Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

# O Pequeno Teorema de Fermat e de Euler para Inteiros Gaussianos

**Cláudio de Oliveira Brandão Junior**

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Cuiabá - MT

outubro

# O Pequeno Teorema de Fermat e de Euler para Inteiros Gaussianos

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Cláudio de Oliveira Brandão Junior e aprovada pela comissão julgadora.

Cuiabá, 18 de outubro de 2019.

Prof. Dr. Martinho da Costa Araújo
Orientador

**Banca examinadora:**

Prof. Dr. Martinho da Costa Araújo
Prof. Dra. Thaís Silva do Nascimento
Prof. Dr. José de Arimatéia Fernandes

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título de **Mestre em Matemática**.

**Dados Internacionais de Catalogação na Fonte.**

B817p Brandão Junior, Cláudio de Oliveira.
O Pequeno Teorema de Fermat e de Euler para Inteiros Gaussianos / Cláudio de Oliveira Brandão Junior. -- 2019
xi, 72 f. : il. color. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) – Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação Profissional em Matemática, Cuiabá, 2019.
Inclui bibliografia.

1. Inteiro Gaussiano. 2. Norma. 3. Pequeno Teorema de Fermat. 4. Função de Euler. 5. Teorema de Euler. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE MATO GROSSO
PRÓ-REITORIA DE ENSINO DE PÓS-GRADUACÃO
Programa de Pós-Graduação em Ensino de Matemática em Rede Nacional - Profmat,
Av. Fernando Corrêa da Costa, 2367 - Boa Esperança - 78.060-900 - Cuiabá/MT
Fone: (65) 3615-8576 – E-mail : profmat@ufmt.br

# FOLHA DE APROVAÇÃO

**Título: "O pequeno teorema de Fermat e de Euler para inteiros gaussianos"**

**Autor**: Cláudio de Oliveira Brandão Júnior

defendida e aprovada em 18/10/2019.

Composição da Banca Examinadora:

Presidente Banca/Orientador Doutor Martinho da Costa Araújo
Instituição: Universidade Federal de Mato Grosso

Examinadora Interna Doutora Thais Silva do Nascimento
Instituição : Universidade Federal de Mato Grosso

Examinador Externo Doutor José de Arimatéia Fernandes
Instituição : Universidade Federal de Campina Grande

Cuiabá, 18/10/2019.

*Muda, que quando a gente muda o mundo muda com a gente. A gente muda o mundo na mudança da mente. E quando a mente muda a gente anda pra frente. (Gabriel, o pensador)*

# Agradecimentos

Primeiramente a DEUS, que sempre está presente no meu caminho me acompanhando e dizendo de infinitas maneiras: Acredita e vai!

À minha família, em especial, meus pais, por sempre acreditarem em meu potencial e investirem no meu crescimento pessoal.

Cleiton Diniz, meu amigo e companheiro em todas as horas. Se tem uma pessoa que sabe tudo que aconteceu na minha vida durante esse Mestrado, é você. Te agradeço pelo que você é e por estar sempre comigo.

Ao meu orientador, Prof. Dr. Martinho da Costa Araújo que indicou o tema deste trabalho, acompanhou o seu desenvolvimento, ajudando sempre que foi solicitado. Só tenho agradecer essa oportunidade.

Renato Fortes, meu amigo de graduação e da vida, agradeço pelo incentivo, pelas puxadas de orelhas, pelas caminhadas, por ser parceiro e por sempre me mostrar que é possível ser melhor.

Valcir Borges, meu colega de trabalho e amigo que o PROFMAT me proporcionou, agradeço o companheirismo e ajuda pelos processos em que fomos submetidos desde o concurso público à apresentação deste trabalho.

Priscila Pacheco, amiga que o PROFMAT me deu e a rainha das festinhas, agradeço pelo companheirismo, seja com as listinhas (que eu odiava fazer), ou até mesmo com palavras de apoio, enxergando um potencial que eu mesmo não percebia.

A todos os professores que ministraram as aulas no PROFMAT na UFMT.

A todos os companheiros de turma 2017, Claudeir, Osvaldo, Zeila, Adriana, Jaqueline Tga, Jaqueline Roo, Juliano (e Marcela), Luiz, Vinícius, Ondrias e Paula. Paula ficou por último, pelas vezes que me alfinetava em sala de aula.

*Não é o conhecimento, mas o ato de aprender, não a posse mas o ato de chegar lá, que concede a maior satisfação.*

Gauss.

# Resumo

Neste trabalho faremos um estudo sobre o conjunto dos inteiros gaussianos, que é formado pelos números da forma a+bi, onde a e b são inteiros. Iremos relembrar algumas propriedades importantes dos Inteiros e estendê-las para o conjunto dos inteiros gaussianos, como divisibilidade, divisão euclidiana, fatoração e aritmética modular. Em seguida, apresentaremos uma classificação para os primos gaussianos, isto é, quais são os inteiros gaussianos que são primos. E por fim, daremos uma versão do Pequeno teorema de Fermat e do Teorema de Euler e uma fórmula fechada para calcular a função phi de Euler para todo inteiro gaussiano.

**Palavras chave:** Inteiro Gaussiano, Norma, Pequeno Teorema de Fermat, Função de Euler, Teorema de Euler, Primos Gaussianos.

# Abstract

In this paper we will study the set of gaussian integer, which is formed by the numbers of the form a + bi , where a and b are integers. We will recall some important properties of integers and extend them to set of gaussian integers, such as divisibility, euclidean division, factorization and modular arithmetic. Next, we present a classification for Gaussian prime, that is, which Gaussian integers are prime. And finally, we will give a version of Fermat's Little Theorem and Euler's Theorem and a closed formula for calculating Euler's phi function for every Gaussian integer.

**Keywords:** Gaussian Integer, Norm, Fermat's Little Theorem, Euler's Function, Euler's Theorem, Gaussian Prime.

# Sumário

# Lista de Figuras

# Introdução

> "A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas."
>
> (Gauss)

Entre os anos de 1808 e 1825, Carl F. Gauss, ao investigar propriedades relacionadas à reciprocidade cúbica ($x^3 \equiv q \mod p$ onde $p$ e $q$ são primos) e a reciprocidade biquadrática ($x^4 \equiv q \mod p$ onde $p$ e $q$ são primos), percebeu que essa investigação poderia ser melhor e mais simples se trabalhasse sobre $\mathbb{Z}[i]$, o anel formado por números complexos da forma $a + bi$, onde $a$, $b \in \mathbb{Z}$ e $i^2 = -1$. Gauss fez a extensão das propriedades de $\mathbb{Z}$ para $\mathbb{Z}[i]$ e percebeu que grande parte da Teoria de Euclides poderia ser transportada para $\mathbb{Z}[i]$, o que consequentemente trouxe diversas contribuições para a Teoria dos Números. Trabalhando em $\mathbb{Z}[i]$, desenvolveu a Teoria da Fatoração em primos e demonstrou que a decomposição em primos é única, idêntica ao que acontece em $\mathbb{Z}$. O anel $\mathbb{Z}[i]$ ficou conhecido como o conjunto dos Inteiros Gaussianos.

Através dessa teoria formulada por Gauss, nosso objetivo neste trabalho é fazer a extensão do Pequeno Teorema de Fermat e a função e teorema de Euler para os inteiros gaussianos.

No primeiro capítulo, faremos uma revisão das principais propriedades da teoria dos inteiros como divisibilidade, algoritmo da divisão, algoritmo de Euclides, fatoração única e a aritmética modular. Nessa última, iremos falar sobre classes residuais, Pequeno Teorema de Fermat e a Função e Teorema de Euler, tomaremos como referência Hefez (2016), Hefez (2006), Piffer (2014), Araújo (2017), de Oliveira Santos (2007) e Rosen (2011).

No segundo capítulo, através dos estudos de Conrad (2008), faremos a extensão para $\mathbb{Z}[i]$ das propriedades estudadas no capítulo 1 e também definiremos a função norma, unidades e associados. Usaremos, como suporte, para a construção deste capítulo, as

referências Campos Filho (2014) e Stein (1976).

No terceiro capítulo, trataremos sobre a aritmética modular em $\mathbb{Z}[i]$, definindo a congruência e verificando que ela é uma relação de equivalência. Construiremos os conjunto das classes residuais módulo algum inteiro gaussiano e faremos a representação das classes residuais geometricamente. Faremos a demonstração do Pequeno Teorema de Fermat em $\mathbb{Z}[i]$, baseado em Conrad (2008), Roberson (2016), e a demonstração da função e teorema de Euler, baseado em May (2015).

# Capítulo 1

# Propriedades clássicas dos Inteiros-$\mathbb{Z}$

Neste capítulo apresentaremos algumas definições, propriedades e teoremas que estão relacionados com a aritmética dos inteiros. Tradicionalmente escrevemos $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.Vamos considerar $\mathbb{N} = \{0, 1, 2, 3, ...\}$ o conjunto dos números naturais, $\mathbb{N}^* = \mathbb{N} - \{0\} = \{1, 2, 3, ...\}$, $\mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\}$ e $\mathbb{Z}^- = \{x \in \mathbb{Z} : x < 0\}$.

## 1.1 Divisibilidade

**Definição 1.** *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$, diremos que $a$ divide $b$, escrevemos $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Quando $a$ divide $b$, dizemos também que $a$ é um divisor de $b$ ou um fator de $b$ e que $b$ é um múltiplo de $a$. Se $a$ não divide $b$, escrevemos $a \nmid b$.*

**Exemplo 1.** *Como $12 = 3 \cdot 4$, então $3|12$.*

**Exemplo 2.** *$4 \nmid 25$, pois se dividisse existiria $c \in \mathbb{Z}$ tal que $25 = 4 \cdot c$ e essa igualdade só é possível se $c = \frac{25}{4}$, mas $\frac{25}{4} \notin \mathbb{Z}$.*

**Proposição 1.** *Se $a$, $b$ e $c$ são inteiros e $a|b$ e $b|c$, então $a|c$.*

*Demonstração.* Como $a|b$ e $b|c$, existem $e$ e $f$ tal que $b = ae$ e $c = bf$. Substituindo a primeira equação na segunda, obtemos $c = (ae)f = a(ef)$. Portanto, $a|c$. □

**Proposição 2.** *Se $a, b, c, m$ e $n$ são inteiros, $c|a$ e $c|b$ então $c|am + bn$.*

*Demonstração.* Se $c|a$ e $c|b$, então $a = k_1c$ e $b = k_2c$ para $k_1, k_2 \in \mathbb{Z}$. Multiplicando essas equações por $m$ e $n$, respectivamente, teremos $ma = mk_1c$ e $nb = nk_2c$. Somando membro a membro, temos que $ma + nb = c(mk_1 + nk_2)$. Portanto, $c|am + bn$. □

**Exemplo 3.** *Como* $3|6$ *e* $3|15$*, então* $3|6 \cdot 7 + 15 \cdot 2$.

## 1.2 Teorema da Divisão

**Teorema 3.** *(Divisão Euclideana) Se* $a$ *e* $b$ *são inteiros com* $b > 0$*, então existem inteiros únicos* $q$ *e* $r$ *tais que*

$$a = b \cdot q + r, \text{ com } 0 \leq r < b.$$

*Demonstração.* Considere $S$ o conjunto de todos os inteiros da forma $a - bk$, onde $k$ é um inteiro, ou seja, $S = \{a - bk : k \in \mathbb{Z}\}$. Seja $T$ o conjunto de todos os números inteiros não negativos em $S$. $T$ não é vazio, pois $a - bk$ é positivo sempre que $k$ é um número inteiro com $k < a/b$.

Pelo Princípio da Boa Ordem, $T$ tem um menor elemento $r = a - bk$. Sabemos que $r \geq 0$, então vamos verificar que $r < b$. Suponha $r \geq b$, então $r > r - b = a - bq - b = a - b(q + 1) \geq 0$, o que é uma contradição, já que $r = a - bq$ é o menor elemento de $T$. Daí, $0 \leq r < b$.

Para mostrar que $q$ e $r$ são únicos, assuma que temos as equações $a = bq_1 + r_1$ e $a = bq_2 + r_2$, com $0 \leq r_1 < b$ e $0 \leq r_2 < b$. Subtraindo a segunda dessas equações pela primeira, descobrimos que

$$0 = b(q_1 - q_2) + (r_1 - r_2).$$

Portanto, vemos que

$$r_2 - r_1 = b(q_1 - q_2).$$

Isso nos diz que $b$ divide $r_2 - r_1$. Como $0 \leq r_1 < b$ e $0 \leq r_2 < b$, temos $-b < r_2 - r_1 < b$. Portanto, $b$ pode dividir $r_2 - r_1$ somente se $r_2 - r_1 = 0$ ou, em outras palavras, se $r_2 = r_1$. Como $bq_1 + r_1 = bq_2 + r_2$ e $r_2 = r_1$, segue que $q_1 = q_2$. Isso mostra que o quociente $q$ e o resto $r$ são únicos. □

**Observação 1.** *No Teorema 3, se* $b < 0$ *então* $-b > 0$*, logo* $a = b(-q) + r$*,* $0 \leq r < -b$.

**Exemplo 4.** *Ache o quociente e o resto da divisão de* 23 *por* 3.

*Considere as diferenças sucessivas:*

$$23 - 3 = 20, 23 - 2 \cdot 3 = 17, 23 - 3 \cdot 3 = 14, 23 - 4 \cdot 3 = 11, 23 - 5 \cdot 3 = 8,$$
$$23 - 6 \cdot 3 = 5, 23 - 7 \cdot 3 = 2 < 3.$$

*Isto nos dá $q = 7$ e $r = 2$.*

## 1.3 O Algoritmo de Euclides

**Definição 2.** *Sejam $a, b$ e $d$ inteiros não nulos. Diremos que $d > 0$ será o máximo divisor comum de $a$ e $b$, quando:*

*i) $d|a$ e $d|b$;*

*ii) $d$ é divisível por todo divisor comum de $a$ e $b$, ou seja, se $c$ é um divisor comum de $a$ e $b$, então $c|d$.*

*Indicamos o máximo divisor comum de $a$ e $b$ por $d = mdc(a, b)$.*

**Teorema 4.** *Se $a, b \in \mathbb{Z}$ e $a = b \cdot q + r$, onde $q$ e $r$ são inteiros, então $mdc(a, b) = mdc(b, r)$.*

*Demonstração.* Da relação $a = b \cdot q + r$ podemos concluir que todo divisor de $b$ e $r$ é um divisor de $a$ (Proposição 2). Esta mesma relação, escrita na forma $r = a - b \cdot q$, nos diz que todo divisor de $a$ e $b$ é um divisor de $r$. Logo o conjunto dos divisores comuns de $a$ e $b$ e o conjunto dos divisores comuns de $b$ e $r$ são iguais, o que nos garante o resultado $mdc(a, b) = mdc(b, r)$. □

**Teorema 5.** *(Algoritmo de Euclides) Tome $a, b \in \mathbb{Z}$, com $b \neq 0$. Aplicando repetidamente o Teorema da Divisão onde o resto é diferente de zero, teremos*

$$a = b \cdot q_1 + r_1, \text{ com } 0 \leq r_1 < b$$
$$b = r_1 \cdot q_2 + r_2, \text{ com } 0 \leq r_2 < r_1$$
$$r_1 = r_2 \cdot q_3 + r_3, \text{ com } 0 \leq r_3 < r_2$$
$$\vdots$$

*Em algum momento, temos $r_k = 0$.*

*Pelo Teorema 4, $mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = mdc(r_2, r_3) = ... = mdc(r_{n-1}, r_n = 0) = r_{n-1}$.*

*Demonstração.* Pela Divisão euclideana, temos que

$$a = b \cdot q_1 + r_1, \text{ com } 0 \leq r_1 < b.$$

Pelo Teorema 4, $mdc(a,b) = mdc(b,r_1)$, desta forma temos duas situações:

- $r_1 = 0$, neste caso $mdc(b,r_1) = b = mdc(a,b)$, pois $b|a$.
- $r_1 \neq 0$, neste caso fazemos a divisão euclideana de $b$ por $r_1$, obtendo

$$b = r_1 \cdot q_2 + r_2, \text{ com } 0 \leq r_2 < r_1$$

Segue que $mdc(b,r_1) = mdc(r_1,r_2)$. Novamente pode ocorrer duas situações:

- $r_2 = 0$, neste caso $mdc(r_1,r_2) = r_1$.
- $r_2 \neq 0$, neste caso fazemos a divisão euclideana de $r_1$ por $r_2$, obtendo

$$r_1 = r_2 \cdot q_3 + r_3, \text{ com } 0 \leq r_3 < r_2.$$

Segue que

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = mdc(r_2,r_3)$$

e assim sucessivamente.

Definindo $r_0 = b$, existe um valor $n$ natural que $r_{n+1} = 0$ e $r_n \neq 0$. De fato, se tivéssemos para todo $n \neq 0$, teríamos uma sequência infinita

$$r_0 > r_1 > r_2 > ... > 0.$$

Segue que

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = ... = mdc(r_n,r_{n+1}) = mdc(r_n,0) = r_n.$$

Portanto, o último resto não nulo $r_n$ deste processo, fornece o valor de $mdc(a,b)$. □

**Definição 3.** *Dizemos que $a$ e $b \in \mathbb{Z}$ são relativamente primos quando $mdc(a,b) = 1$.*

**Exemplo 5.** *Calcule o mdc de 372 e 162.*

*Fazendo as divisões sucessivas, temos*

$$372 = 162 \cdot 2 + 48$$

$$162 = 48 \cdot 3 + 18$$

$$48 = 18 \cdot 2 + 12$$

$$18 = 12 \cdot 1 + 6$$

$$12 = 6 \cdot 2 + 0.$$

*Como o último resto diferente de zero é 6, então $mdc(372,162) = 6$.*

**Exemplo 6.** *Calcule o mdc de* 194 *e* 175.

*Fazendo as divisões sucessivas, temos*

$$\begin{aligned} 194 &= 175 \cdot 1 + 19 \\ 175 &= 19 \cdot 9 + 4 \\ 19 &= 4 \cdot 4 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

*Como o último resto diferente de zero é* 1*, então* $mdc(194, 175) = 1$ *e* 194 *e* 175 *são relativamente primos.*

## 1.4 O Teorema de Bezóut

**Teorema 6.** *(Teorema de Bézout) Seja* $a, b \in \mathbb{Z}$*, diferentes de zero e* $mdc(a, b) = c$*. Então* $c = ax + by$*, para algum* $x, y \in \mathbb{Z}$*.*

*Demonstração.* Considere o conjunto $C$ sendo todas as combinações lineares possíveis de $a$ e $b$. Pelo Princípio da Boa Ordem, existe $n = ax_0 + by_0$, onde $n$ é o menor elemento de $C$. Suponha, por absurdo, que $n \nmid a$. Então $a = nq + r$, com $0 < r < n$.

$$\begin{aligned} r &= a - nq = a - (ax_0 + by_0)q \\ &= a - ax_0q - by_0q \\ &= a(1 - x_0q) + b(-y_0q). \end{aligned}$$

Então $r \in C$, pois $r > 0$ e $r < n$, contradizendo o fato de $n$ ser o menor elemento de $C$. Portanto, $n|a$. Analogamente, podemos mostrar que $n|b$. Assim, $n$ é o divisor comum de $a$ e $b$. Vamos mostrar que $n = d$. De fato, pois se $d = mdc(a, b)$, então $a = dq_1$ e $b = dq_2$. Agora $n = ax_0 + by_0 \Rightarrow n = d(q_1x_0 + q_2y_0) \Rightarrow d|n \Rightarrow d \leq n \Rightarrow d = n$. □

**Corolário 7.** *Sejam* $a, b$ *inteiros relativamente primos, então existem* $x, y \in \mathbb{Z}$ *tal que* $ax + by = 1$*.*

*Demonstração.* Como $a$ e $b$ são relativamente primos, então $mdc(a, b) = 1$. Pelo Teorema 6, existem $x, y \in \mathbb{Z}$ tal que $ax + by = 1$. □

**Exemplo 7.** *Vimos no Exemplo 6 que* 194 *e* 175 *são relativamente primos, pois* $mdc(194, 175) = 1$. *Agora escreveremos* 1 *como uma combinação linear de* 194 *e* 175*, conforme o Teorema de Bezóut:*

$$\begin{aligned}
1 &= 4 - 3 \cdot 1 \\
1 &= 4 - (19 - 4 \cdot 4) \cdot 1 \\
1 &= 4 \cdot 5 - 19 \cdot 1 \\
1 &= (175 - 19 \cdot 9) \cdot 5 - 19 \cdot 1 \\
1 &= 175 \cdot 5 - 19 \cdot 46 \\
1 &= 175 \cdot 5 - (194 - 175 \cdot 1) \cdot 46 \\
1 &= 175 \cdot 51 - 194 \cdot 46 \\
1 &= 175 \cdot 51 + 194 \cdot (-46).
\end{aligned}$$

**Teorema 8.** *Se* $a|bc$ *e* $mdc(a, b) = 1$*, então* $a|c$.

*Demonstração.* Como $mdc(a, b) = 1$, então existem $m, n \in \mathbb{Z}$ tal que $am + bn = 1$ (Corolário 7). Multiplicando todos os lados dessa igualdade por $c$ temos, $n(ac)+m(bc) = c$. Como $a|ac$ e, por hipótese, $a|bc$ então, pela Proposição 2, $a|c$. □

**Teorema 9.** *Seja* $a, b, c \in \mathbb{Z}$ *tal que* $mdc(a, b) = 1$ *e* $c = a \cdot b$*. Então para algum* $k \in \mathbb{Z}$*,* $mdc(c, k) = 1$ *se, e somente se* $mdc(a, k) = 1$ *e* $mdc(b, k) = 1$.

*Demonstração.* Seja $a, b, c \in \mathbb{Z}$ tal que $a$ e $b$ são relativamente primos e $c = a \cdot b$. Assuma que $mdc(a, k) \neq 1$ ou $mdc(b, k) \neq 1$. Sem perda de generalidade, assuma que $mdc(a, k) = m$ para algum $m \in \mathbb{Z}$, $m > 1$. Então $m|a$ e $m|k$. Além disso, já que $a|c$, sabemos que $m|c$. Como $m|c$ e $m|k$, sabemos que $m$ é um divisor comum, diferente de 1, de $c$ e $k$. Então $c$ e $k$ não são relativamente primos. O mesmo acontece se supomos $mdc(b, k) = m$ com $m \neq 1$. Por contrapositiva, temos que se $mdc(c, k) = 1$ então $mdc(a, k) = 1$ e $mdc(b, k) = 1$.

Agora, suponha que o $mdc(a, k) = 1$ e $mdc(b, k) = 1$. Então, $af + kg = 1$ e $bh + ki = 1$ para algum $f, g, h, i \in \mathbb{Z}$. Multiplicando as equações membro a membro,

temos

$$(af + kg)(bh + ki) = 1$$
$$afbh + afki + kgbh + kgki = 1.$$

Como $c = a \cdot b$,

$$c(fh) + k(afi + gbh + gki) = 1.$$

Portanto, $mdc(c, k) = 1$. □

## 1.5 Fatoração Única

**Definição 4.** *Um número primo é um número inteiro positivo maior do que* 1 *que é divisível apenas por* 1 *e ele próprio.*

**Definição 5.** *Um número inteiro positivo maior que* 1 *que não é primo é chamado de composto.*

**Lema 10.** *Se $p|ab$, $p$ primo, então $p|a$ ou $p|b$.*

*Demonstração.* Se $p \nmid a$, então $mdc(a, p) = 1$ o que implica, pelo Teorema 8, $p|b$. □

**Teorema 11.** *(Fatoração Única) Todo inteiro maior do que* 1 *pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos, não necessariamente distintos.*

*Demonstração.* Faremos a prova por contradição. Vamos supor que algum número inteiro positivo não possa ser escrito como um produto de números primos. Seja $n$ o menor número inteiro com tal propriedade, se $n$ é primo, então não há nada a ser demonstrado, pois é um produto de primo. Se $n$ é composto, então $n = ab$, com $1 < a < n$ e $1 < b < n$. Como $a$ e $b$ são menores que $n$, eles devem ser um produto de números primos. Então, como $n = ab$, concluímos que $n$ também é um produto de números primos. Essa contradição mostra que todo número inteiro positivo pode ser escrito como um produto de números primos.

Para mostrarmos a unicidade iremos supor que $n$ possua duas fatorações diferentes em números primos:

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_t,$$

onde $p_1, p_2, ..., p_s$ e $q_1, q_2, ..., q_t$ são primos, com $p_1 \leq p_2 \leq ... \leq p_s$ e $q_1 \leq q_2 \leq ... \leq q_t$.

Ao remover todos os primos comuns das duas fatorações, obtemos

$$p_{i_1} p_{i_2} ... p_{i_u} = q_{j_1} q_{j_2} ... q_{j_v}$$

onde os números primos no lado esquerdo são diferentes daqueles do lado direito, com $u \geq 1$ e $v \geq 1$. No entanto, isso leva a uma contradição do Lema 10, porque por esse Lema, $p_{i_1}$ deve dividir $q_{j_k}$, para algum $k$, o que é impossível, pois cada $q_{j_k}$ é primo e é diferente de $p_{i_1}$. Portanto, a fatoração em primos de um número inteiro positivo $n$ é única. □

## 1.6 Aritmética Modular

**Definição 6.** *Sejam $a, b, n \in \mathbb{Z}$. Dizemos que $a$ é congruente a $b$ módulo $n$, indicado por $a \equiv b (\mod n)$, quando $n|a-b$. Ou seja, $a - b = nk$, para algum $k \in \mathbb{Z}$. Se $a$ não é congruente a $b$ módulo $n$, indicaremos por $a \not\equiv b (\mod n)$.*

**Exemplo 8.** *Vamos verificar se $17 \equiv 11 (\mod 5)$. Por definição de congruência para que seja verdade esta relação, $5|17-11$. Como $5 \nmid 6$, então $17 \not\equiv 11 (\mod 5)$.*

**Exemplo 9.** $21 \equiv 13 (\mod 2)$, *já que* $2|21-13$.

**Propriedades: 1.** *Sejam $a, a', b, b' \in \mathbb{Z}$. Se $a \equiv a' (\mod n)$ e $b \equiv b' (\mod n)$:*

*i)* $a + b \equiv a' + b' (\mod n)$;

*ii)* $ab \equiv a'b' (\mod n)$.

*Demonstração.* i) Usando a definição de congruência, existe $r, s \in \mathbb{Z}$ tal que $a - a' = nr$ e $b - b' = ns$. Somando as equações membro a membro, temos

$$a - a' + b - b' = nr + ns$$
$$a + b - (a' + b') = n(r + s)$$

o que nos dá que $n|a + b - (a' + b')$, portanto $a + b \equiv a' + b' (\mod n)$.

ii) Usando as equações do item i), iremos multiplicar a primeira por $b$ e a segunda por $a'$ e por fim faremos a soma delas.

$$b(a-a')+a'(b-b')=b(nr)+a'(ns)$$
$$ba-ba'+a'b-a'b'=nbr+na's$$
$$ab-a'b'=n(br+a's)$$

portanto, $n|ab-a'b'$, e assim pela definição de congruência, $ab \equiv a'b'(\bmod n)$.

□

**Exemplo 10.** *Como* $21 \equiv 13(\bmod 2)$ *e* $7 \equiv 5(\bmod 2)$. *Somando as congruências, temos* $28 \equiv 18(\bmod 2)$. *O que de fato é verdade, pois* $2|28-18$. *Multiplicando as congruências, temos* $147 \equiv 65(\bmod 2)$. *De fato verdadeiro, pois* $2|147-65$.

A congruência é uma relação de equivalência.

**Propriedades: 2.** *Sejam* $a, b, c, n \in \mathbb{Z}$.

*i) (Reflexiva)* $a \equiv a(\bmod n)$;

*ii) (Simétrica) Se* $a \equiv b(\bmod n)$, *então* $b \equiv a(\bmod n)$;

*iii) (Transitiva) Se* $a \equiv b(\bmod n)$ *e* $b \equiv c(\bmod n)$, *então* $a \equiv c(\bmod n)$.

*Demonstração.* i) Temos que $a-a=0$ e 0 é divisível por $n$ ou seja, $n|0$, que implica $n|a-a$, pela definição de congruência $a \equiv a(\bmod n)$.

ii) Como $n|a-b$ por hipótese, então existe $k \in \mathbb{Z}$ tal que $a-b=nk$, somando $b-a-nk$ em ambos os membros, temos que $-nk=b-a$ que nos dá $n(-k)=b-a$, assim $n|b-a$, pela definição de congruência, $b \equiv a(\bmod n)$.

iii) Por hipótese, se $a \equiv b(\bmod n)$ e $b \equiv c(\bmod n)$, então $n|a-b$ e $n|b-c$, respectivamente. Existem $k_1, k_2 \in \mathbb{Z}$ tal que $a-b=nk_1$ e $b-c=nk_2$, somando membro a membro as equações, temos

$$a-b+b-c=nk_1+nk_2$$
$$a-c=n(k_1+k_2)$$

ou seja, $n|a-c$, pela definição de congruência, $a \equiv c(\bmod n)$.

□

**Definição 7.** *Sejam $a, b \in \mathbb{Z}$. Chamamos de classe residual de $a$ módulo $n$, o conjunto*

$$\overline{a} = \{b \in \mathbb{Z}; b \equiv a(\bmod n)\}.$$

*O conjunto de todas as classes residuais módulo $n$ é indicado por $\frac{\mathbb{Z}}{(n)}$. Escrevemos também $\frac{\mathbb{Z}}{(n)} = \mathbb{Z}_n$.*

**Exemplo 11.** *Enumere as possíveis classes residuais de $\frac{\mathbb{Z}}{(5)}$.*

*As classes residuais de $\frac{\mathbb{Z}}{(5)}$ são os possíveis restos na divisão por 5: $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ e $\overline{4}$. Para enumerar, basta somarmos e subtrairmos 5 em cada classe residual:*

$\overline{0} = \{..., -15, -10, -5, 0, 5, 10, 15, ...\}$;

$\overline{1} = \{..., -14, -9, -4, 1, 6, 11, 16, ...\}$;

$\overline{2} = \{..., -13, -8, -3, 2, 7, 12, 17, ...\}$;

$\overline{3} = \{..., -12, -7, -2, 3, 8, 13, 18, ...\}$;

$\overline{4} = \{..., -11, -6, -1, 4, 9, 14, 19, ...\}$.

**Teorema 12.** *Se $p$ é primo em $\mathbb{Z}$, então $ab \equiv 0(\bmod p)$ se, e somente se $a \equiv 0(\bmod p)$ ou $b \equiv 0(\bmod p)$.*

*Demonstração.* Como $p$ é primo e $ab \equiv 0(\bmod p)$, então $p|ab$, ou seja $p|a$ ou $p|b$, em outras palavras, $a \equiv 0(\bmod p)$ ou $b \equiv 0(\bmod p)$. Reciprocamente, se $a \equiv 0(\bmod p)$, temos que $a = pk$ para algum $k \in \mathbb{Z}$, multiplicando essa equação por $b$, temos $ab = p(kb)$ portanto, $p|ab$ e $ab \equiv 0(\bmod p)$. Analogamente quando $b \equiv 0(\bmod p)$. □

**Definição 8.** *Sejam $a, b \in \mathbb{Z}$. Diremos que $a$ possui inverso módulo $b$, se existir $a' \in \mathbb{Z}$ tal que $aa' \equiv 1(\bmod b)$.*

**Teorema 13.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então $ax \equiv 1(\bmod b)$ tem solução se, e somente se $mdc(a, b) = 1$ em $\mathbb{Z}$.*

*Demonstração.* Pela definição de congruência, $b|ax-1$ portanto, $ax-1 = bk$ o que implica em $ax + b(-k) = 1$. Como o número 1 pode ser escrito como uma combinação linear de

$a$ e $b$ assim, $a$ e $b$ são relativamente primos. Uma vez que $a$ possui inverso $(\bmod b)$, multiplicamos a congruência pelo inverso de $a(\bmod b)$

$$a'ax \equiv a'k(\bmod b)$$
$$x \equiv a'k(\bmod b),$$

$x \equiv a'k(\bmod b)$ é a solução única. □

**Exemplo 12.** $42x \equiv 1(\bmod 4)$ *tem solução?*

*Para verificarmos, basta calcularmos o* $mdc(42, 4)$.

$$42 = 4 \cdot 10 + 2$$
$$4 = 2 \cdot 2 + 0$$

*Como o último resto não nulo é* 2, *então* $mdc(42, 4) = 2$, *ou seja, pelo Teorema 13,* $42x \equiv 1(\bmod 4)$ *não possui solução.*

**Corolário 14.** *Seja* $p$ *um inteiro primo. Cada* $a \not\equiv 0(\bmod p)$ *tem um inverso multiplicativo módulo* $p$ *e qualquer congruência polinomial*

$$C_n x^n + C_{n-1}x^{n-1} + ... + C_1 x + C_0 \equiv 0(\bmod p)$$

*onde* $C_i \in \mathbb{Z}$ *e* $C_n \not\equiv 0(\bmod p)$, *tem no máximo* $n$ *soluções módulo* $p$.

*Demonstração.* Como $p$ é um inteiro primo, qualquer $a \in \mathbb{Z}$, onde $a \not\equiv 0(\bmod p)$, então podemos dizer que $p$ é relativamente primo como $a$, portanto para cada $a$, existe um inteiro gaussiano que é inverso de $a(\bmod p)$, pelo Teorema 13. Assim, como todo elemento de $\mathbb{Z}_p$, com exceção do 0, possui inverso em $\mathbb{Z}$, então $\mathbb{Z}_p$ é um corpo. Portanto, este corolário é um caso especial, quando polinômios de grau $n$, tem no máximo $n$ raízes. □

### 1.6.1 Pequeno Teorema de Fermat

**Teorema 15.** *(Pequeno Teorema de Fermat) Seja* $p$ *primo. Se* $mdc(a, p) = 1$, *então*

$$a^{p-1} \equiv 1(\bmod p).$$

*Demonstração.* Consideremos os $p - 1$ inteiros múltiplos de $a$:

$$1.a, 2.a, 3.a, ..., (p-1).a$$

i) Nenhum desses inteiros são divisíveis por $p$, ou seja, nenhum é congruente a $0(\mod p)$. De fato, pelo Teorema 8 se $p|j.a$ então $p|j$, pois $mdc(a,p) = 1$, o que é impossível visto que $1 \leq j \leq p-1$.

ii) Quaisquer dois desses inteiros são incongruentes módulo $p$. De fato, se fossem congruentes, teríamos

$$j.a \equiv k.a(\mod p) \text{ com } j \neq k.$$

Digamos $1 \leq j < k \leq p-1$. Como $mdc(a,p) = 1$, teríamos $j \equiv k(\mod p)$, o que é impossível, pois $j$ e $k$ são inteiros positivos menores do que $p$.

Por i) e ii) cada um dos inteiros

$$1.a, 2.a, 3.a, ..., (p-1).a$$

são congruentes módulo $p$ a somente um dos inteiros

$$1, 2, 3, ..., (p-1)$$

em uma certa ordem. O produto desses inteiros módulo $p$

$$(1.a)(2.a)(3.a)...((p-1).a) \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)(\mod p)$$
$$a^{p-1}(p-1)! \equiv (p-1)!(\mod p)$$

Como $mdc((p-1)!, p) = 1$, pois $p$ é primo. Logo, $p \nmid (p-1)!$, temos que

$$a^{p-1} \equiv 1(\mod p).$$

□

**Exemplo 13.** *Para $p = 5$ e $a = 2$, temos*

$$(1 \cdot 2) \cdot (2 \cdot 2) \cdot (3 \cdot 2) \cdot (4 \cdot 2) \equiv 2 \cdot 4 \cdot 1 \cdot 3(\mod 5)$$
$$2^4 \cdot (4!) \equiv 4!(\mod 5)$$
$$2^4 \equiv 1(\mod 5).$$

**Exemplo 14.** *Mostre que* $5^{38} \equiv 4(\bmod 11)$. *Pelo PTF* $5^{10} \equiv 1(\bmod 11)$.

$$5^{38} = 5^{10\cdot 3+8} = (5^{10})^3 \cdot (5^2)^4 \equiv 1^3 \cdot 3^4(\ \bmod 11)$$
$$5^{38} \equiv 81 \equiv 4(\ \bmod 11).$$

### 1.6.2 A Função $\phi$-Euler e o Teorema de Euler

**Definição 9.** *A função $\phi$-Euler indicada por $\phi(n)$ é o número de inteiros $k$ que são maiores ou igual a 1 e menor que $n$ e são relativamente primos com $n$.*

**Observação 2.** *Escrevemos* $\phi(n) = |\{k \in \mathbb{Z}/1 \leq k < n, (k, n) = 1\}|$.

**Definição 10.** *Dados dois inteiros $a$ e $n$ com $mdc(a, n) = 1$, chama-se inverso de $a$ módulo $n$ qualquer um dos inteiros $x$ tais que $ax \equiv 1(\bmod n)$.*

**Teorema 16.** *Sejam $a, n \in \mathbb{Z}$ com $a < n$. Então $a$ e $n$ são relativamente primos se, e somente se $a$ é invertível módulo $n$.*

*Demonstração.* Como $a$ e $n$ são relativamente primos, existem $x, y \in \mathbb{Z}$ tais que $ax+ny = 1$. Isso implica que $ny = 1-ax$. Reescrevendo a equação, temos $n(-y) = ax-1$, ou seja, $n|ax-1$. Pela definição de congruência, $ax \equiv 1(\bmod n)$. Então $a$ é invertível módulo $n$. Reciprocamente, se $a$ é invertível módulo $n$ então $aj \equiv 1(\bmod n)$ para algum $j \in \mathbb{Z}$. Isso implica que $n|aj-1$. Então existe $k \in \mathbb{Z}$ tal que $aj-1 = nk$. Assim, podemos escrever $aj + n(-k) = 1$. Portanto, $a$ e $n$ são relativamente primos. □

Pelo Teorema 16 temos a seguinte definição

**Definição 11.** *Para $n \in \mathbb{Z}$, diferente de zero. Então $\phi(n) = |U(\mathbb{Z}_n)|$, ou seja, o número de classes residuais invertíveis módulo $n$.*

**Observação 3.** *Quando $n = p$ é primo, todo inteiro diferente de zero módulo $p$ é invertível, então*

$$\phi(p) = |U(\mathbb{Z}_p)| = p - 1.$$

**Exemplo 15.** $\phi(5) = 5-1 = 4$. *Ou seja, o número 5 possui 4 classes residuais invertíveis módulo 5.*

**Exemplo 16.** $\phi(17) = 17 - 1 = 16$. *Ou seja, o número 17 possui 16 classes residuais invertíveis módulo 17.*

Agora vamos calcular $\phi(n)$ para $n = a \cdot b$ com $mdc(a, b) = 1$.

**Teorema 17.** *Para $a, b \in \mathbb{Z}$ e $mdc(a, b) = 1$, então $\phi(ab) = \phi(a)\phi(b)$, ou seja, $\phi$ é multiplicativa.*

*Demonstração.* Sejam $a, b \in \mathbb{Z}$ com $mdc(a, b) = 1$. Pelo Teorema 16 e Teorema 9 podemos escrever,

$$\begin{aligned}\phi(ab) &= |\{x \in U(\mathbb{Z}_{ab})\}| \\ &= |\{(y, z) \in U(\mathbb{Z}_a) \times U(\mathbb{Z}_b)\}| \\ &= |U(\mathbb{Z}_a)|\,|U(\mathbb{Z}_b)| \\ &= \phi(a)\phi(b).\end{aligned}$$

□

**Teorema 18.** *Se $p$ é primo, então $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.*

*Demonstração.* Considere $\mathbb{Z}_{p^k}$ o conjunto de todas as classes residuais módulo $p^k$. Para calcularmos $\phi(p^k)$ devemos subtrair de $\mathbb{Z}_{p^k}$ todos os elementos que não são invertíveis módulo $p^k$. Ou seja, devemos subtrair todos os elementos que dividem $p^k$: $p, 2p, 3p, ..., (p^{k-1})p$. Então, $\left|U\left(\mathbb{Z}_{p^k}\right)\right| = p^k - p^{k-1}$, portanto, pela Definição 11, $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$. □

**Teorema 19.** *Para $n \in \mathbb{Z}$, então $\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$.*

*Demonstração.* Se $n$ for primo, já temos o resultado da Observação 3. Se não, $n$ pode ser escrito como um produto de fatores primos, ou seja, $n = p_1^{r_1}p_2^{r_2}...p_s^{r_s}$. Então,

$$\phi(n) = \phi(p_1^{r_1}p_2^{r_2}...p_s^{r_s}).$$

Como $\phi$ é multiplicativa, pelo teorema 17, temos

$$\phi(n) = \phi(p_1^{r_1})\phi(p_2^{r_2})...\phi(p_s^{r_s}).$$

Agora, pelo Teorema 18

$$\begin{aligned}\phi(n) &= p_1^{r_1}\left(1 - \frac{1}{p_1}\right)p_2^{r_2}\left(1 - \frac{1}{p_2}\right)...p_s^{r_s}\left(1 - \frac{1}{p_s}\right) \\ \phi(n) &= p_1^{r_1}p_2^{r_2}...p_s^{r_s}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_s}\right).\end{aligned}$$

Como os $s$ primeiros termos multiplicados é $n$, então

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

□

**Exemplo 17.** *Calcule* $\phi(36)$*. Como* 36 *é composto sua fatoração é* $2^2 \cdot 3^2$*. Logo,*

$$\begin{aligned}
\phi(36) &= \phi(2^2 \cdot 3^2) \\
\phi(36) &= \phi(2^2)\phi(3^2) \\
\phi(36) &= 2^2\left(1 - \frac{1}{2}\right) \cdot 3^2\left(1 - \frac{1}{3}\right) \\
\phi(36) &= 4 \cdot \frac{1}{2} \cdot 9 \cdot \frac{2}{3} \\
\phi(36) &= 2 \cdot 6 \\
\phi(36) &= 12.
\end{aligned}$$

**Teorema 20.** *(Teorema de Euler) Sejam* $a$ *e* $n$ *inteiros e* $mdc(a, n) = 1$*, então*

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

*Demonstração.* Seja $U(\mathbb{Z}_n) = \{n_1, n_2, ..., n_{\phi(n)}\}$ o conjunto das classes residuais invertíveis módulo $n$, então $U(\mathbb{Z}_n)$ possui $\phi(n)$ elementos. Consideremos agora a sequência $an_1, an_2, ..., an_{\phi(n)}$. Suponha que $an_i \equiv an_j(\bmod n)$ para algum $i$ e $j$ inteiros. Como $mdc(a, n) = 1$, então $a$ é invertível módulo $n$ (Teorema 13). Multiplicando a congruência pelo inverso de $a$ módulo $n$, temos que $n_i \equiv n_j(\bmod n)$, o que é um absurdo, pois são classes residuais distintas módulo $n$, portanto, $an_1, an_2, ..., an_{\phi(n)}$ é um conjunto de classes residuais módulo $n$. Como $mdc(n_i, n) = 1$ e $mdc(a, n) = 1$, então $mdc(an_i, n) = 1$ (Teorema 9). Portanto, $an_1, an_2, ..., an_{\phi(n)}$ é também um conjunto das classes residuais invertíveis módulo $n$. Cada $an_i$ deve ser congruente a um único elemento de $U(\mathbb{Z}_n)$ módulo $n$, temos então a multiplicação desses elementos

$$\begin{aligned}
an_1an_2...an_{\phi(n)} &\equiv n_1n_2...n_{\Phi(n)}(\ \bmod n) \\
a^{\phi(n)}n_1n_2...n_{\phi(n)} &\equiv n_1n_2...n_{\phi(n)}(\ \bmod n)
\end{aligned}$$

Como $n_i$ e $n$ são relativamente primos, podemos fazer o cancelamento em ambos os lados

da congruência. Portanto,

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

□

**Exemplo 18.** *Calcule o resto da divisão de* $35^{2019}$ *por* 24.

*Como o* $mdc(35, 24) = 1$ *podemos utilizar o Teorema de Euler. Vamos calcular* $\phi(24)$.

$$\begin{aligned}\phi(24) &= \phi(2^3 \cdot 3)\\ &= \phi(2^3)\phi(3)\\ &= 2^3\left(1 - \frac{1}{2}\right)(3-1)\\ &= 4 \cdot 2\\ &= 8.\end{aligned}$$

*Então,*

$$\begin{aligned}35^{\phi(24)} &\equiv 1(\text{ mod } 24)\\ 35^8 &\equiv 1(\text{ mod } 24).\end{aligned}$$

*Como* $2019 = 8 \cdot 252 + 3$, *temos*

$$35^{2016} \equiv 1(\text{ mod } 24).$$

*Como* $35^3 \equiv 11(\text{ mod } 24)$, *ao multiplicarmos as congruências, temos*

$$\begin{aligned}35^{2016} \cdot 35^3 &\equiv 1 \cdot 11(\text{ mod } 24)\\ 35^{2019} &\equiv 11(\text{ mod } 24).\end{aligned}$$

*Portanto o resto da divisão de* $35^{2019}$ *por* 24 *é* 11.

# Capítulo 2

# Os Inteiros Gaussianos

Neste capítulo, estenderemos para os inteiros gaussianos as clássicas propriedades de $\mathbb{Z}$, que serão suporte para as demonstrações do Pequeno Teorema de Fermat e Teorema de Euler em $\mathbb{Z}[i]$.

## 2.1 Propriedades dos Inteiros Gaussianos

**Definição 12.** *Seja* $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}, i^2 = -1\}$ *e* $\alpha \in \mathbb{Z}[i]$ *é chamado de inteiro gaussiano.*

Os Inteiros Gaussianos são a extensão natural dos inteiros para o plano complexo. Como $\mathbb{Z}$ e $\mathbb{Z}[i]$ possuem estruturas parecidas, muitas propriedades que trabalhamos em $\mathbb{Z}$ podem ser estendidas para $\mathbb{Z}[i]$. Vejamos algumas delas.

Como $\mathbb{Z}[i]$ é um subconjunto de $\mathbb{C}$, então eles compartilham das mesmas propriedades de adição e de multiplicação. Ou seja, dados $\alpha$, $\beta$, $\omega \in \mathbb{Z}[i]$, temos:

Na adição:

i) Associatividade: $\alpha + (\beta + \omega) = (\alpha + \beta) + \omega$

ii) Existência de um elemento Neutro: $\alpha + 0 = 0 + \alpha = \alpha$

iii) Existência de um elemento simétrico: $\exists\ -\alpha \in \mathbb{Z}[i]$ tal que $\alpha + (-\alpha) = 0$

iv) Comutatividade: $\alpha + \beta = \beta + \alpha$

Na Multiplicação:

i) Associatividade: $\alpha \cdot (\beta \cdot \omega) = (\alpha \cdot \beta) \cdot \omega$

ii) Distributividade: $\alpha \cdot (\beta + \omega) = \alpha \cdot \beta + \alpha \cdot \omega$

iii) Existência de um elemento neutro: $\exists 1 \in \mathbb{Z}[i]$ tal que $1 \cdot \alpha = \alpha \cdot 1 = \alpha$

iv) Comutatividade: $\alpha \cdot \beta = \beta \cdot \alpha$.

Com relação ao inverso multiplicativo, trataremos na Seção 2.3.

**Definição 13.** *Seja $\alpha = a+bi$ um inteiro gaussiano, então o conjugado de $\alpha$ é $\overline{\alpha} = a-bi$.*

**Propriedades: 3.** *Sejam $\alpha = a + bi$ e $\beta = c + di$ inteiros gaussianos, então:*

*i)* $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;

*ii)* $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$.

*Demonstração.* i)

$$\begin{aligned}
\overline{\alpha + \beta} &= (a + c) - (b + d)i \\
&= a + c - bi - di \\
&= a - bi + c - di \\
&= (a - bi) + (c - di) \\
&= \overline{\alpha} + \overline{\beta}.
\end{aligned}$$

ii)

$$\begin{aligned}
\overline{\alpha \cdot \beta} &= \overline{\alpha} \cdot \overline{\beta} \\
\overline{(a + bi)(c + di)} &= \overline{(a + bi)} \cdot \overline{(c + di)} \\
\overline{(ac - bd) + (ad + bc)i} &= (a - bi)(c - di) \\
(ac - bd) - (ad + bc)i &= (a - bi)(c - di) \\
ac - bd - adi - bci &= ac - adi - bci - bd
\end{aligned}$$

□

## 2.2 Função Norma

A função Norma é muito importante para o estudo dos Inteiros Gaussianos. Em $\mathbb{Z}$, o tamanho do número é medido pelo valor absoluto, já em $\mathbb{Z}[i]$, pela Norma.

**Definição 14.** *A função* $N : \mathbb{Z}[i] \to \mathbb{Z}_+$ *chamada norma, tal que para todo* $\alpha = a + bi \in \mathbb{Z}[i]$, $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$.

**Exemplo 19.** $N(2 + 7i) = 2^2 + 7^2 = 4 + 49 = 53$

**Exemplo 20.** $N(2i) = 0^2 + 2^2 = 0 + 4 = 4$

**Exemplo 21.** *Para* $m \in \mathbb{Z}$, *então* $N(m) = m^2$.

Podemos verificar que a função norma é multiplicativa, e essa propriedade será de grande importância para os resultados deste trabalho.

**Teorema 21.** *Sejam* $\alpha = a + bi$, $\beta = c + di \in \mathbb{Z}[i]$. *Então* $N(\alpha\beta) = N(\alpha)N(\beta)$

*Demonstração.* Para $\alpha = a + bi$, $\beta = c + di \in \mathbb{Z}[i]$. Então

$$\begin{aligned} N(\alpha\beta) &= N((a + bi)(c + di)) \\ &= N((ac - bd) + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2) \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(a + bi)N(c + di) \\ &= N(\alpha)N(\beta) \end{aligned}$$

□

**Exemplo 22.** *Verifique se* $N(\alpha\beta) = N(\alpha)N(\beta)$, *para* $\alpha = 1 + i$ *e* $\beta = 2 + 4i$.

*Calculando as normas de* $\alpha$ *e* $\beta$, *temos*

$N(\alpha) = N(1 + i) = 1^2 + 1^2 = 1 + 1 = 2$,

$N(\beta) = N(2 + 4i) = 2^2 + 4^2 = 4 + 16 = 20$, *então*

$N(\alpha)N(\beta) = 2 \cdot 20 = 40$.

*Por outro lado,*

$\alpha\beta = (1 + i)(2 + 4i) = -2 + 6i$, *calculando norma de* $\alpha\beta$, *temos*

$N(\alpha\beta) = N(-2 + 6i) = (-2)^2 + 6^2 = 4 + 36 = 40$.

*Portanto,* $N(\alpha\beta) = N(\alpha)N(\beta)$.

Observe que, a norma de cada inteiro gaussiano é um inteiro positivo, mas não é verdade que cada inteiro positivo é uma norma, pois as normas são inteiros positivos da forma $a^2 + b^2$, e nem todo inteiro conseguiremos escrever dessa maneira, que é o caso do 3, 7, 11, entre outros.

## 2.3 Unidades e Associados

**Definição 15.** *Dizemos que $\alpha$ é invertível em $\mathbb{Z}[i]$, se existir $\beta \in \mathbb{Z}[i]$ tal que $\alpha \cdot \beta = 1$.*

Daqui em diante, quando dizemos $\alpha$ invertível, significa $\alpha$ invertível em $\mathbb{Z}[i]$. Pelo Teorema 21, podemos verificar a existência de inteiros gaussianos que possuem inverso multiplicativo, ou seja $\alpha \cdot \beta = 1$.

**Teorema 22.** *Os únicos inteiros gaussianos que são invertíveis em $\mathbb{Z}[i]$ são $\pm 1$ e $\pm i$.*

*Demonstração.* Tome $\alpha$ e $\beta \in \mathbb{Z}[i]$ tal que $\alpha\beta = 1$. Aplicando a função Norma em ambos os membros da equação temos que $N(\alpha\beta) = N(1)$, pelo Teorema 21, $N(\alpha)N(\beta) = 1$. Como $N(\alpha)$ e $N(\beta)$ são inteiros positivos diferente de 0, então $N(\alpha) = N(\beta) = 1$. Tomando $\alpha = a + bi$, então $N(\alpha) = a^2 + b^2 = 1$, assim $a^2 = 1$ ou $b^2 = 1$. Caso $a^2 = 1$, então $a = 1$ ou $a = -1$. Caso $b^2 = 1$, então $b = 1$ ou $b = -1$. O mesmo acontece para $\beta$. Portanto, os únicos números possíveis para $\alpha$ e $\beta$ são $-1, 1, i$ e $-i$. □

**Definição 16.** *Chamamos os elementos invertíveis de $\mathbb{Z}[i]$ de unidades.*

**Teorema 23.** *$\alpha = a + bi$ é uma unidade em $\mathbb{Z}[i]$ se, e somente se $N(\alpha) = 1$.*

*Demonstração.* Primeiro, suponha para algum $\alpha = a + bi \in \mathbb{Z}[i]$ que $N(\alpha) = 1$. Então $a^2 + b^2 = 1$, o que implica que $a^2 = 1 - b^2$. Para que $a^2 \geq 0$, consideremos dois casos:
Caso 1: Para $b^2 = 0$. Então $b = 0$ e $a^2 = 1 - 0 = 1$. Logo $a = 1$ ou $a = -1$. Se $a = 1$, então $\alpha = 1 + 0i$. Como $N(1 + 0i) = 1$, $\alpha = 1 + 0i$ é uma unidade em $\mathbb{Z}[i]$. Se $a = -1$, então $\alpha = -1 + 0i$. Como $N(-1 + 0i) = 1$, $\alpha = -1 + 0i$ é uma unidade em $\mathbb{Z}_[i]$.
Caso 2: Para $b^2 = 1$. Então $a^2 = 1 - 1 = 0$. Logo $a = 0$ e $b = 1$ ou $b = -1$. Se $b = 1$, então $\alpha = 0 + i$. Como $N(0 + i) = 1$, $\alpha = 0 + i$ é uma unidade em $\mathbb{Z}[i]$. Se $b = -1$, então $\alpha = 0 - i$. Como $N(0 - i) = 1$, $\alpha = 0 - i$ é uma unidade em $\mathbb{Z}[i]$.
Em seguida, suponha que exista algum $\alpha = a + bi \in \mathbb{Z}[i]$ em que $\alpha$ é uma unidade. Então existe $\beta = c + di \in \mathbb{Z}[i]$, onde $c$ e $d$ são diferentes de 0, tal que $\alpha\beta = 1$. Aplicando a

função norma na equação temos que $N(\alpha\beta) = N(1)$ e pelo Teorema 21 podemos dizer que $N(\alpha)N(\beta) = N(1)$. Logo $(a^2 + b^2)(c^2 + d^2) = 1$. Como $a^2 + b^2, c^2 + d^2 \in \mathbb{Z}_+$ e $(a^2+b^2)(c^2+d^2) = 1$ sabemos que $a^2+b^2$ e $c^2+d^2$ são unidades em $\mathbb{Z}$. Pois $a^2+b^2$ e $c^2+d^2$ são diferentes de 0, então devem ser iguais a 1. Então $1 = a^2+b^2 = N(a+bi) = N(\alpha)$. □

**Definição 17.** *Sejam $\alpha, \beta \in \mathbb{Z}[i]$ serão associados se $\alpha = u \cdot \beta$ e $N(\alpha) = N(\beta)$, onde $u \in \{-1, 1, i, -i\}$.*

**Exemplo 23.** *$5 + 7i$ é associado a $7 - 5i$, pois $5 + 7i = i \cdot (7 - 5i)$.*

**Exemplo 24.** *$2i$ é associado a $2$, pois $2i = -i \cdot 2$.*

## 2.4 Divisibilidade

Assim como em $\mathbb{Z}$, podemos falar de divisibilidade em $\mathbb{Z}[i]$.

**Definição 18.** *Dados dois números inteiros gaussianos $\alpha$ e $\beta$ com $\alpha \neq 0$, diremos que $\alpha$ divide $\beta$, escrevendo $\alpha|\beta$, quando existir $\omega \in \mathbb{Z}[i]$ tal que $\beta = \alpha \cdot \omega$.*

**Exemplo 25.** *Como $14 - 3i = (4 + 5i)(1 - 2i)$, $4 + 5i$ divide $14 - 3i$.*

**Exemplo 26.** *$4 + 5i \nmid 14 + 3i$ pois, ao fazermos esta divisão e racionalizando o denominador:*

$$\frac{14 + 3i}{4 + 5i} = \frac{(14 + 3i)(4 - 5i)}{(4 + 5i)(4 - 5i)} = \frac{71 - 58i}{41} = \frac{71}{41} - \frac{58}{41}i.$$

*Esse número não está em $\mathbb{Z}[i]$, pois as partes real e a imaginária não são números inteiros. Portanto, $4 + 5i \nmid 14 + 3i$ em $\mathbb{Z}[i]$.*

**Teorema 24.** *Um inteiro gaussiano $\alpha = a + bi$ é divisível por um inteiro $c$ se, e somente se $c|a$ e $c|b$ em $\mathbb{Z}$.*

*Demonstração.* Como $c|(a+bi)$, então existe $\beta = m+ni \in \mathbb{Z}[i]$ tal que $a+bi = c(m+ni)$. Fazendo a distributiva e comparando as partes reais e imaginárias do inteiro gaussiano, temos que $a = cm$ e $b = cn$, ou seja $c|a$ e $c|b$. □

**Proposição 25.** *Se $\alpha, \beta, \gamma$ são inteiros gaussianos, $\gamma|\alpha$ e $\gamma|\beta$, então existem $\delta, \eta \in \mathbb{Z}[i]$ tal que $\gamma|\alpha\delta + \beta\eta$.*

*Demonstração.* Como $\gamma|\alpha$ e $\gamma|\beta$, então $\alpha = \gamma\zeta_1$ e $\beta = \gamma\zeta_2$. Multiplicando as equações por $\delta$ e $\eta$, respectivamente, obtemos $\alpha\delta = \gamma\zeta_1\delta$ e $\beta\eta = \gamma\zeta_2\eta$. Somando as equações temos que $\alpha\delta + \beta\eta = \gamma(\zeta_1\delta + \zeta_2\eta)$. Portanto, $\gamma|\alpha\delta + \beta\eta$. □

**Teorema 26.** *Para $\alpha, \beta \in \mathbb{Z}[i]$, se $\alpha|\beta$ em $\mathbb{Z}[i]$, então $N(\alpha)|N(\beta)$ em $\mathbb{Z}$.*

*Demonstração.* Como $\alpha|\beta$, então existe $\gamma \in \mathbb{Z}[i]$, tal que $\beta = \alpha\gamma$. Aplicando norma nesta equação, $N(\beta) = N(\alpha\gamma)$, como a norma é uma função multiplicativa, $N(\beta) = N(\alpha)N(\gamma)$. Portanto $N(\alpha)|N(\beta)$ já que a norma é uma função em $\mathbb{Z}$. □

**Exemplo 27.** *Encontre todos os divisores de $1 + 3i$ em $\mathbb{Z}[i]$.*

*Temos que encontrar os inteiros gaussianos $\alpha = a + bi$, tal que $\alpha|1 + 3i$. Se $1 + 3i = \alpha\gamma$, $\gamma \in \mathbb{Z}[i]$. Aplicando a função Norma, temos*

$$N(1 + 3i) = N(\alpha\gamma)$$
$$10 = N(\alpha)N(\gamma).$$

*Pelo Teorema 26, se $\alpha|1+3i$ então $N(\alpha)|10 \Rightarrow N(\alpha) \in \{1, 2, 5, 10\}$. Fazendo $\alpha = a+bi$, temos:*
$N(\alpha) = a^2 + b^2 = 1$, *então* $\alpha \in \{\pm 1, \pm i\}$,
$N(\alpha) = a^2 + b^2 = 2$, *então* $\alpha \in \{\pm(1 + i), \pm(1 - i)\}$,
$N(\alpha) = a^2 + b^2 = 5$, *então* $\alpha \in \{\pm(1 + 2i), \pm(1 - 2i), \pm(2 + i), \pm(2 - i)\}$ *e*
$N(\alpha) = a^2 + b^2 = 10$, *então* $\alpha \in \{\pm(1 + 3i), \pm(1 - 3i), \pm(3 + i), \pm(3 - i)\}$.

*Portanto, encontramos 24 possíveis divisores de $1+3i$. Ao fazermos a verificação, os divisores de $1 + 3i$ são $\{\pm 1, \pm i, \pm(1 + i), \pm(1 - i), \pm(1 - 2i), \pm(2 + i), \pm(2 - i), \pm(1 + 3i), \pm(3 - i)\}$.*

**Corolário 27.** *Um inteiro gaussiano tem norma par se, e somente se é um múltiplo de $1 + i$.*

*Demonstração.* Como $N(1+i) = 2$, qualquer múltiplo de $1+i$ tem Norma par. Por outro lado, seja $\alpha = a + bi \in \mathbb{Z}[i]$ com Norma par, ou seja $a^2 + b^2 = 2t$, $t \in \mathbb{Z}$. Para $a^2 + b^2$ ser par, $a$ e $b$ tem que ser ambos pares ou ambos ímpares. Tomando $a + bi = (1 + i)(m + ni)$ para alguns $m, n \in \mathbb{Z}$, temos que $a + bi = (m - n) + (m + n)i$, que tem solução $m = \dfrac{a + b}{2}$ e $y = \dfrac{b - a}{2}$. Como $a$ e $b$ tem a mesma paridade, $m$ e $n$ são números inteiros. Portanto $\alpha$ é um múltiplo de $1 + i$. □

**Exemplo 28.** *A Norma de* $1+3i$ *é* $10$ *e* $1+3i=(1+i)(2+i)$.

**Exemplo 29.** *A Norma de* $1-i$ *é* $2$ *e* $1-i=(1+i)(-i)$.

## 2.5 Teorema da Divisão em $\mathbb{Z}[i]$

**Teorema 28.** *Para* $\alpha,\beta\in\mathbb{Z}[i]$*, com* $\beta\neq 0$*, existem* $\gamma,\delta\in\mathbb{Z}[i]$ *de tal forma que* $\alpha=\beta\gamma+\delta$ *e* $\delta=0$ *ou* $N(\delta)<N(\beta)$.

*Demonstração.* Ao fazermos a divisão de $\alpha$ por $\beta$, obtemos $\dfrac{\alpha}{\beta}=x+yi$, onde $x$ e $y$ podem ser inteiros ou racionais. Se $x$ e $y$ forem inteiros, $\gamma=x+yi$ e $\delta=0$. Mas se $x$ e $y$ forem racionais, devemos procurar $m$ e $n$, os inteiros mais próximos de $x$ e $y$, respectivamente, então $|x-m|\leq\dfrac{1}{2}$ e $|y-n|\leq\dfrac{1}{2}$. Tomando $\gamma=m+ni$ e $\delta=\alpha-\beta\gamma$, temos que

$$\begin{aligned}N\left(\frac{\alpha}{\beta}-\gamma\right)&=N((x+yi)-(m+ni))\\&=N((x-m)+(y-n)i)\\&=(x-m)^2+(y-n)^2.\end{aligned}$$

Como $|x-m|\leq\dfrac{1}{2}$ e $|y-n|\leq\dfrac{1}{2}$, então $(x-m)^2\leq\dfrac{1}{4}$ e $(y-n)^2\leq\dfrac{1}{4}$, assim

$$N\left(\frac{\alpha}{\beta}-\gamma\right)=(x-m)^2+(y-n)^2\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}.$$

Como $N\left(\dfrac{\alpha}{\beta}-\gamma\right)\leq\dfrac{1}{2}$ e $\dfrac{1}{2}<1$, então $N\left(\dfrac{\alpha}{\beta}-\gamma\right)<1$. Multiplicando por $N(\beta)$ esta desigualdade, obtemos

$$\begin{aligned}N\left(\frac{\alpha}{\beta}-\gamma\right)N(\beta)&<N(\beta)\\N\left(\left(\frac{\alpha}{\beta}-\gamma\right)\beta\right)&<N(\beta)\\N(\alpha-\beta\gamma)&<N(\beta)\\N(\delta)&<N(\beta).\end{aligned}$$

□

**Exemplo 30.** *Considere* $\alpha = 27-23i$ *e* $\beta = 8+i$*. Vamos fazer a divisão para escrevermos da forma* $\alpha = \beta\gamma + \delta$*, como* $N(\beta) = 65$*, então* $N(\delta) < 65$*.*

$$\frac{27-23i}{8+i} = \frac{27-23i}{8+i}\frac{(8-i)}{(8-i)} = \frac{193-211i}{65} = \frac{193}{65} - \frac{211}{65}i.$$

*Como* $\frac{193}{65} = 2,969...$ *e* $-\frac{211}{65} = -3,246...$*, temos que encontrar o número inteiro mais próximos deles. Logo,* $\gamma = 3-3i$ *e assim temos:*

$$27-23i = (8+i)(3-3i) + (-2i),$$

*já que* $\delta = -2i$ *e* $N(-2i) = 4$*,* $N(\delta) < 65$*.*

**Exemplo 31.** *Considere* $\alpha = 1+8i$ *e* $2-4i$*. Vamos fazer a divisão para escrevermos da forma* $\alpha = \beta\gamma + \delta$*, como* $N(\beta) = 20$*, então* $N(\delta) < 20$*.*

$$\frac{1+8i}{2-4i} = \frac{1+8i}{2-4i}\frac{(2+4i)}{(2+4i)} = \frac{-30+20i}{20} = -\frac{3}{2} + i.$$

*Como* $-\frac{3}{2} = -1,5$*, e como* $-1,5$ *está exatamente entre* $-2$ *e* $-1$*, temos duas opções para* $\gamma$*,* $\gamma = -1+i$ *ou* $\gamma = -2+i$*, assim temos:*

$$1+8i = (2-4i)(-1+i) + (-1+2i),\ N(-1+2i) = 5 < 20$$

*ou*

$$1+8i = (2-4i)(-2+i) + (1-2i),\ N(1-2i) = 5 < 20.$$

*Logo o quociente e o resto não são necessariamente únicos.*

## 2.6 O Algoritmo de Euclides

**Definição 19.** *Sejam* $\alpha, \beta, \gamma$ *inteiros gaussianos não nulos. Diremos que* $\gamma$ *será o máximo divisor comum de* $\alpha$ *e* $\beta$*, quando:*

*i)* $\gamma|\alpha$ *e* $\gamma|\beta$*;*

*ii) Se existe* $\delta \in \mathbb{Z}[i]$ *tal que* $\delta|\alpha$ *e* $\delta|\beta$*, então* $N(\delta) \leq N(\gamma)$*.*

*Em outras palavras, o mdc entre dois ou mais inteiros gaussianos será o divisor comum com a maior norma.*

*Indicamos o máximo divisor comum de* $\alpha$ *e* $\beta$ *por* $\gamma = mdc(\alpha, \beta)$*.*

**Teorema 29.** *Se $\alpha, \beta \in \mathbb{Z}[i]$ e $\alpha = \beta\gamma + \delta$, onde $\gamma, \delta$ são inteiros gaussianos, então $mdc(\alpha, \beta) = mdc(\beta, \delta)$.*

*Demonstração.* Da relação $\alpha = \beta\gamma + \delta$ podemos concluir que todo divisor de $\beta$ e $\delta$ é um divisor de $\alpha$ (Proposição 25). Esta mesma relação, escrita na forma $\delta = \alpha - \beta\gamma$, nos diz que todo divisor de $\alpha$ e $\beta$ é um divisor de $\delta$. Logo o conjunto de divisores comuns de $\alpha$ e $\beta$ é igual ao conjunto de divisores de $\beta$ e $\delta$, o que nos garante que $mdc(\alpha, \beta) = mdc(\beta, \delta)$. □

**Teorema 30.** *(Algoritmo de Euclides) Tome $\alpha, \beta \in \mathbb{Z}[i]$, diferentes de zero. Aplicando repetidamente o Teorema da Divisão onde o resto é diferente de zero, teremos*

$$\alpha = \beta\gamma_1 + \delta_1, \text{ com } N(\delta_1) < N(\beta)$$
$$\beta = \delta_1\gamma_2 + \delta_2, \text{ com } N(\delta_2) < N(\delta_1)$$
$$\delta_1 = \delta_2\gamma_3 + \delta_3, \text{ com } N(\delta_3) < N(\delta_2)$$
$$.$$
$$.$$
$$.$$

*O último resto diferente de zero é divisível por todos os divisores comuns de $\alpha$ e $\beta$ e será divisor comum, por isso é um máximo divisor comum de $\alpha$ e $\beta$.*

*Demonstração.* Pela Divisão euclideana, temos

$$\alpha = \beta\gamma_1 + \delta_1, \text{ com } N(\delta_1) < N(\beta).$$

Pelo Teorema 29, $mdc(\alpha, \beta) = mdc(\beta, \delta_1)$, desta forma temos duas situações:

- $N(\delta_1) = 0$, neste caso $mdc(\beta, \delta_1) = \beta$.
- $N(\delta_1) \neq 0$, neste caso fazemos a divisão euclideana de $\beta$ por $\delta_1$, obtendo

$$\beta = \delta_1\gamma_2 + \delta_2, \text{ com } N(\delta_2) < N(\delta_1)$$

Segue que $mdc(\beta, \delta_1) = mdc(\delta_1, \delta_2)$. Novamente pode ocorrer duas situações:

- $N(\delta_2) = 0$, neste caso $mdc(\delta_1, \delta_2) = \delta_1$.
- $N(\delta_2) \neq 0$, neste caso fazemos a divisão euclideana de $\delta_1$ por $\delta_2$, obtendo

$$\delta_1 = \delta_2\gamma_3 + \delta_3, \text{ com } N(\delta_3) < N(\delta_2).$$

Segue que

$$mdc(\alpha, \beta) = mdc(\beta, \delta_1) = mdc(\delta_1, \delta_2) = mdc(\delta_2, \delta_3)$$

e assim sucessivamente.

Definindo $\delta_0 = \beta$, existe um valor $n$ natural que $\delta_{n+1} = 0$ e $\delta_n \neq 0$. De fato, se tivéssemos para todo $n \neq 0$, teríamos uma sequência infinita em $\mathbb{N}$

$$N(\delta_0) > N(\delta_1) > N(\delta_2) > ... > 0.$$

Segue que

$$mdc(\alpha, \beta) = mdc(\beta, \delta_1) = mdc(\delta_1, \delta_2) = ... = mdc(\delta_n, \delta_{n+1}) = mdc(\delta_n, 0) = \delta_n.$$

Portanto, o último resto não nulo $\delta_n$ deste processo, fornece o valor de $mdc(\alpha, \beta)$. □

**Definição 20.** *Dizemos que $\alpha, \beta \in \mathbb{Z}[i]$, são relativamente primos, quando têm as unidades como máximo divisor comum.*

**Exemplo 32.** *Calcule o $mdc(27 + 4i, 5 + 2i)$.*

*Calculamos o máximo divisor comum de $27 + 4i$ e $5 + 2i$ através do Teorema da divisão e aplicando o Algoritmo de Euclides, encontramos*

$$27 + 4i = (5 + 2i)(5 - i) + (-i)$$
$$5 + 2i = (-i)(-2 + 5i) + 0$$

*O último resto diferente de zero é $-i$, então $mdc(27 + 4i, 5 + 2i) = -i$. Portanto, $27 + 4i$ e $5 + 2i$ são relativamente primos.*

**Exemplo 33.** *Mostre que os conjugados $7 - 2i$ e $7 + 2i$ são relativamente primos.*

*Basta mostrar que o $mdc(7-2i, 7+2i)$ é igual a uma unidade. Fazendo a divisão e aplicando o Algoritmos de Euclides, temos*

$$7 - 2i = (7 + 2i)(1 - i) + (-2 + 3i)$$
$$7 + 2i = (-2 + 3i)(-1 - 2i) + (-1 + i)$$
$$-2 + 3i = (-1 + i)(2 - i) + (-1)$$
$$-1 + i = (-1)(1 - i) + 0$$

*O último resto diferente de zero é $-1$, então $mdc(7 - 2i, 7 + 2i) = -1$. Portanto, $7 - 2i$ e $7 + 2i$ são relativamente primos.*

**Exemplo 34.** *Calcule o* $mdc(11-3i, 5+7i)$.

*Calculamos o máximo divisor comum de* $11-3i$ *e* $5+7i$ *através do Teorema da divisão e aplicando o Algoritmo de Euclides, encontramos*

$$\begin{aligned} 11-3i &= (5+7i)(-i)+(4+2i) \\ 5+7i &= (4+2i)(2+i)+(1+i) \\ 4+2i &= (1+i)(3-i)+0 \end{aligned}$$

*O último resto diferente de zero é* $1+i$, *então* $mdc(11-3i, 5+7i) = 1+i$.

## 2.7 O Teorema de Bézout

**Lema 31.** *Se* $\beta|\alpha$ *e* $N(\beta) = 1$ *ou* $N(\beta) = N(\alpha)$, *então ou* $\beta$ *é uma unidade ou é um associado de* $\alpha$.

*Demonstração.* Se $N(\beta) = 1$, então $\beta$ é uma unidade, pelo Teorema 23. Se $N(\beta) = N(\alpha)$, como $\beta|\alpha$, então $\alpha = \beta\gamma$ para algum $\gamma \in \mathbb{Z}[i]$. Aplicando a Função Norma, temos $N(\alpha) = N(\beta)N(\gamma)$. Como a norma de um inteiro gaussiano não nulo é um número inteiro positivo, podemos efetuar o cancelamento, então $N(\gamma) = 1$. Portando, $\beta$ é um associado de $\alpha$. □

**Teorema 32.** *(Teorema de Bézout) Seja* $\alpha, \beta \in \mathbb{Z}[i]$, *diferentes de zero, e* $mdc(\alpha, \beta) = \gamma$. *Então* $\gamma = \alpha x + \beta y$, *para algum* $x, y \in \mathbb{Z}[i]$.

*Demonstração.* Considere o conjunto $C$ sendo todas as combinações lineares de $\alpha$ e $\beta$ e $n = \alpha x_0 + \beta y_0$, onde $n$ é o elemento de menor norma de $C$. Suponha, por absurdo, que $n \nmid \alpha$. Então $\alpha = nq + r$, com $N(r) < N(n)$.

$$\begin{aligned} r &= \alpha - nq = \alpha - (\alpha x_0 + \beta y_0)q \\ &= \alpha - \alpha x_0 q - \beta y_0 q \\ &= \alpha(1 - x_0 q) + \beta(-y_0 q). \end{aligned}$$

Então $r \in C$, $N(r) < N(n)$, mas $n$ é o elemento de menor norma em $C$, portanto, $n|\alpha$. Analogamente, $n|\beta$. Assim, $n$ é o divisor comum de $\alpha$ e $\beta$. Vamos mostrar que $n = \gamma$. De

fato, como $mdc(\alpha, \beta) = \gamma$, então $\gamma|\alpha$ e $\gamma|\beta$. Logo existem $q_1, q_2 \in \mathbb{Z}[i]$ tais que $\alpha = \gamma q_1$ e $\beta = \gamma q_2$. Como $n = \alpha x_0 + \beta y_0$, então

$$n = (\gamma q_1)x_0 + (\gamma q_2)y_0$$
$$n = \gamma(q_1 x_0 + q_2 y_0),$$

Se $\gamma|n \Rightarrow N(\gamma)|N(n)$. Como $n$ é o menor elemento de $C$, $N(\gamma) = N(n)$. Se $\gamma|n$ e $N(\gamma) = N(n)$ então $\gamma$ e $n$ são associados $\Rightarrow \gamma = n \cdot u \Rightarrow \gamma = \alpha x_0 u + \beta y_0 u \Rightarrow \gamma = \alpha x + \beta y$, para algum $x, y \in \mathbb{Z}[i]$. □

**Corolário 33.** *Sejam $\alpha, \beta$ inteiros gaussianos relativamente primos, então existem $x, y \in \mathbb{Z}[i]$ tal que $\alpha x + \beta y = 1$.*

*Demonstração.* Como $\alpha$ e $\beta$ são relativamente primos, então $mdc(\alpha, \beta) = m$ onde $m \in \{-1, 1, -i, i\}$. Pelo Teorema 32, existem $x, y \in \mathbb{Z}[i]$ tal que $\alpha x + \beta y = m$.

Temos quatro casos:

- Para $m = 1$, então $\alpha x + \beta y = 1$;
- Para $m = -1$, então $\alpha x + \beta y = -1$, multiplicando a equação por $-1$, temos que $\alpha(-x) + \beta(-y) = 1$.
- Para $m = i$, então $\alpha x + \beta y = i$, multiplicando a equação por $-i$, temos que $\alpha(-xi) + \beta(-yi) = 1$.
- Para $m = -i$, então $\alpha x + \beta y = -i$, multiplicando a equação por $i$, temos que $\alpha(xi) + \beta(yi) = 1$.

Portando, em todos os casos conseguimos escrever $\alpha x + \beta y = 1$. □

**Exemplo 35.** *Ja vimos que $7 - 2i$ e $7 + 2i$ são relativamente primos, pois $mdc(7 - 2i, 7 + 2i) = -1$. Agora escreveremos $-1$ como uma combinação linear de $7 - 2i$*

*e* $7+2i$*, conforme o Teorema de Bézout:*

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

*Pelo Corolário 33, ao multiplicarmos por* $-1$*, podemos escrever como:*

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

**Teorema 34.** *Seja* $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ *tal que* $mdc(\alpha, \beta) = 1$ *e* $\gamma = \alpha\beta$*. Então para todo* $\delta \in \mathbb{Z}[i]$*,* $mdc(\gamma, \delta) = 1$ *se, e somente se* $mdc(\alpha, \delta) = 1$ *e* $mdc(\beta, \delta) = 1$*.*

*Demonstração.* Seja $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ tal que $\alpha$ e $\beta$ são relativamente primos e $\gamma = \alpha\beta$. Assuma que $mdc(\alpha, \delta) \neq 1$ ou $mdc(\beta, \delta) \neq 1$. Sem perda de generalidade, assuma que $mdc(\alpha, \delta) = \mu$ para algum $\mu \in \mathbb{Z}[i]$, não unidade. Então $\mu|\alpha$ e $\mu|\delta$. Além disso, já que $\alpha|\gamma$, sabemos que $\mu|\gamma$. Como $\mu|\gamma$ e $\mu|\delta$, sabemos que $\mu$ é um divisor comum, diferente da unidade, de $\gamma$ e $\delta$. Então $\gamma$ e $\delta$ não são relativamente primos, pois $2 \leq N(\mu) \leq N(\gamma)$.

Agora, suponha que o $mdc(\alpha, \delta) = 1$ e $mdc(\beta, \delta) = 1$. Então, $\alpha\kappa_1 + \delta\kappa_2 = 1$ e $\beta\kappa_3 + \delta\kappa_4 = 1$ para algum $\kappa_1, \kappa_2, \kappa_3, \kappa_4 \in \mathbb{Z}[i]$. Multiplicando as equações membro a membro, temos

$$\begin{aligned}
(\alpha\kappa_1 + \delta\kappa_2)(\beta\kappa_3 + \delta\kappa_4) &= 1 \\
\alpha\kappa_1\beta\kappa_3 + \alpha\kappa_1\delta\kappa_4 + \delta\kappa_2\beta\kappa_3 + \delta\kappa_2\delta\kappa_4 &= 1.
\end{aligned}$$

Como $\gamma = \alpha\beta$,

$$\gamma(\kappa_1\kappa_3) + \delta(\alpha\kappa_1\kappa_4 + \kappa_2\beta\kappa_3 + \kappa_2\delta\kappa_4) = 1.$$

Portanto, $mdc(\gamma, \delta) = 1$. □

## 2.8 Fatoração Única

Quando $N(\alpha) > 1$, temos pelo menos oito divisores de $\alpha$: $\pm 1, \pm i, \pm\alpha$ e $\pm i\alpha$, esses são chamados de fatores triviais de $\alpha$. Qualquer outro fator de $\alpha$ é chamado de não trivial.

**Definição 21.** *Seja $\alpha$ um inteiro gaussiano com $N(\alpha) > 1$. O inteiro gaussiano $\alpha$ será chamado de composto se possuir algum divisor não trivial. Se possuir apenas divisores triviais, então ele será chamado de primo.*

**Teorema 35.** *Se a norma de um inteiro Gaussiano $\alpha$ é um número primo em $\mathbb{Z}$, então $\alpha$ será um número primo em $\mathbb{Z}[i]$.*

*Demonstração.* Suponha $N(\alpha) = p$, $p$ é primo em $\mathbb{Z}$. Considere qualquer fatoração de $\alpha$, sendo como $\alpha = \beta\gamma$ para $\beta, \gamma \in \mathbb{Z}[i]$. Aplicando a função Norma, temos que $N(\alpha) = N(\beta)N(\gamma)$, então $N(\beta)N(\gamma) = p$. Como $p$ é primo, então temos duas possibilidades: ou $N(\beta) = 1$ e $N(\gamma) = p$ ou $N(\beta) = p$ e $N(\gamma) = 1$. Podemos observar que $\beta$ é uma unidade e $\gamma$ é um associado de $\alpha$ ou $\beta$ é um associado de $\alpha$ e $\gamma$ é uma unidade e, portanto, $\alpha$ possui apenas divisores triviais, ou seja, $\alpha$ é primo. □

**Exemplo 36.** *$1 + i$ é primo em $\mathbb{Z}[i]$, pois $N(1 + i) = 2$ e $2$ é primo em $\mathbb{Z}$.*

**Exemplo 37.** *$2 + i$ é primo em $\mathbb{Z}[i]$, pois $N(2 + i) = 5$ e $5$ é primo em $\mathbb{Z}$.*

**Teorema 36.** *Seja $\alpha \in \mathbb{Z}[i]$, como $N(\alpha) > 1$. Então $\alpha$ pode ser escrito como um produto de números primos em $\mathbb{Z}[i]$.*

*Demonstração.* A prova será feita por indução em $N(\alpha)$. Suponha que $N(\alpha) = 2$, então $\alpha$ é um primo gaussiano (Pelo Teorema 35). Agora, vamos supor para $n \geq 2$ e que se $\beta \in \mathbb{Z}[i]$ tal que $1 < N(\beta) < n$ então é um produto de números primos em $\mathbb{Z}[i]$. Vamos supor que há inteiros gaussianos com norma $n$. Se temos um número inteiro de Gauss $\alpha$

como a norma $n$, que é composto, então podemos escrever $\alpha = \beta\gamma$. Aplicando a norma, temos $N(\alpha) = N(\beta)N(\gamma)$, onde $N(\beta) < N(\alpha) = n$. Por hipótese indutiva, $\beta$ e $\gamma$ são produtos de primos em $\mathbb{Z}[i]$.Portanto, $\alpha$ também é um produto de primos em $\mathbb{Z}[i]$. □

**Lema 37.** *Sejam $\pi$ um primo em $\mathbb{Z}[i]$ e $\alpha\beta \in \mathbb{Z}[i]$. Se $\pi|\alpha\beta$, então $\pi|\alpha$ ou $\pi|\beta$.*

*Demonstração.* Suponha que $\pi \nmid \alpha$. Se $\pi \nmid \alpha$, então $mdc(\alpha, \pi)$ é uma unidade, isso significa que $\alpha$ e $\beta$ são relativamente primos. Sendo assim, podemos escrever como uma combinação linear, $\alpha x + \pi y = 1$. Multiplicando por $\beta$, temos $\beta\alpha x + \beta\pi y = \beta$. Como $\pi|\alpha\beta$, $\pi|\pi$, temos que $\pi|(\beta\alpha x + \beta\pi y)$ e, portanto, $\pi|\beta$. □

**Teorema 38.** *(Fatoração Única) Qualquer $\alpha \in \mathbb{Z}[i]$, com $N(\alpha) > 1$, tem uma fatoração de primos. Essa fatoração é única a menos da ordem dos fatores e associados.*

*Demonstração.* No Teorema 36 mostra que cada $\alpha \in \mathbb{Z}[i]$, com $N(\alpha) > 1$, tem uma fatoração. Quando $\alpha$ é primo, não há nada a fazer pois sua fatoração é, obviamente, única. Agora vamos mostrar a unicidade, em geral, por indução em $N(\alpha)$. Tome $N(\alpha) = 2$, já foi estabelecido $\alpha = \pm 1 \pm i$. Agora suponha que $n \geq 3$ e $1 < N(\alpha) < n$ com $\alpha$ tendo uma fatoração única. Podemos supor que há inteiros gaussianos com a norma $n$. Considere duas fatorações de primos de $\alpha$ como na demonstração do Teorema 11. Seja $\pi_1|\alpha$, podemos escrever:

$$\pi_1|\pi'_1\pi'_2...\pi'_s.$$

Pelo Lema , $\pi_1|\pi'_j$, para algum $j$. Podemos supor que $j = 1$, ou seja, $\pi_1|\pi'_1$. Os únicos fatores não unitários de $\pi'_1$ são múltiplos unitários de $\pi'_1$, então $\pi_1 = u\pi'_1$ para alguma unidade $u \in \{-1, 1, -i, i\}$. Observando as duas fatorações de $\alpha$:

$$\alpha = u\pi'_1\pi_2...\pi_r = \pi'_1\pi'_2...\pi'_s.$$

Cancelando $\pi'_1$ em ambos os lados, temos:

$$u\pi_2...\pi_r = \pi'_2...\pi'_s, \tag{2.1}$$

sendo $\beta = \pi'_2...\pi'_s$, então $N(\beta) = N(\alpha)/N(\pi'_1) < N(\alpha)$. Embora $u$ é uma unidade, e $u\pi_2$ é um produto sobre o lado esquerdo de (2.1), ele é realmente um primo, de modo (2.1) têm duas fatorações de primos de $\beta$, com $(r-1)$ primos do lado esquerdo e $(s-1)$ primos do lado direito. Como $N(\beta) < n$, a hipótese indutiva diz que $\beta$ tem fatoração única, então

$(r-1) = (s-1)$, que implica $r = s$ e, após nova rotulagem apropriada, temos que $u\pi_2$ e $\pi_2'$ são múltiplos unitários $\pi_i$, $\pi_i'$ são múltiplos unitários para $i > 2$. Seja $u\pi_2$ e $\pi_2'$ são múltiplos unitários, de modo que vemos todos os $\pi_i$ é um múltiplo unitário de $\pi_i'$ e a prova está completa. □

**Exemplo 38.** *Vamos fatorar* $3 + 4i$. *Sabemos que* $N(3 + 4i) = 25 = 5 \cdot 5$. *Já que* 5 *é a norma de uma fator não trivial de* $3 + 4i$, *podemos escrever* $5 = (1 + 2i)(1 - 2i)$. *Considerando* $\alpha = 1 + 2i$ *e* $\beta = 1 - 2i$, *temos as seguintes possibilidades:*

- $\alpha \cdot \alpha = (1 + 2i)(1 + 2i) = -3 + 4i$
- $\alpha \cdot \beta = (1 + 2i)(1 - 2i) = 5$
- $\beta \cdot \beta = (1 - 2i)(1 - 2i) = -3 - 4i$.

*Multiplicando c) por* $-1$, *temos que:*

$$3 + 4i = -(1 - 2i)(1 - 2i) = -(1 - 2i)^2.$$

*Portanto, a fatoração de* $3 + 4i$ *é* $-(1 - 2i)^2$.

**Exemplo 39.** $1 + 3i$ *é primo?*

*Podemos verificar calculando* $N(1 + 3i) = 10$, *como a norma de* $1 + 3i$ *é par, nos indica que um dos fatores de* $1 + 3i$ *é* $1 + i$*(Pelo Corolário 27). Ao fatorarmos* $N(1 + 3i) = 2 \cdot 5$, *temos que* $N(1 + i) = 2$. *Para que* $N(\alpha) = 5$, $\alpha = \pm 1 \pm 2i$ *ou* $\alpha = \pm 2 \pm i$. *Fazendo as possíveis combinações de* $1 + i$ *e* $\alpha$, *temos:*

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

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

*Portanto,* $1+3i$ *não é primo e sua fatoração é* $(1+i)(2+i)$.

**Exemplo 40.** *Vamos encontrar a fatoração de* $5+7i$*? Sua norma é* $74$*, cuja fatoração em* $\mathbb{Z}$ *é* $2 \cdot 37$*. Já sabemos pelo Corolário 27 que um dos fatores de* $5+7i$ *é* $1+i$*.*

*Vamos observar os inteiros gaussianos com norma* $37$*, em seguida iremos multiplicá-los a* $1+i$ *para obtermos* $5+7i$*. Vamos representar o número* $37$ *como soma de dois quadrados:*

$$37 = 6^2 + 1^2 = 1^2 + 6^2.$$

*Assim, podemos fatorar em primos gaussianos:*

$$37 = (6+i)(6-i) \text{ } ou \text{ } 37 = (1+6i)(1-6i).$$

*Os inteiros gaussianos são primos, pois suas normas são primos em* $\mathbb{Z}$*. Então, temos as seguintes combinações:*

- $(1+i)(6+i) = 5+7i$;
- $(1+i)(6-i) = 7+5i$;
- $(1+i)(1+6i) = -5+7i$;
- $(1+i)(1-6i) = 7-5i$.

*Portanto, a fatoração de* $5+7i$ *é* $(1+i)(6+i)$.

### 2.8.1 Elementos primos em $\mathbb{Z}[i]$

Nesta seção vamos estudar algumas propriedades algébricas de $\mathbb{Z}[i]$ com mais profundidade. Em particular, caracterizar os primos em $\mathbb{Z}[i]$.

**Lema 39.** $\alpha$ *é primo em* $\mathbb{Z}[i]$ *se, e somente se* $\overline{\alpha}$ *é primo em* $\mathbb{Z}[i]$.

*Demonstração.* Iremos provar por negação. Suponha que $\alpha$ não seja primo em $\mathbb{Z}[i]$, então $\alpha = \gamma\beta$, onde $\gamma, \beta \in \mathbb{Z}[i]$ são divisores não triviais de $\alpha$. Por conjugação, temos $\overline{\alpha} = \overline{\gamma\beta} = \overline{\gamma}\overline{\beta}$ e portanto $\overline{\alpha}$ tem uma fatoração de números não triviais, ou seja, $\overline{\alpha}$ não é primo em $\mathbb{Z}[i]$. A reciproca é verdadeira já que o conjugado do conjudado de $\alpha$ é o próprio $\alpha$. □

**Lema 40.** *Se $\alpha = a + bi$ com $a \cdot b \neq 0$ é primo em $\mathbb{Z}[i]$, então $N(\alpha) = a^2 + b^2$ é primo em $\mathbb{Z}$.*

*Demonstração.* Note que $N(\alpha) = a^2 + b^2 = (a+bi)(a-bi)$ é um múltiplo de $\alpha$. Suponha que $N(\alpha) = a^2 + b^2$ não é primo em $\mathbb{Z}$, ou seja, $N(\alpha) = a^2 + b^2 = m \cdot n$, com $m, n \geq 2$. Por hipótese, $\alpha = a + bi$ é primo em $\mathbb{Z}[i]$, então $\alpha | m \cdot n$, logo $\alpha | m$ ou $\alpha | n$ (Pelo Lema 37). Digamos que $m$ seja um múltiplo de $\alpha = a + bi$, então $m = \gamma \cdot \alpha$, para algum $\gamma \in \mathbb{Z}[i]$, ou seja, $m$ não pode ser associado $\alpha$, logo multiplicando por $n$, temos:

$$m \cdot n = \gamma \cdot \alpha \cdot n = (a + bi)(a - bi)$$
$$\gamma \cdot n = (a - bi).$$

Como $n$ não é uma unidade, então $a - bi$ não é primo, o que é um absurdo, pelo Lema 2.8.1. □

**Exemplo 41.** *$2 + 3i$ é primo em $\mathbb{Z}[i]$ e $N(2 + 3i) = 2^2 + 3^2 = 4 + 9 = 13$ é primo em $\mathbb{Z}$.*

**Lema 41.** *Seja $\alpha = a + bi \in \mathbb{Z}[i]$ com $a \cdot b \neq 0$. Então $\alpha = a + bi$ é primo em $\mathbb{Z}[i]$ se, e somente se $a^2 + b^2 = p$ é um número primo em $\mathbb{Z}$ com $p \equiv 1 (\bmod 4)$ ou $p = 2$.*

*Demonstração.* $\Rightarrow$) Suponha que $\alpha = a + bi$ é primo em $\mathbb{Z}[i]$. Usando a aritmética módulo 4, vamos calcular a soma de $a^2 + b^2$ módulo 4:

$$0^2 \equiv 0 (\bmod 4), 1^2 \equiv 1 (\bmod 4), 2^2 \equiv 0 (\bmod 4) \text{ e } 3^2 \equiv 1 (\bmod 4),$$

logo um quadrado módulo 4 é igual a 0 ou 1. E sua soma módulo 4 é $0, 1$ ou 2, ou seja,

$$p \equiv 0 (\bmod 4), p \equiv 1 (\bmod 4) \text{ ou } p \equiv 2 (\bmod 4).$$

Se $p \equiv 0 (\bmod 4)$, então $4|p$, logo $p$ não é primo. Pelo Lema 40, $p = a^2 + b^2 \equiv 1 (\bmod 4)$ ou $p = a^2 + b^2 \equiv 2 (\bmod 4)$ e o único primo $p \equiv 2 (\bmod 4)$ é $p = 2$.

$\Leftarrow$) Suponha que $a^2 + b^2 = p$ é um número primo e que $\alpha = a + bi$ não é primo, ou seja $a + bi = \gamma \cdot \beta$ para algum $\gamma, \beta \in \mathbb{Z}[i]$. Então,

$$N(a + bi) = N(\gamma \cdot \beta) = N(\alpha)N(\beta)$$
$$a^2 + b^2 = N(\gamma)N(\beta)$$
$$p = N(\gamma)N(\beta).$$

Como $p$ é primo, então $N(\gamma) = 1$ ou $N(\beta) = 1$. Logo $\gamma$ ou $\beta$ é uma unidade, o que é um absurdo. Portanto $\alpha = a + bi$ é primo. □

**Exemplo 42.** *$-2 + 5i$ é primo em $\mathbb{Z}[i]$, pois $N(-2 + 5i) = 29$ e $29 \equiv 1 (\mathrm{mod}\ 4)$.*

**Observação 4.** *A soma $a^2 + b^2$ nunca é congruente a 3 módulo 4.*

**Observação 5.** *Se $a + bi$ é um primo em $\mathbb{Z}[i]$ com $a^2 + b^2 = p = 2$, então $a + bi$ é um dos quatro elementos:*
*Se $a = 1$ e $b = 1$, então $\alpha = 1 + i$;*
*Se $a = 1$ e $b = -1$, então $\alpha = 1 - i$;*
*Se $a = -1$ e $b = 1$, então $\alpha = -1 + i$;*
*Se $a = -1$ e $b = -1$, então $\alpha = -1 - i$.*

**Observação 6.** *Considerando elementos da forma $a$ ou $bi$ em $\mathbb{Z}[i]$, tem-se $bi$ é um associado de $b$, pois $b = -i(bi)$. Agora os elementos da forma $a + 0i \in \mathbb{Z}[i]$. Note que, se $n$ é um inteiro composto em $\mathbb{Z}$, então $n$ é um inteiro composto em $\mathbb{Z}[i]$, pois para $n = r \cdot s$ como $r, s > 1$ em $\mathbb{Z}$, temos $n = r \cdot s = (r + 0i)(s + 0i) \in \mathbb{Z}[i]$.*

**Lema 42.** *Se $p$ é primo em $\mathbb{Z}$ com $p \equiv 3 (\mathrm{mod}\ 4)$, então $p$ também é primo em $\mathbb{Z}[i]$.*

*Demonstração.* Suponha que $p$ não é primo em $\mathbb{Z}[i]$, então $p = \alpha\beta$ onde nem $\alpha$ e nem $\beta$ são unidades em $\mathbb{Z}[i]$, logo

$$N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$$
$$p^2 = N(\alpha)N(\beta).$$

Como $N(\alpha) > 1$ e $N(\beta) > 1$, temos $N(\alpha) = N(\beta) = p$. Mas $N(\alpha) = N(\beta)$ é a soma de dois quadrados e a soma de dois quadrados nunca pode ser congruente a 3 módulo 4 (Observação 4). Portanto, a hipótese de $p$ não ser primo em $\mathbb{Z}[i]$ é falsa, logo $p$ é primo em $\mathbb{Z}[i]$. □

**Exemplo 43.** *2 não é primo em $\mathbb{Z}[i]$ já que não é congruente a 3 módulo 4. Mas 11 é primo em $\mathbb{Z}[i]$, pois $11 \equiv 3 (\mathrm{mod}\ 4)$.*

Em $\mathbb{Z}[i]$, o inteiro 2 pode ser fatorado em dois fatores primos, ou seja, $2 = (1 + i)(1 - i)$. É só multiplicar.

**Lema 43.** *Seja $p$ um primo em $\mathbb{Z}$. Se $p \equiv 1(\bmod 4)$, então a congruência $x^2 \equiv -1(\bmod p)$ tem solução.*

*Demonstração.* Considere $p \neq 2$ e o polinômio

$$T^{p-1} - 1 = (T^{\frac{p-1}{2}} - 1)(T^{\frac{p-1}{2}} + 1) \text{ módulo } p.$$

Vamos contar as raízes desses polinômios módulo $p$. Já vimos que um polinômio de grau $d$ não tem mais que $d$ raízes módulo $p$. Assim,

- $T^{p-1} - 1$, tem $p - 1$ raízes diferentes módulo $p$;
- $T^{\frac{p-1}{2}} - 1$, tem $\dfrac{p-1}{2}$ raízes diferentes módulo $p$.

Portanto, $T^{\frac{p-1}{2}} + 1$ tem que ter raízes módulo $p$, ou seja, deve existir algum inteiro $C$ tal que

$$C^{\frac{p-1}{2}} + 1 \equiv 0(\ \bmod p)$$
$$C^{\frac{p-1}{2}} \equiv -1(\ \bmod p).$$

Como $p \equiv 1(\bmod 4)$, então $\dfrac{p-1}{2} = 2k$ é par. Portanto, $(C^k)^2 \equiv -1(\bmod p)$, ou seja, $x^2 \equiv -1(\bmod p)$ tem solução. □

**Lema 44.** *Se $p$ é um primo em $\mathbb{Z}$ com $p \equiv 1(\bmod 4)$, então $p$ não é primo em $\mathbb{Z}[i]$, mas tem uma fatoração em primos da forma $p = (a + bi)(a - bi)$.*

*Demonstração.* Pelo Lema 43, exite $m \in \mathbb{Z}$ tal que $p|m^2 + 1$. Agora, considere o inteiro $p$ em $\mathbb{Z}[i]$. Note que $m^2 + 1 = (m + i)(m - i)$, assim $p|m^2 + 1 = (m + i)(m - i)$, temos então que $p|m + i$ ou $p|m - i$ (Pelo Lema 21), o que é um absurdo, pois teríamos que $p| \pm 1$ ou $p| \pm i$. Portanto, $p$ não é primo em $\mathbb{Z}[i]$. Assim, existem fatores não triviais $\alpha, \beta \in \mathbb{Z}[i]$ tais que $p = \alpha\beta$. Aplicando norma em ambos os membros dessa equação, temos $N(p) = N(\alpha)N(\beta) = p^2$. Portanto, $N(\alpha) = N(\beta) = p$. Escrevendo $\alpha = a+bi$ e $\beta = c+di$, temos $p = a^2 + b^2 = (a + bi)(a - bi)$, ou seja, $c + di = a - bi$. □

**Exemplo 44.** *5 é primo em $\mathbb{Z}$ e $5 \equiv 1(\bmod 4)$, então $5 = (2 + i)(2 - i)$.*

**Exemplo 45.** *13 é primo em $\mathbb{Z}$ e $13 \equiv 1(\bmod 4)$, então $13 = (3 + 2i)(3 - 2i)$.*

Resumindo os resultados dos Lemas 40, 41, 42, 43 e 44 temos:

**Teorema 45.** *Os elementos primos em $\mathbb{Z}[i]$ são os seguintes:*

*(1) associados dos inteiros da forma $p + 0i$, onde $p$ é primo com $p \equiv 3 (\mod 4)$;*

*(2) associados de $1 + i$ e $1 - i$; e*

*(3) elementos $a + bi$ tais que $N(a + bi) = a^2 + b^2 = p$ um número primo com $p \equiv 1 (\mod 4)$.*

*Demonstração.* (1) Segue do Lema 42;

(2) Segue da Observação 5; e

(3) Segue dos Lemas 40, 41, 43 e 44.

□

# Capítulo 3

# Aritmética Modular em $\mathbb{Z}[i]$

Neste capítulo vamos nos dedicar a um estudo sobre a aritmética modular dos inteiros gaussianos. Veremos que algumas propriedades de $\mathbb{Z}$ serão transportadas para $\mathbb{Z}[i]$. Faremos também a construção das classes residuais módulo um inteiro gaussiano. E por fim a extensão do Pequeno Teorema de Fermat para $\mathbb{Z}[i]$, como também o Teorema de Euler.

## 3.1 Aritmética Modular em $\mathbb{Z}[i]$

**Definição 22.** *Sejam $\alpha$, $\beta$ e $\eta$ inteiros gaussianos. Dizemos que $\alpha$ é congruente a $\beta$ módulo $\eta$, indicado por $\alpha \equiv \beta(\mod \eta)$, quando $\eta|\alpha - \beta$. Ou seja, $\alpha - \beta = \eta\delta$, para algum $\delta \in \mathbb{Z}[i]$.*

**Exemplo 46.** *Vamos verificar se $2+4i \equiv 2-i(\mod 1+i)$.Por definição de congruência para que seja verdade esta relação, $1+i|(2+4i)-(2-i)$, ou seja $\exists \delta \in \mathbb{Z}[i]$ tal que*

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

*como $\frac{5}{2}+\frac{5}{2}i \notin \mathbb{Z}[i]$, então $2+4i \not\equiv 2-1(\mod 1+i)$.*

**Exemplo 47.** *Vamos verificar se* $1+5i \equiv -3-2i(\bmod 2+i)$.*Por definição de congruência para que seja verdade esta relação,* $2+i|(1+5i)-(-3-2i)$*, ou seja* $\exists\delta \in \mathbb{Z}[i]$ *tal que*

$$\begin{aligned}(1+5i)-(-3-2i) &= (2+i)\delta \\ \frac{(1+5i)-(-3-2i)}{(2+i)} &= \delta \\ \frac{(4+7i)}{(2+i)}\frac{(2-i)}{(2-i)} &= \delta \\ \frac{15+10i}{5} &= \delta \\ 3+2i &= \delta\end{aligned}$$

*como* $3+2i \in \mathbb{Z}[i]$*, então* $1+5i \equiv -3-2i(\bmod 2+i)$.

**Exemplo 48.** *Quais os possíveis valores de* $\alpha$ *para que* $2i \equiv \alpha(\bmod i)$*. Adotando* $\alpha = a+bi$ *e* $\beta = m+ni$*. Para que a congruência seja válida,* $i|2i-(a+bi)$.

$$\begin{aligned}2i-(a+bi) &= i(m+ni) \\ -a+(2+b)i &= -n+mi\end{aligned}$$

*Pela igualdade obtemos os seguintes resultados:* $a = n$ *e* $b = \frac{m}{2}$*. Como* $a$ *e* $b$ *devem ser números inteiros, qualquer combinação de* $a$ *e* $b$*, onde o número* $b$ *seja um número divisível por* $2$ *satisfaz a congruência. Vejamos para o seguinte caso:* $a = 2$ *e* $b = 4$*, temos a congruência* $2i \equiv 2+4i(\bmod i)$ *que de fato é verdadeira pois*

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

Quando temos congruência módulo 0, ou seja para $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha \equiv \beta(\bmod 0)$, por definição, $0|\alpha-\beta$, então $\alpha-\beta = 0$, obtemos uma igualdade $\alpha = \beta$. Daqui em diante assumiremos que será módulo diferente de zero.

Na congruência para inteiros gaussianos, assim como nos inteiros, as propriedades da soma e da multiplicação são válidas, vejamos:

**Propriedades: 4.** *Sejam* $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}[i]$. *Se* $\alpha \equiv \alpha' (\bmod \eta)$ *e* $\beta \equiv \beta' (\bmod \eta)$, *então:*

*i)* $\alpha + \beta \equiv \alpha' + \beta' (\bmod \eta)$

*ii)* $\alpha\beta \equiv \alpha'\beta' (\bmod \eta)$

*Demonstração.* i) Usando a definição de congruência, existe $\gamma, \delta \in \mathbb{Z}[i]$ tal que $\alpha - \alpha' = \eta\gamma$ e $\beta - \beta' = \eta\delta$. Somando as equações membro a membro, temos

$$\alpha - \alpha' + \beta - \beta' = \eta\gamma + \eta\delta$$
$$\alpha + \beta - (\alpha' + \beta') = \eta(\gamma + \delta)$$

o que nos dá que $\eta | \alpha + \beta - (\alpha' + \beta')$, portanto $\alpha + \beta \equiv \alpha' + \beta' (\bmod \eta)$.

ii) Usando as equações do item i), iremos multiplicar a primeira por $\beta$ e a segunda por $\alpha'$ e por fim faremos a soma delas.

$$\beta(\alpha - \alpha') + \alpha'(\beta - \beta') = \beta(\eta\gamma) + \alpha'(\eta\delta)$$
$$\beta\alpha - \beta\alpha' + \alpha'\beta - \alpha'\beta' = \eta\beta\gamma + \eta\alpha'\delta$$
$$\alpha\beta - \alpha'\beta' = \eta(\beta\gamma + \alpha'\delta)$$

portanto, $\eta | \alpha\beta - \alpha'\beta'$, pela definição de congruência, $\alpha\beta \equiv \alpha'\beta' (\bmod \eta)$.

□

Vejamos um exemplo aplicando essas propriedades.

**Exemplo 49.** *Sejam* $1 + 12i \equiv 2 - i (\bmod 3 + i)$ *e* $11 + 5i \equiv 2 + 2i (\bmod 3 + i)$. *Somando as congruências, obtemos* $12 + 17i \equiv 4 + i (\bmod 3 + i)$. *O que de fato é verdade pois,*

$$\begin{aligned}
\frac{(12 + 17i) - (4 + i)}{(3 + i)} &= \frac{(8 + 16i)}{(3 + i)} \frac{(3 - i)}{(3 - i)} \\
&= \frac{24 - 8i + 48i + 16}{10} \\
&= \frac{40}{10} + \frac{40}{10} i \\
&= 4 + 4i
\end{aligned}$$

$e\ 4+4i \in \mathbb{Z}[i]$.

*Ao multiplicarmos, obtemos* $-49+137i \equiv 6+2i(\bmod 3+i)$, *que é verdade, pois*

$$\begin{aligned}\frac{(-49+137i)-(6+2i)}{(3+i)} &= \frac{(-55+135i)}{(3+i)}\frac{(3-i)}{(3-i)}\\ &= \frac{-165+55i+405i+135}{10}\\ &= \frac{-30+460i}{10}\\ &= -3+46i,\end{aligned}$$

*assim* $-3+46i \in \mathbb{Z}[i]$.

Um inteiro gaussiano pode ser reduzido módulo $\alpha$, para isso fazemos a divisão por $\alpha$, obtendo assim um inteiro gaussiano como norma reduzida, utilizando o resto.

**Exemplo 50.** *Vamos calcular* $(1+2i)^3(\bmod 1+i)$. *Calculando a potência, temos*

$$\begin{aligned}(1+2i)^3 &= (1+2i)^2(1+2i)\\ &= (-3+4i)(1+2i)\\ &= -11-2i\end{aligned}$$

*fazendo a divisão de* $-11-2i$ *por* $1+i$, *temos*

$$\begin{aligned}\frac{(-11-2i)}{(1+i)}\frac{(1-i)}{(1-i)} &= \frac{-11+11i-2i-2}{2}\\ &= \frac{-13}{2}+\frac{9}{2}i\end{aligned}$$

*como* $-\dfrac{13}{2} = -6,5$ *e* $\dfrac{9}{2} = 4,5$, *podemos usar* $-7+4i$ *como quociente dessa divisão,*

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

*portanto,* $(1+2i)^3 \equiv i(\bmod 1+i)$.

É muito importante, para os resultados deste trabalho, ressaltarmos que a congruência modular em $\mathbb{Z}[i]$ é uma relação de equivalência pois é: reflexiva, simétrica e

transitiva.

**Propriedades: 5.** *Sejam* $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[i]$.

*i)* $\alpha \equiv \alpha(\bmod \gamma)$

*ii) Se* $\alpha \equiv \beta(\bmod \gamma)$, *então* $\beta \equiv \alpha(\bmod \gamma)$

*iii) Se* $\alpha \equiv \beta(\bmod \gamma)$ *e* $\beta \equiv \delta(\bmod \gamma)$, *então* $\alpha \equiv \delta(\bmod \gamma)$.

*Demonstração.* i) Temos que $\alpha - \alpha = 0$ e 0 é divisível por $\gamma$ ou seja, $\gamma|0$, que implica $\gamma|\alpha - \alpha$, pela definição de congruência $\alpha \equiv \alpha(\bmod \gamma)$.

ii) Como $\gamma|\alpha - \beta$ por hipótese, então existe $\kappa \in \mathbb{Z}[i]$ tal que $\alpha - \beta = \gamma\kappa$, somando $\beta - \alpha - \gamma\kappa$ em ambos os membros, temos que $-\gamma\kappa = \beta - \alpha$ que nos dá $\gamma(-\kappa) = \beta - \alpha$, assim $\gamma|\beta - \alpha$, pela definição de congruência, $\beta \equiv \alpha(\bmod \gamma)$.

iii) Por hipótese, se $\alpha \equiv \beta(\bmod \gamma)$ e $\beta \equiv \delta(\bmod \gamma)$, então $\gamma|\alpha - \beta$ e $\gamma|\beta - \delta$, respectivamente. Existem $\kappa_1, \kappa_2 \in \mathbb{Z}[i]$ tal que $\alpha - \beta = \gamma\kappa_1$ e $\beta - \delta = \gamma\kappa_2$, somando membro a membro as equações, temos

$$\begin{aligned} \alpha - \beta + \beta - \delta &= \gamma\kappa_1 + \gamma\kappa_2 \\ \alpha - \delta &= \gamma(\kappa_1 + \kappa_2) \end{aligned}$$

ou seja, $\gamma|\alpha - \delta$, pela definição de congruência, $\alpha \equiv \delta(\bmod \gamma)$.

□

Como vimos, a congruência módulo $\gamma \in \mathbb{Z}[i]$ é uma relação de equivalência, agrupando os inteiros gaussianos em classes de equivalência, chamadas de classes residuais módulo $\gamma$, indicadas por $\mathbb{Z}[i]/(\gamma)$.

**Definição 23.** *Sejam* $\alpha, \beta \in \mathbb{Z}[i]$. *Chamamos de classe residual* $\alpha$, *o conjunto*

$$\bar{\alpha} = \{\beta \in \mathbb{Z}[i]; \beta \equiv \alpha(\bmod \gamma)\}.$$

Em outras palavras, o conjunto das classes residuais módulo $\gamma$, indicado por $\mathbb{Z}[i]/(\gamma)$, é formado pelos restos da divisão de $\beta$ por $\gamma$, ou seja $\beta = \alpha + \gamma\eta$, para algum $\eta \in \mathbb{Z}[i]$, onde $0 \leq N(\alpha) < N(\gamma)$.

Em $\mathbb{Z}$, para construirmos a classe residual de algum número inteiro, é praticamente uma tarefa simples, já em $\mathbb{Z}[i]$ essa tarefa requer um pouco mais de atenção. Para $\gamma \in \mathbb{Z}[i]$, todos os elementos de uma classe residual têm o mesmo resto na divisão por $\gamma$, desde que na divisão o quociente e o resto sejam únicos.

Assim, enumerar as classes residuais é enumerar os possíveis restos na divisão por $\gamma$, portanto a quantidade de classes residuais de $\mathbb{Z}[i]/(\gamma)$ é finita, pois existe uma quantidade finita de elementos de $\mathbb{Z}[i]$ que possuem norma menor que $N(\gamma)$.

Para construirmos as classes residuais de $\mathbb{Z}[i]/(\gamma)$, é necessário levarmos em consideração que: ou a classe residual é formada pelos múltiplos de $\gamma$, ou pelos possíveis restos da divisão por $\gamma$. Para o primeiro caso, $\beta \equiv 0(\bmod \gamma)$ que é equivalente a dizer que $\beta = \gamma\eta$, para algum $\eta \in \mathbb{Z}[i]$. Se $\eta = a + bi$, então

$$\beta = \gamma(a + bi) = a\gamma + b(i\gamma),$$

ou seja, $\beta$ é uma combinação linear dos inteiros gaussianos $\gamma$ e $i\gamma$. Já no segundo caso, $\beta \equiv \alpha(\bmod \gamma)$ que implica em $\beta = \alpha + \gamma\eta$ para algum $\eta \in \mathbb{Z}[i]$ e $0 \leq N(\alpha) < N(\gamma)$. Como a norma é um número inteiro positivo, então pelo Principio da Boa Ordem, as possíveis normas de $\alpha$ são:

$$\begin{aligned}
N(\alpha) &= N(\gamma) - 1,\\
N(\alpha) &= N(\gamma) - 2,\\
N(\alpha) &= N(\gamma) - 3,\\
&\vdots\\
N(\alpha) &= 1,\\
N(\alpha) &= 0.
\end{aligned}$$

Portanto, o conjunto $\mathbb{Z}[i]/(\gamma)$ é finito e seus elementos são distintos. Vamos indicar o número de elementos de $\mathbb{Z}[i]/(\gamma)$ por $|\mathbb{Z}[i]/(\gamma)|$.

**Exemplo 51.** *Encontre as possíveis classes residuais de* $3 - i$ *ou seja, os elementos de* $\mathbb{Z}[i]/(3 - i)$.

*Como* $N(3 - i) = 10$*, temos as possíveis classes residuais:*

- $N(\alpha) = N(3-i) - 1 = 9$, $\alpha \in \{\pm 3, \pm 3i\}$;
- $N(\alpha) = N(3-i) - 2 = 8$, $\alpha \in \{\pm(2+2i), \pm(-2+2i)\}$;
- $N(\alpha) = N(3-i) - 3 = 7$, *não existe elemento em* $\mathbb{Z}[i]$ *com norma 7;*
- $N(\alpha) = N(3-i) - 4 = 6$, *não existe elemento em* $\mathbb{Z}[i]$ *com norma 6;*
- $N(\alpha) = N(3-i) - 5 = 5$, $\alpha \in \{\pm(1+2i), \pm(2+i), \pm(-1+2i), \pm(-2+i)\}$;
- $N(\alpha) = N(3-i) - 6 = 4$, $\alpha \in \{\pm 2, \pm 2i\}$;
- $N(\alpha) = N(3-i) - 7 = 3$, *não existe elemento em* $\mathbb{Z}[i]$ *com norma 3;*
- $N(\alpha) = N(3-i) - 8 = 2$, $\alpha \in \{\pm(1+i), \pm(-1+i)\}$;
- $N(\alpha) = N(3-i) - 9 = 1$, $\alpha \in \{\pm 1, \pm i\}$;
- $N(\alpha) = N(3-i) - 10 = 0$, $\alpha \in \{0\}$.

*Temos a princípio* 29 *classes residuais, mas, para considerarmos nessa contagem, temos que verificar quais são congruentes módulo* $3-i$. *Fazendo esta análise podemos constatar que:*

- $1 \equiv -3i \equiv -2+i (\mod 3-i)$, *pois* $1$, $-3i$ *e* $-2+i$ *pertencem a mesma classe residual;*
- $2 \equiv -2-2i \equiv -1+i (\mod 3-i)$, *pois* $2$, $-2-2i$ *e* $-1+i$ *pertencem a mesma classe residual;*
- $i \equiv -1-2i \equiv 3 (\mod 3-i)$, *pois* $i$, $-1-2i$ *e* $3$ *pertencem a mesma classe residual;*
- $1+i \equiv -2+2i \equiv -2i (\mod 3-i)$, *pois* $1+i$, $-2+2i$ *e* $-2i$ *pertencem a mesma classe residual;*
- $2+i \equiv -2-i \equiv -1+2i \equiv 1-2i (\mod 3-i)$, *pois* $2+i$, $-2-i$, $-1+2i$ *e* $1-2i$ *pertencem a mesma classe residual;*
- $-1-i \equiv 2-2i \equiv 2i (\mod 3-i)$, *pois* $-1-i$, $2-2i$ *e* $2i$ *pertencem a mesma classe residual;*

- $-i \equiv 1+2i \equiv -3 (\mod 3-i)$, *pois* $-i$, $1+2i$ *e* $-3$ *pertencem a mesma classe residual;*
- $-2 \equiv 2+2i \equiv 1-i (\mod 3-i)$, *pois* $-2$, $2+2i$ *e* $1-i$ *pertencem a mesma classe residual;*
- $-1 \equiv 3i \equiv 2-i (\mod 3-i)$, *pois* $-1$, $3i$ *e* $2-i$ *pertencem a mesma classe residual; e*
- $0$ *representa os múltiplos de* $3-i$.

*Portanto, ao invés de* 29 *classes, obtemos* 10 *classes disjuntas que são*

$$\overline{-(1+i)}, \overline{-2}, \overline{-i}, \overline{-1}, \overline{0}, \overline{1}, \overline{i}, \overline{2}, \overline{1+i}, \overline{2+i}.$$

*Assim,* $|\mathbb{Z}[i]/(3-i)| = 10$.

*Para enumerarmos cada classe residual, basta somarmos ou subtrairmos* $3-i$,

$\overline{-(1+i)} = \{..., -10+2i, -7+i, -4, -(1+i), 2-2i, 5-3i, 8-4i, ...\}$,

$\overline{-2} = \{..., -11+3i, -8+2i, -5+i, -2, 1-i, 4-2i, 7-3i, ...\}$,

$\overline{-i} = \{..., -9+2i, -6+i, -3, -i, 3-2i, 6-3i, 9-4i, ...\}$,

$\overline{-1} = \{..., -10+3i, -7+2i, -4+i, -1, 2-i, 5-2i, 8-3i, ...\}$,

$\overline{0} = \{..., -9+3i, -6+2i, -3+i, 0, 3-i, 6-2i, 9-3i, ...\}$,

$\overline{1} = \{..., -8+3i, -5+2i, -2+i, 1, 4-i, 7-2i, 10-3i, ...\}$,

$\overline{i} = \{..., -9+4i, -6+3i, -3+2i, i, 3, 6-i, 9-2i, ...\}$,

$\overline{2} = \{..., -7+3i, -4+2i, -1+i, 2, 5-i, 8-2i, 11-3i, ...\}$,

$\overline{1+i} = \{..., -8+4i, -5+3i, -2+2i, 1+i, 4, 7-i, 10-2i, ...\}$,

$\overline{2+i} = \{..., -7+4i, -4+3i, -1+2i, 2+i, 5, 8-i, 11-2i, ...\}$.

Uma outra maneira de analisarmos e obtermos as classes residuais módulo $\gamma \in \mathbb{Z}[i]$ é através de uma análise geométrica, onde esboçamos os múltiplos inteiros gaussianos no plano complexo.

**Exemplo 52.** *Geometricamente, quais as classes de* $\mathbb{Z}[i]/(3-i)$*?*
*Para* $\beta$ *múltiplo de* $3-i$ *temos* $\beta \equiv 0 (\mod 3-i)$, *então* $\exists\ \alpha = m+ni \in \mathbb{Z}[i]$ *tal que*

$$\begin{aligned}
\beta &= (3-i)(m+ni) \\
\beta &= (3-i)m + (3-i)ni \\
\beta &= (3-i)m + (1+3i)n,
\end{aligned}$$

*portanto, $\beta$ é a combinação linear dos vetores $(3,-1)$ e $(1,3)$.*

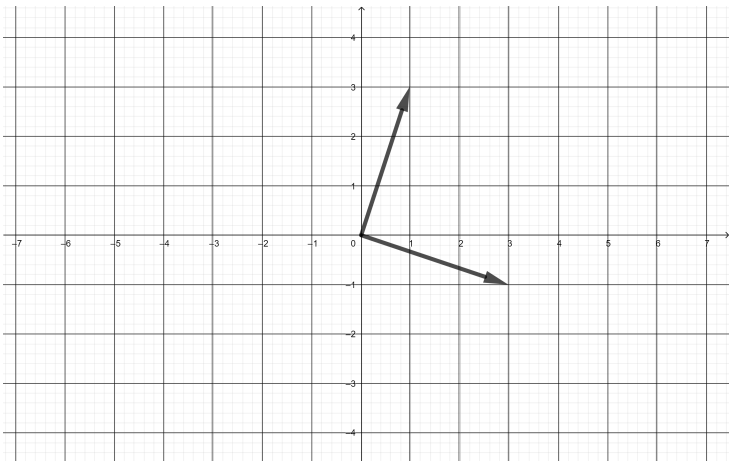

Figura 3.1: Vetores $3-i$ e $1+3i$

*Os múltiplos de $3-i$ são as combinações dos vetores da figura 3.1, produzindo a imagem da figura 3.2, onde o plano é "coberto"por quadrados, através dos múltiplos gaussianos de $3-i$, como vértices destes quadrados. Quando dizemos que inteiros gaussianos são congruentes, graficamente significa que eles estão na mesma posição relativa dentro dos diferentes quadrados da figura 3.2.*

*Observe que $2-i$ e $3+2i$ estão na mesma posição relativa dentro de um quadrado, portanto são congruentes módulo $3-i$, o que podemos verificar algebricamente se $2-i \equiv 3+2i(\bmod\ 3-i)$:*

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

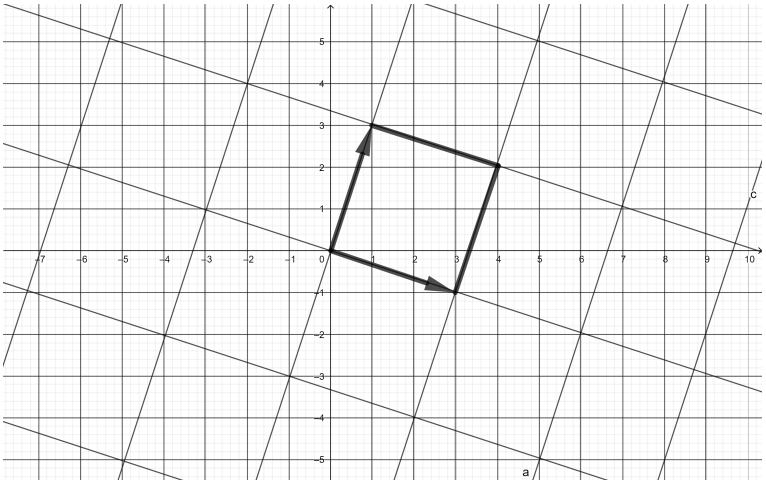

Figura 3.2: Múltiplos de $3-i$

*Observando a figura 3.3, os vértices dos quadrados são os múltiplos de* $3-i$*, por isso contamos só um dos vértices e cada ponto dentro desse quadrado é uma classe de equivalência módulo* $3-i$*. Portanto para* $3-i$ *temos* $10$ *classes residuais:* $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{1+i}$*,* $\overline{2+i}$*,* $\overline{3+i}$*,* $\overline{1+2i}$*,* $\overline{2+2i}$*,* $\overline{3+2i}$*, ou seja,* $|\mathbb{Z}[i]/(3-i)| = 10$*. Quaisquer outros inteiros gaussianos são congruentes a algum dos elementos de uma destas classes, visto que cada quadrado compartilha seus lados com quatro quadrados, cujo vértices são obtidos adicionando* $(3-i), -(3-i), (1+3i)$ *e* $-(1+3i)$*. Ou ainda, dado um quadrado, obtemos outro quadrado cujos vértices é um múltiplo de* $3-i$*.*

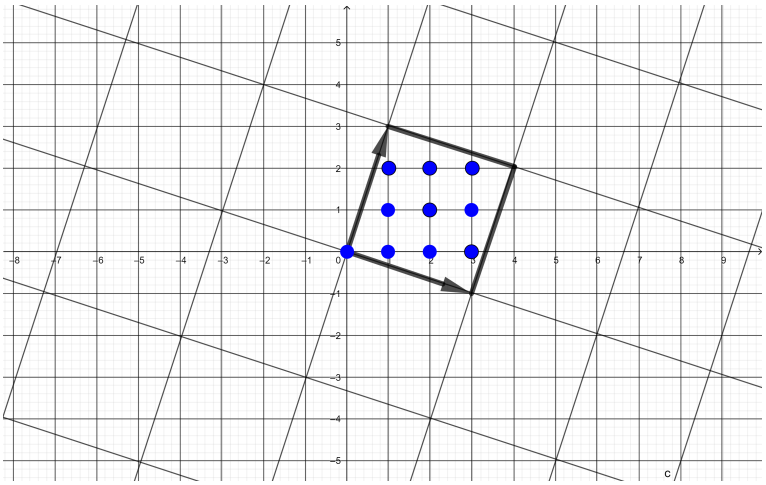

Figura 3.3: Classes residuais módulo $3-i$

**Exemplo 53.** *Quais as classes residuais de* $\mathbb{Z}[i]/(2-i)$*?*
*Para* $\beta$ *múltiplo de* $2-i$ *temos que* $\beta \equiv 0(\bmod\ 2-i)$*, então* $\exists\ \alpha = m+ni \in \mathbb{Z}[i]$ *tal que*

$$\begin{aligned}\beta &= (2-i)(m+ni)\\ \beta &= (2-i)m + (2-i)ni\\ \beta &= (2-i)m + (1+2i)n,\end{aligned}$$

*portanto,* $\beta$ *é a combinação linear dos vetores* $(2,-1)$ *e* $(1,2)$*.*

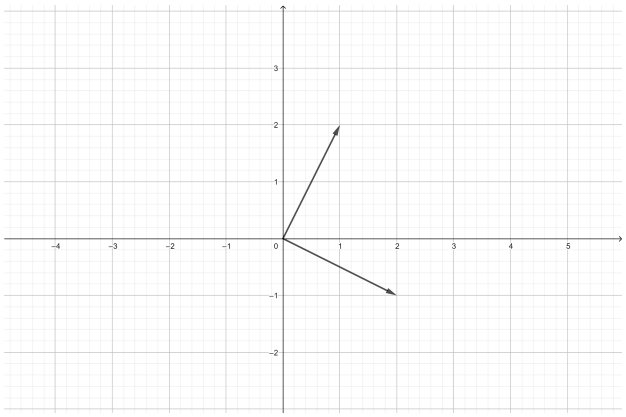


Figura 3.4: Vetores $2-i$ e $1+2i$

*Os múltiplos de* $2-i$ *são as combinações dos vetores figura 3.4, produzindo a imagem da figura 3.5, onde o plano é "coberto"por quadrados, através dos múltiplos gaussianos de* $2-i$*, como vértices destes quadrados. Quando dizemos que inteiros gaussianos são congruentes, graficamente significa que eles estão na mesma posição relativa dentro dos diferentes quadrados da figura 3.5.*

*Observe que* $1+i$ *e* $2+3i$ *estão na mesma posição relativa dentro de um quadrado, portanto são congruentes módulo* $2-i$*, o que podemos verificar algebricamente se* $1+i \equiv 2+3i(\bmod\ 2-i)$*:*

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

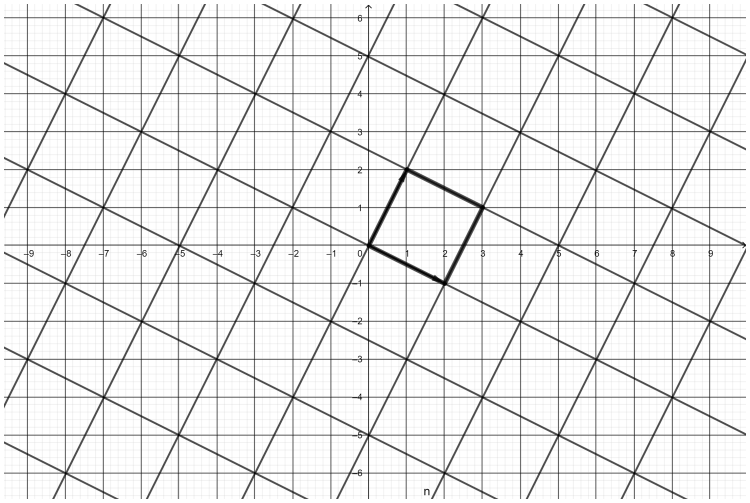

Figura 3.5: Múltiplos de $2 - i$

*Observando a figura 3.6, os vértices dos quadrados são os múltiplos de* $2 - i$*, por isso contamos só um dos vértices e cada ponto dentro desse quadrado é uma classe de equivalência módulo* $2-i$*. Portanto para* $2-i$ *temos 5 classes residuais:* $\overline{0}, \overline{1}, \overline{2}, \overline{1+i}, \overline{2+i}$*, ou seja,* $|\mathbb{Z}[i]/(2-i)| = 5$*. Quaisquer outros inteiros gaussianos são congruentes a algum dos elementos de uma destas classes, visto que cada quadrado compartilha seus lados com quatro quadrados, cujo vértices são obtidos adicionando* $(2-i), -(2-i), (1+2i)$ *e* $-(1+2i)$*. Ou ainda, dado um quadrado, obtemos outro quadrado cujos vértices é um múltiplo de* $2 - i$*.*

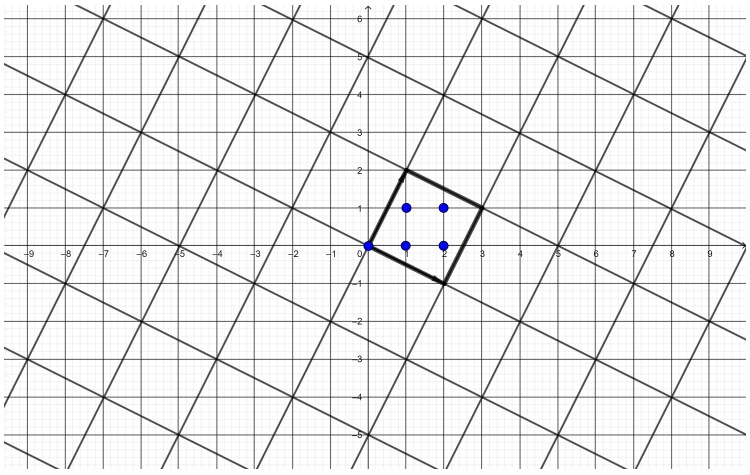

Figura 3.6: Classes residuais módulo $2 - i$

**Exemplo 54.** *Quantas classes residuais de* $\mathbb{Z}[i]/(2 + 2i)$*?*

*Para* $\beta$ *múltiplo de* $2+2i$*, temos que* $\beta \equiv 0(\bmod 2+2i)$*, então* $\exists \alpha = m+ni \in \mathbb{Z}[i]$

*tal que*

$$\beta = (2+2i)(m+ni)$$
$$\beta = (2+2i)m + (2+2i)ni$$
$$\beta = (2+2i)m + (-2+2i)n,$$

*portanto,* $\beta$ *é a combinação linear dos vetores* $(2,2)$ *e* $(-2,2)$*.*

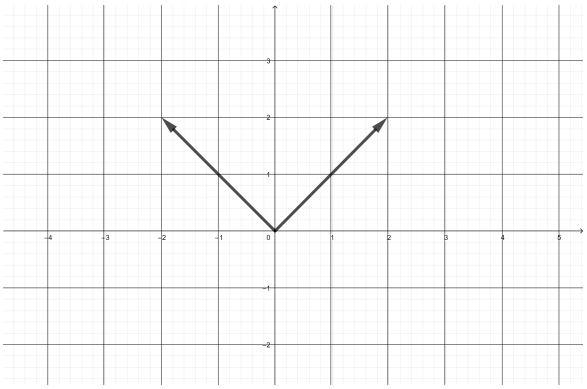

Figura 3.7: Vetores $2+2i$ e $-2+2i$

*Os múltiplos de* $2+2i$ *são as combinações dos vetores da Figura 3.7, produzindo a imagem da Figura 3.8 onde o plano é completado através dos múltiplos gaussianos de* $2+2i$*, como os vértices destes quadrados.*

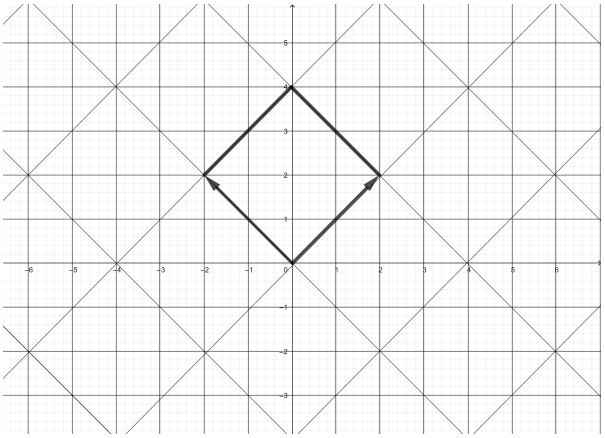

Figura 3.8: Múltiplos de $2+2i$

*Diferente do exemplo anterior, não haviam inteiros gaussianos nos lados dos quadrados. Então um conjunto de classes residuais módulo* $2+2i$ *são todos os inteiros gaussianos dentro de um quadrado e em dois lados adjacentes, contando apenas um vértice.*

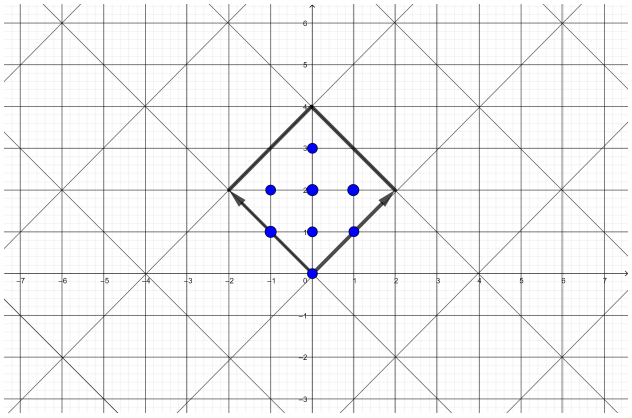

Figura 3.9: Classes residuais módulo $2+2i$

*Portanto,* $\mathbb{Z}[i]/(2+2i)$ *tem 8 classes residuais:* $\overline{0}, \overline{-1+i}, \overline{i}, \overline{1+i}, \overline{-1+2i}, \overline{2i}, \overline{1+2i}$ *e* $\overline{3i}$*. Quaisquer outros inteiros gaussianos são congruentes a algum destes números, logo* $|\mathbb{Z}[i]/(2+2i)| = 8$*.*

*Observe que* $2i$ *e* $6+4i$ *estão na mesma posição relativa no quadrado, então eles pertencem a mesma classe residual módulo* $2+2i$*.*

Vejamos algumas propriedades da aritmética modular em $\mathbb{Z}[i]$ que foram facilmente transportadas de $\mathbb{Z}$.

**Teorema 46.** *Se* $\pi$ *é primo em* $\mathbb{Z}[i]$*, então* $\alpha\beta \equiv 0(\bmod \pi)$ *se, e somente se* $\alpha \equiv 0(\bmod \pi)$ *ou* $\beta \equiv 0(\bmod \pi)$*.*

*Demonstração.* Como $\pi$ é primo e $\alpha\beta \equiv 0(\bmod \pi)$, então $\pi|\alpha\beta$, ou seja $\pi|\alpha$ ou $\pi|\beta$, em outras palavras, $\alpha \equiv 0(\bmod \pi)$ ou $\beta \equiv 0(\bmod \pi)$. Reciprocamente, se $\alpha \equiv 0(\bmod \pi)$, temos que $\alpha = \pi\kappa$ para algum $\kappa \in \mathbb{Z}[i]$, multiplicando essa equação por $\beta$, temos $\alpha\beta = \pi(\kappa\beta)$ portanto, $\pi|\alpha\beta$ e $\alpha\beta \equiv 0(\bmod \pi)$. Analogamente quando $\beta \equiv 0(\bmod \pi)$. □

**Teorema 47.** *Sejam* $\alpha, \beta \in \mathbb{Z}[i]$*, com* $\beta \neq 0$*. Então* $\alpha x \equiv 1(\bmod \beta)$ *tem solução se, e somente se* $mdc(\alpha, \beta) = 1$ *em* $\mathbb{Z}[i]$*. Se* $\alpha$ *e* $\beta$ *são relativamente primos, então* $\alpha x \equiv \gamma(\bmod \beta)$ *tem solução única* $x$*.*

*Demonstração.* Pela definição de congruência, $\beta|\alpha x - 1$ portanto, $\alpha x - 1 = \beta\gamma$ o que implica em $\alpha x + \beta(-\gamma) = 1$. Como o número 1 pode ser escrito como uma combinação linear de $\alpha$ e $\beta$ assim, $\alpha$ e $\beta$ são relativamente primos. Uma vez que $\alpha$ possui inverso

$(\mod \beta)$, multiplicamos a congruência pelo inverso de $\alpha(\mod \beta)$

$$\alpha'\alpha x \equiv \alpha'\gamma(\mod \beta)$$
$$x \equiv \alpha'\gamma(\mod \beta),$$

$x \equiv \alpha'\gamma(\mod \beta)$ é a solução única. □

**Exemplo 55.** $(1+5i)x \equiv 1(\mod 7+11i)$ *tem solução?*

*Para responder essa pergunta, precisamos verificar se* $1+5i$ *é relativamente primo a* $7+11i$*. Utilizando o algoritmo de Euclides temos que*

$$7+11i = (1+5i)(2-i)+(2i)$$
$$1+5i = (2i)(2-i)+(-1+i)$$
$$2i = (-1+i)(1-i)+0.$$

*Como* $mdc(1+5i, 7+11i) = -1+i$ *e seus associados, então não conseguiremos resolver esta equação.*

**Exemplo 56.** *Podemos resolver* $(5+3i)x \equiv 1(\mod 2-i)$*?*

*Vamos verificar se* $5+3i$ *é relativamente primo com* $2-i$*.*

$$5+3i = (2-i)(2+2i)+(-1+i)$$
$$2-i = (-1+i)(-2-i)+(-1)$$
$$(-1+i) = (-1)(1-i)+0,$$

*como o máximo divisor comum entre* $5+3i$ *e* $2-i$ *é* $-1$ *e seus associados, portanto são primos entre si. Agora vamos encontrar a solução para a equação utilizando o algoritmo*

*estendido de Euclides.*

$$\begin{aligned}
-1 &= (2-i) - (-1+i)(-2-i) \\
-1 &= (2-i) - [(5+3i) - (2-i)(2+2i)](-2-i) \\
-1 &= (2-i) - (5+3i)(-2-i) + (2-i)(2+2i)(-2-i) \\
-1 &= (2-i)[1 + (2+2i)(-2-i)] - (5+3i)(-2-i) \\
-1 &= (2-i)(-1-6i) - (5+3i)(-2-i) \\
1 &= (2-i)(1+6i) + (5+3i)(-2-i)
\end{aligned}$$

*Então a solução* $x = -2 - i$.

**Corolário 48.** *Seja* $\pi$ *um primo gaussiano. Cada* $\alpha \not\equiv 0(\bmod \pi)$ *tem um inverso multiplicativo módulo* $\pi$ *e qualquer congruência polinomial*

$$C_n x^n + C_{n-1}x^{n-1} + ... + C_1 x + C_0 \equiv 0(\bmod \pi)$$

*onde* $C_i \in \mathbb{Z}[i]$ *e* $C_n \not\equiv 0(\bmod \pi)$*, tem no máximo* $n$ *soluções módulo* $\pi$.

*Demonstração.* Como $\pi$ é um primo gaussiano, qualquer $\alpha \in \mathbb{Z}[i]$, onde $\alpha \not\equiv 0(\bmod \pi)$, então podemos dizer que $\pi$ é relativamente primo como $\alpha$, portanto para cada $\alpha$, existe um inteiro gaussiano que é inverso de $\alpha(\bmod \pi)$, pelo Teorema 47. Assim, como todo elemento de $\mathbb{Z}[i]/(\pi)$, com exceção do 0, possui inverso em $\mathbb{Z}[i]$, então $\mathbb{Z}[i]/(\pi)$ é um corpo. Portanto, este corolário é um caso especial, quando polinômios de grau $n$, tem no máximo $n$ raízes. □

Ao fazermos as congruências com inteiros gaussianos, nos deixa a dúvida se as congruências que são válidas em $\mathbb{Z}$, deixam de existir em $\mathbb{Z}[i]$. Porém, o Teorema a seguir nos garante que não.

**Teorema 49.** *Para* $a, b$ *e* $c \in \mathbb{Z}$*,* $a \equiv b(\bmod c)$ *em* $\mathbb{Z}$ *se, e somente se* $a \equiv b(\bmod c)$ *em* $\mathbb{Z}[i]$.

*Demonstração.* Reescrevendo o Teorema em termos de divisibilidade, temos

$$c|(a-b) \text{ em } \mathbb{Z} \rightarrow c|(a-b) \text{ em } \mathbb{Z}[i].$$

Pelo Teorema 24, a divisibilidade dos inteiros não muda quando se trabalha em $\mathbb{Z}[i]$. Portanto, $a \equiv b(\bmod c)$ em $\mathbb{Z}$ se, e somente se $a \equiv b(\bmod c)$ em $\mathbb{Z}[i]$. □

## 3.2 Pequeno Teorema de Fermat

Até agora, a aritmética modular em $\mathbb{Z}[i]$ tem o comportamento parecido com $\mathbb{Z}$, mas quando tratamos do Pequeno Teorema de Fermat, não é tão simples assim. Em $\mathbb{Z}$, se $p$ é primo e $a \not\equiv 0(\bmod p)$, então $a^{p-1} \equiv 1(\bmod p)$. Em $\mathbb{Z}[i]$ não podemos estender naturalmente o Pequeno Teorema de Fermat. De fato, para o primo $\pi = 3$ em $\mathbb{Z}[i]$ e $\alpha = i$, temos

$$\alpha \not\equiv 0(\bmod \pi) \text{ e } \alpha^{\pi-1} = i^2 = -1 \not\equiv 1(\bmod 3).$$

Vamos nos inspirar na prova do Pequeno Teorema de Fermat em $\mathbb{Z}$ e ver como apareceu a potência $a^{p-1}$: comparando os dois conjuntos $\{1, 2, 3, ..., p-1\}$ e $\{1 \cdot a, 2 \cdot a, 3 \cdot a, ..., (p-1) \cdot a\}$, com $mdc(a, p) = 1$. Temos que o produto, $(p-1)!$, dos elementos de cada conjunto é congruente módulo $p$, cancelando o fator comum, obtemos que $a^{p-1} \equiv 1(\bmod p)$. Logo, a origem de $a^{p-1}$ vem do fato de que existem $p-1$ fatores não nulos módulo $p$, ou seja, o expoente de $a^{p-1}$ é o número de elementos não-nulos módulo $p$. Logo, o número de classes residuais distintas não-nulas módulo $p$ é $p-1$. Assim, podemos ter o Pequeno Teorema de Fermat em $\mathbb{Z}[i]$.

**Teorema 50.** *Seja $\pi$ um primo gaussiano e $n(\pi) = |\mathbb{Z}[i]/(\pi)|$ o número de classes residuais módulo $\pi$. Se $\alpha \not\equiv 0(\bmod \pi)$ para $\alpha \in \mathbb{Z}[i]$, então $\alpha^{n(\pi)-1} \equiv 1(\bmod \pi)$.*

*Demonstração.* Seja $\mathbb{Z}[i]/(\pi)$ o conjunto das classes residuais módulo $\pi$. Como $n(\pi)$ é o número de inteiros gaussianos módulo $\pi$, então $\mathbb{Z}[i]/(\pi)$ é formado pelas $n(\pi)$ classes residuais distintas $\beta_1, \beta_2, ..., \beta_{n(\pi)-1}, \beta_{n(\pi)}$ onde $\beta_{n(\pi)} = 0$. Consideremos agora a sequência $\alpha\beta_1, \alpha\beta_2, ..., \alpha\beta_{n(\pi)-1}$. Suponha que $\alpha\beta_i \equiv \alpha\beta_j(\bmod \pi)$ para algum $i$ e $j$ inteiros. Ao multiplicarmos essa congruência pelo inverso de $\alpha(\bmod \pi)$ (é possível pois $\alpha \not\equiv 0(\bmod \pi)$) temos que $\beta_i \equiv \beta_j(\bmod \pi)$, o que é um absurdo, pois são classes residuais distintas, portanto $\alpha\beta_1, \alpha\beta_2, ..., \alpha\beta_{n(\pi)-1}$ também é um conjunto de classes residuais módulo $\pi$. Assim ao multiplicarmos as classes residuais congruentes diferentes de 0, mantemos a congruência, temos então

$$\beta_1 \cdot \beta_2 \cdot ... \cdot \beta_{n(\pi)-1} \equiv (\alpha\beta_1) \cdot (\alpha\beta_2) \cdot ... \cdot (\alpha\beta_{n(\pi)-1})(\bmod \pi)$$
$$\beta_1 \cdot \beta_2 \cdot ... \cdot \beta_{n(\pi)-1} \equiv \alpha^{n(\pi)-1}(\beta_1 \cdot \beta_2 \cdot ... \cdot \beta_{n(\pi)-1})(\bmod \pi)$$

Como cada $\beta_i$ é diferente de zero módulo $\pi$ podemos cancelá-los em ambos os lados da congruência, pois $\pi$ é um primo gaussiano e $mdc(\pi, \beta_i) = 1$, temos que

$$1 \equiv \alpha^{n(\pi)-1}(\mod \pi),$$

assim,

$$\alpha^{n(\pi)-1} \equiv 1(\mod \pi).$$

□

Vamos apresentar uma maneira de calcular $n(\pi)$.

**Lema 51.** *Se $x \neq 0$ em $\mathbb{Z}$, então $n(x) = x^2$.*

*Demonstração.* Sabemos que um inteiro gaussiano $a + bi$ é divisível por $x$ quando $x|a$ e $x|b$. Assim sendo, vimos que $a + bi \equiv c + di(\mod x)$ se, e somente se $a \equiv c(\mod x)$ e $b \equiv d(\mod x)$. Portanto, o número de classes residuais incongruentes módulo $x$ é igual a $x \cdot x = x^2$. □

**Lema 52.** *Se $\gamma \neq 0$ em $\mathbb{Z}[i]$, então $n(\gamma) = n(\overline{\gamma})$.*

*Demonstração.* Sabemos que para $\alpha, \beta, \gamma \in \mathbb{Z}[i]$, se $\alpha \equiv \beta(\mod \gamma)$, então $\overline{\alpha} \equiv \overline{\beta}(\mod \gamma)$. De fato, se $\alpha \equiv \beta(\mod \gamma)$, então $\gamma|\alpha - \beta$, daí $\alpha - \beta = \delta\gamma$ para algum $\gamma \in \mathbb{Z}[i]$. Por conjugação, temos $\overline{\alpha - \beta} = \overline{\delta\gamma}$, então $\overline{\alpha} - \overline{\beta} = \overline{\delta}\overline{\gamma}$, portanto $\overline{\alpha} \equiv \overline{\beta}(\mod \gamma)$.

Assim, o número de classes residuais módulo $\gamma$ é igual ao número de classes residuais módulo $\overline{\gamma}$, ou seja, $n(\gamma) = n(\overline{\gamma})$. □

**Lema 53.** *Se $\alpha, \beta \in \mathbb{Z}[i]$, diferentes de zero, então $n(\alpha\beta) = n(\alpha)n(\beta)$.*

*Demonstração.* Seja $x_1, x_2, ..., x_r$ o conjunto das classes residuais módulo $\alpha$ e $y_1, y_2, ..., y_s$ o conjunto das classes residuais módulo $\beta$, então $n(\alpha) = r$ e $n(\beta) = s$. Dado qualquer $z \in \mathbb{Z}[i]$, temos que $z \equiv x_i(\mod \alpha)$, para algum $i$. Assim, $z - x_i = \alpha t$, para $t \in \mathbb{Z}[i]$, e $t \equiv y_j(\mod \beta)$ para algum $j$. Escrevendo $t - y_j = \beta w$ para algum $w \in \mathbb{Z}[i]$, então $t = y_j + \beta w$. Substituindo a segunda equação na primeira, temos

$$z = \alpha t + x_i = \alpha(y_j + \beta w) + x_i = x_i + \alpha y_j + \alpha\beta w \equiv x_i + \alpha y_j(\mod \alpha\beta).$$

Assim os $r \cdot s$ números $x_i + \alpha y_j$ são um conjunto de classes residuais módulo $\alpha\beta$. Precisamos mostrar que as classes são disjuntas. Suponha que $x_i + \alpha y_j \equiv x_{i'} + \alpha y_{j'} (\bmod \alpha\beta)$ [1], vamos mostrar que $i = i'$ e $j = j'$. Reduzindo ambos os lados módulo $\alpha$, $x_i \equiv x_{i'} (\bmod \alpha)$. Como os $x$'são classes residuais módulo $\alpha$, disjuntas, então $x_i = x_{i'}$, ou seja $i = i'$. Agora subtraímos $x_i$ em ambos os lados da equação [1], então $\alpha y_j \equiv \alpha y_{j'} (\bmod \alpha\beta)$, agora dividindo por $\alpha$ toda a congruência, temos que $y_j \equiv y_{j'} (\bmod \beta)$. Como os $y$'s são classes residuais módulo $\beta$, disjuntas, então $y_j = y_{j'}$, ou seja $j = j'$. Portanto, $n(\alpha\beta) = r \cdot s = n(\alpha)n(\beta)$. □

Podemos verificar essas propriedades geometricamente, pelos exemplos a seguir.

**Exemplo 57.** *Calcule o número de classes residuais módulo* 2.

$2(m+ni) = 2m+2in$, *são os múltiplos de* 2. *Podemos formar um quadrado com os vetores* $(2,0)$ *e* $(0,2)$.

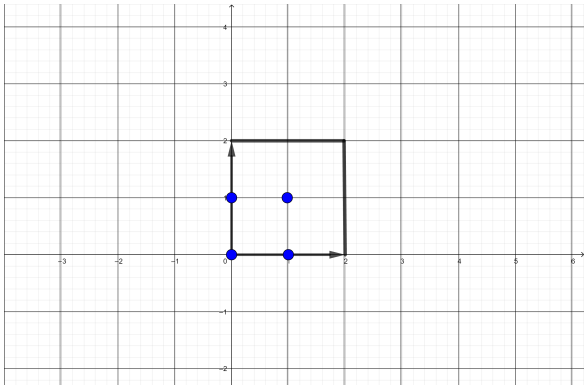

Figura 3.10: Classes residuais módulo 2

*O conjunto de representantes módulo* 2, *é formado a partir dos inteiros gaussianos dentro e no quadrado. Usando apenas um dos vértices e dois lados adjacentes, pois os outros vértices e lados são congruentes, temos* 4 *representantes:* $\overline{0}, \overline{1}, \overline{i}$ *e* $\overline{1+i}$.

*Portanto,* $n(2) = 4 = 2^2$.

**Exemplo 58.** *Calcule o número de classes residuais módulo* $\alpha = -2+1$ *e de* $\overline{\alpha} = -2-i$, *seu conjugado.*

$(-2+i)(m+ni) = (-2+i)m+(-1-2i)n$, *são os múltiplos de* $-2+i$. *Podemos formar um quadrado com os vetores* $(-2,1)$ *e* $(-1,-2)$.

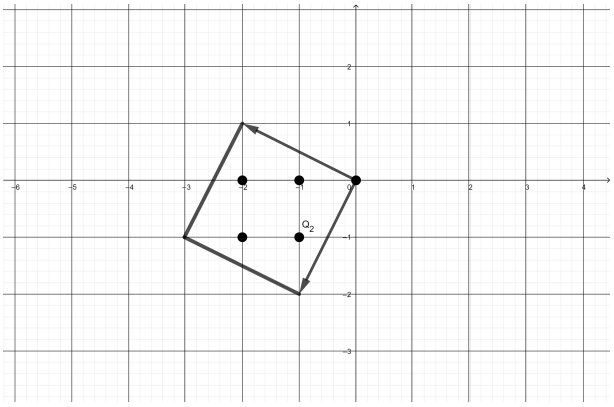

Figura 3.11: Classes residuais módulo $-2+i$

$(-2-i)(m+ni) = (-2-i)m + (1-2i)n$, *são os múltiplos de* $-2-i$. *Podemos formar um quadrado com os vetores* $(-2,-1)$ *e* $(1,-2)$.

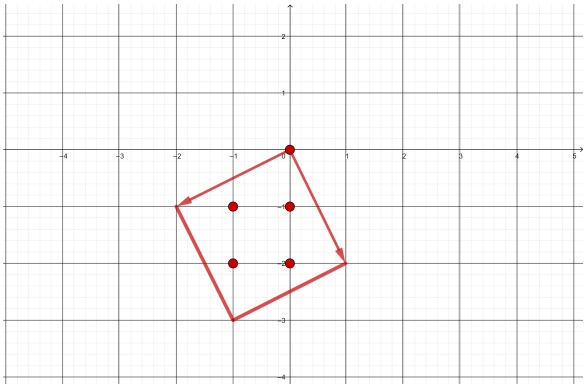

Figura 3.12: Classes residuais módulo $-2-i$

*O conjunto de representantes módulo* $-2+i$, *é formado a partir dos inteiros gaussianos dentro e no quadrado. Usando apenas um dos vértices,temos* 5 *representantes:* $\overline{0}, \overline{-1}, \overline{-2}, \overline{-1-i}$ *e* $\overline{-2-i}$ *e o conjunto de representantes módulo* $-2-i$, *é formado a partir dos inteiros gaussianos dentro e no quadrado. Usando apenas um dos vértices, pois os outros são congruentes, temos* 5 *representantes:* $\overline{0}, \overline{-i}, \overline{-2i}, \overline{-1-i}$ *e* $\overline{-1-2i}$.

*Portanto,* $n(\alpha) = 5 = n(\overline{\alpha})$.

**Exemplo 59.** *Calcule o número de classes residuais módulo* $\alpha\beta$, *onde* $\alpha = 3$ *e* $\beta = -2+i$.

$\alpha\beta = (3)(-2+i) = -6+3i$

$(-6+3i)(m+ni) = (-6+3i)m + (-3-6i)n$, *são os múltiplos de* $-6+3i$. *Podemos formar um quadrado com os vetores* $(-6,3)$ *e* $(-3,-6)$.

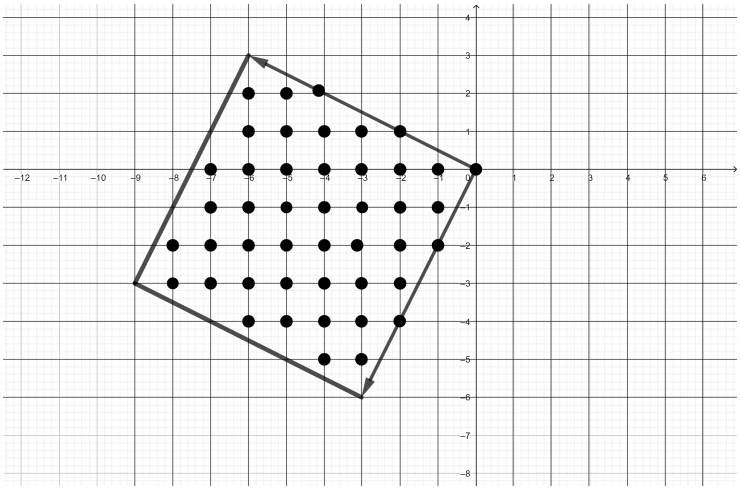

Figura 3.13: Classes residuais módulo $-6+3i$

*O conjunto de representantes módulo* $-6+3i$*, é formado a partir dos inteiros gaussianos dentro e no quadrado. Usando apenas um dos vértices e dois lados adjacentes, temos* 45 *representantes.*

*Portanto,* $n(\alpha\beta) = 45 = 9 \cdot 5 = n(\alpha)n(\beta)$

Agora temos condições de construir uma fórmula para calcularmos a quantidade de classes residuais módulo $\alpha$.

**Teorema 54.** *Se* $\alpha \neq 0$ *em* $\mathbb{Z}[i]$*, então* $n(\alpha) = N(\alpha)$*, ou seja, o número de elementos de* $\mathbb{Z}[i]/(\alpha)$ *é* $N(\alpha)$*.*

*Demonstração.* Note que $n(\alpha\overline{\alpha}) = n(\alpha)n(\overline{\alpha})$ (Pelo Lema 53). Então $n(\alpha\overline{\alpha}) = n(\alpha)n(\alpha) = n(\alpha)^2$ (Pelo Lema 52). Como $\alpha\overline{\alpha} = N(\alpha) \in \mathbb{Z}$, então $n(\alpha\overline{\alpha}) = n(N(\alpha)) = N(\alpha)^2$ (Pelo Lema 51). Portanto, $n(\alpha)^2 = N(\alpha)^2$, ou seja, $n(\alpha) = N(\alpha)$.

□

Essa fórmula nos permite calcular o número de elementos de $\mathbb{Z}[i]/(\alpha)$ sem listar todos os representantes das classes residuais módulo $\alpha$.

**Exemplo 60.** *Calcule a quantidade de representantes da classe residual módulo* $3+2i$*.*

*Como vimos, basta calcularmos* $N(3+2i) = 3^2 + 2^2 = 9 + 4 = 13$*. Portanto,* $\mathbb{Z}[i]/(3+2i)$ *tem* 13 *classes residuais distintas.*

Com o Teorema 54, podemos dar um novo formato para o Pequeno Teorema de Fermat.

**Corolário 55.** *Seja $\pi$ um primo gaussiano e $\alpha \not\equiv 0(\bmod \pi)$, então*

$$\alpha^{N(\pi)-1} \equiv 1(\bmod \pi).$$

Vejamos agora alguns exemplos aplicando este importante resultado para os Inteiros Gaussianos.

**Exemplo 61.** *Para $\pi = 3$ primo em $\mathbb{Z}[i]$. O conjunto das classes residuais módulo 3 é $\mathbb{Z}[i]/(3)$. Temos $N(3) = 3^2 = 9$ classes residuais.*

$\mathbb{Z}[i]/(3) = \{\overline{0}, \overline{1}, \overline{2}, \overline{i}, \overline{1+i}, \overline{2+i}, \overline{2i}, \overline{1+2i}, \overline{2+2i}\}$.

$\forall \alpha \neq 0 \in \mathbb{Z}[i]/(3)$, $\alpha^8 \equiv 1(\bmod 3)$. *Se $\alpha = i$, então $i^8 = 1 \equiv 1(\bmod 3)$.*

**Exemplo 62.** *Calcule o resto da divisão de $(7+4i)^{157}$ por $7-2i$.*

*Como $7-2i$ é primo e $7+4i \not\equiv 0(\bmod 7-2i)$, pois*

$$\frac{7+4i}{7-2i}\frac{(7+2i)}{(7+2i)} = \frac{41+42i}{53} = \frac{41}{53} + \frac{42}{53}i \notin \mathbb{Z}[i].$$

*Pelo Pequeno Teorema de Fermat,*

$$(7+4i)^{N(7-2i)-1} \equiv 1(\ \bmod 7-2i)$$
$$(7+4i)^{53-1} = (7+4i)^{52} \equiv 1(\ \bmod 7-2i)$$

*Elevando por 3 em ambos os lados da congruência, temos*

$$((7+4i)^{52})^3 \equiv 1^3(\ \bmod 7-2i)$$
$$(7+4i)^{156} \equiv 1(\ \bmod 7-2i)$$

*Como $7+4i \equiv 6i(\bmod 7-2i)$, multiplicando as duas congruências*

$$(7+4i)^{156} \cdot (7+4i) \equiv 1 \cdot 6i(\ \bmod 7-2i)$$
$$(7+4i)^{157} \equiv 6i(\ \bmod 7-2i).$$

*Portanto o resto da divisão de $(7+4i)^{157}$ por $7+2i$ é $6i$.*

**Exemplo 63.** *Mostre que $(4+5i)^{37} + (4-7i)^{56} \equiv 0(\bmod 2+i)$.*

*Como* $2+i$ *é primo e* $4+5i \not\equiv 0(\bmod 2+i)$ *e* $4-7i \not\equiv 0(\bmod 2+i)$*, pelo Pequeno Teorema de Fermat, temos*

$$\begin{aligned}(4+5i)^{N(2+i)-1} &\equiv 1(\bmod 2+i)\\ (4+5i)^{5-1} = (4+5i)^4 &\equiv 1(\bmod 2+i)\\ ((4+5i)^4)^9 &\equiv 1^9(\bmod 2+i)\\ (4+5i)^{36} &\equiv 1(\bmod 2+i)\\ (4+5i)^{36}\cdot(4+5i) &\equiv 1\cdot(4+5i)(\bmod 2+i)\\ (4+5i)^{37} &\equiv (4+5i)(\bmod 2+i)\end{aligned}$$

*e*

$$\begin{aligned}(4-7i)^{N(2+i)-1} &\equiv 1(\bmod 2+i)\\ (4-7i)^{5-1} = (4-7i)^4 &\equiv 1(\bmod 2+i)\\ ((4-7i)^4)^{14} &\equiv 1^{14}(\bmod 2+i)\\ (4-7i)^{56} &\equiv 1(\bmod 2+i)\end{aligned}$$

*Somando as congruências,*

$$\begin{aligned}(4+5i)^{37}+(4-7i)^{56} &\equiv (4+5i)+1(\bmod 2+i)\\ &\equiv 5+5i \equiv 0(\bmod 2+i).\end{aligned}$$

*De fato* $5+5i \equiv 0(\bmod 2+i)$*, pois*

$$\frac{5+5i}{2+i}\frac{(2-i)}{(2-i)} = \frac{15+5i}{5} = 3+i \in \mathbb{Z}[i].$$

*Portanto,* $(4+5i)^{37}+(4-7i)^{56} \equiv 0(\bmod 2+i)$.

## 3.3 Função $\phi$ de Euler

A função $\phi$ de Euler em $\mathbb{Z}$ conta o número de inteiros $k$ maiores que 1 e menores que $n$, que são relativamente primos com $n$. Já vimos anteriormente que $\phi(n) = |\{k \in \mathbb{Z} : 1 < k < n, mdc(k,n) = 1\}|$, ou seja, o número de elementos invertíveis

módulo $n$, que vamos indicar por $\phi(n) = |U(\mathbb{Z}_n)|$. Sabemos também que não podemos comparar inteiros gaussianos. Para dar significado a função $\phi$ em $\mathbb{Z}[i]$, vamos considerar $\alpha = a+bi$, $\alpha \neq 0$ e olhar para $\phi(\alpha) = \phi(a+bi)$ como sendo o número de inteiros gaussianos que são invertíveis módulo $\alpha$.

**Definição 24.** *Para cada $\alpha \in \mathbb{Z}[i]$ com $\alpha \neq 0$, definimos o número de elementos invertíveis módulo $\alpha$ por $|U(\mathbb{Z}[i]_\alpha)|$. Assim, $\phi(\alpha) = |\,U(\mathbb{Z}[i]/(\alpha))| = |U(\mathbb{Z}[i]_\alpha)|$.*

**Observação 7.** *Quando $\alpha = \pi$ é primo em $\mathbb{Z}[i]$, todo inteiro gaussiano $\beta$ diferente de zero é invertível módulo $\pi$, logo*

$$\phi(\pi) = |U(\mathbb{Z}[i]/(\pi))| = N(\pi) - 1.$$

*De fato, como $\mathbb{Z}[i]/(\pi)$ tem $N(\pi)$ classes residuais módulo $\pi$, mas ao retirarmos a classe do zero, ficam apenas com $N(\pi) - 1$ classes residuais dos inteiros gaussianos invertíveis módulo $\pi$.*

**Exemplo 64.** *Seja $2 + i$ primo em $\mathbb{Z}[i]$, então $\phi(2 + i) = N(2 + i) - 1 = 5 - 1 = 4$.*

**Exemplo 65.** *Seja $7 - 2i$ primo em $\mathbb{Z}[i]$, então $\phi(7 - 2i) = N(7 - 2i) - 1 = 53 - 1 = 52$.*

Devemos tomar cuidado quando estamos com a função $\phi$ em $\mathbb{Z}[i]$, pois ela pode não ser igual a função $\phi$ em $\mathbb{Z}$. Por exemplo, $\phi(3) = 2$ em $\mathbb{Z}$, mas em $\mathbb{Z}[i]$, $\phi(3) = 8$.

Podemos calcular também a quantidade de classes residuais invertíveis módulo $\mu$, onde $\mu$ é um número gaussiano composto. Para isso, precisaremos verificar se em $\mathbb{Z}[i]$, vale as propriedades da multiplicatividade e da potência, as quais valem em $\mathbb{Z}$.

**Teorema 56.** *Para $\alpha$, $\beta \in \mathbb{Z}[i]$ e $mdc(\alpha, \beta) = 1$, então $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$.*

*Demonstração.* Sejam $\alpha, \beta \in \mathbb{Z}[i]$ com $\alpha$ e $\beta$ relativamente primos. Pelo Teorema 34:

$$\begin{aligned}
\phi(\alpha\beta) &= |U(\mathbb{Z}[i]/(\alpha\beta))| \\
&= |U(\mathbb{Z}[i]/(\alpha)) \times U(\mathbb{Z}[i]/(\beta))| \\
&= |U(\mathbb{Z}[i]/(\alpha))|\,|U(\mathbb{Z}[i]/(\beta))| \\
&= \phi(\alpha)\phi(\beta).
\end{aligned}$$

□

Sendo esta função multiplicativa podemos encontrar uma fórmula para a função $\phi$ em $\mathbb{Z}[i]$.

**Teorema 57.** *Se $\pi$ é um primo gaussiano, então $\phi(\pi^k) = N(\pi)^k \left(1 - \frac{1}{N(\pi)}\right)$.*

*Demonstração.* Para fazermos esta prova, devemos considerar dois casos:

Caso 1: $\pi = a + bi$, onde $a$ e $b$ são diferentes de zero.

Pelo Teorema 54, $n(\pi^k) = N(\pi^k)$, como a Norma é multiplicativa $N(\pi^k) = N(\pi)^k$, isso nos diz que o número de inteiros gaussianos módulo $\pi^k$ é $N(\pi)^k$. Para calcularmos $\phi(\pi^k)$, devemos subtrair desse conjunto todos os elementos que não são invertíveis módulo $\pi^k$. Ou seja, devemos subtrair todos os elementos que dividem $\pi^k$. Pelo Teorema 26, sabemos que se para algum $\alpha \in \mathbb{Z}[i]$, $\alpha | \pi^k$, então $N(\alpha) | N(\pi^k)$. Pelo Teorema 45, $N(\pi)$ deve ser primo em $\mathbb{Z}$. Então os únicos divisores de $N(\pi)^k$ são $1, N(\pi), N(\pi)^2, ..., N(\pi)^{k-1}(N(\pi))$. Existem $N(\pi)^{k-1}$ desses divisores. Então

$$\begin{aligned}\phi(\pi^k) &= N(\pi)^k - N(\pi)^{k-1} \\ &= N(\pi)^k \left(1 - \frac{1}{N(\pi)}\right).\end{aligned}$$

Caso 2: Seja $\pi = ua$, onde $u \in \{-1, 1, -i, i\}$ e $a$ é um primo ímpar em $\mathbb{Z}[i]$, tal que $a \equiv 3 (\text{ mod } 4)$.

Pelo Teorema 54, $n(\pi^k) = N(\pi^k)$, como a função Norma é multiplicativa $N(\pi^k) = N(\pi)^k$. Então o total de inteiros gaussianos módulo $\pi^k$ é $N(\pi)^k = N(ua)^k = (N(u)N(a))^k = (a^2)^k$. Como no caso anterior, devemos subtrair todos os inteiros que não são relativamente primos a $a^{2k}$. Como $a$ é um número primo, os únicos divisores de $a^{2k}$ são $a^2, a^3, ..., (a^2)^{k-1}(a^2)$. Existem $(a^2)^{k-1}$ desses divisores. Então

$$\begin{aligned}\phi(\pi^k) &= (a^2)^k - (a^2)^{k-1} \\ &= N(\pi)^k - N(\pi)^{k-1} \\ &= N(\pi)^k \left(1 - \frac{1}{N(\pi)}\right) \\ &= N(\pi^k) \left(1 - \frac{1}{N(\pi)}\right).\end{aligned}$$

□

Agora, podemos calcular a função $\phi$ de Euler para quaisquer inteiros gaussianos.

**Teorema 58.** *Seja $\mu$ inteiro gaussiano diferente de zero,*

$$\phi(\mu) = N(\mu)\prod_{\pi|\mu}\left(1-\frac{1}{N(\pi)}\right).$$

*Demonstração.* Se $\mu$ for primo, já temos o resultado na Observação 7, $\phi(\mu) = N(\mu) - 1$. Se não, $\mu$ pode ser escrito como um produto de fatores primos, ou seja, $\mu = \pi_1^{r_1}\pi_2^{r_2}...\pi_n^{r_n}$. Então,

$$\phi(\mu) = \phi(\pi_1^{r_1}\pi_2^{r_2}...\pi_n^{r_n}).$$

Como $\phi$ é multiplicativa, pelo Teorema 56, temos

$$\phi(\mu) = \phi(\pi_1^{r_1})\phi(\pi_2^{r_2})...\phi(\pi_n^{r_n}).$$

Agora, pelo Teorema 57

$$\phi(\mu) = N(\pi_1^{r_1})\left(1-\frac{1}{N(\pi_1)}\right)N(\pi_2^{r_2})\left(1-\frac{1}{N(\pi_2)}\right)...N(\pi_n^{r_n})\left(1-\frac{1}{N(\pi_n)}\right)$$
$$\phi(\mu) = N(\pi_1^{r_1})N(\pi_2^{r_2})...N(\pi_n^{r_n})\left(1-\frac{1}{N(\pi_1)}\right)\left(1-\frac{1}{N(\pi_2)}\right)...\left(1-\frac{1}{N(\pi_n)}\right)$$

Como os $n$ primeiros termos multiplicados é $N(\mu)$, então

$$\phi(\mu) = N(\pi_1^{r_1}\pi_2^{r_2}...\pi_n^{r_n})\left(1-\frac{1}{N(\pi_1)}\right)\left(1-\frac{1}{N(\pi_2)}\right)...\left(1-\frac{1}{N(\pi_n)}\right)$$
$$\phi(\mu) = N(\mu)\prod_{\pi|\mu}\left(1-\frac{1}{N(\pi)}\right)$$

□

**Exemplo 66.** *Considere $\alpha = 24 + 23i$. Ao fazermos a fatoração de $\alpha$ em primos gaussianos. $N(\alpha) = 24^2 + 23^2 = 576 + 529 = 1105$. Fatorando o número $1105 = 5 \cdot 13 \cdot 17$. Podemos escrever $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$ e $17 = 1^2 + 4^2$.*

*Os inteiros gaussianos com norma 5 são $1 + 2i$ e $1 - 2i$*

*Os inteiros gaussianos com norma 13 são $2 + 3i$ e $2 - 3i$*

*Os inteiros gaussianos com norma 17 são $1 + 4i$ e $1 - 4i$*

*Então a fatoração de* $\alpha = 24 + 23i = (1 + 2i)(2 + 3i)(1 - 4i)$. *Usando a fórmula pra obtermos* $\phi(\alpha)$,

$$\begin{aligned}
\phi(\alpha) &= \phi(24 + 23i) \\
&= N(24 + 23i)\left(1 - \frac{1}{N(1 + 2i)}\right)\left(1 - \frac{1}{N(2 + 3i)}\right)\left(1 - \frac{1}{N(1 - 4i)}\right) \\
&= 1105\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{17}\right) \\
&= 1105\left(\frac{4}{5}\right)\left(\frac{12}{13}\right)\left(\frac{16}{17}\right) \\
&= 1105\left(\frac{768}{1105}\right) \\
&= 768.
\end{aligned}$$

**Exemplo 67.** *Quantas classes residuais invertíveis módulo* $3 + 4i$ *existem?*

*Basta calcularmos* $\phi(3 + 4i)$. *Como* $N(3 + 4i) = 25 = 5 \cdot 5$, *podemos escrever* $5 = 2^2 + 1^2$, *então* $3 + 4i = (2 + i)^2$. *Assim,*

$$\begin{aligned}
\phi(3 + 4i) &= \phi((2 + i)^2) \\
&= N(2 + i)^2\left(1 - \frac{1}{N(2 + i)}\right) \\
&= 5^2\left(1 - \frac{1}{5}\right) \\
&= 25 \cdot \frac{4}{5} \\
&= 20.
\end{aligned}$$

*Portanto, existem 20 elementos invertíveis módulo* $3 + 4i$.

**Exemplo 68.** *Calcule* $\phi(5)$.

*A fatoração em primos é* $5 = (1+2i)(1-2i)$. *Como* $1+2i$ *e* $1-2i$ *são relativamente*

*primos, então*

$$\begin{aligned}\phi(5) &= \phi((1+2i)(1-2i)) \\ &= \phi(1+2i)\phi(1-2i) \\ &= (N(1+2i)-1)(N(1-2i)-1) \\ &= (5-1)(5-1) \\ &= 16.\end{aligned}$$

**Teorema 59.** *(Teorema de Euler) Sejam $\alpha$ e $\mu$ inteiros gaussianos e $mdc(\alpha,\mu)=1$, então*

$$\alpha^{\phi(\mu)} \equiv 1(\bmod\ \mu).$$

*Demonstração.* Seja $U(\mathbb{Z}[i]/(\mu)) = \{\mu_1, \mu_2, ..., \mu_{\phi(\mu)}\}$ o conjunto das classes residuais invertíveis módulo $\mu$, então $U(\mathbb{Z}[i]/(\mu))$ possui $\phi(\mu)$ elementos. Consideremos agora a sequência $\alpha\mu_1, \alpha\mu_2, ..., \alpha\mu_{\phi(\mu)}$. Suponha que $\alpha\mu_i \equiv \alpha\mu_j(\bmod\ \mu)$ para algum $i$ e $j$ inteiros. Como $mdc(\alpha,\mu)=1$, então $\alpha$ é invertível módulo $\mu$ (Teorema 47). Multiplicando a congruência pelo inverso de $\alpha$ módulo $\mu$, temos que $\mu_i \equiv \mu_j(\bmod\ \mu)$, o que é um absurdo, pois são classes residuais distintas módulo $\mu$, portanto, $\alpha\mu_1, \alpha\mu_2, ..., \alpha\mu_{\phi(\mu)}$ é um conjunto de classes residuais módulo $\mu$. Como $mdc(\mu_i,\mu)=1$ e $mdc(\alpha,\mu)=1$, então $mdc(\alpha\mu_i,\mu)=1$ (Teorema 34). Portanto, $\alpha\mu_1, \alpha\mu_2, ..., \alpha\mu_{\phi(\mu)}$ é também um conjunto das classes residuais invertíveis módulo $\mu$. Cada $\alpha\mu_i$ deve ser congruente a um único elemento de $U(\mathbb{Z}[i]/(\mu))$ módulo $\mu$, temos então a multiplicação desses elementos

$$\begin{aligned}\alpha\mu_1\alpha\mu_2...\alpha\mu_{\phi(\mu)} &\equiv \mu_1\mu_2...\mu_{\phi(\mu)}(\bmod\ \mu) \\ \alpha^{\phi(\mu)}\mu_1\mu_2...\mu_{\phi(\mu)} &\equiv \mu_1\mu_2...\mu_{\phi(\mu)}(\bmod\ \mu)\end{aligned}$$

Como $\mu_i$ e $\mu$ são relativamente primos, podemos fazer o cancelamento em ambos os lados da congruência. Portanto,

$$\alpha^{\phi(\mu)} \equiv 1(\bmod\ \mu).$$

□

O Teorema de Euler é uma generalização do Pequeno Teorema de Fermat, pois

quando $\mu = \pi$ primo, temos que $\alpha^{\phi(\pi)} \equiv 1(\bmod \pi) \Leftrightarrow \alpha^{N(\pi)-1} \equiv 1(\bmod \pi)$.

**Exemplo 69.** *Calcule o resto da divisão de* $(7+4i)^{401}$ *por* $-2+2i$.

*Como* $-2+2i$ *não é um primo gaussiano, podemos escrevê-lo como um produto de primos, então* $-2+2i = (1+i)^3$. *Como* $mdc(7+4i, -2+2i) = 1$, *então podemos utilizar o Teorema de Euler. Vamos calcular* $\phi(-2+2i)$*:*

$$\begin{aligned}
\phi(-2+2i) &= \phi((1+i)^3) \\
&= N(1+i)^3 \left(1 - \frac{1}{N(1+i)}\right) \\
&= 2^3 \left(1 - \frac{1}{2}\right) \\
&= \frac{8}{2} \\
&= 4.
\end{aligned}$$

*Então,*

$$\begin{aligned}
(7+4i)^{\phi(-2+2i)} &\equiv 1(\mod -2+2i) \\
(7+4i)^4 &\equiv 1(\mod -2+2i).
\end{aligned}$$

*Elevando a congruência a* 100*, temos*

$$(7+4i)^{400} \equiv 1(\mod -2+2i),$$

*multiplicando por* $7+4i$ *a congruência*

$$(7+4i)^{401} \equiv 7+4i(\mod -2+2i)$$

*Como* $N(7+4i) > N(-2+2i)$*, podemos fazer a redução de* $7+4i$ *módulo* $-2+2i$*,*

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

*Portanto,* $(7+4i)^{401} \equiv -1(\bmod -2+2i)$.

# Considerações finais

.

Ao fazermos a extensão do Pequeno Teorema de Fermat e da função e teorema de Euler sobre $\mathbb{Z}[i]$, observamos que a função norma cumpre um papel essencial para o objetivo desse trabalho. No Pequeno Teorema de Fermat em $\mathbb{Z}$, o $p$ não é apenas um número primo, mas sim a quantidade de classes residuais módulo $p$. Porém, em $\mathbb{Z}[i]$, a função norma é quem fornece o número de classes residuais módulo $\pi$ e não o número primo $\pi$. Já para a função e teorema de Euler a função norma é necessária para obtermos o números de classes residuais invertíveis módulo $\alpha \in \mathbb{Z}[i]$.

Para a demonstração do teorema de Euler, foi necessário utilizarmos as propriedades multiplicativas e a da potência de um número primo para a função $\phi$, já que podemos aplicá-lo para quaisquer inteiros gaussianos $\alpha, \mu \in \mathbb{Z}[i]$ desde que $\alpha$ e $\mu$ sejam relativamente primos. Ou seja, se $\mu$ for um número primo, então basta aplicar o Pequeno Teorema de Fermat, caso contrário este número será composto, podendo ser decomposto em fatores de primos. Daí pudemos perceber que em $\mathbb{Z}[i]$ temos dois tipos de números primos: aqueles que são primos em $\mathbb{Z}$ e $\mathbb{Z}[i]$, como o número 3 e aqueles que são primos gaussianos da forma $a + bi$. Por isso foi necessário a demonstração da função $\phi$ para estes dois casos. E por fim, assim como na prova do Pequeno Teorema de Fermat em $\mathbb{Z}[i]$, na prova do Teorema de Euler utilizamos argumentos parecidos.

Enfatizamos que a Teoria do Números, ou seja, a Aritmética dos Inteiros é um assunto fundamental para o professor que atua na Educação Básica, porque os inteiros constituem o alicerce para o bom entendimento das operações básicas e propriedades operacionais dos números, mesmo no conjunto dos Reais. Então entender mais aprofundadamente a Aritmética dos Inteiros ajuda o professor da Educação Básica a entender e a saber explicar e justificar de onde vem vários resultados importantes como o Algoritmo da Divisão de Euclides e o Teorema da Fatoração Única. Por isso, esse trabalho constitui

um material didático para que os que se interessam em aprofundar-se na Aritmética dos Inteiros, através do estudo dos Inteiros Gaussianos.

Enfim, encerramos este trabalho com o desejo de aprofundar mais na teoria dos inteiros de Gauss e buscar ideias e práticas para que possamos aplicá-las, a fim de contribuir de maneira significativa em sala de aula, assim como contribuiu para minha formação como professor.

# Referências Bibliográficas


Araújo, M. C. (2017). Notas de aula de teoria elementar dos números ii - 2018.

Campos Filho, L. F. M. (2014). Algumas propriedades dos inteiros de gauss.

Conrad, K. (2008). The gaussian integers. *Pre-Print, paper edition*.

de Oliveira Santos, J. P. (2007). *Introdução à teoria dos números*. Instituto Nacional de Matemática Pura e Aplicada.

Hefez, A. (2006). *Elementos de aritmética*. Sociedade Brasileira de Matemática.

Hefez, A. (2016). Aritmética. In *Coleção PROFMAT*, página 298p. Sociedade Brasileira de Matemática, 2nd edição.

May, C. A. (2015). Application of the euler phi function in the set of gaussian integers.

Piffer, A. M. (2014). Aplicações da função de euler.

Roberson, M. (2016). Extension and generalization of fermats little theorem to the gaussian integers.

Rosen, K. H. (2011). *Elementary Number Theory: and Its Applications*. Pearson Education, 5th edição.

Stein, R. G. (1976). Exploring the gaussian integers. *The Two-Year College Mathematics Journal*, 7(4):4–10.

# Apêndice: Material adicional

.

## A.1 Os Princípios da Boa Ordem e da Indução Finita

$A_0$ **Princípio da Boa Ordem (PBO)**: Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.

$A_1$ **Primeira forma do Princípio da Indução Finita**: Seja $B$ um subconjunto de inteiros positivos. Se $B$ possui as duas propriedades

i) $1 \in B$

ii) $k+1 \in B$ sempre que $k \in B$

então $B$ contém todos os inteiros positivos.

$A_2$ **Segunda forma do Princípio de Indução Finita**: Seja $B$ um subconjunto dos inteiros positivos. Se $B$ possui as duas seguintes propriedades

i) $1 \in B$

ii) $k+1 \in B$ sempre que $1, 2, ..., k \in B$

então $B$ contém todos os inteiros positivos.