DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf University of Msila
Faculty of Mathematics and Computer Sciences
Department of Mathematics

Master MEMORY

Field : Mathematics and Computer Sciences
Branch : Mathematics
Option : Algebra and Discrete Mathematics

Theme

Gaussian Integers

Presented by :
Remili Liamine

The jury composed of :

Mr Amroune Abdelaziz	Prof,	University of Msila	**President**.
Mr Boudaoud Abdelmadjid	Prof,	University of Msila	**Supervisor**.
Mr Ladjlat Lahcene	MAA,	University of Msila	**Examiner**.

University year 2020/2021

Thanks

I first of all thank my god who gave me the strength to finish this modest work.

I would like to thank my promoter: the doctor **A. Boudaoud** for the advice given, his encouragements and his patience.

In the end I thank all those who have helped me from near or far, in particular my parents, my fiancée and my generous family who accompanied me throughout my studies.

#Thank you

Contents

Introduction

In number theory, we are sometimes led to consider more general numbers, called algebraic numbers. The branch dealing with the study of rings and fields formed by these numbers is called "Algebraic number theory". The content of this memory, falls within this branch is entitled " Gaussian integers ". Gaussian integers are the elements of the "integral domain"

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

The content of this memory is a part of the well-known branch "Theory of numbers", where this specialty has known for a long time an appreciated evolution, within our department of mathematics at the university Mohamed Boudiaf of Msila (Algeria). The bibliography used and consulted by the author reflects this observation.

This memory is designed in such a way that some fundamental and common notions of any integral ring are the subject of the first chapter.

In the second chapter we deal with the concepts related to Gaussian Integers as: unit, Gaussian prime, greatest common divisor, factorization and unique factorization of Gaussian integers, Bezout's identity.

In the third chapter we give two important applications concerning the writing of positive integers as sum of two squares and the solution of the famous Diophantine equation, namely,

$$y^2 = x^3 - 1.$$

Chapter 1

Integral Domains

The most used references in this chapter are ([1], [13], [15]).

1.1 Important definitions and properties

Definition 1.1.1 *A commutative ring that has a multiplicative identity but no divisors of zero, is called an integral domain.*

Remark 1.1.2 *A commutative ring has a divisors of zero if there exist* $a \neq 0$, $b \neq 0$ *and* $ab = 0$.

Notation 1.1.3 *An integral domain* D *is called a field if for each* $s \in D$, $s \neq 0$, *there exists* $t \in D$ *with* $st = 1$.

Example 1.1.4 **a**) $\mathbb{Z} + \mathbb{Z}i = \{u + vi \mid u, v \in \mathbb{Z}\}$, *is an integral domain. The elements of* $\mathbb{Z} + \mathbb{Z}i$ *are called Gaussian integers.*
b) *The ring of integers numbers (* $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$*) of all integers is an integral domain.*

Properties of an Integral Domain

Let **D** be an integral domain. Then the following properties hold:

1. The identity element of D is unique, for if 1 and $1'$ are two identities for **D** then

$$1' = 1'.1(\text{as } 1 \text{ is an identity}) = 1(\text{as } 1' \text{ is an identity}).$$

2. D possesses a left cancellation law, that is:

$$uv = uw, u \neq 0 \Rightarrow v = w(u, v, w \in D).$$

Also a right cancellation law

$$uw = vw, w \neq 0 \Rightarrow u = v(u, v, w \in D).$$

3. It is well known that if D is an integral domain then there exists a field $\mathbb{F}$, called the field of quotients of D or the quotient field of D, that contains an isomorphic copy D' of D . In practice it is usual to identify D with D' and so consider D as a subdomain of $\mathbb{F}$. The quotient field of $\mathbb{Z}$ is the field of rational numbers $\mathbb{Q}$. The quotient field of the polynomial domain $\mathbb{F}[X]$ (where $\mathbb{F}$ is a field) is the field $\mathbb{F}(X)$ of rational functions in X.

1.1.1 Divisor

Definition 1.1.5 *Let α and β belong to the integral domain D $(\alpha, \beta \in D)$. The element α is said to be a divisor of β (or α divides β) if there exists an element κ of D such that $\beta = \kappa\alpha$.*

Notation 1.1.6 *If α is a divisor of β, we write $\alpha|\beta$. If α is not a divisor of β, we write $\alpha\not|\beta$.*

Example 1.1.7 *:*

1. $(1 + 2i)|5$ in $\mathbb{Z} + \mathbb{Z}i$ as $5 = (1 - 2i)(1 + 2i)$ $\quad (\kappa = 1 - 2i)$.
2. $(x^2 + 2x - 5)|(x^3 + 3x^2 - 3x - 5)$ in $\mathbb{Z}[x]$ as $x^3 + 3x^2 - 3x - 5 = (x + 1)(x^2 + 2x - 5)$.
3. $(x^2 - 2)\not|(x^3 + 4x^2 - 2x - 3)$ in $\mathbb{Z}[x]$ as $(x^3 + 4x^2 - 2x - 3) = (x + 4)(x^2 - 2) + 5$.

Properties of divisors

Let α, β, $\gamma \in D$, where D is an integral domain. Then the following properties hold

1. $\alpha|\alpha$ (reflexive property).
2. $\alpha|\beta$ and $\beta|\gamma$ implies $\alpha|\gamma$ (transitive property).
3. $\alpha|\beta$ and $\alpha|\gamma$ implies $\alpha|x\beta + y\gamma$ for any $x \in D$ and $y \in D$.
4. $\alpha|\beta$ implies $\alpha\gamma|\beta\gamma$.
5. $\alpha\gamma|\beta\gamma$ and $\gamma \neq 0$ implies $\alpha|\beta$.
6. $1|\alpha$.
7. $\alpha|0$.
8. $0|\alpha$ implies $\alpha = 0$.

Proof. We will provide proof of the above properties

1) $\alpha = 1.\alpha$ so $\kappa = 1$.
2) $\alpha|\beta$ and $\beta|\gamma$, then $\beta = \kappa\alpha$ and $\gamma = \kappa'\beta$. Hence $\gamma = \kappa'\kappa\alpha$.
3) $\alpha|\beta$ and $\alpha|\gamma$ then $\beta = \kappa\alpha$ and $\gamma = \kappa'\alpha$ so $x\beta + y\gamma = (x\kappa + y\kappa')\alpha$.
4) $\alpha|\beta$ such that $\beta = \kappa\alpha$. Then $\beta\gamma = \kappa(\gamma\alpha)$.
5) $\alpha\gamma|\beta\gamma$ and $\gamma \neq 0$, it main $\beta\gamma = \kappa\alpha\gamma$ dives by γ, so $\beta = \kappa\alpha$.
6) $\alpha = \alpha.1$, such that $1|\alpha$.
7) we have $0 = 0.\alpha$, then $\alpha|0$.
8) $0|\alpha$ such that $\alpha = \kappa \cdot 0 = 0$. ■

Example 1.1.8 *We have some examples for division in integral domain*

1. $5 + i|5 + i$ in $\mathbb{Z} + \mathbb{Z}i$ (*prop*.1).
2. $x + 2|x^2 - 4$ in $\mathbb{Z}[x]$ and $x^2 - 4|3x^3 + x^2 - 12x - 4$ in $\mathbb{Z}[x]$, so $x + 2|3x^3 + x^2 - 12x - 4$ (*prop*.2).

3. $1+i|3-i$ in $\mathbb{Z}+\mathbb{Z}i$ and $1+i|-7+3i$ in $\mathbb{Z}+\mathbb{Z}i$,so $1+i|(3i)(3-i)+(1+i)(-7+3i)$ in $\mathbb{Z}+\mathbb{Z}i(prop.3)$.

4. $3-x|x^2-9$ in $\mathbb{Z}[x]$, then $(3-x)(-4+x)|(x2-9)(-4+x)$ $(prop.4)$.

5. $1|x^2+2x-7$ as $x^2+2x-7/1=x^2+2x-7$ in $\mathbb{Z}[x]$ $(prop.6)$.

6. $0=0.(3+5i)\in\mathbb{Z}[x]$, so $3+5i|0$ $(prop.7)$.

1.1.2 Unit

Definition 1.1.9 *We say that the element α of an integral domain D is a unit if $\alpha|1$.*

Notation 1.1.10 *The set of units of D is denoted by $U(D)$.*

Example 1.1.11 *We have*

1. $1,-1$ are units of $\mathbb{Z}$ and we writing $1,-1\in U(\mathbb{Z})$.

2. $4\nmid 1$ so $4\notin U(\mathbb{Z})$.

Properties of units

Let D be an integral domain. Then $U(D)$ has the following properties

a) $\pm 1\in U(D)$.

b) If $\alpha\in U(D)$, then $-\alpha\in U(D)$.

c) If $a\in U(D)$, then $a^{-1}\in U(D)$.

d) If $a\in U(D)$, and $b\in U(D)$ then $ab\in U(D)$.

e) If $a\in U(D)$, then $\pm a^n\in U(D)$ for any $n\in\mathbb{Z}$.

Example 1.1.12 ± 1, $\pm i\in U(\mathbb{Z}+\mathbb{Z}i)$ *as* $-1|1$, $1|1$, $-i|1$ *and* $i|1$.

1.1.3 Associate

Definition 1.1.13 *Let α and β be nonzero elements of an integral domain D, α and β are called associates, if each divides the other($\alpha|\beta$ and $\beta|\alpha$).*

Notation 1.1.14 *If α and β are associates we write $\alpha \sim \beta$, otherwise $\alpha \nsim \beta$.*

Properties of associates

Let $\alpha, \beta, \gamma \in D^* = D\backslash\{0\}$, where D is an integral domain. The following properties hold

1. $\alpha \sim \alpha$ (reflexive property).
2. $\alpha \sim \beta$ if and only if $\beta \sim \alpha$ (symmetric property).
3. $\alpha \sim \beta$ and $\beta \sim \gamma$ imply $\alpha \sim \gamma$ (transitive property).
4. $\alpha \sim \beta$ if and only if $\alpha\beta^{-1} \in U(D)$.
5. $\alpha \sim 1$ if and only if α is a unit.

Example 1.1.15 -1, $1, -i$, i *are associates two by tow in* $\mathbb{Z} + \mathbb{Z}i$.

1.2 Irreducibles and primes

Definition 1.2.1 *Prime number is an integer $p > 1$, that has no positive divisors other then* 1 *and itself.*

Example 1.2.2 2, 3, 5, 7, 11, 13, ..., 67, 71, ...

Definition 1.2.3 *A nonzero, nonunit element p of an integral domain D is called a prime if $p|uv$, where $u, v \in D$, implies that $p|u$ or $p|v$.*

Example 1.2.4 *2 is a prime in $\mathbb{Z}$. Suppose $2|mn$, where $m, n \in \mathbb{Z}$, so that mn is even. Since the product of two odd integers is odd, at least one of m and n must be even, that is, a divide 2 or b divide 2, showing that 2 is prime.*

Definition 1.2.5 *(Irreducible) Let α be a nonzero nonunit of D. α is called to be irreducible if it is not a product of two nonunits .*

Example 1.2.6 *3 is irradicable in $\mathbb{Z}$, for if $3 = uv$ with $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$ then either $u = \pm 1$ or $v = \pm 1$.*

Theorem 1.2.7 *In any integral domain D a prime is irreducible.*

Proof. Let $p \in D$ be a prime and suppose that $p = uv$, where $u, v \in D$. As $uv = p.1$ we have $p|uv$, and so, as p is prime, we deduce that $p|u$ or $p|v$, that is, $u/p \in D$ or $v/p \in D$. Since $1 = u/p.v$ or $1 = u.v/p$, either v is a unit or u is a unit of D. This proves that p is an irreducible element of D. ■

Example 1.2.8 *$1+i$ is a prime in $\mathbb{Z}+\mathbb{Z}i$. To show this, suppose that $1+i\ |(u+vi)(l+mi)$, where $u, v, l, m \in \mathbb{Z}$.*

Then there exist integers x and y such that

$$(u + vi)(l + mi) = (1 + i)(x + yi).$$

Taking the modulus of both sides of this equation, we obtain:

$$(u^2 + v^2)(l^2 + m^2) = 2(x^2 + y^2).$$

As 2 is a prime in $\mathbb{Z}$, we have either $2|u^2 + v^2$ or $2|c^2 + d^2$. Interchanging $u + vi$ and $l + mi$, if necessary, we may suppose that $2|u^2 + v^2$. Thus, either u and v are both even or they are both odd. In the former case $u = 2r$ and $v = 2s$, where r and s are integers, and $u + vi = 2(r + si) = (1 + i)((r + s) + (-r + s)i)$, so that $1 + i|u + vi$. In the latter case $u = 2r + 1$ and $v = 2s + 1$, where r and s are integers, and $u + vi = 2(r + si) + (1 + i) = (1 + i)((r + s + 1) + (-r + s)i)$, so that $1 + i|u + vi$. Hence $1 + i$ is a prime in $\mathbb{Z} + \mathbb{Z}i$.

By last theorem $1 + i$ is irreducible.

1.3 Factorization domain

Below we will provide important definitions.

Definition *Let D be an integral domain. Then D is said to be a factorization domain if every nonzero, nonunit element of D can be expressed as a finite product of irreducible elements of D.*

1.4 Unique factorization domain

Definition 1.4.1 *Let D be a factorization domain. Suppose that every nonzero, nonunit element a of D has a unique factorization as a product of irreducible elements of D. Then D is called a unique factorization domain.*

Example 1.4.2 *It is shown that $\mathbb{Z}$, $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$, $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-3}}{2})$, $\mathbb{Z} + \mathbb{Z}\sqrt{6}$ are unique factorization domains.*

Chapter 2

Gaussian Integers

The most used references in this chapter are ([**1**], [**13**]).

2.1 Definitions and elementary notions

We define the set of *Gaussian integers* by

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

where $i = \sqrt{-1}$.

Example 2.1.1 *$2 + 5i$, $7 - 3i$, $1 + i$ are Gaussian integers.*

Proposition 2.1.2 *Every integer is a Gaussian integer and that the sum, difference and product of Gaussian integers is a Gaussian integers.*

Example 2.1.3 *Calculate : $(2 + 4i) + (-3 - i)$, $5i - (5 + 2i)$, $(1 - i)(-2 + i)$.*
$(2 + 4i) + (-3 - 6i) = -1 - 2i.$
$5i - (5 + 2i) = -5 + 3i.$
$(1 - i)(-6 + 2i) = -4 + 8i.$

Notation 2.1.4 *If $\alpha = x + iy$ is a Gaussian integer, then the conjugate of α is the Gaussian integer $\overline{\alpha} = x - iy$.*

Example 2.1.5 *The conjugate of $7 + 2i$ (resp of $3 + i$). Is $7 - 2i$ (resp of $3 - i$).*

Definition 2.1.6 *Let α and β be Gaussian integers. We say that α divides β if there is a Gaussian integer γ such that $\beta = \gamma\alpha$.*

Example 2.1.7 $5 + i = (2 + 3i)(1 - i)$ *then* $(2 + 3i)|(5 + i)$ *and* $(1 - i)|(5 + i)$.
$1 - 2i$ *divide* $3 + 4i$?

$$\begin{aligned}
\frac{3+4i}{1-2i} &= \frac{(3+4i)\overline{(1-2i)}}{(1-2i)\overline{(1-2i)}} \\
&= \frac{(3+4i)(1+2i)}{(1-2i)(1+2i)} \\
&= \frac{3+6i+4i-8}{1^2+2^2} \\
&= \frac{-5+10i}{5} \\
&= -1+2i \in \mathbb{Z}[i].
\end{aligned}$$

So $(1 - 2i)|(3 + 4i)$.

$$\begin{aligned}
\frac{5+2i}{4-i} &= \frac{(5+2i)(4+i)}{(4-i)(4+i)} \\
&= \frac{20+5i+8i-2}{4^2+1^2} \\
&= \frac{18+13i}{17} \notin \mathbb{Z}[i].
\end{aligned}$$

So $(4 - i) \nmid (3 + 4i)$.

Definition 2.1.8 *If $\alpha = x + iy$, then the norm of α is:*

$$\begin{aligned}
N(\alpha) &= \alpha\overline{\alpha} \\
&= (x+iy)(x-iy) \\
&= x^2 + y^2.
\end{aligned}$$

Example 2.1.9 *Find the norm of* $2+3i$.

$$\begin{aligned} N(2+3i) &= (2+3i)\overline{(2+3i)} \\ &= (2+3i)(2-3i) \\ &= 2^2+3^2 \\ &= 13. \end{aligned}$$

Theorem 2.1.10 *Let* α *and* β *be Gaussian integers then*

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Proof. Let $\alpha = u+iv$ and $\beta = s+it$. Then

$$\begin{aligned} \alpha\beta &= (u+vi)(s+ti) \\ &= (us-vt)+(ut+vs)i. \end{aligned}$$

It follows that

$$\begin{aligned} N(\alpha\beta) &= (us-vt)^2+(ut+vs)^2 \\ &= (u^2+v^2)(s^2+t^2) \\ &= N(\alpha)N(\beta). \end{aligned}$$

■

Example 2.1.11 $N((2-i)(1+3i)) = 50$. *Indeed*

$$N(2-i) = 2^2+(-1)^2 = 5.$$

$$N(1+3i) = 1^2+3^2 = 10.$$

Then

$$\begin{aligned} N((2-i)(1+3i)) &= N(2-i)N(1+3i) \\ &= 5\times 10 \\ &= 50. \end{aligned}$$

Lemma 2.1.12 **i**) *The Gaussian integer α is a unit if and only if $N(\alpha) = 1$.*
ii) *The only Gaussian integer which are units are ± 1 and $\pm i$.*

Proof. **i**) ($\Longrightarrow$) Let be $\alpha\beta = 1$, for some *Gaussian integer* β, and hence $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Since the norms of α and β are nonnegative integer, it follows that $N(\alpha) = 1$.

($\Longleftarrow$) If $N(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, in particular, α divides 1 and so α is a unit.

Then

$$\alpha \textit{ is a unit} \Leftrightarrow N(\alpha) = 1.$$

ii) Let $\alpha = s + it$, then $N(\alpha) = s^2 + t^2$. Clearly, $N(\alpha) = 1$ if and only if $t = 0$ and $s = \pm 1$ or $s = 0$ and $t = \pm 1$, hence the only *Gaussian units* are ± 1 and $\pm i$. ■

2.1.1 Gaussian primes

Let us begin with the following characterization of *Gaussian primes*

Theorem 2.1.13 *The Gaussian integer α is a Gaussian prime if and only if one the following holds*

1. α is $1 - i$ or an associate;
2. α is a rational prime of the from $4k + 3$ or an associate;
3. $N(\alpha) = p$, where p is a rational prime of the form $4k + 1$.

Example 2.1.14 *We list some gaussian primes*

1. 7, 19, 71 are *Gaussian primes* , since they are natural numbers of the form $4k + 3$.
2. $3i$, $-7i$, since they are associate of 3 and 7.
3. $6 + i$ is *Gaussian prime*. Because ($a = 6$, $b = 1$), then

$$\begin{aligned} N(6+i) &= 6^2 + 1^2 \\ &= 36 + 1 \\ &= 37 \end{aligned}$$

witch is positive integers prime of the form $4k + 3$.

2.1.2 Division Algorithm

Theorem 2.1.15 *Let α and β be Gaussian integers with α nonzero. Then there exist Gaussian integers λ and δ such that $\beta = \lambda\alpha + \delta$ and $N(\delta) < N(\alpha)$.*

Proof. Let $\beta/\alpha = x + yi$, where x and y are real numbers, and let a and b be, respectively, integers nearest to x and y .

Define $\lambda = a + bi$, and set $\delta = \beta - \lambda\alpha$, clearly, $\beta = \lambda\alpha + \delta$. It remains to verify that $N(\delta) < N(\alpha)$. Since $\beta = (x + yi)\alpha$, we have $\delta = ((x - a) + (y - b)i)\alpha$. But $\mid x - a \mid \leq 1/2$ and $\mid y - b \mid \leq 1/2$. Therefore $N(\delta) \leq 1/2N(\alpha) < N(\alpha)$, then $N(\delta) < N(\alpha)$, and the result follows. ■

Example 2.1.16 *Let α and β be Gaussian integers such that $\alpha = 1 + 3i$ and β=6+2i*

$$\begin{aligned} \beta/\alpha &= \frac{6+2i}{1+3i} \\ &= \frac{(6+2i)(1-3i)}{(1+3i)(1-3i)} \\ &= \frac{6-18i+2i+6}{1^2+3^2} \\ &= \frac{12-16i}{10} \\ &= \frac{6}{5} - \frac{8}{5}i \ \textit{(closes } 1-2i\textit{).} \end{aligned}$$

We take $\lambda = 1 - 2i$.

$\beta = \lambda\gamma + \delta$ *then* $\delta = \beta - \lambda\alpha$

$$\begin{aligned} \delta &= \text{6+2i-}(1-2i)(1+3i) \\ &= 6 + 2i - 1 - 3i + 2i - 6 \\ &= -1 + i \ . \end{aligned}$$

We find $\lambda = 1 - 2i$ and $\delta = -1 + i$.
So 6+2i=$(1 - 2i)(1 + 3i) + (-1 + i)$. $N(\delta) = N(-1 + i) < N(\alpha) = N(1 + 3i)$.

2.1.3 Greatest common divisor

Definition 2.1.17 *The Gaussian integer γ is a greatest common divisor of α and β if **(i)** γ divides α and β and **(ii)** γ is divisible by every common divisor of α and β.*

Proposition 2.1.18 *The greatest common divisor of α and β, is divisible by every common divisor of α and β.*

1. $\gcd(\alpha, \beta) = \gcd(\beta, \alpha)$.
2. if $\alpha|\beta$, so $\gcd(\alpha, \beta) = \alpha$.

Example 2.1.19 $\gcd(4+3i, 2-i) = \gcd(2-i, 4+3i) = 2-i$.

$$\begin{aligned} \frac{4+3i}{2-i} &= \frac{(4+3i)(2+i)}{(2-i)(2+i)} \\ &= \frac{8+4i+6i-3}{2^2+1^2} \\ &= \frac{5+10i}{5} \\ &= 1+2i. \end{aligned}$$

Then $\gcd(4+3i, 2-i) = 2-i$.

Theorem 2.1.20 *A Euclidean Algorithm for Gaussian Integers. Let $\varphi_0 = \alpha$ and $\varphi_1 = \beta$ be nonzero Gaussian integers. If the divison algorithm for Gaussian integers is successively applied to obtain $\varphi_j = \varphi_{j+1}\delta_{j+1} + r_{j+2}$; with $N(\varphi_{j+2}) < N(\varphi_{j+1})$ for $j = 0, 1, ..., n-2$ and $\varphi_{n+1} = 0$, then last nonzero remainder, is a greatest common divisor α and β.*

Example 2.1.21 $\gcd(7+4i, 1-5i) = 2+3i$.

$$\begin{aligned}\frac{7+4i}{1-5i} &= \frac{(7+4i)(1+5i)}{(1-5i)(1+5i)} \\ &= \frac{7+35i+4i-20}{1^2+5^2} \\ &= \frac{-13+39i}{26} \\ &= \frac{-1+3i}{2} \\ &= -\frac{1}{2}+\frac{3i}{2} \notin \mathbb{Z}[i].\end{aligned}$$

$\frac{7+4i}{1-5i}$ closes i or $-1+i$ or $-1+2i$ or $2i$ (λ *not unique*).

Use $\lambda = -1+i$.

$7+4i = (-1+i)(1-5i)+\delta$

then

$$\begin{aligned}\delta &= 7+4i-(-1+i)(1-5i) \\ &= 7+4i+1-5i-i-5 \\ &= 3-2i.\end{aligned}$$

We find $7+4i = (-1+i)(1-5i)+3-2i$.

$1-5i = \lambda(3-2i)+\delta$

$$\begin{aligned}\frac{1-5i}{3-2i} &= \frac{(1-5i)(3+2i)}{(3-2i)(3+2i)} \\ &= \frac{3+2i-15i+10}{3^2+2^2} \\ &= \frac{13-13i}{13} \\ &= 1-i \in \mathbb{Z}[i].\end{aligned}$$

Then $1-5i=(1-i)(3-2i)+0 \qquad (\lambda=1-i \text{ and } \delta=0)$.
So $\gcd(7+4i,1-5i)=3-2i$ (Last remaining division before 0).

Notation 2.1.22 *The greatest common divisor of two Gaussian integers is not unique, but is defined up to the multiplication by a unit. That is, given a greatest common divisor d of a and b, the greatest common divisors of a and b are d, $-d$, id and $-id$.*

Example 2.1.23 *Determine the greatest common divisor of $4+2i$ and $1-3i$.*

Solution 2.1.24 *$N(4+2i)=20$ and $N(1-3i)=10$. Then we will count $(4+2i)/(1-3i)$*

$$\begin{aligned}\frac{4+2i}{1-3i} &= \frac{(4+2i)(1+3i)}{(1-3i)(1+3i)}\\ &= \frac{4+12i+2i-6}{1^2+3^2}\\ &= \frac{-2+14i}{10} \notin \mathbb{Z}[i] \ (\frac{-2+14i}{10} \text{ closes } i).\end{aligned}$$

Then $4+2i=(i)(1-3i)+\delta=i+3+\delta$
Hence $\delta=4+2i-3-i=1+i$.

$$\begin{aligned}\frac{1-3i}{1+i} &= \frac{(1-3i)(1-i)}{(1+i)(1-i)}\\ &= \frac{1-i-3i-3}{2}\\ &= \frac{-2-4i}{2}\\ &= -1-2i \ \in \mathbb{Z}[i].\end{aligned}$$

then $1-3i=(-1-2i)(1+i)+0$
so $\gcd(4+2i,1-3i)=1+i$. *(The other greatest common divisor of $4+2i$ and $1-3i$ are $-1-i,-1+i,1-i$).*

2.2 Factorization for Gaussian integer

Theorem 2.2.1 *If α is a Gaussian integer other than 0 or a unit($N(\alpha) \geq 2$), then α can be expressed as a product of Gaussian primes.*

Proof. The proof is by induction on the norm of α. Suppose that the result is true for all Gaussian integers of norm less than n, we show that the resultust then hold for *Gaussian integers* α of norm n. If α is *Gaussian prime*, there is nothing to prove. Otherwise, there exist *Gaussian integers* β and γ, neither of which is a unit, such that $\alpha = \beta\gamma$. But since $N(\alpha) = N(\beta)N(\gamma)$, and neither β nor γ is a unit, we must have $N(\beta) < n$ and $N(\gamma) < n$. Thus by the induction hyphothesis, both β and γ can be expressed as a product of *Gaussian primes*, and therefore α is also a product of *Gaussian primes*. ■

Example 2.2.2 *Let be $-3+7i$ Gaussian integer, then $N(-3+7i) = 58 = 2 \times 29$.*
Thus $-3+7i$ has one factor of $1+i$ and one factor $a+bi$ with norm 29.
Then $-3+7i = (1+i)(a+bi)$

$$\begin{aligned} a+bi &= \frac{-3+7i}{1+i} \\ &= \frac{(-3+7i)(1-i)}{(1+i)(1-i)} \\ &= \frac{-3+3i+7i+7}{2} \\ &= \frac{4+10i}{2} \\ &= 2+5i. \end{aligned}$$

So $-3+7i = (1+i)(2+5i)$, where both $1+i$ and $2+5i$ are *Gaussian primes*.

Particulars cases

Corollary 2.2.3 *It follows that there are three cases for the factorization of a prime number p in the Gaussian integers:*

1. If p is congruent to 3 *modulo* 4, then it is a *Gaussian prime*, in the language of algebraic number theory, p is said to be *inert* in the *Gaussian integers* (for example $7, 19, 67....$).

2. If p is congruent to 1 *modulo* 4, then it is the product of a *Gaussian prime* by its conjugate, both of which are non-associated *Gaussian primes* (neither is the product of the other by a unit), p is said to be a *decomposed prime* in the *Gaussian integers* ($5 = (2+i)(2-i)$, $13 = (2+3i)(2-3i)$ and $97 = (9-4i)(9+4i)$).

3. If $p = 2$, we have $2 = (1+i)(1-i) = i(1-i)^2$, that is, 2 is the product of the square of a *Gaussian prime* by a *unit*, it is the unique *ramified prime* in the *Gaussian integers*.

2.3 Unique factorization

Theorem 2.3.1 *Suppose that $\alpha_1\alpha_2.....\alpha_p = \varepsilon\beta_1\beta_2.....\beta_q$, Where the α_i and β_i are Gaussian primes and ε is a unit. Then $p = q$, and the β_i can be rearranged so that for all i, β_i is an associate of α_i.*

Proof. Let $\delta = \alpha_1\alpha_2.....\alpha_r$. The result is clean when δ is a *Gaussian prime*, for then $p = q = 1$ and $\alpha_1 = \varepsilon\beta_1$. We prove the result in general by induction on p. Thus suppose that the unique factorization result holds for all *Gaussian integers* that have least one factorization as product of $p-1$ prime factors, we will show that must hold for all *Gaussian integers* that have en expression as the product of p prime factors.

Suppose that $\alpha_1\alpha_2.....\alpha_p = \varepsilon\beta_1\beta_2.....\beta_q$. Since α_p divides the product of the β_i, it must divide at least one of the β_i. By rearranging the factors it necessary, we may assume that $\alpha_p|\beta_q$. Since β_q is prime, it must be an associate of α, thus $\beta_q = \varepsilon'\alpha_p$, where $\varepsilon'$is a unit

Cancelling α_p from both sides the equation

$$\alpha_1\alpha_2.....\alpha_p = \varepsilon\varepsilon'\beta_1\beta_2.....\beta_{q-1}\alpha_p$$

We obtain

$$\alpha_1\alpha_2.....\alpha_{p-1} = \varepsilon\varepsilon'\beta_1\beta_2.....\beta_{q-1}$$

By the induction hypothesis, we therefore have $p-1 = q-1$, and hence $p = q$.

It also follows from the induction hypothesis that the numbers $\beta_1\beta_2.....\beta_{q-1}$, which proves can be reared so that they are associates of $\alpha_1\alpha_2.....\alpha_{p-1}$, which proves the theorem.

■

Example 2.3.2 *We will factorize* $5+3i$

$$\begin{aligned} N(5+3i) &= 5^2+3^2 \\ &= 25+9 \\ &= 34. \\ &= 2\cdot 17 \end{aligned}$$

Then $5+3i$ has one factor of $1+i$ and one factor of $1\pm 4i$.

Now we will divide $5+3i$ by $1+i$

$$\begin{aligned} \frac{5+3i}{1+i} &= \frac{(5+3i)(1-i)}{(1+i)(1-i)} \\ &= \frac{5-5i+3i+3}{2} \\ &= \frac{8-2i}{2} \\ &= 4-i \\ &= -i(1+4i). \end{aligned}$$

Such that $5+3i = -i(1+i)(1+4i)$.

Exercise 2.3.3 *Let* $8-14i$ *and* $7+17i$ *be a Gaussian integers.*

1. Factorize $8 - 14i$ and $7 + 17i$ into *Gaussian primes*.

2. Find $\gcd(8 - 14i, 7 + 17i)$.

Solution 2.3.4 *The norm of is* $8 - 14i$.

$$\begin{aligned} N(8 - 14i) &= 8^2 + 14^2 \\ &= 260 \\ &= 2^2 \times 5 \times 13 \end{aligned}$$

Then $8 - 14i$ *has two factors of* $1 + i$ *and one factor of* $1 \pm 2i$ *and one factor of* $2 \pm 3i$.
We have $(1 + i)^2 = 2i$.
We divide by $2i$

$$\begin{aligned} \frac{8 - 14i}{(1 + i)^2} &= \frac{8 - 14i}{2i} \\ &= -7 - 4i. \end{aligned}$$

Then $8 - 14i = -(1 + i)^2(7 + 4i)$

Divide by $2 + 3i$.

$$\begin{aligned} \frac{7 + 4i}{2 + 3i} &= \frac{(7 + 4i)(2 - 3i)}{13} \\ &= \frac{14 - 21i + 8i + 12}{13} \\ &= \frac{26 - 13i}{13} \\ &= 2 - i. \end{aligned}$$

So

$$\begin{aligned} 7+4i &= (2-i)(2+3i) \\ &= -i(1+2i)(2+3i). \end{aligned}$$

Implies that

$$\begin{aligned} 8-14i &= -(1+i)^2(-i(1+2i)(2+3i)) \\ &= i(1+i)^2(1+2i)(2+3i). \end{aligned}$$

Now we cosider the integer $7+17i$.

$$\begin{aligned} N(7+17i) &= 7^2+17^2 \\ &= 338 \\ &= 2\times 13^2. \end{aligned}$$

Thus $7+17i$ *has one factor of* $1+i$ *and two factors of* $2\pm 3i$.
First we divide by $1+i$

$$\begin{aligned} \frac{7+17i}{1+i} &= \frac{(7+17i)(1-i)}{(1+i)(1-i)} \\ &= \frac{7-7i+17i+17}{2} \\ &= \frac{7-7i+17i+17}{2} \\ &= \frac{24+10i}{2} \\ &= 12+5i. \end{aligned}$$

Now we divide $12+5i$ *by* $2+3i$*:*

$$\begin{aligned}\frac{12+5i}{2+3i} &= \frac{(12+5i)(2-3i)}{(2+3i)(2-3i)}\\ &= \frac{24-36i+10i+15}{13}\\ &= \frac{39-26i}{13}\\ &= 3-2i.\end{aligned}$$

So

$$\begin{aligned}12+5i &= (3-2i)(2+3i)\\ &= -i(2+3i)(2+3i)\\ &= -i(2+3i)^2.\end{aligned}$$

We find : $7+17i = -i(1+i)(2+3i)^2$

Hence

$$\begin{aligned}\gcd(7+17i, 8-14i) &= (1+i)(2+3i)\\ &= 2+3i+2i-3\\ &= -1+5i.\end{aligned}$$

Theorem 2.3.5 (*Bezout's identity*) *If* α *and* β *are Gaussian integers, not both zero, then* α *and* β *have a greatest common divisor* d *, which can be represented as* $d = \lambda\alpha + \mu\beta$*, where* λ *and* μ *are Gaussian integres.*

Proof. Let J be the set of all numbers of the form $s\alpha + t\beta$. where s and t rang over the *Gaussian integers*. Let d be an element of J of smallest positive norm, and suppose that $d = \lambda\alpha + \mu\beta$. We show that d is *Greatest common divisor* of α and β.

We first prove that $d|\alpha$. we have $\alpha = \kappa d + \delta$, where $N(\delta) < N(d)$.

Then

$$\begin{aligned} \delta &= \alpha - \kappa d \\ &= \alpha - \kappa(\lambda\alpha + \mu\beta) \\ &= (1 - \kappa\lambda)\alpha + (-\kappa\mu)\beta. \end{aligned}$$

And so we have expressed δ is a linear combination of α and β. Since $N(\delta) < N(d)$, this contradicts of d unless the remainder δ is 0.

Thus we conclude that $d|\alpha$, similarly $d|\beta$. It is obvious that if $\gamma|\alpha$ and $\gamma|\beta$, then $\gamma|\lambda\alpha + \mu\beta$ and therefore $\gamma|d$. thus d is a *greatest common divisor* of α and β. ■

Example 2.3.6 *Consider* $32 + 9i$ *and* $4 + 11i$. *The Euclidean Algorithm gives us the following equalities.*

$$\begin{aligned} 32 + 9i &= (4 + 11i)(2 - 2i) + 2 - 5i \\ 4 + 11i &= (2 - 5i)(-2 + i)) + 3 - i \\ 2 - 5i &= (3 - i)(1 - i) - i \\ 3 - i &= -i(1 + 3i) + 0. \end{aligned}$$

So we know that $-i$ *is a greatest common divisor of* $32+9i$ *and*$4+11i$, *and so we know that* $32 + 9i$ *and* $4 + 11i$ *are relatively prime. Let us try to find a solution to the Diophantine equation:*

$$\lambda(32 + 9i) + \mu(4 + 11i) = 1.$$

Performing reverse substitution, we see that

$$\begin{aligned}
-i &= (2-5i) - (3-i)(1-i) \\
&= (2-5i) - (4+11i-(2-5i)(-2+i))(1-i) \\
&= (2-5i) - (4+11i)(1-i) + (2-5i)(-2+1)(1-i) \\
&= (2-5i)(3i) - (4+11i)(1-i) \\
&= (2-5i)(3i) - (4+11i)(2-2i))(3i) - (4+11i)(1-i) \\
&= (32+9i)3i - (4+11i)(2-2i)(3i) - (4+11i)(1-i) \\
&= (32+9i)3i - (4+11i)(7+5i).
\end{aligned}$$

Multiplying by i, we have

$$1 = (32+9i)(-3) + (4+11i)(5-7i).$$

So one solution is $(\lambda, \mu) = (-3, 5-7i)$.

Chapter 3

Application of Gaussian Integers

The most used references in this chapter are ([**1**], [**13**]).

3.1 Solving of the equation: $y^2 = x^3 - 1$

Theorem 3.1.1 *The only solution of* $x^2 + 1 = y^3$ *is the integers* $x = 0$, $y = 1$.

Proof. Let us give to our equation the following equivalent form

$$(x + i)(x - i) = y^3.$$

first we prove that if x and y is a solution of the equation then $x + i$, $x - i$ are relatively prime. Indeed if they are not, there is a Gaussian prime π which divides $x + i$ and $x - i$, then $\pi|2$, since π divides $(x + i) - (x - i)$. It is easy to see that x must be even, for if x is odd, then $x^2 + 1 \equiv 2 (\mathrm{mod}\, 4)$, and no cube can be congruent to 2 modulo 4. Since x is even, we have $\pi|x$; since $\pi|x + i$ by assumption, it follows that $\pi|i$, which is impossible. ■

To continue our proof we need the following

Lemma 3.1.2 *If* α, β *and* γ *are Gaussian integers and* n *is a positive integer such that* $\alpha\beta = \gamma^n$ *and* α *and* β *are relatively prime, then* $\alpha = \epsilon\delta^n$, *where* ϵ *is a unit and* δ *is a Gaussian integer.*

Proof. Let the prime factorization of $\gamma = \pi_1\pi_2...\pi_k$. Then the unique prime factorization of γ^n is $\gamma^n = \pi_1^n\pi_2^n...\pi_k^n = \alpha\beta$. For each Gaussian prime π_j,we have $\pi_j|\alpha\beta$ and so either $\pi_j|\alpha$ or $\pi_j|\beta$ but not both. ■

because $\alpha$and β are relatively prime. Therefore $\pi_j^n|\alpha$ or $\pi_j^n|\beta$. So, after re-indexing if necessary, there is an index r such that $\pi_1^n\pi_2^n...\pi_r^n|\alpha$ and $\pi_{r+1}^n\pi_2^n...\pi_k^n|\beta$. And because $N(\gamma) = N(\alpha)N(\beta) = N(\pi_1^n\pi_2^n...\pi_r^n)N(\pi_{r+1}^n\pi_2^n...\pi_k^n)$, we see that $N(\alpha) = (\pi_1^n\pi_2^n...\pi_r^n)$, and $\pi_1^n\pi_2^n...\pi_r^n$ are associates.

Therefore $\alpha = \varepsilon\pi_1^n\pi_2^n...\pi_r^n = \varepsilon(\pi_1\pi_2...\pi_r)^n = \varepsilon\delta^n$ where epsilon is a unit.

By the above lemma $x+i$ can be expressed in the form $\varepsilon\delta^3$, where ε is a unit. It is easy to check that for any unit ε, we have $\varepsilon^3 = \varepsilon$, so in fact $x+i = (\varepsilon\delta)^3$.

Let $x+i = (u+vi)^3 = (u^3-3uv^2)+(3u^2v-v^3)i$; then $x = u^3-3uv^2$ and $1 = 3u^2v-v^3$.

Since $v(3u^2-v^2) = 1$, it follows that $v = \pm 1$. If $v = 1$, then $3u^2-v^2 = 1$ and hence $3u^2 = 2$, which is impossible. If $v = -1$, then $3u^2-v^2 = -1$, giving $u = 1$. Thus $x = 1$,and therefore $y = 1$. We conclude that the only solution in integers of the Diophantine equation $x^2+1 = y^3$ is $x = 0, y = 1$.

3.2 Sum of Two Squares and Gaussian integers

We restrict the application to the following two theorems where we recall that if a Gaussian prime $\pi|\alpha\beta$ then $\pi|\alpha$ or $\pi|\beta$.

Theorem 3.2.1 *Every p of the form $4k+1$ is a sum of two squares.*

Proof. We show first that p is not a Gaussian prime. Since -1 is a quadratic residue of p, there is a rational integer x such that $x^2 \equiv -1(\mathrm{mod}\, p)$. Thus $P|x^2+1$ and therefore $P|(x-i)(x+i)$. If p were a Gaussian prime, it would follow that $P|(x-i)$ or $P|(x+i)$, but plainly neither is the case.

Since p is not a Gaussian prime, there exist Gaussian integers α and β, neither of which is a unit, such that $p = \alpha\beta$. Since $N(p) = p^2 = N(\alpha)N(\beta)$ and neither $N(\alpha)$ or $N(\beta)$ is equal to 1, it follows that $N(\alpha) = N(\beta) = p$.

Thus if $\alpha = u + iv$, then $p = u^2 + v^2$, and hence p is a sum of two squares. ■

Let $N(n)$ denote the number of representation of the n as a sum of two squares the unique factorization theorem for Gaussian integers can be used to find $N(n)$

Theorem 3.2.2 *Let $n = 2^a \prod p_j^{a_j} \prod q_j^{b_j}$, where the p_j are $4k+1$ primes, the q_j are $4k+3$ primes, and each b_j is even. Then*

$$N(n) = 4 \prod (a_j + 1).$$

(A product of the no terms is interpreted to be 1).

Example 3.2.3 89 *is a prime number, and*

$$89 \equiv 1 (\mathrm{mod}\, 4)$$

Hince, 89 can be represented as a sum of two squares:

$$\begin{aligned} 89 &= 25 + 64 \\ &= 5^2 + 8^2. \end{aligned}$$

Conclusion

Reading the concepts presented in this memory puts the reader in a practical and suitable position to initiate and do some research in the field related to Gaussian integers. This is due to the fact that the concepts given in this work are fundamental for this line of research. Then we can try to treat other Diophantine equations, represent positive integers, ...

Bibliography

[1] A. Adler,J E. Cloury, The theory of numbers_a text and source book of problems, Jones and Bartlett, 1995.

[2] A. Boudaoud, Decomposition of terms in Lucas sequences, J. Log. Anal. 1:4 (2009), 1-23; Published: 16 April 2009; https://doi.org/10.4115/jla.2009.1.4.

[3] A. Boudaoud, Diophantine approximation with improvement of the simultaneous control of the error and of the denominator, arXiv preprint arXiv:1605.02538 (2016).

[4] A Boudaoud, La conjecture de Dickson et classes particulière d'entiers, Ann. Math. Blaise Pascal. 13 (2006), 103-109; https://doi.org/10.5802/ambp.215.

[5] A. Boudaoud, Modélisation de phénomènes discrets et approximations diophantiennes infinitésimales, Thèse de Doctorat en Mathématiques, Université de Haute Alsace Mulhouse - France 1988.

[6] A. Boudaoud, Sur l'approximation simultanée au sens infinitésimal de réels à cardinal illimité , Rendiconti del Seminario della Facoltà di Scienze dell'Università di Cagliari 74(1-2) : 17-22(2004).

[7] Bellaouar Djamel, Boudaoud Abdelmadjid, Özen Özer, ON A SEQUENCE FORMED BY ITERATING A DIVISOR OPERATOR, Czechoslovak Mathematical Journal, 69 (144) (2019), 1177–1196.

[8] D. Bellaouar, A. Boudaoud, Notes on certain arithmetic inequalities involving two consecutive primes. Malays, J. Math. Sci. 10 (2016), 253-268.

[9] D. Evan, Number Theory. Part 4, unique factorization and applications v, 2.10, 2020.

[10] De Koninck, J. M. and Mercier, A. (2004). 1001 problèmes en théorie classique des nombres. In Number Theory, Paris. Ellipses.

[11] M B Nathanson, Elementary methods in number theory, Springer-Verlag, New York (2000); https://doi.org/10.1007/b98870.

[12] R A Mollin, Fundamental number theory with applications. Second Edition, Chapman & Hall/Crc (2008); https://doi.org/10.1201/b15895.

[13] R. Kenneth Elementary Number theory and its applications, PEARSON, Monmouth University 2011.

[14] Said Boudaoud, Djamel Bellaouar, Abdelmadjid Boudaoud, Nonclassical Study on certain Diophantine Inequalities involving Multiplicative Arithmetic Functions, Malaysian Journal of Mathematical Sciences 14(1): 17-39 (2020), Journal homepage: http://einspem.upm.edu.my/journal.

[15] S. Alaca, K S. Williams, Introductory algebraic number theory, Cambridge University press 2004.

[16] S. Badidja, A. Boudaoud, Unique representation of positive integers as a sum of distinct tribonacci numbers, Journal of Mathematics and Statistics, 2017; http://www.ceser.in/ceserp/index.php/ijms.

[17] Wells, D. (2005), Prime numbers, the most mysterious figures in math. In Number Theory, Canada. Wiley & Sons, Inc.

[18] Wikipedia, Gaussian integers, https://en.wikipedia.org/wiki/Gaussian_integer.

Abstract. **This memory is formed by three chapters. The first one contains some fundamental and common notions of any integral ring. The concepts related to Gaussian Integers as: units, Gaussian prime, greatest common divisor, factorization and unique factorization of Gaussian integers, Bezout's identity, … are the subject of the second chapter. The third chapter is devoted to two squares and the solution of the Diophantine equation $y^2 = x^3-1$.**

Résumé. **Ce mémoire est formé de trois chapitres. Le premier contient quelques notions fondamentales et communes de tout anneau intégral. Les concepts liés aux entiers gaussiens comme : unités, nombre premier gaussien, plus grand commun diviseur, factorisation et factorisation unique des entiers gaussiens, identité de Bezout, … font l'objet du deuxième chapitre. Le troisième chapitre est consacré à deux applications importantes concernant l'écriture d'entiers positifs comme somme de deux carrés et la résolution de l'équation diophantienne $y^2 = x^3-1$.**

الملخص. تتكون هذه الرسالة من ثلاثة فصول. الفصل الأول يحتوي على بعض المفاهيم الأساسية و المشتركة لأي حلقة متكاملة. المفاهيم المتعلقة بالأعداد الصحيحة الغاوسية مثل: الوحدات, العدد الأولي الغاوسي, القاسم المشترك الأكبر, التحليل الى العوامل و العوامل الفريدة للأعداد الصحيحة الغاوسية, نظرية بيزوت..... موضوع الفصل الثاني.الفصل الثالث مخصص لتطبيقين مهمين يتعلقان بكتابة الأعداد الصحيحة الموجبة كمجموع مربعين وحل معادلة ديوفانتين $y^2 = x^3-1$.