannot be further factored.

This example is useful to think that Gaussian primes can be the elements of the form $p = a^2+b^2$, with p prime in $\mathbb{Z}$ such that this equation has no solution and this will be useful later for the classification. Moreover, we observe that we can think of a Gaussian prime as a Gaussian integer that is not the product of Gaussian integers with smaller norm.

3.1.6 Factorization

Now, we would like to focus on the problem of factorization into irreducible elements in $\mathbb{Z}[i]$. Since every Gaussian integer can be factored into irreducibles, irreducible numbers are primes. Moreover, every nonzero Gaussian integer, different than a unit, can be factored uniquely into irreducibles.

Proposition 3.11. *(Prime factorization in $\mathbb{Z}[i]$) Any Gaussian integer factorizes into Gaussian Primes.*

Remark.
- This proof tries to imitate the proof in $\mathbb{Z}$.
- As we have already said, this factorization is unique since $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. Let z be any Gaussian integer. If z is prime, then it is already factored. If z is not a prime, then there exist two Gaussian integers v and w with norm smaller than $N(z)$, such that $z = vw$. Now, if v and w are not Gaussian primes, we can factorize them into Gaussian integers, whose norm is smaller than $N(v)$ and $N(w)$. Since the norms are natural numbers, they cannot decrease infinitely many times, so we can iterate this process until we get a Gaussian prime factorization. □

3.1.7 Classification of Gaussian primes

If we take any prime number p in $\mathbb{Z}$ of the form $p = a^2 + b^2$, then if there exist in $\mathbb{Z}[i]$ two factors of p, $a+bi$ and $a-bi$, they must be Gaussian primes, since their norm is exactly the prime p. Moreover, these two factors are one the conjugate of the other, so we know that they come in pairs. Unique prime factorization in $\mathbb{Z}[i]$ establishes that this is the only decomposition of p, up to multiplication by ± 1 and $\pm i$. The other possible Gaussian primes are the integer primes that cannot be further decomposed in $\mathbb{Z}[i]$. Using a congruence argument, we would like to describe such these elements.

Proposition 3.12. *Let m be an integer.*

- *If m is odd, $m^2 \equiv 1 \pmod 4$.*
- *If m is even, $m^2 \equiv 0 \pmod 4$.*

Proof.
- If m is odd, it is possible to write it as $m = 2n + 1$ for some $n \in \mathbb{Z}$, so $m^2 = (2n + 1)^2 = 4n^2 + 4n + 1$ which implies $m^2 - 1 = 4(n^2 + n)$. Rewriting this equation through the module, we obtain $m^2 \equiv 1 \pmod 4$.
- If m is even, it is possible to write it as $m = 2n$ for some $n \in \mathbb{Z}$, so $m^2 = 4n^2$ which implies $m^2 \equiv 0 \pmod 4$ using the module.

□

Theorem 3.7. *If $p \in \mathbb{Z}$ is a prime of the form $4n + 1$, then there exists a element $m \in \mathbb{Z}$ such that $p \mid m^2 + 1$.*

Theorem 3.8 (Fermat two square Theorem)**.** *If p is a prime number ($p > 2$) such that $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.*

The proofs can be found in [Stillwell, p. 109].

Thanks to Fermat's two square Theorem, we find that all the rational integers of the form $4n + 1$, being able to be written as the sum of two squares, can be factored in $\mathbb{Z}[i]$. Using again the congruence modulo 4, it follows that the remaining elements, i.e. the numbers we can write as $4n+3$, must be the integers which is not possible to write as sum of two squares and therefore the prime elements in $\mathbb{Z}[i]$:

Proposition 3.13. *An integer prime p is a Gaussian prime if and only if $p \equiv 3 \pmod 4$*

This proof is in [Stillwell, p. 113].

Remark. Finally, summarizing, we call **Gaussian prime** a Gaussian integer with the classical form $z = a + bi$ following these properties:

(i) Given a, b nonzero elements of $\mathbb{Z}$, $z = a + bi$ is a Gaussian prime if and only if $\delta(z)$ is an ordinary prime;

(ii) Given $a = 0$, $z = bi$ is a Gaussian prime if and only if $|b|$ is an ordinary prime and $|b| \equiv 3 \pmod 4$.

(iii) Given $b = 0$, $z = a$ is a Gaussian prime if and only if $|a| \equiv 3 \pmod 4$.

Chapter 4

$\mathbb{Z}[\sqrt{2}]$

The second purpose set at the beginning of the thesis was to extend the RSA algorithm not only to the set of Gaussian integer, but also to a different set. What we would like to study now are sets of the form $\mathbb{Z}[\sqrt{d}]$, in particular, when $d = 2$, to see how its elements behave inside the set and if the construction of a "good" algorithm is possible. To succeed in this purpose, we follow the same structure of the previous chapter, starting with the description of sets of the form $\mathbb{Z}[\sqrt{d}]$ looking at [Niven], talking about $\mathbb{Z}[\sqrt{2}]$ through [Beachy-Blair] and [Artin] and finally by trying to construct the algorithm.

4.1 Sets of the form $\mathbb{Z}[\sqrt{d}]$

The purpose of introducing $\mathbb{Z}[\sqrt{d}]$ is to find roots for the polynomial x^2-dy^2, allowing the decomposition

$$x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y),$$

which is not possible in $\mathbb{Z}$, unless d is a square number. Constructing an element D such that $D^2 = d$, we can obtain the root we need and adding the element D to $\mathbb{Z}$, we finally have a set where the decomposition of the polynomial $x^2 - dy^2$ is allowed. In this chapter, we are not interested in finding a decomposition of polynomials, but the purpose is to use $\mathbb{Z}[\sqrt{d}]$ for the creation of the RSA algorithm. To ensure a proper use of this algorithm, we also need to guarantee that every element in the set has a unique factorization, but this is not always true. For this reason, after starting with a general discussion about sets of the form $\mathbb{Z}[\sqrt{d}]$, we will move to the specific case $d = 2$. Then, by proving $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain, we have found a domain for the construction of the algorithm.

The set $\mathbb{Z}[\sqrt{d}]$ is the ring generated by $\sqrt{d}$ and it can be considered as the smallest subring of $\mathbb{C}$ containing $\sqrt{d}$. Since a ring is closed under multiplication, if it contains $\sqrt{d}$, it also contains all the positive powers of

$\sqrt{d}$, with their sums and differences, including the unit 1. Following these statements, the ring contains all the complex numbers that can be expressed as a combination of powers of $\sqrt{d}$. In other words, the subring $\mathbb{Z}[\sqrt{d}]$ contains all the complex numbers of the form:

$$\beta = a_0 + a_1\sqrt{d} + a_2\sqrt{d}^2 + \cdots + a_n\sqrt{d}^n$$

so that β is obtained evaluating a polynomial whose coefficients are powers of $\sqrt{d}$ and all the a_i are in $\mathbb{Z}$.

Definition 4.1. Let d be a fixed square-free integer different than 0 and 1. **The set generated by** $\sqrt{d}$, represented by $\mathbb{Z}[\sqrt{d}]$, is defined to be the set containing all the elements of the form $a + b\sqrt{d}$, with $a, b \in \mathbb{Z}$. This set can be represented as:

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

We obtain a different behaviour depending on whether d is positive or negative. This detail is necessary, because the sets behave in a different way due to the sign of d. In particular, if $d > 0$ we have a positive real square and $\mathbb{Z}[d] \subset \mathbb{R}$ while, if $d < 0$, it is a imaginary square root so $\mathbb{Z}[d] \subset \mathbb{C}$.

Example 13. Let $d = 11$, we would like to factorize the polynomial $x^2 - \sqrt{11}x - 22$ in the set $\mathbb{Z}[\sqrt{11}]$:

$$(x + \sqrt{11})(x - 2\sqrt{11}).$$

Proposition 4.1. *Let d and f be two different non-zero rational integers, square-free and different than 1, then*

$$\mathbb{Z}[\sqrt{d}] \neq \mathbb{Z}[\sqrt{f}].$$

Proof. Suppose $\sqrt{d} \in \mathbb{Z}[\sqrt{f}]$ and so there exists $a, b \in \mathbb{Z}$ such that $\sqrt{d} = a + b\sqrt{f}$. Now, writing

$$d = a^2 + 2ab\sqrt{f} + b^2 f$$

and considering the fact that a, b, d and f are in $\mathbb{Z}$, we obtain $\sqrt{f}$ must be a rational integer. But f is square-free by definition of $\mathbb{Z}[\sqrt{f}]$ so we found a contradiction and $\sqrt{d} \notin \mathbb{Z}[\sqrt{f}]$. Since the same argument is true for $\sqrt{f} \notin \mathbb{Z}[\sqrt{d}]$, the fact that the two sets are different is proven. □

Example 14. Let $d = 2$ and $f = 3$, then $\mathbb{Z}[\sqrt{2}] \neq \mathbb{Z}[\sqrt{3}]$. In fact, $\sqrt{2} \notin \mathbb{Z}[\sqrt{3}]$ and conversely $\sqrt{3} \notin \mathbb{Z}[\sqrt{2}]$.

Proposition 4.2. $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ *is a ring.*

Proof. Let a, b, d, e, f be elements of $\mathbb{Z}$, then:

(i) it contains the zero element $0 = 0 + 0\sqrt{d}$ and the unit element $1 = 1 + 0\sqrt{d}$;

(ii) it is closed under addition: $(a+b\sqrt{d})+(e+f\sqrt{d}) = (a+e)+(b+f)\sqrt{d}$ implies $(a+e), (b+f) \in \mathbb{Z}$.

(iii) it is closed under multiplication: $(a+b\sqrt{d})(e+f\sqrt{d}) = ae+af\sqrt{d}+be\sqrt{d}+bfd = (ae+bfd)+(af+be)\sqrt{d}$ implies $(ae+bfd), (af+be) \in \mathbb{Z}$;

(iv) Additivity, commutativity and distributivity hold because $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$.

□

4.1.1 Description

Norm

Now, trying to imitate the description we have previously done of the set of Gaussian integers, we describe the set generated by $\sqrt{d}$. First of all, we introduce the notion of norm, that exists since $\mathbb{Z}[\sqrt{d}]$ is a subring of $\mathbb{C}$:

Definition 4.2. We call **norm** the function $N : \mathbb{Z}[\sqrt{\alpha}] \to \mathbb{Z}$ defined as the product of a number $\alpha = a + b\sqrt{d}$ and its conjugate $\overline{\alpha} = a - b\sqrt{d}$:

$$N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

Proposition 4.3. *If α is a non-zero element of $\mathbb{Z}[\sqrt{d}]$ and $\overline{\alpha}$ is its conjugate, then $N(\alpha) = N(\overline{\alpha})$.*

This statement is obvious from the definition of norm.

Remark. We remind that, if $\alpha \in \mathbb{Z}[\sqrt{d}]$ is a rational integer, then for the properties of the conjugate we know $\overline{\alpha}$ is a rational integer as well and $\alpha = \overline{\alpha}$.

Now we describe some properties of the norm:

Proposition 4.4. *The norm is multiplicative.*

Proof. Using the definition of conjugate, it is easy to see that $\overline{zw} = \bar{z}\bar{w}$. Now, applying that to the definition of norm:

$$N(zw) = zw\overline{zw} = z\bar{z}w\overline{w} = N(z)N(w).$$

□

Example 15. Let $d = 7$ and compute the norm of $2 + 2\sqrt{7}$ and $1 - \sqrt{7}$ in $\mathbb{Z}[\sqrt{7}]$:

$$N(2 + 2\sqrt{7}) = (2 + 2\sqrt{7})(2 - 2\sqrt{7}) = 2^2 - 7 \cdot 2^2 = -24;$$

$$N(1 - \sqrt{7}) = (1 - \sqrt{7})(1 + \sqrt{7}) = 1^2 - 7 \cdot 1^2 = -6.$$

Now, if we compute the norm of -12, we notice that, since $-12 = (1 - \sqrt{7})(2 + 2\sqrt{7})$, we can use the multiplicativity, then

$$N(-12) = N\big((1-\sqrt{7})(2+2\sqrt{7})\big) = N(1-\sqrt{7})N(2+2\sqrt{7}) = -24 \cdot -6 = 144.$$

Proposition 4.5. *Let $\alpha \in \mathbb{Z}[\sqrt{d}]$ and $N(\alpha)$ be its norm. Then:*

(i) $N(\alpha) = 0$ *if and only if* $\alpha = 0$*;*

(ii) $N(\alpha) = \pm 1$ *if and only if* α *is a unit.*

(iii) If an integer α *is not zero or a unit, then* $|N(\alpha)| > 1$*.*

Proof. (i) If $\alpha = 0$, then $\overline{\alpha} = 0$ and $N(\alpha) = 0$; conversely, if $N(\alpha) = 0$, $\alpha\overline{\alpha} = 0$ so $\alpha = 0$ and $\overline{\alpha} = 0$ because one of them must be zero and the other must be zero as well for implication.

(ii) If α is any element of $\mathbb{Z}\sqrt{2}$ and $N(\alpha) = \pm 1$, this means $N(\alpha) = \alpha\overline{\alpha} = \pm 1$, so $\alpha | 1$ or $\overline{\alpha} | 1$ which implies α is a unit. Conversely, if α is a unit, there exists an element β such that $\alpha\beta = 1$ by definition. Then $N(\alpha)N(\beta) = N(1) = 1$, but the value of the norm is an integer so $N(\alpha)$ can be either 1 or -1.

(iii) Using item (i) and (ii), this comes directly.

□

Proposition 4.6. *Let α, β be two nonzero elements of $\mathbb{Z}[\sqrt{d}]$. If $\alpha \mid \beta$ in $\mathbb{Z}[\sqrt{d}]$ then $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$.*

Proof. Since $\alpha \mid \beta$, then there exists an element γ such that $\beta = \alpha\gamma$. Then $N(\beta) = N(\alpha\gamma) = N(\alpha)N(\gamma)$ using the multiplicativity. So $N(\alpha) \mid N(\beta)$. □

Corollary 4.1. *If $\alpha \mid \beta$ then $\overline{\alpha} \mid \overline{\beta}$.*

Units

When the value of d changes, we find a number of difference between the rings. Most important, the number of units: if $d < 0$, the set has a finite number of units, while if $d > 0$, it has infinitely many units. We are more interested in the second case.

Theorem 4.2. *If d is a negative integer square-free, $\mathbb{Z}[\sqrt{d}]$ has a finite number of units. In particular, if $d = -1$ the units are ± 1 and $\pm i$; if $d = -3$ the units are ± 1, $\frac{1 \pm \sqrt{-3}}{2}$ and $\frac{-1 \pm \sqrt{-3}}{2}$, while for every other d the units are ± 1.*

Theorem 4.3. *If d is a positive square-free integer, then $\mathbb{Z}[\sqrt{d}]$ has infinitely many units.*

The proofs can be found, in detail, in [Niven, p. 428].

Irreducible elements

Definition 4.3. An integer α in $\mathbb{Z}[\sqrt{d}]$ is called **irreducible** if its divisors are only its associates and the units of $\mathbb{Z}[\sqrt{d}]$.

Theorem 4.4. *Let α be an integer in $\mathbb{Z}[\sqrt{d}]$. If α is different than zero and different than a unit, then it can be factored as a product of irreducibles.*

Proof. Let α be an element such that it is possible to write it as $\alpha = \beta\gamma$, with β, γ non-unit in $\mathbb{Z}[\sqrt{d}]$. If β and γ are irreducibles, then the process stops. If they are not, we repeat the procedure with β and γ until we find their decomposition into irreducibles. Now, $|N(\alpha)| = |N(\beta)N(\gamma)|$ by the multiplicativity of the norm, which implies

$$|N(\beta)| < |N(\alpha)| \quad \text{and} \quad |N(\gamma)| < |N(\alpha)|,$$

so the process has an end. □

This theorem establish that we have a factorization, but not if this factorization is unique. Actually, this statement cannot be shown for $\mathbb{Z}[\sqrt{d}]$ because it is not true for all values of d.

Theorem 4.5. *Let α be an integer in $\mathbb{Z}[\sqrt{d}]$ and p an irreducible in $\mathbb{Z}$. If $N(\alpha) = \pm p$ then α is irreducible in $\mathbb{Z}[\sqrt{d}]$.*

Proof. Suppose α is not irreducible, so that there exists two elements $\beta, \gamma \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha = \beta\gamma$. Using the multiplicativity of the norm, we know that

$$N(\alpha) = N(\beta)N(\gamma) = \pm p$$

that means $N(\beta)$ divides 1 or -1 and $N(\gamma)$ divides p or $-p$, or vice-versa. This implies either β or γ is a unit and the other element is an associate of p, implying p is irreducible. □

Corollary 4.6. *Let p be irreducible and u be a unit in $\mathbb{Z}[\sqrt{d}]$. Then the product pu is irreducible.*

Proof. Using Theorem 4.5, it is sufficient to say that $N(pu)$ is prime. But we know $N(p)$ is prime in $\mathbb{Z}$ and $N(u) = 1$, so using multiplicativity $N(pu) = N(p)N(u)$ which is the product of a prime by one, so $N(pu)$ is prime and pu cannot be factored, i.e. it is irreducible. □

Example 16. The number 3 is irreducible in $\mathbb{Z}[i]$, but not in $\mathbb{Z}[\sqrt{6}]$. We proved that 3 is a Gaussian prime in Example 12, so it is also irreducible since $\mathbb{Z}[i]$ is a Euclidean domain. Now we would like to show its factorization in $\mathbb{Z}[\sqrt{6}]$. We compute $N(3) = 9$ in $\mathbb{Z}[\sqrt{6}]$, so the factors we are searching are a and b in $\mathbb{Z}$ such that:

$$9 = 3 \cdot 3 = (a + b\sqrt{6})(a - b\sqrt{6})$$

and this implies $N(a+b\sqrt{6}) = N(a-b\sqrt{6}) = 3$. This equation is satisfied with $a = 3$ and $b = 1$, so 3 is not irreducible in $\mathbb{Z}[\sqrt{6}]$ since we have found a factorization

$$3 = (3-\sqrt{6})(3+\sqrt{6}).$$

Unique factorization

The purpose we have set at the beginning of this work was to find a suitable set for the construction of the RSA algorithm. Since the final aim of the algorithm is to encrypt and decrypt a message, it is necessary that all the communications can be exclusively represented. For this reason, we have to exclude all the sets which do not guarantee a unique factorization. Specifically, $\mathbb{Z}[\sqrt{d}]$ is it not necessarily a unique factorization domain, so is not in general suitable for our aim.

Example 17. We would like to show that the ring $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ is not a unique factorization domain. The norm on this ring is defined to be

$$N(a+b\sqrt{5}) = (a+b\sqrt{5})(a-b\sqrt{5}) = a^2 - 5b^2.$$

Let 6 be the element in $\mathbb{Z}[\sqrt{-5}]$ we would like to decompose and we write it as:

$$3 \cdot 2 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

Now, we need to show these elements are all irreducible:

- We show that the equation $a^2 - 5b^2 = 2$ has no integer solution, so there not exists in $\mathbb{Z}[\sqrt{-5}]$ elements with norm 2. We suppose it is possible to write $2 = xy$ a decomposition with x and y non-units in $\mathbb{Z}[\sqrt{-5}]$ whose norm is $N(2) = N(xy) = N(x)N(y) = 4$. But the only possible combinations to obtain 4 are $N(x) = 1$ and $N(y) = 4$, which are not possible since x is not a unit, and $N(x) = N(y) = 2$, that is a contradiction because the equation of the norm has no solution for 2.

- We use a similar argument to show that 3 is irreducible.

- Now, we consider the element $1+\sqrt{-5}$ and we would like to show there exists a decomposition $1+\sqrt{-5} = xy$ with x and y non-units in $\mathbb{Z}[\sqrt{-5}]$. We compute the norm $N(1+\sqrt{-5}) = N(x)N(y) = 6$ and since the previous arguments are still true, $N(x)$ and $N(y)$ cannot be 2 or 3 and therefore not even 6. This implies the norm cannot be decomposed so the element is irreducible.

- Since $N(1+\sqrt{-5}) = N(1-\sqrt{-5})$, we use the same argument to say $1-\sqrt{-5}$ is irreducible.

4.2 The ring $\mathbb{Z}[\sqrt{2}]$

Let d be 2 and study the ring generated by $\sqrt{2}$. The reason we decide to focus on this set is that we need an Euclidean domain for the creation of a working RSA algorithm, so the final purpose of this section is to describe $\mathbb{Z}[\sqrt{2}]$ and to show it is such this domain.

This ring, denoted by $\mathbb{Z}[\sqrt{2}]$ has the form:

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

The set generated by $\sqrt{2}$, $\mathbb{Z}[\sqrt{2}]$, is the smallest ring containing $\mathbb{Z}$ and the root $\sqrt{2}$ and, since $d > 0$, it is a subring of $\mathbb{R}$. Inside this set, we are able to factor all the polynomials that have $\sqrt{2}$ as a solution, such as $x^2 - 2$, which is decomposable as

$$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}).$$

Example 18. We would like to decompose the polynomial $x^4 - x^2 - 2$. The first step can be done in $\mathbb{Z}$, since $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$. Then $x^2 - 2$ can be further divided in $\mathbb{Z}[\sqrt{2}]$ into $(x + \sqrt{2})(x - \sqrt{2})$ obtaining:

$$x^4 - x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})(x^2 + 1).$$

We notice $x^2 + 1$ is not factorizable in $\mathbb{Z}[\sqrt{2}]$ since it not contains the roots $\pm i$. On the other hand, in $\mathbb{Z}[i]$ the factorization would have been $x^4 - x^2 - 2 = (x + i)(x - i)(x^2 - 2)$, while in $\mathbb{C}$ we would have both of them

$$x^4 - x^2 - 2 = (x + i)(x - i)(x + \sqrt{2})(x - \sqrt{2}).$$

Proposition 4.7. *If α can be written as $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, with $a, b \in \mathbb{Z}$, this is the unique representation of the element in the ring.*

Proof. Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$. Then $a_1 - a_2 = (b_1 - b_2)\sqrt{2}$ with $a_1 - a_2 \neq 0$ and $b_1 - b_2 \neq 0$, so we can divide by $b_1 - b_2$. This means $\sqrt{2}$ is rational, which is a contradiction. So $a_1 = a_2$ and $b_1 = b_2$ giving the uniqueness of the representation. □

Units

We have already seen in Proposition 4.3 that a set with $d > 0$ has infinitely many units, so this is true for $d = 2$. What we would like to know now is how the units of $\mathbb{Z}[\sqrt{2}]$ look like:

Proposition 4.8. *The elements of the form $(1 + \sqrt{2})^n$, with $n \in \mathbb{Z}$ are units in $\mathbb{Z}[\sqrt{2}]$.*

Proof. We know from Proposition 4.5 that all the units are elements with norm ± 1 so that $N(a + b\sqrt{2}) = a^2 - 2b^2 = \pm 1$. It is easy to choose $a = 1$ and $b = 1$ to find a solution to this equation, so $1 + \sqrt{2}$ is a unit. Moreover, all its powers satisfies the equation, giving that $(1 + \sqrt{2})^n$ are all units with $n \in \mathbb{Z}$. □

Example 19. In the proposition, n is taken to be a rational integer, so here an example with negative power:

$$(1+\sqrt{2})^{-1} = 1-\sqrt{2}.$$

This proposition ensure that the ring generated by $\sqrt{2}$ has infinitely many units, since we can find infinitely any elements of the form $(1+\sqrt{2})^n$. What we do not know is if there are units with a different form. To answer to this question, we need to introduce the Pell's equation. It turns out that any unit must be in this form, see for example [Conrad2].

Euclidean Domain

Using the definition previously seen, we notice that the norm here is the function $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ such that, if $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, then:

$$N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2.$$

It is important to notice that the norm is not necessary positive. For this reason we cannot use this definition of norm to construct a Euclidean domain. What we can do, then, is taking the absolute value of the norm and prove:

Theorem 4.7. *Using the the norm function with the absolute value, $\mathbb{Z}[\sqrt{2}]$ is a Euclidean Domain.*

Proof. To prove $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain, it is enough to show that it satisfies the properties of the definition using the norm with the absolute value. Let $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$ two non-zero elements of $\mathbb{Z}[\sqrt{2}]$:

(i) From the definition of norm, $|N(\alpha)| = |a^2 - 2b^2|$ and

$$|N(\alpha\beta)| = |(a^2-2b^2)(c^2-2d^2)| = |(a^2-2b^2)| \cdot |(c^2-2d^2)|.$$

Now, $\beta \neq 0$ implies $|c^2 - 2d^2| \neq 0$ and $|c^2-2d^2| \geq 1$ thanks to the absolute value, so the first statement follows:

$$|N(\alpha\beta)| \geq |a^2-2b^2| = |N(\alpha)|.$$

(ii) Having α and β, we want to find two elements $\rho, \gamma \in \mathbb{Z}[\sqrt{2}]$ such that $\alpha = \beta\gamma + \rho$. First, we write this equation as

$$\rho = \beta\Big(\frac{\alpha}{\beta} - \gamma\Big)$$

with $\frac{\alpha}{\beta}$, not necessarily in $\mathbb{Z}[\sqrt{2}]$. Since we are not sure $\frac{\alpha}{\beta} \in \mathbb{Z}[\sqrt{2}]$, we cannot apply the given definition of norm to it. For this reason, after computing $\frac{\alpha}{\beta}$, supposing $\frac{\alpha}{\beta} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$, we round the values a and b to the nearest integer $\tilde{a}$ and $\tilde{b}$, obtaining $\tilde{\alpha} = \tilde{a} + \tilde{b}\sqrt{2}$ so

that we are sure $\tilde{\alpha}$ is in $\mathbb{Z}[\sqrt{2}]$. What we have now are $\rho = \beta\left(\frac{\alpha}{\beta} - \gamma\right)$ and $\rho = \beta(\tilde{\alpha} - \gamma)$ with $\tilde{\alpha} \in \mathbb{Z}[\sqrt{2}]$ and $\frac{\alpha}{\beta} \in \mathbb{R}$, but not necessarily in $\mathbb{Z}[\sqrt{2}]$. This two different evaluations of ρ are not necessarily the same, since $\tilde{\alpha}$ and $\frac{\alpha}{\beta}$ are not necessarily equal. Then we write $\frac{\alpha}{\beta} = x + y\sqrt{2}$ with $x, y \in \mathbb{Q}$ and, rounding off x and y respectively to the nearest integer, we obtain $\tilde{x} + \tilde{y}\sqrt{2}$. This value is in $\mathbb{Z}[\sqrt{2}]$, since $\tilde{x}$ and $\tilde{y}$ are in $\mathbb{Z}$ and it is assigned to γ. Now, $\rho = \alpha - \gamma\beta$ turns out to be in $\mathbb{Z}[\sqrt{2}]$ as well and we have found two elements $\gamma, \rho \in \mathbb{Z}[\sqrt{2}]$ which make the equation $\alpha = \gamma\beta + \rho$ true. Now we need to guarantee $|N(\rho)| < |N(\beta)|$. We would like to compute the norm of ρ, but we need to use the classical definition with the absolute value since $\frac{\alpha}{\beta}$ is not necessarily an element of $\mathbb{Z}[\sqrt{2}]$and we are not sure $N(\frac{\alpha}{\beta})$ is defined. Then

$$|N(\rho)| = |N(\alpha - \gamma\beta)| = |N(\beta)|\left|\frac{\alpha}{\beta} - \rho\right|.$$

In order to complete the proof, we need $\left|\frac{\alpha}{\beta} - \rho\right| < 1$, but this is easily done by reminding that the notion of norm is a distance. In fact, $\frac{\alpha}{\beta}$ was defined as $x + y\sqrt{2}$ while ρ is $\tilde{x} + \tilde{y}\sqrt{2}$ and substituting

$$\left|\frac{\alpha}{\beta} - \rho\right| = \left|(x - \tilde{x})^2 - 2(y - \tilde{y})^2\right| \leq |x - \tilde{x}|^2 + 2|y - \tilde{y}|^2 \leq \left(\frac{1}{4} + 2 \cdot \frac{1}{4}\right) = \frac{3}{4}.$$

Substituting in the previous inequality, this yields

$$|N(\rho)| \leq |N(\beta)|.$$

□

Being a Euclidean domain implies that $\mathbb{Z}[\sqrt{2}]$ is also a unique factorization domain. For this reason prime elements and irreducible elements coincide on it.

Chapter 5

RSA extended algorithm

5.1 Modular arithmetic

5.1.1 Modular arithmetic in $\mathbb{Z}[i]$

The aim of this section is to describe modular arithmetic in the ring of Gaussian integers and its properties, trying to imitate what happens for integers. To do that, we refer to [Conrad] to better understand what happens in $\mathbb{Z}[i]$ and then we look at [Beachy-Blair] for the congruence of rational integers, to do the same with Gaussian integers.

Definition 5.1. Let z, w, γ be Gaussian integers. We say z is **congruent** to w modulo γ, and we write $z \equiv w \pmod{\gamma}$ when $\gamma \mid (z - w)$, i.e. there exists a Gaussian integer α, such that $z = w + \alpha\gamma$. We say γ is the **module** of the congruence relation.

Proposition 5.1. *The congruence relation is an equivalence relation.*

Proof.

- Reflexivity: $z \equiv z \pmod{\gamma}$ since $\gamma | z - z = 0$;
- Symmetry: $z \equiv w \pmod{\gamma}$ implies $w \equiv z \pmod{\gamma}$. In fact, $\gamma|(z - w)$ implies $\gamma| - (w - z) = -w + z$;
- Transitivity: $z \equiv w \pmod{\gamma}$ and $w \equiv x \pmod{\gamma}$ implies $z \equiv x \pmod{\gamma}$. In fact, $\gamma|(w - z)$ and $\gamma|(x - w)$ implies $\gamma|(x - z) = (x - w + w + z)$.

□

Let us consider $a \equiv b \pmod{n}$ in $\mathbb{Z}$, then we may assume $0 \leq b < n$. In fact, since $a = nc + b$ for some $c \in \mathbb{Z}$ by definition of module, using the division theorem algorithm it is clear that b is the remainder of the division by n. Once again, we need to introduce the notion of norm to compare Gaussian integers. Moreover, writing an equivalence relation in $\mathbb{Z}$, the possible values for b are $0, 1, \ldots, n-1$, so what we would like to ensure now is $N(w) < N(\gamma)$. Let us focus our attention on the division theorem in $\mathbb{Z}[i]$ which becomes:

Theorem 5.1 (Division Theorem for Gaussian integers)**.** *Let z and w be non-zero Gaussian integers, then there exist $\gamma, \rho \in \mathbb{Z}[i]$ such that*

$$z = \gamma w + \rho$$

with $N(\rho) < N(w)$ or $\rho = 0$.

The proof of this theorem comes directly from the fact that the ring of Gaussian integers is a Euclidean domain (Theorem 3.4).

We notice that the size of the remainder, given by the norm, is bound by the size of w so that this theorem still preserves a property of reduction. To better understand the application of the theorem, we are going to see an example:

Example 20. Let $z = 21 - 13i$ and $w = 5 + 3i$. We want to do the division, obtaining as a result a number inside $\mathbb{Z}[i]$. We proceed with the classical division:

$$\frac{(21 - 13i)(5 - 3i)}{(5 + 3i)(5 - 3i)} = \frac{66 - 128i}{34} = \frac{33}{17} - \frac{64}{17}i.$$

The problem is that $\frac{33}{17}$ and $-\frac{64}{17}$ are not integers, so this is not a Gaussian integer. This issue is solved by rounding off those values to the nearest integer, in such a way that $\frac{33}{17} \approx 2$ while $-\frac{64}{17} \approx -4$ and we put $\gamma = 2 - 4i$. Then, using the division theorem, $\rho = z - w\gamma$ and substituting, we obtain:

$$\rho = (21 - 13i) - (5 + 3i)(2 - 4i) = -1 + i.$$

Finally, it is necessary to compute $N(\rho) = N(-1 + i) = 2$ and $N(w) = N(5 + 3i) = 34$ to check $N(\rho) < N(w)$ so that the condition of the theorem is verified.

Remark. Looking at this proof, we notice another difference between the division theorem algorithm in $\mathbb{Z}$ and in $\mathbb{Z}[i]$: here, the fact that γ and ρ are unique is missing. So the property of uniqueness in $\mathbb{Z}[i]$ is not satisfied.

We would like to see the behaviour of rational integers inside the set of Gaussian integers, to verify that the congruences in $\mathbb{Z}$ are not changed by the introduction of modules in $\mathbb{Z}[i]$. Then, we want to come to the conclusion that modular arithmetic in $\mathbb{Z}[i]$ behaves like modular arithmetic in $\mathbb{Z}$. To do that, we use:

Proposition 5.2. *Let $a, b, n \in \mathbb{Z}$, then $a \equiv b \pmod{n}$ in $\mathbb{Z}$ if and only if $a \equiv b \pmod{n}$ in $\mathbb{Z}[i]$.*

Proof. Using the definition of congruence, we can rewrite $a \equiv b \pmod{n}$ as $n \mid (a - b)$, so the problem is now about divisibility. Any rational integer c divides a Gaussian integer $z = x + yi$ if and only if there exists two elements $k, h \in \mathbb{Z}$ such that $x + yi = c(h + ki)$, i.e. $x = ch$ and $y = ck$. This is

equivalent to say that $c \in \mathbb{Z}$ divides $z = x + yi \in \mathbb{Z}[i]$ if and only if $c \mid x$ and $c \mid y$. Then, supposing $y = 0$, $z = x$ is a rational integer, so divisibility in $\mathbb{Z}[i]$ preserves divisibility in $\mathbb{Z}$ which means modular arithmetic in $\mathbb{Z}[i]$ preserves modular arithmetic in $\mathbb{Z}$, by definition 5.1. □

Therefore, if the congruence is zero, this means equality between z and γ so, in general, we assume $w \neq 0$. Then, if we use the division algorithm, we notice $z = \gamma w + \rho$, with $0 \leq N(\rho) < N(w)$, and it follows immediately that $z \equiv \rho \pmod{\gamma}$.

Example 21. The equivalence $9 + 14i \equiv 2 + 3i \pmod{1 - 2i}$ is true, since $9 + 14i = (2 + 3i) + (-3 + 5i)(1 - 2i)$. To check this fact, it is enough to subtract and divide, obtaining:

$$\frac{(9 + 14i) - (2 + 3i)}{1 - 2i} = \frac{7 + 11i}{1 - 2i} = \frac{(7 + 11i)(1 + 2i)}{(1 - 2i)(1 + 2i)} = -\frac{15}{5} + \frac{25}{5}i = -3 + 5i.$$

In the same way we create a division algorithm, it is possible to do the analogous for the Euclidean algorithm: let $z, w \in \mathbb{Z}[i]$ be two Gaussian integers such that $z > w > 0$, then applying recursively the division algorithm we obtain the following:

$$\begin{array}{ccc} z = w\gamma_0 + \rho_0 & \text{with} & N(\rho_0) < N(w) \\ w = \rho_0\gamma_1 + \rho_1 & \text{with} & N(\rho_1) < N(\rho_0) \\ \rho_0 = \rho_1\gamma_2 + \rho_2 & \text{with} & N(\rho_2) < N(\rho_1) \\ \vdots & & \vdots \end{array}$$

The proof has the same procedure as the proof in $\mathbb{Z}$. We can see it in [Conrad, p. 7].

Proposition 5.3. *Let z and w be Gaussian integers and $d \in \mathbb{Z}[i]$ a greatest common divisor of z and w. Then $N(d) \mid N(z)$ and $N(d) \mid N(w)$.*

The proof of this proposition comes directly from the definition of norm, applying the multiplicativity property. Using it, we can give the following:

Example 22. We compute $d = (z, w)$ using the Euclidean algorithm. Let $z = 87 - 53i$ and $w = 28 - 6i$, then $d = 3 + 2i$ by the following computations:

$$\begin{array}{rcccccc} 87 - 53i = & (3 - i) & \cdot & (28 - 6i) & + & 9 - 7i \\ 28 - 6i = & (2 + i) & \cdot & (9 - 7i) & + & 3 + 2i \\ 9 - 7i = & (1 - 3i) & \cdot & (3 + 2i). & & \end{array}$$

Proposition 5.4. *Let z and w be Gaussian integers and $d \in \mathbb{Z}[i]$ be their greatest common divisor obtained by the use of the Euclidean algorithm. Any other greatest common divisor of z and w is given by the multiplication of d by a unit.*

5.1.2 Modular arithmetic in $\mathbb{Z}[\sqrt{2}]$

We would like to describe also what happens in the ring generated by $\sqrt{2}$, the second set we are going to use to create the RSA algorithm. As we have already done in Chapter 3, we generalize the theory written for Gaussian integers. Actually, we are not going to prove all the properties again, but we generalize the definition of modular arithmetic and we show some examples to see how modules behave in this set. The different notions can be in some sense rewritten by replacing $\mathbb{Z}[i]$ with $\mathbb{Z}[\sqrt{2}]$.

First, let us take two elements z and w to see how modular arithmetic behaves with them:

Example 23. We would like to check if the following equivalence is true: $27 - 8\sqrt{2} \equiv 4 + 3\sqrt{2} \pmod{5 - 3\sqrt{2}}$. In other words, we are asking if there exists an element w such that $27 - 8\sqrt{2} = (5 - 3\sqrt{2})w + (4 + 3\sqrt{2})$. This is true for $w = 7 + 2\sqrt{2}$.

The division algorithm turns out to be:

Example 24. If $z = 45 - 11\sqrt{2}$ and $w = 4 + 5\sqrt{2}$, then dividing z by w:

$$\frac{(45 - 11\sqrt{2})(4 - 5\sqrt{2})}{(4 + 5\sqrt{2})(4 - 5\sqrt{2})} = \frac{290 - 269\sqrt{2}}{-34} = -\frac{290}{34} + \frac{269}{34}\sqrt{2}.$$

Now, $-\frac{290}{34}$ and $\frac{269}{34}$ are not elements of $\mathbb{Z}$, so we try to round them of to obtain two suitable values. Allocating the values

$$-\frac{290}{34} \approx -9 \quad \text{and} \quad \frac{269}{34} \approx 8$$

we obtain

$$r = (45 - 11\sqrt{2}) - (4 + 5\sqrt{2})(-9 + 8\sqrt{2}) = 1 + 2\sqrt{2}$$

and since the norms computed with the absolute value are $|N(1+2\sqrt{2})| = 7$ and $|N(4+5\sqrt{2})| = 34$, $N(r) < N(w)$ and the division algorithm is correct.

Let us finally compute a greatest common divisor using the Euclidean algorithm in $\mathbb{Z}[\sqrt{2}]$:

Example 25. We are searching $(67 + 47\sqrt{2}, 7 + 2\sqrt{2}) = 3 + 2\sqrt{2}$:

$$\begin{aligned}
67 + 47\sqrt{2} &= (7 + 2\sqrt{2}) \cdot (5 + 6\sqrt{2}) + (-4 - 5\sqrt{2}) \\
7 + 2\sqrt{2} &= (-4 - 5\sqrt{2}) \cdot (2 - \sqrt{2}) + (5 + 3\sqrt{2}) \\
-4 - 5\sqrt{2} &= (5 + 3\sqrt{2}) \cdot (1 - 2\sqrt{2}) + (3 + 2\sqrt{2}) \\
5 + 3\sqrt{2} &= (3 + 2\sqrt{2}) \cdot (3 - \sqrt{2}).
\end{aligned}$$

5.1.3 Representation of elements of $\mathbb{Z}[i]$

We have already said that the ring of Gaussian integers is included in the ring of complex numbers and, for this reason, it is possible to represent all the elements of $\mathbb{Z}[i]$ on the Cartesian plane. We are going to show an example to see what happens. Suppose we would like to plot an element $z \in \mathbb{Z}[i]$ and all its multiples: let $z = 3 + 2i$ and compute its multiples, which have the form

$$(3 + 2i)(x + yi) = (3 + 2i)x + (3 + 2i)yi = (3 + 2i)x + (3i - 2)y$$

with $x, y \in \mathbb{Z}$. We start putting the element $z = 3 + 2i$ on the Cartesian

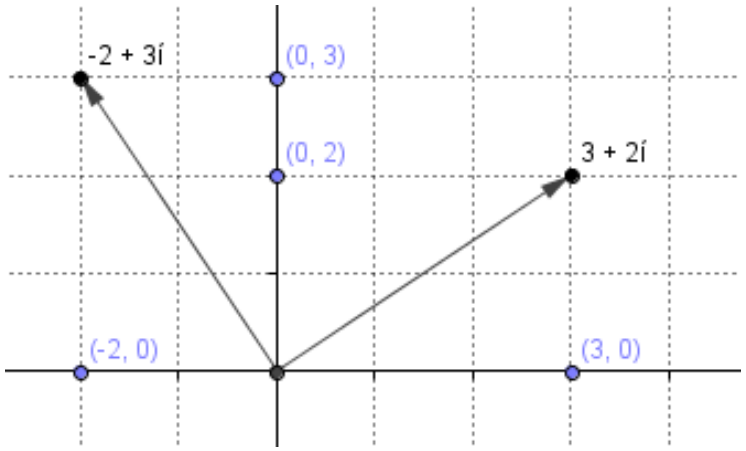

Figure 5.1: The elements $3 + 2i$ and $-2 + 3i$.

plane, in the position $Z = (3, 2)$, while $w = 3i - 2$ is the point $W = (-2, 3)$ (see Figure 5.1). So, in general, we can plot every Gaussian integer of the form $a + bi$ into the point (a, b), so that we have the correspondence

$$a + bi \leftrightarrow (a, b)$$

in the same way we do for complex numbers. All the multiples of $3 + 2i$ are now the integral combinations of w and z as we can see in Figure 5.2, where the multiples of $3 + 2i$, which is a vertex of one of the squares, come out to be the vertices of all the squares. Thinking inside modular arithmetic, all these vertices are the numbers w which satisfy the equivalence

$$w \equiv 0 \pmod{3 + 2i}.$$

In other words, two Gaussian integers are congruent if they are located in the same position on the squares. It is possible to generalize this condition, saying that two Gaussian integers are congruent if they are located in the same position also inside the squares. But, why this is possible? We notice

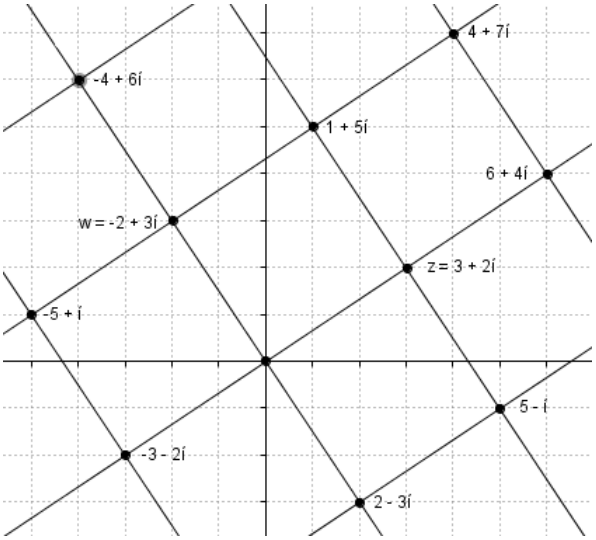

Figure 5.2: The multiples of $3+2i$.

in the figure that every square shares every side with another square and, in particular, with four other squares. If we want to move from one square to a next one, it is enough to add one of the following numbers:

$$3+2i; -3-2i; -2+3i; 2-3i,$$

i.e.

$$3+2i; -1(3+2i); i(3+2i); -i(3+2i).$$

In the same way, if we want to move in any square of the plane, we add one of the Gaussian multiple of $3+2i$.

As we can see in Figure 5.3, the Gaussian integers $5+2i$, $3i$ and $3+5i$ are congruent modulo $3+2i$. In fact, we can write them as:

$$\begin{array}{rcccccc} 5+2i = & (3+2i) & \cdot & 1 & + & 2 \\ 3i = & (3+2i) & \cdot & i & + & 2 \\ 3+5i = & (3+2i) & \cdot & (1+i) & + & 2 \end{array}$$

In Figure 5.4, we can see another example in which all the Gaussian integers congruent $4+i$ modulo $3+2i$ are shown. We notice they are of the form

$$w \equiv 1-i \pmod{3+2i}$$

and the number $1-i$ can be deduce from the graph, considering the distance of the points with the vertices of the squares.

Remark. Using this representation, it is easy to notice the non uniqueness of the representation of a number. In fact, we can consider the distance of every point with four different vertices, so we have four different possible way to write it.

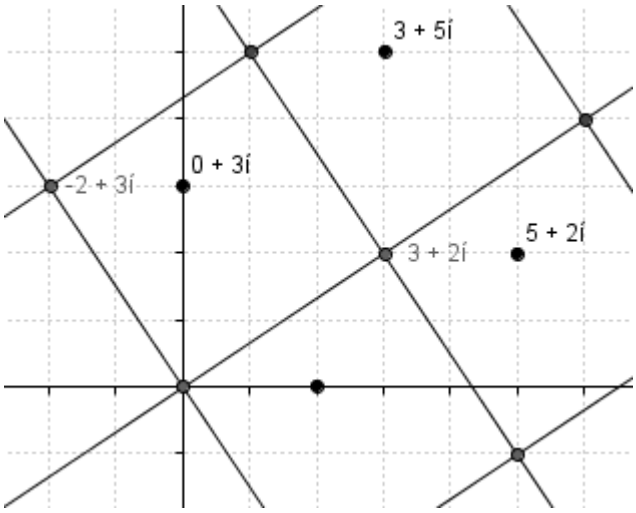

Figure 5.3: Congruences modulo $3 + 2i$.

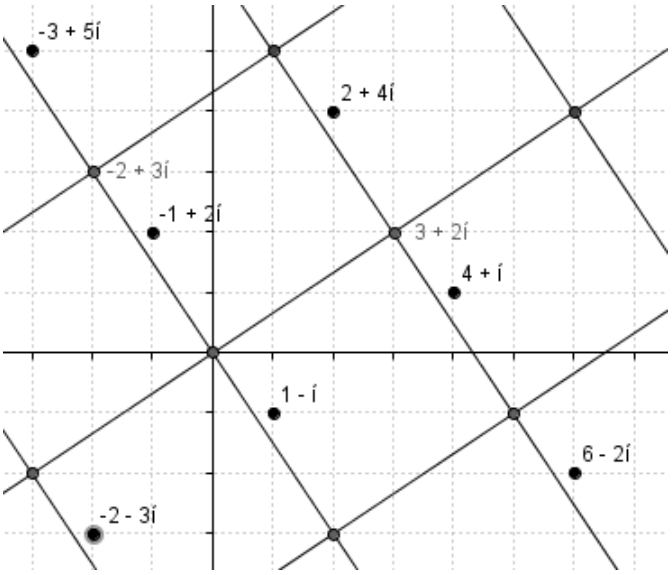

Figure 5.4: Congruences modulo $3 + 2i$.

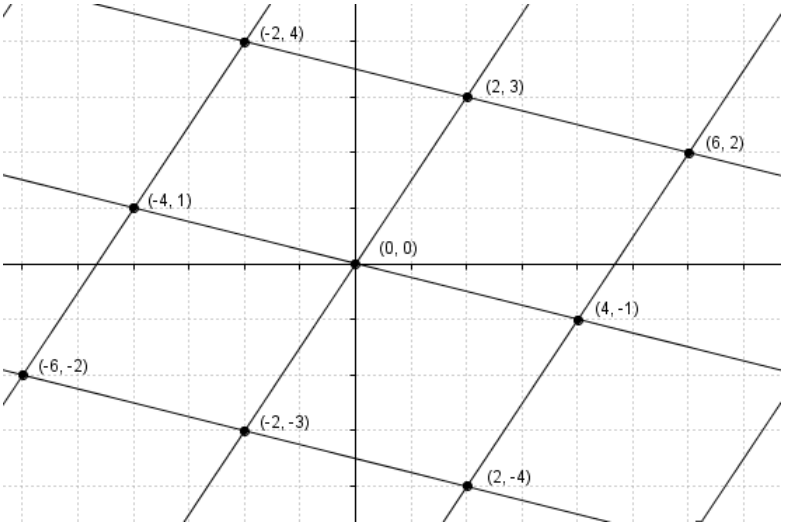

Figure 5.5: Multiples of $3 + 2\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$.

5.1.4 Representation of elements of $\mathbb{Z}[\sqrt{2}]$

The same representation can be use to see what happens in the ring generated by $\sqrt{2}$. In fact, we can plot every number of the form $a + b\sqrt{2}$ inside the Cartesian plane, in the point (a, b). In this way, the value of a is plotted on the x axis, while the value of b, corresponding to the number multiplied by $\sqrt{2}$, is plotted on the y axis.

We can see in Figure 5.5 what happens for the value $2 + 3\sqrt{2}$. We can write all the multiples of $2 + 3\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ as:

$$(2 + 3\sqrt{2})(x + y\sqrt{2}) = (2 + 3\sqrt{2})x + (6 + 2\sqrt{2})y,$$

i.e. as the linear combination of $2+3\sqrt{2}$ and $6+2\sqrt{2}$. For example, if $x = 1$ and $y = -1$, we obtain the value

$$(2 + 3\sqrt{2}) - (6 + 2\sqrt{2}) = -4 + \sqrt{2}$$

while if $x = 2$ and $y = -1$ we have

$$2(2 + 3\sqrt{2}) - (6 + 2\sqrt{2}) = -2 + 4\sqrt{2}.$$

Now, searching the points which have the same position inside the squares, we find once again all the elements congruent modulo $2 + 3\sqrt{2}$ to the same value. For example, in Figure 5.6 we notice that $2, -3\sqrt{2}, -2 + \sqrt{2}, -4 - \sqrt{2}, 4 + \sqrt{2}, \ldots$ are congruent to 2 modulo $2 + 3\sqrt{2}$. In fact:

$$\begin{aligned} 2 &= (2 + 3\sqrt{2}) \cdot 0 + 2 \\ -3\sqrt{2} &= (2 + 3\sqrt{2}) \cdot (-1) + 2 \\ -2 + \sqrt{2} &= (2 + 3\sqrt{2}) \cdot (1 - \sqrt{2}) + 2. \end{aligned}$$

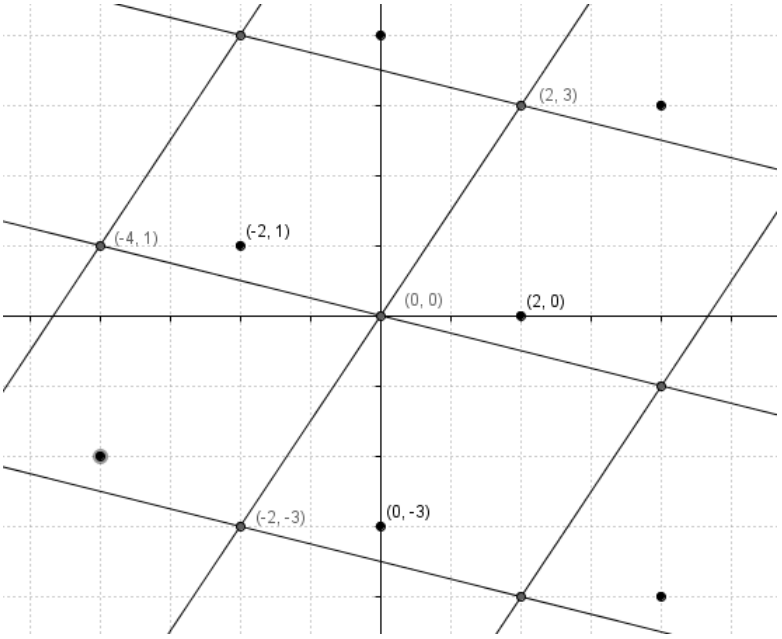

Figure 5.6: Congruences in $\mathbb{Z}[\sqrt{2}]$.

5.2 Euler's ϕ-function

From now on, we will talk about $\mathbb{Z}[\sqrt{d}]$ implying $d = -1$ or $d = 2$, so that we are sure that we are working with Euclidean Domains, i.e. inside rings where the factorization is unique. The aim of this section is to give the definition of Euler's ϕ-function inside the extensions of $\mathbb{Z}$ previously analysed. At the end, we would like to give a new version of Euler's and Fermat's Little Theorems. To write this section we mostly consider [Conrad].

Reminding the statement of Fermat's Little Theorem in $\mathbb{Z}$ (Theorem 2.4), an intuitive way to rewrite it in $\mathbb{Z}[\sqrt{2}]$ will be: given z and p non-zero elements in $\mathbb{Z}[\sqrt{d}]$, with p prime, then

$$z^{p-1} \equiv 1 \pmod{p}.$$

Unfortunately, this equivalence is not true. In fact, it is easy to find a counterexample in $\mathbb{Z}[i]$: taking the Gaussian prime $p = 7$ and the unit $z = i$ (we have previously shown 7 is a Gaussian prime) and applying the theorem, we get

$$i^{7-1} = i^6 = -1 \not\equiv 1 \pmod{7}.$$

Despite this new version of the theorem is not working, there is a way to find a good one. We start going back to the meaning of the value a^{p-1}, where a is any rational integer and p is a prime integer. We defined the ϕ-function to be the number of all possible integers ranging from 1 to p, coprime with

p itself. In other words, $\phi(p) = p - 1$ is the number of non-zero elements modulo p that are the possible solutions for the equivalence

$$a \equiv b \pmod{p}$$

with $a, b, p, \in \mathbb{Z}$, i.e. $1, 2, \ldots, p-1$. So the exponent is given by the number of all non-zero elements modulo p. What we need now, is to find a formula to compute the number of such elements, which we define to be the size $s(z)$ of the set of all non-zero elements modulo p. To do that, we first need some propositions:

Proposition 5.5. *Let a be a non-zero element of $\mathbb{Z}$. Then the size is*

$$s(a) = a^2.$$

Proposition 5.6. *Let $z = a + b\sqrt{d}$ be a non-zero element of $\mathbb{Z}[\sqrt{d}]$, with $a, b \in \mathbb{Z}$. Then, writing $\overline{z} = a - b\sqrt{d}$, we obtain*

$$s(z) = s(\overline{z}).$$

Proposition 5.7. *The size function is multiplicative, so for z and w in $\mathbb{Z}[\sqrt{d}]$:*

$$s(zw) = s(z)s(w).$$

It is possible to find the proofs of these propositions in [Conrad, p. 22] and, putting them together, we will obtain finally:

Theorem 5.2. *Let z be a non-zero element of $\mathbb{Z}[\sqrt{d}]$. Then*

$$s(z) = N(z).$$

So this theorem gives a proof of the fact that this size function is exactly the norm. So, now we have a value for the size, we obtain:

Theorem 5.3 (Fermat's little Theorem)**.** *Let p be a prime number in $\mathbb{Z}[\sqrt{d}]$. Then, for every $z \in \mathbb{Z}[\sqrt{d}]$,*

$$z^{N(p)-1} \equiv 1 \pmod{p}.$$

This proof is in [Conrad, p. 21].

Theorem 5.4 (Euler's Theorem)**.** *If z and w are coprime in $\mathbb{Z}[\sqrt{d}]$, then*

$$z^{\phi(w)} \equiv 1 \pmod{w}.$$

This proof is done trying to imitate the proof in $\mathbb{Z}$, so we remind to [Beachy-Blair, p. 41].

To let the RSA algorithm work, we need the value of the Euler's ϕ-function of a number $n \in \mathbb{Z}[\sqrt{d}]$, composed by the product of two coprime

numbers p and q in $\mathbb{Z}[\sqrt{d}]$. Even if we proved the multiplicativity of the size function, we cannot use this property to compute all the norms as the product of primes factor of a number. On the other hand, in the RSA algorithm we are not computing the norm af a product of two general numbers. In fact, since p and q are primes different from each other, they are coprime numbers. We proved in Chapter 2 some theorems about the totient function and, in particular, using Theorem 2.1 with $k = 1$, we obtain

$$\phi(p) = N(p) - 1$$

when p is prime in $\mathbb{Z}[\sqrt{d}]$. Moreover, when p and q are coprimes,

$$\phi(pq) = \phi(p)\phi(q)$$

using Theorem 2.1. So, putting together these two statements, we obtain:

Theorem 5.5. *Let p and q be two elements of $\mathbb{Z}[\sqrt{d}]$ and suppose p and q are coprime. Then the Euler's ϕ-function of $n = pq$ is:*

$$\phi(n) = \phi(p)\phi(q) = (N(p) - 1)(N(q) - 1).$$

Chapter 6

Analysis of the algorithm

Now we are going to show in detail the RSA modified algorithms for both $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$. In general, these codes follow the steps of the RSA classical algorithm described in Section 2.3, but all the properties described in Chapter 3 and 4 must be taken into account, to be sure we are creating a working and usable algorithm. Before starting, we should point out that the full version of the codes can be found in Appendix A at the end of this work.

6.1 The codes

Before proceeding with the description, we briefly describe the codes written: in fact, to achieve our purpose the creation of four different codes was necessary. Two algorithms are the proper RSA, one for each of the two considered rings and, like in the classical case, they can be both divided into three different algorithms:

- the creation of the public key and the secret key. They contain all the elements we need for the successive computations and they are created taking into account all the properties needed. The two keys given as output are of the form:

$$P_k = [n, e] \quad \text{and} \quad S_k = [p, q, d];$$

- the encryption algorithm, which takes the plaintext as input and gives back the ciphertext:

$$P^e \equiv C \pmod{n};$$

- the decryption algorithm, which transforms the ciphertext into the original message:

$$C^d \equiv P \pmod{n}.$$

As we can see, to let these algorithms work, we must be able to compute modules inside $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$. This is the reason for writing the two algorithms `functmod` and `functmod2`. These two algorithms, even if with some differences, work in the same way:

- by taking as input the plaintext or the ciphertext, P, the encryption or decryption exponent e and the modular power n;
- by computing the division of P^e by n and by rounding off the result, using the division theorem, obtaining q;
- by computing
$$P^e - n \cdot q,$$
which is the output of these algorithms.

6.1.1 Theoretical aspects

Inside the RSA algorithm, besides the computations, we also use some checks, to ensure that every theoretical property is satisfied and so that mistakes are avoided.

(i) First of all, we write a `while` loop to let the norms of p and q be primes, so that p and q are primes as well. The primality condition of the two numbers is a request of the RSA algorithm.

(ii) Then, after computing the encryption and the decryption exponent, we verify $ed \equiv 1 \pmod{s}$, in accordance with Fermat's Little Theorem.

(iii) Another important rule we need to satisfy is that the norm of the message must be less than the norm of n. The reason behind this request comes from the fact that a bigger norm would signify that also the number is bigger than n but this implies we would never obtain the same message back, since the modular computations provide results smaller than the module itself.

(iv) Finally, we insert an `if` statement at the end of the algorithm, to be sure that the original message and the final message correspond, i.e. that the transmission occurred correctly.

6.1.2 Practical aspects

When we decide to write the code, we need to remind that we do not have the possibility to be realistic, since the security of this algorithm is based on the creation of very large numbers, unusable by our computers. This is the reason we create an algorithm working only for small numbers, even if it would be possible to increase the size, having a more powerful calculator. In

fact, the first step of the algorithm is to compute randomly the four rational integers a, b, c, d, which will compose the two primes p and q. This four rationals are chosen inside an interval, called I. To let these algorithms work, we put $I = [1, 8]$, which is a very small interval if we think that this provides a number of combinations for p and q so small that the algorithm is unsafe. On the other hand, it will be sufficient to increase this interval enough to obtain a safe and working algorithm with a realistic values.

Moreover, it was necessary an extra function to let the algorithm work, and this is `sym`. This is the function which creates symbolic variables (see [www.mathworks.com]) and we use it for a practical aim: since erasing to a power generates a very big number, we need to allocate the variable. In fact, if the numbers are too big, what `Matlab` does is to break off the number and this gives a wrong result or none at all.

6.1.3 Examples

Now we see an application of the codes written.

In $\mathbb{Z}[i]$

- The two Gaussian primes randomly selected by the algorithm are $p = 7 + 8i$ and $q = 6 + i$ and we are sure they are primes since their norms are integer primes: $N(p) = 113$ and $N(q) = 37$.
- Then, we compute n and its norm $N(n) = 4181$.
- The Euler's ϕ-function of n is given by the product $(N(p)-1)(N(q)-1)$, so $s = 4032$. Using this number, we select the random exponent, in this case $e = 1123$.
- Successively, $d = 1867$ comes out to be the inverse of e modulo s, i.e. our decryption exponent.
- Now, we insert the plaintext to be

  $$21 + 12i$$

  and, since its norm is less than the norm of n, we can proceed with the computation.
- The ciphertext, is now

  $$11 - 19i.$$
- Finally, we compute the message back, as the receiver should do, and we obtain the message. The algorithm gives as output `'ok'`, which means the check is done and the sender's message coincide with the receiver's message.

In $\mathbb{Z}[\sqrt{2}]$

- The two Gaussian primes randomly selected by the algorithm are $p = 1 + 4\sqrt{2}$ and $q = 7 + 2\sqrt{2}$ and we are sure they are primes since their norms are integer primes: $N(p) = 31$ and $N(q) = 41$.
- Then, we compute $n = 23 + 30\sqrt{2}$ and its norm $N(n) = 1271$.
- The Euler's ϕ-function of n is given by the product $(N(p)-1)(N(q)-1)$, so $s = 1200$. Using this number, we select the random exponent, in this case $e = 851$.
- Successively, $d = 251$ comes out to be the inverse of e modulo s, i.e. our decryption exponent.
- Now, we insert the plaintext to be

  $$13 + 15\sqrt{2}$$

  and, since its norm $N(P) = 281$ is less than the norm of n, we can proceed with the computation.
- The ciphertext, is now

  $$-17 - \sqrt{2}.$$

- Finally, we compute the message back, as the receiver should do, and we obtain the message. The algorithm gives as output `'ok'`, which means the check is done and the sender's message coincide with the receiver's message.

Remark. We notice that both this algorithms work using integers, i.e. can be used as the classical RSA algorithm. It is enough to write every integer a as $a + 0i$ in $\mathbb{Z}[i]$ or $a + 0\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$.

6.2 Differences between $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$

We would like to consider the differences between the RSA algorithm written with numbers of the form $z = a + bi \in \mathbb{Z}[i]$ and $\alpha = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, with $a, b, x, y \in \mathbb{Z}$.

- First, the norm of $\mathbb{Z}[\sqrt{2}]$ is taken with the absolute value. This is a condition needed for the proof that this domain is a Euclidean domain, while in the ring of Gaussian integers this condition is already satisfied by the definition of norm. In both cases, we need the norm to be a positive integer.

- Secondly, $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ whereas $\mathbb{Z}[\sqrt{2}]$ is contained in $\mathbb{R}$. For this reason, we are working with rationals when we are in $\mathbb{Z}[\sqrt{2}]$. At the same time the information about the message is contained inside x and y but, doing the computations with `Matlab`, everything is lost since the program computes everything into $\mathbb{R}$ no longer distinguishing the two numbers because, as we said, $\alpha = x + y\sqrt{2}$ is in $\mathbb{R}$. For this reason, we need to keep the two pieces of information distinct and, at the same time, we need to introduce the changes given by $\sqrt{2}$ inside the multiplications. So, the entire algorithm is based on the use of two different values x and y: keeping them separate is the only way we have to save all the information and to avoid losses.

Chapter 7

Discussion

The field of cryptography is constantly changing: we are always looking for new algorithms to use, because the creation of increasingly powerful calculators let previous algorithms be unsafe. For this reason, the decision to produce an extended version of the RSA algorithm is to look for inside security. In the last twenty years, there have been a lot of researches which have tried to find new sets in which the construction of RSA algorithm is possible, safe and usable. For example, in [El-Kassar-Haraty-Awad], they described the RSA modified version for both the ring of Gaussian integers and for polynomials over finite fields.

When we want to find a set to use, different than the ring of integers, it is obvious to think about the ring of complex numbers. Unfortunately, it is a set with lots of properties, not easy to analyse. For this reason, we decide to start from the subset $\mathbb{Z}[i]$ and then we try to generalise $\mathbb{Z}[\sqrt{-1}]$, using $\mathbb{Z}[\sqrt{d}]$. Knowing that for the creation of a working RSA algorithm it is necessary to be in a Unique Factorization Domain, we select d to be 2, so that we are in a Euclidean Domain where the property of uniqueness is satisfied.

Therefore, the successive investigations include the security of the algorithm and the comparison of the RSA extended algorithm in $\mathbb{Z}[\sqrt{2}]$ with the previous analysed schemes.

7.1 Security

As already stated in Paragraph 2.3.1, even selecting large prime factors p and q, we cannot be sure about the security of the algorithm (we already mentioned Pollard $p-1$ Method). Moreover, besides all the security aspects we have in the classical algorithm, we need to consider some new properties which follow from the introduction of extensions of $\mathbb{Z}$. In particular, the concept of norm provides new information about the numbers we are using to construct the algorithm and we need to consider in which way that in-

formation can be used by a third person to discover the message. We said that a way to discover the secret key is to find the factorization of n and, since n is part of the public key, its norm is also publicly available because it is easily computable. For this reason, we need to take precautions in the choice of the norm of n.

First of all, it must be difficult to factorize: in fact, if we apply the multiplicative property of the norm, having a factorization of $N(n)$ implies having the values of $N(p)$ and $N(q)$, so it is possible to give a list of values for p and q, facilitating the factorization of n. This problem can be avoided using the same rule we follow for the factorization of n, i.e. by letting the value $N(n)$ be big. This is not so difficult to do in $\mathbb{Z}[i]$: using the definition of the norm, $N(z) = a^2 + b^2$ for $z \in \mathbb{Z}[i]$ and it is enough to choose a and b such that they are big, which is the same condition for n. On the other hand, if $\alpha = x + y\sqrt{2}$ is an element of $\mathbb{Z}[\sqrt{2}]$, the norm

$$|N(\alpha)| = |x^2 - 2y^2|,$$

is taken with the absolute value to let the construction of the Euclidean domain be possible (see Theorem 4.7). Here things become more difficult, since we need to satisfy both n big and $N(n)$ big, but we have a negative sign: this is an open question that will not be answered in this paper.

7.2 Advantages and disadvantages

When we consider the problem of computation time, we need to distinguish the algorithm between the block responsible of the generation of the keys and the block which deals with encryption and decryption. The generation of the keys and also the creation of n is the part in which we use bigger numbers, so it is possible to have problems due to the big size of the numbers themselves. This first step is however the same for the three algorithms: in fact, the classical algorithm and the ones on $\mathbb{Z}[i]$ and on $\mathbb{Z}[\sqrt{2}]$ require the same amount of calculations. Then, we need to consider the second step, with the encryption and the decryption. In this case, it is necessary to remind that the number of times we use the algorithm is much higher. In fact, after computing a working and usable key, we can leave aside this first part, but we continue with encryption and decryption on many documents. In this second part, it is important to underline a big difference between the algorithm in $\mathbb{Z}[i]$ and in $\mathbb{Z}[\sqrt{2}]$, recalling also what we saw in Paragraph 6.2.

The encryption and the decryption work basically with the two functions which compute the modules, so the computation time is to search inside them. Both of them work following the same steps, but we need to remind a big difference given from the representation of the elements of the sets<T the element $x + y\sqrt{2}$ of $\mathbb{Z}[\sqrt{2}]$ can be written as the vector (x, y) and, in the same way, $a + bi \in \mathbb{Z}[i]$ can be written as (a, b). Taking this representation in

mind, it is obvious to say that computationally the two algorithms have no difference. On the other hand, we can notice the difference is basically in the representation of the elements inside `Matlab`. In fact, the program is able to recognise the Gaussian integers as complex numbers and si it allocates them in the vector automatically, while it is necessary to write a specific line in the code to do the same with the elements of $\mathbb{Z}[\sqrt{2}]$. Generalising, it is interesting to notice that this difference is true only for the ring $\mathbb{Z}[i]$. When $d > 1$, $\mathbb{Z}[\sqrt{d}]$ behaves in the same way as $\mathbb{Z}[\sqrt{2}]$, but this is true for $d < 1$ as well. Indeed, even if the elements of such this set $\mathbb{Z}[\sqrt{d}]$ are complex numbers, they have the particular form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ and in this case $b\sqrt{d} \in \mathbb{C}$, but we want to keep the information contained in the element b separate from $\sqrt{d}$, so the trick is the same used for $d = 2$. In conclusion, all the algorithms we can create inside rings of the form $\mathbb{Z}[\sqrt{d}]$ have the same number of operations, but for $d = -1$ they are easier to write inside `Matlab`.

A second point to consider is the fact that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units. We showed in Chapter 5 that it is possible to represent the elements of the ring in the Cartesian plane. Then, we decided to draw modules trough some squares with the property that all the vertices of the squares are the elements congruent to 0 modulo a selected n. In the same way, all the elements congruent to a given value w are represented as the points with the same position inside the squares. Using this representation, it is easy to see that it is possible to move from one point to another, if they are congruent to the same value, just multiplying one of the element by a unit. To conclude, the fact that there are infinite many units inside the ring can influence our result, but this problem is solvable by selecting one of the squares and consequently all the elements which belong to it and by agreeing to work on it. For example, the square with vertex in zero and all the elements in the first quadrant. Even if in a smaller way, we need to be careful also inside $\mathbb{Z}[i]$, where the units are only four but can still change the final result.

7.3 Future investigations

To be sure about the security of this algorithm, there are some more investigations needed. In fact, it is necessary to analyse the factorization of elements of the form $a + b\sqrt{d}$, to be sure there is not an easy method to find the elements of the secret key, knowing the public key.

Moreover, there are some possible future extensions which come up easily to our mind, considering this work. Since $\mathbb{Z}[\sqrt{2}]$ is a suitable set, being an Euclidean domain, then all the sets of the form $\mathbb{Z}[\sqrt{d}]$ must be considered, if they are Euclidean domains as well. So it will be possible to do the same analysis for all the other Euclidean domains of the form $\mathbb{Z}[\sqrt{d}]$, following the same steps of this work.

Appendix A

Matlab codes

A.1 RSA algorithm for Gaussian integers

```
%Construction of the two random prime numbers p and q
%and calculation of their prime norms Np and Nq
I=8;
a=randi(I);
b=randi(I);
c=randi(I);
d=randi(I);
Np=a^2+b^2;
Nq=c^2+d^2;

while isprime(Np)==0
        a=randi(I);
                b=randi(I);
                Np=a^2+b^2;
end

while isprime(Nq)==0 %&& Nq==Np
                c=randi(I);
                d=randi(I);
                Nq=c^2+d^2;
end
Np
Nq

%Compute N and its norm
p=a+b*i;
q=c+d*i;
N=p*q;
```

```
NN=N*conj(N)

%Compute the Euler's Phi function of N
s=(Np-1)*(Nq-1)

%Find randomly the integer encryption exponent
%It must be less than s and coprime with s
e=randi(s-1);
while gcd(e, s)~=1
      e=randi(s-1);
end
e

%Compute the decryption exponent
w=input('INSERT sym(e^(s-1)):  ');
d=mod(w, N)

%Check that the computation is correct
z=mod(e*d, N)
if z~=1
    disp('There is an error')
end

%Give as output the Public key and the Secret key
Pk=[N, e];
Sk=[p, q, d];

%ENCRYPTION ALGORITHM:
%Insert the plaintext and check its validity
P=input('INSERT the plaintext:  ');
NP=P*conj(P);
while NP > NN
   P=input('INSERT again the plaintext:  ');
   NP=P*conj(P)
end

%Compute the ciphertext
e=input('INSERT sym(e):  ');
C=functmod(P^e, N)

%DECRYPTION ALGORITHM:
%Compute the text back
d=input('INSERT sym(d):  ');
T=functmod(C^d, N)
```

```
%Verify if the original text and the received text are equals
%This must happens up to a multiplication by a unit
if P==T
    disp('ok')
else
    e1=T*(-1)
    e2=T*(1i)
    e3=T*(-1i)
end
```

A.2 functmod

```
%Compute the modules inside
%the ring of Gaussian integers

function y=functmod(a, n)

n1=conj(n);
x=(a*n1)/(n*n1);
e=real(x);
f=imag(x);
E=round(e);
F=round(f);

q=(E+F*1i);
y=a-n*q;
```

A.3 RSA algorithm in the ring generated by $\sqrt{2}$

```
%Construction of the two random prime numbers p and q
%and calculation of their prime norms Np and Nq
%REMEMBER: the norms must be taken with the absolute value
I=8;
a=randi(I);
b=randi(I);
c=randi(I);
d=randi(I);
Np=abs(a^2-2*b^2)
Nq=abs(c^2-2*d^2)

while isprime(Np)==0
        a=randi(I);
                b=randi(I);
```

```
                    Np=abs(a^2-2*b^2)
end

while isprime(Nq)==0 && Nq==Np
                    c=randi(I);
                    d=randi(I);
                    Nq=abs(c^2-2*d^2)
end
Np
Nq

%Compute N and its norm
Nx=a*c+2*b*d
Ny=a*d+c*b
NN=abs((Nx)^2-2*(Ny)^2)

%Compute the Euler's Phi function of N
s=(Np-1)*(Nq-1)

%Find randomly the integer encryption exponent
%It must be less than s and coprime with s
e=randi(s-1);
while gcd(e, s)~=1
      e=randi(s-1);
end
e

%Compute the decryption exponent
w=input('INSERT sym(e^(s-1)):  ');
d=mod(w, s)

%Check that the computation is correct
z=mod(e*d, s)
if z~=1
    disp('There is an error')
end

%Give as output the Public key and the Secret key
Pk=[Nx, Ny, e];
Sk=[p, q, d];

%ENCRYPTION ALGORITHM
%Insert the plaintext
Px=input('INSERT Px:  ');
```

```
Py=input('INSERT Py:    ');

%Verify the condition on the norm
NP=abs((Px)^2-2*(Py)^2)
if NP > NN
   P=input('The plaintext is too big');
end

%Compute the ciphertext
e=input('INSERT sym(e):    ');
[Cx, Cy]=functmod2(Px, Py, e, Nx, Ny)

%DECRYPTION ALGORITHM
%Compute the original message
d=input('INSERT sym(d):    ');
[Tx, Ty]=functmod2(Cx, Cy, d, Nx, Ny)

%Check that the original text and the received one are the same
if Px==Tx && Py==Ty
    disp('ok')
end
```

A.4 functmod2

```
%Compute the modules inside
%the ring generated by sqrt(2)

function [a, b]=functmod2(x, y, e, nx, ny)
n=nx+sqrt(2)*ny;
n1=nx-sqrt(2)*ny;
norm=n*n1;

X=x;
Y=y;
i=1;

for i=1:(e-1)
    i=i+1;
    Ax=X*x+2*Y*y;
    Ay=X*y+Y*x;
    Bx=Ax*nx-2*Ay*ny;
    By=-Ax*ny+Ay*nx;
    Qx=round(Bx/norm);
    Qy=round(By/norm);
```

```
    Cx=Qx*nx+2*Qy*ny;
    Cy=Qx*ny+Qy*nx;
    X=Ax-Cx;
    Y=Ay-Cy;
end

a=X;
b=Y;
```

Bibliography

[Aluffi] Paolo Aluffi; *Algebra: Chapter 0*, American Marhemaical Society, 2009.

[Anderson-Bell] James A. Anderson, James M. Bell; *Number Theory with applications*, Prentice Hall, 1996.

[Artin] Michael Artin; *Algebra*, second edition, Pearson education inc., 2011.

[Bandyopadhyay] S. Bandyopadhyay; *Euclidean domains and the Gaussian integers: an application*, Chennai Mathematical Institute, http://www.cmi.ac.in/ shreejit/Gaussian.pdf, July 2013.

[Beachy-Blair] John A. Beachy & William D. Blair; *Abstract Algebra*, third edition, Waveland press inc., 2006.

[Cao-Fu] Y. Y. Cao & C. Fu; *An efficient implementation of RSA digital signature algorithm*, International Conference of Intelligent Computation Technology and Automation, p. 100-103, 2008.

[Clark] P. L. Clark; *The Gaussian integers I: fundamental theorem*, http://math.uga.edu/ pete/4400gaussian.pdf; March 2017.

[Conrad] Keith Conrad; *The Gaussian integers*, University of Connecticut, http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/Zinotes.pdf, march 2017.

[Conrad2] Keith Conrad; *Pell's equation: I*, University of Connecticut, http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/pelleqn1.pdf, march 2017.

[Diffie-Hellman] W. Diffie & M. Hellman; *New directions in cryptography*, IEEE Trans. in Information Theory, Vol. 22, p. 644-654, 1976.

[El-Kassar-Haraty-Awad] A. n. El-Kassar, R. Haraty & Y. A. Awad; *Modified RSA in the domains of Gaussian integers and Polynomials over finite fields*, CAINE, 2005.

[Hoffstein-Pipher-Silverman] Hoffstein, Pipher & Silverman; *An introduction to mathematical cryptography*, second edition, Springer, 2014.

[www.mathworks.com] *sym*, https://it.mathworks.com/help/symbolic/sym.html?searchHighlight=sym, September 2017.

[Niven] I. Niven, Herbert S. Zuckerman & Hugh L. Montgomery; *An introduction to the theory of numbers* Fifth edition, John Wiley & Sons, Inc., 1991.

[Pal] A. Pal; *Notes for algebraic number theory*, Imperial College London, http://wwwf.imperial.ac.uk/ apal4/algnumnotes.pdf, March 2017.

[Pradhan-Sharma] S. Pradhan & B. K. Sharma; *A Modified Variant of RSA Algorithm for Gaussian Integers*, International Journal of Information & Network Security (IJINS), Vol.2, No.4, p. 322-326, August 2014.

[Rivest-Shamir-Adleman] R. Rivest, A. Shamir & L. Adleman; *A method for obtaining digital signatures and public key cryptosystems*; Communications of the Association for Computer Machines, Vol. 21, No. 2, p. 120-126, 1978.

[Stillwell] J. Stillwell; *Elements of Number Theory*, Springer, p. 101-116, 2003.

Linnæus University
Sweden

Faculty of Technology
SE-391 82 Kalmar | SE-351 95 Växjö
Phone +46 (0)772-28 80 00
teknik@lnu.se
Lnu.se/faculty-of-technology?l=en