UNIVERSIDADE DO ESTADO DO AMAZONAS
ESCOLA NORMAL SUPERIOR
LICENCIATURA EM MATEMÁTICA

ELIAS DA SILVA LIMA

INTEIROS GAUSSIANOS: UMA ABORDAGEM INTRODUTÓRIA AOS ASPECTOS ARITMÉTICOS COMPARADOS AO CONJUNTO DOS INTEIROS.

MANAUS, MARÇO
2023

ELIAS DA SILVA LIMA

INTEIROS GAUSSIANOS: UMA ABORDAGEM INTRODUTÓRIA AOS ASPECTOS ARITMÉTICOS COMPARADOS AO CONJUNTO DOS INTEIROS.

Trabalho de conclusão de curso elaborado junto às disciplinas TCC I e TCC II do curso de Licenciatura em Matemática da Universidade do Estado do Amazonas para obtenção do grau de Licenciado em Matemática.

Orientador: Prof. Dr. Almir Cunha da Graça Neto

MANAUS, MARÇO
2023

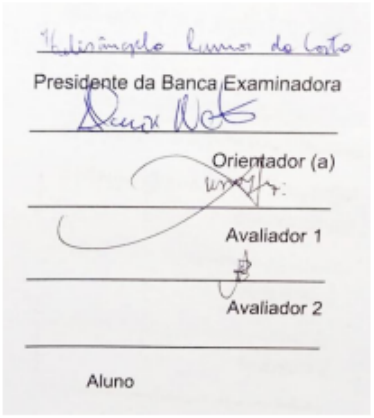
FOLHA DE APROVAÇÃO

TERMO DE APROVAÇÃO DE TRABALHO DE CONCLUSÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA DA UNIVERSIDADE DO ESTADO DO AMAZONAS

Ata de Defesa do Trabalho de Conclusão de Curso em Licenciatura em Matemática da Escola Normal Superior-UEA de **ELIAS DA SILVA LIMA.**

Em 16 de março de 2023, às 19:10h, na Sala Maria Clara Dantas da Escola Normal Superior da UEA na presença da Banca Examinadora composta pelos professores: Dr. Almir Cunha da Graça Neto, Me. Alessandro Monteiro de Menezes e Me. Alexandra Salerno Pinheiro, o aluno **ELIAS DA SILVA LIMA** apresentou o Trabalho de Conclusão do Curso intitulado: "**INTEIROS GAUSSIANOS: UMA ABORDAGEM INTRODUTÓRIA AOS ASPECTOS ARITMÉTICOS COMPARADOS AO CONJUNTO DOS INTEIROS"** A Banca Examinadora deliberou e decidiu pela APROVAÇÃO do referido trabalho, com o conceito 9,4 divulgando o resultado ao aluno e demais presentes.

Manaus, 16 de março de 2023.



AGRADECIMENTOS

Agradeço primeiramente a Deus pela força e foco para está concluindo mais uma etapa acadêmica, mediante as provações encontradas neste período.

Agradeço ao orientador Prof. Dr. Almir Cunha da Graça Neto pela a oportunidade de realizar a pesquisa sobre suas orientações, desde a apresentação da temática da pesquisa até os esclarecimentos dos conteúdos. Agradeço também, à Prof. Me. Helisângela Ramos da Costa que orientou sobre as formatações, estrutura e escrita da pesquisa. De forma geral, a todos os professores que poderam compartilhar de suas habilidades e conhecimento nesse período acadêmico.

Aos familiares que sempre estão ao meu lado e poderam mais uma vez me ajudar durante essa etapa. Agradeço as amizades que fiz durante essa etapa da vida, amigos que me auxiliaram e ajudam até os dias atuais.

Lista de Tabelas

Lista de Figuras

RESUMO

Nesta pesquisa, é apresentado o conjunto dos Inteiros Gaussianos com um embasamento comparativo ao conjunto dos números inteiros. Assim, o objetivo da pesquisa é compreender o conjunto dos Inteiros Gaussianos apresentado propriedades aritméticas da teoria dos números por meio de uma analogia com o conjunto dos Inteiros. Foi abordado os conjuntos e conceitos necessários para a compreensão dos Inteiros Gaussianos assim como seus contextos históricos. Por meio de uma descrição comparativa, a pesquisa apresenta os aspectos relacionados à divisibilidade, aos números primos e ao algoritmo da divisão.

Palavras chves: Inteiros Gaussianos. Inteiros. Teoria dos números. Primos Gaussianos. Algoritmo da Divisão.

Sumário

Introdução

Desde muito cedo, no ensino básico temos o contato direto com o conjunto dos números Inteiros, em que é apresentada sua estrutura e as operações. No nível superior, outros resultados podem ser obtidos para o conjunto dos inteiros no ramo da Teoria dos Números.

Ainda no ensino básico, é introduzido o conjunto dos números complexos em que é apresentando sua definição e propriedades. No nível superior pode ser explorado um subconjunto dos complexos chamado de Inteiros Gaussianos em que há uma associação aritmética entre os Inteiros e os Complexos.

Desse modo, as aplicações dos aspectos aritméticos dos Inteiros em outros arranjos numéricos apresentam resultados semelhantes, em especial nos inteiros Gaussianos. Para compreender a comparação entre os dois conjuntos, foi delimitado o estudo dos aspectos aritméticos da teoria dos números, na qual se trabalhou os seguintes aspectos; Divisibilidade, Números Primos e Algoritmo da Divisão.

Este trabalho, dispõe como objetivo geral compreender o conjunto dos Inteiros Gaussianos e propriedades aritméticas através de uma analogia com as propriedades aritméticas dos números Inteiros. Destaca-se; apresentar os contextos históricos dos conjuntos; verificar as propriedades de divisibilidade dos inteiros e demonstrar propriedades análogas para os Inteiros Gaussianos; definir as unidades e associados dos Inteiros Gaussianos; definir os Primos Gaussianos, a partir da noção existente de números primos no conjunto dos Inteiros; e por fim demonstrar o algoritmo da divisão nos Inteiros Gaussiano.

Construída em três capítulos, a pesquisa segue uma maneira investigativa e motivadora a acadêmicos, buscando fundamentos alinhados a teoria aritmética dos números e seguindo o rigor matemático, foram apresentadas as definições, teoremas e demonstrações, alinhados a uma construção exemplificativa dos Inteiros Gaussianos.

No capítulo 1, trata dos aspectos históricos e preliminares, no qual é apresentado um contexto histórico sobre o matemático Carl Friedrich Gauss (1777-1855) em termos de biografia, prosseguindo é mencionado sobre os conjuntos que foram abordados no trabalho assim como, propriedades e definições importantes como caráter prévio.

O capítulo 2, compreende a metodologia da pesquisa, em que este se estabe-

lece o caminho que foi percorrido para a construção da pesquisa, de acordo com os parâmetros metodológicos apresentando sua abordagem, estratégia e procedimento no qual a pesquisa foi construída.

No capítulo 3, é então apresentado os aspectos aritméticos que foram delimitados para a analogia entre os Inteiros e os Inteiros Gaussianos com suas definições, propriedades e demonstrações, seguindo de uma estrutura lógica que facilite a comparação entre os mesmos, isto é, cada seção do capítulo trata de um aspecto aritmético e o mesmo é apresentado de forma sequenciada em ambos conjuntos.

Para o apoio referencial da pesquisa destaca-se os autores; (SANTOS, 2020), (BOYER, 1996), (ROSEN, 2011), (HEFEZ, 2002), (MARTINEZ, 2018).

Capítulo 1

Aspectos históricos e preliminares

1.1 Carl Friedrich Gauss

Intitulado por muitos como o príncipe da Matemática, o Alemão Carl Friedrich Gauss (1777-1855) foi um dos mais renomados contribuintes para o desenvolvimento do mundo científico pois o mesmo se destacava em diversas áreas através de suas pesquisas e resultados publicados. Desde cedo, assim afirmam historiadores, que o mesmo foi capaz de deduzir a fórmula da soma de n termos de uma progressão aritmética(PA), e relatos afirmam que ele aprendeu a calcular antes mesmo de aprender a ler e que com apenas 3 anos de idade foi capaz de encontrar erros nos cálculos de seu pai(BOYER, 1996).

De família humilde, com 14 anos Gauss foi apresentado ao Duque de Brunswick que financiou seus estudos e pesquisas, e assim em outubro de 1795 ingressou no ensino superior no qual antes mesmo dos 25 anos já era famoso como matemático e astrônomo. Ainda na sua fase de estudante, dentre as suas descobertas as que mais se destacaram foi justamente a do método dos mínimos quadrados e a prova da reciprocidade quadrática na teoria dos números. Dispondo suas descobertas em um diário em que o mesmo continha vários trabalhos e pensamentos que nem mesmo haviam sido publicados(BOYER, 1996).

Durante um processo rápido, Gauss ingressou na universidade de Helmstadt na qual lhe foi concedido o doutorado no ano de 1798, que tinha como tese o enunciado que hoje conhecemos como o teorema fundamental da álgebra, fornecendo que em toda equação polinomial P(z) tem pelo menos uma raiz, independentemente

dos coeficientes serem reais ou imaginários. Inicialmente sua prova foi mediante a considerações geométricas e que anos depois chegou a publicar outras 3 formas de demonstração do teorema (BOYER, 1996).

Não deixando de lado, o trabalho mais significante de Gauss com o tratado em especial a teoria dos números é o de seu livro **Disquisitiones arithmeticae**, em que por meio dessa enorme contribuição novos conceitos foram introduzidos a teoria dos números como a de congruência, que fornece uma classe de equivalência (BOYER, 1996).

As seções seguintes, foi introduzido os conjuntos que serão retratados no decorrer da pesquisa com seus conceitos e propriedades importantes para o contexto das futuras demonstrações(a palavra inteiros estará se referindo ao conjunto dos inteiros).

1.2 Teoria dos números

É notório que o mundo em que vivemos está rodeado por números e que os mesmos são de suma importância para o desenvolvimento e andamento do meio social. Dando o foco a uma das ramificações da Matemática, a Teoria dos números é o ramo que se dedica a estudar as propriedades aritméticas e estruturas dos conjuntos numéricos em especial os números inteiros, em que apresentam uma gama de trabalhos desenvolvidos ao longo dos tempos que foram de fundamental importância para o avanço intelectual e tecnológico do mundo, em que a aplicação em relação ao uso dos resultado de números primos na área da criptografia (GALDINNO, 2014).

Ao lado da geometria euclidiana a teoria dos números é um dos ramos mais antigos da Matemática, que em especial Euclides nos seus volumes os **Elementos** destina os quatro primeiros capítulos a esse tema e com a desenvoltura de futuros trabalhos desenvolvidos (BERTONE, 2014).

A teoria dos números, está consolidada e dividida em três área, Teoria Elementar, Teoria analítica e Teoria Algébrica. A pesquisa está alinhada a Teoria Elementar, por conta dos seus aspectos apresentados em cima de resultados elementares como divisibilidade, números primos e algoritmo da divisão. E ao longo do tempo os problemas propostos dentro desse ramo matemático, vem desafiando seus pesquisadores, uma vez que a complexidade na resolução dos mesmos não depende somente do trato

algébrico, e sim de uma interdisciplinaridade entre diferentes áreas como a análise, geometria e outras formas de imaginação para resolver tal problema (SANTOS, 2020).

1.3 Conjunto dos Inteiros $\mathbb{Z}$

Os números Inteiros[1] ou apenas Inteiros são os elementos naturais e simétricos, ou seja:

$$\cdots -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4, \ldots$$

cujo conjunto é denotado por $\mathbb{Z}$, isto é:

$$\mathbb{Z} = \{\ldots, -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4, \ldots\}.$$

Dispondo das propriedades dos Inteiros, é importante ressaltar que esse conjunto é fechado sobre a adição, subtração e multiplicação, ou seja, ao efetuar algumas dessas três operações entre inteiros, o resultado ainda é um inteiro. E é importante também relembrar algumas definições que serão utilizadas mais à frente.

Definição 1.3.1. *Chama-se valor absoluto de um Inteiro a, o inteiro que se indica por $|a|$ e tal que:*

$$|a| = \begin{cases} a, & se \quad a \geq 0 \\ -a, & se \quad a < 0. \end{cases}$$

Esta definição tem como interpretação geométrica; o valor absoluto ou módulo de um número a, denotado por $|a|$, que indica a distância de a até a origem 0 na reta real. Vejamos alguns exemplos:

- $|13| = 13$
- $|-8| = 8$
- $|-22| = 22.$

[1] As definições estão de acordo com (FILHO, 1981)

Outra definição será importante para determinar alguns resultados mais adiante.

Definição 1.3.2. [2]*Seja $x \in \mathbb{R}$, definimos piso ou parte inteira de x denotado por $\lfloor x \rfloor$ como sendo o único $k \in \mathbb{Z}$ tal que $k \leq x < k+1$. Definimos o teto de x, denotado por $\lceil x \rceil$, como sendo o único $k \in \mathbb{Z}$ tal que $k-1 < x \leq k$.*

Exemplo 1. *Determinar o piso e o teto de $\sqrt{3}$.*

Solução: Pela definição, para determinar o piso temos que encontrar um inteiro k, de maneira que, $k \leq \sqrt{3} < k+1$. Uma vez que $\sqrt{3} \approx 1,73$, o único valor possível pa k é 1, desse modo, $\lfloor \sqrt{3} \rfloor = 1$. Para determinar o teto, devemos encontrar um inteiro k tal que $k-1 < \sqrt{3} \leq k$, nesse caso o único valor possível é $k = 2$. Logo $\lceil \sqrt{3} \rceil = 2$.

Exemplo 2. *Determinar o piso e o teto de π.*

Solução: Pela definição, para determinar o piso temos que encontrar um inteiro k, de maneira que, $k \leq \pi < k+1$. Uma vez que $\pi \approx 3,14$, o único valor possível pa k é 3, desse modo, $\lfloor \pi \rfloor = 3$. Para determinar o teto, devemos encontrar um inteiro k tal que $k-1 < \pi \leq k$, nesse caso o único valor possível é $k = 4$. Logo $\lceil \pi \rceil = 4$.

1.4 Conjunto dos complexos $\mathbb{C}$

Tendo hoje suas aplicações nas mais variadas áreas, os números complexos no início apareceram pela tentativa de soluções de equações quadráticas, isto é, por volta do século XVI equações que admitiam como solução a raiz quadrada de um número negativo, não havia solução.

Com os estudos a respeito dessas soluções, o matemático Niccolò Fontana(1500-1557), mais conhecido como Tartaglia, tendo sido desafiado na época a resolver equações do terceiro grau desenvolveu tal método para as suas soluções. Consequentemente, outro contribuidor da época Girolamo Cardano(1501-1576), ficou sabendo que havia soluções para tais equações e com isso pediu a Tartaglia que ensinase o método utilizado, após insistir bastante e prometer não divulgar tal método, Tartaglia cedeu a Cardano o método de resolução e não cumprindo com o trato de divulgar, Cardano divulgou o método para equações do terceiro grau somente mencionado Tartaglia, tendo assim como se ele mesmo tivesse desenvolvido tal método,

[2]A definição é de acordo com (MARTINEZ, 2018)

pegando os créditos pela resolução e assim é conhecido até hoje como “Fórmula de Cardano”(ROONEY, 2012).

> Logo após aparecerem as soluções das equações cúbicas e quadráticas Cardano-Tartaglia, o matemático Rafael Bombelli (c. 1526-72) tornou-se o primeiro a calcular usando números complexos (números complexos são aqueles que envolvem a $\sqrt{-1}$, i).
> Trabalhando com raízes cúbicas, ele desenvolveu equações que usavam raízes imaginárias como palco na derivação de soluções finais que são números reais. Ele a descreveu como “pensamento selvagem” e elas não ajudaram de fato seus cálculos, mas sinalizaram para importância que os números complexos teriam para álgebra no futuro.(ROONEY, 2012, p.138)

Simbolicamente foi o ilustre matemático Leonhard Euler(1707-1783) , que introduziu ao imaginário o símbolo para a representação da $\sqrt{-1}$, ou seja, a letra i. Segundo essa definição para o imaginário, Euler foi capaz de visualizar a própria forma de um complexo já que existe a parte real, logo imaginou-se um número na forma $z = x + yi$ para o qual x e y são números reais e $i^2 = -1$.

Porém, essa representação só foi aceita justamente quando Gauss a publicou, e com suas contribuições para o novo número, juntamente com os estudos de Caspar Wessel(1745-1818) sobre a representação geométrica do número e publicada por Jean Argand(1768-1822), Gauss retomou as ideias apresentadas por eles e intensificou os estudos introduzindo o termo números complexos e dando um conforto para os matemáticos a respeito desses números, isto é, agora poderá visualizar o imaginário, de acordo com sua representação por coordenadas no plano que hoje leva o nome de Argand-Gauss(ROONEY, 2012).

> No nível mais elementar, é interessante observar que a representação dos complexos foi descoberta em 1797 por Caspar Wessel(1745-1818) e publicada nas atas da academia dinamarquesa de 1798; mas o trabalho de Wessel ficou praticamente ignorado, daí usualmente hoje ser o plano dos complexos chamado o plano de Gauss, embora Gauss só publicasse sua idéia 30 anos mais tarde.(ROONEY, 2012, p.350)

Essa descoberta, como citado acima, abriu portas para trabalhos importantes na álgebra e consequentemente para outras aplicações e soluções de equações polinomiais e suas derivações. Após esse contexto, formalizando a construção do conjunto dos complexos[3] temos:

[3]As definições e propriedades para o conjunto dos complexos estão de acordo com (IEZZI, 2013)

Seja $\mathbb{R}$ o conjunto dos números reais. Considerando o produto cartesiano $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$:

$$\mathbb{R}^2 = \{(x,\ y) | \quad x \in \mathbb{R} \quad e \quad y \in \mathbb{R}\}.$$

Isto é, $\mathbb{R}^2$ é o conjunto dos pares ordenados $(x,\ y)$ em que x e y são números reais.

Vamos tomar dois elementos, $(a,\ b)$ e $(c,\ d)$, de $\mathbb{R}^2$ para dar três definições importantíssimas:

1. **Igualdade:** dois pares ordenados são iguais se, e somente se, apresentarem primeiros termos iguais e segundos termos iguais:

$$(a,\ b) = (c,\ d) \iff a = c\ e\ b = d.$$

2. **Adição:** chama-se soma de dois pares ordenados a um novo par ordenado cujos primeiro e segundo termos são, respectivamente, a soma dos primeiros e a soma dos segundos termos dos pares dados:

$$(a,\ b) + (c,\ d) = (a + c,\ b + d).$$

3. **Multiplicação:** chama-se produto de dois pares ordenados a um novo par ordenado cujo primeiro termo é a diferença entre o produto dos primeiros termos e o produto dos segundos termos dos pares dados e o segundo termos é a soma dos produtos do primeiro termo de cada par dado pelo segundo termo do outro:

$$(a,\ b) \cdot (c,\ d) = (ac - bd,\ ad + bc).$$

A partir dessa relação podemos definir o conjunto dos complexos:

Definição 1.4.1. *Chama-se conjunto dos números complexos, e representa-se por $\mathbb{C}$, o conjunto dos pares ordenados de números reais para os quais estão definidas a igualdade, adição e multiplicação.*

É usual representar-se cada elemento $(x,\ y) \in \mathbb{C}$, com o símbolo z, portanto:

$$z \in \mathbb{C} \iff z = (x,\ y),\ sendo\ x, y \in \mathbb{R}.$$

Chamamos unidade imaginária e indicamos por i o número complexo$(0,\ 1)$. Tendo

como propriedade básica da unidade imaginária:

$$i^2 = -1.$$

Do qual podemos obter uma representação mais usual e prática para trabalhar com os complexo. Sendo assim, dado um complexo $z = (x,\ y)$ temos:

$$\begin{aligned} z = (x,\ y) &= (x,\ 0) + (0,\ y) \\ &= (x,\ 0) + (y \cdot 0 - 0 \cdot 1,\ y \cdot 1 + 0 \cdot 0) \\ &= (x,\ 0) + (y,\ 0) \cdot (0,\ 1). \end{aligned}$$

Isto é:

$$z = x + y \cdot i.$$

Assim, todo número complexo $z = (x,\ y)$ pode ser escrito como $z = x+yi$, chamada forma algébrica de z. O número real x é chamado de parte real de z e y é chamado de parte imaginária de z. Em simbolos indica-se:

$$z = (x, y) \Rightarrow \begin{cases} Re(z) = x \\ Im(z) = y. \end{cases}$$

Exemplo 3.

- $z = 2 + 5i, \quad Re(z) = 2 \quad e \quad Im(z) = 5.$
- $z = 6i, \quad Re(z) = 0 \quad e \quad Im(z) = 6.$
- $z = 13 \quad Re(z) = 13 \quad e \quad Im(z) = 0.$

Tendo sua representação gráfica no plano de Argand-Gauss, no qual consiste no modelo do plano cartesiano, ou seja, utiliza-se como base os eixos das abicissas e ordenadas para identificar respectivamente as partes real e imaginária de um dado complexo. Por exemplo, dado um complexo $z = 5 + 4i$ sua representação gráfica é de acordo com a figura 1.1.

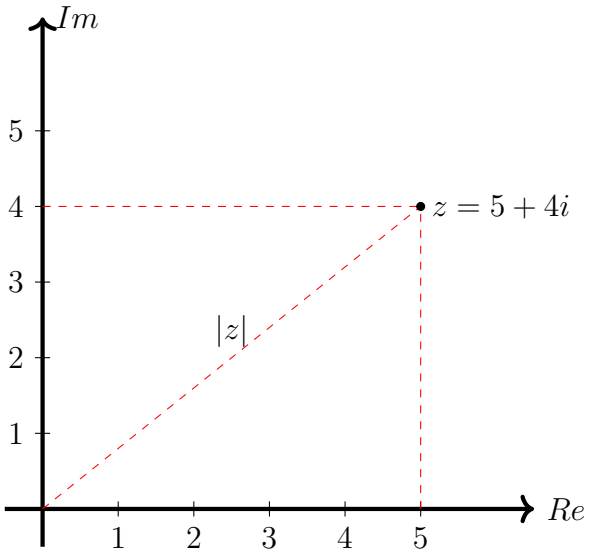


Figura 1.1: Representação gráfica de um complexo.

E de posse da representação gráfica, assim como mencionado para os inteiros, a distância de um complexo z até a origem é definido como módulo e denotada por $|z|$, em que nos fornece geometricamente o quanto esse complexo está distante da origem do plano Argand-Gauss.

Os complexos, assim como os demais conjuntos numéricos, apresentam suas propriedades e operações definidas. Sendo assim, dados os complexos $z_1 = a + bi$ e $z_2 = c + di$, temos as seguintes operações:

Adição em $\mathbb{C}$:

$$z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)i.$$

Isto é, a soma de dois complexos é um complexo cuja a parte real é a soma das partes reais das parcelas e cuja a parte imaginária é a soma das partes imaginárias das parcelas.

Exemplo 4.

- $(2 + 12i) + (7 + 22i) = (2 + 7) + (12 + 22)i = 9 + 34i.$

Multiplicação em $\mathbb{C}$: O produto de dois números complexos é o resultado do desenvolvimento de $(a+bi)\cdot(c+di)$, aplicando a propriedade distribuitiva e levando em conta

que $i^1 = -1$:

$$\begin{aligned} z_1 \cdot z_2 &= (a+bi)\cdot(c+di) \\ &= a\cdot c + a\cdot di + bi\cdot c + bi\cdot di \\ &= a\cdot c + a\cdot di + c\cdot bi + b\cdot di^2 \\ &= a\cdot c + a\cdot di + c\cdot bi + b\cdot d(-1) \\ &= (a\cdot c - b\cdot d) + (a\cdot d + b\cdot c)i. \end{aligned}$$

Exemplo 5. *Dados,* $z_1 = 4 + 9i$ *e* $z_2 = 3 - 7i$*, efetuando* $z_1 \cdot z_2$*, temos:*

$$\begin{aligned} z_1 \cdot z_2 &= (4+9i)\cdot(3-7i) \\ &= 4\cdot 3 + 4\cdot(-7i) + 9i\cdot 3 + 9i\cdot(-7i) \\ &= 12 - 28i + 27i - 63i^2 \\ &= 12 - i + 63 \\ &= 75 - i. \end{aligned}$$

Para entender o processo de divisão entre dois complexos, é necessária a seguinte definição:

Definição 1.4.2. *Chama-se conjugado de um complexo* $z = x + yi$*, ao complexo* $\bar{z} = x - yi$*, isto é:*

$$z = x + yi \iff \bar{z} = x - yi.$$

Exemplo 6.

- $z = 7 + 27i, \quad \bar{z} = 7 - 27i.$
- $z = -9i, \quad \bar{z} = 9i.$
- $z = 115, \quad \bar{z} = 115.$

De posse desse resultado, temos:

Divisão em $\mathbb{C}$:

Dado $z = a + bi$, é utilizado um processo prático baseado em que:

$$z \cdot \bar{z} = (a + bi) \cdot (a - bi) = a^2 + b^2.$$

Com isso:

$$\begin{aligned}
\frac{z_1}{z_2} &= \frac{z_1}{z_2} \cdot \frac{\bar{z_2}}{\bar{z_2}} \\
&= \frac{(a+bi)}{(c+di)} \cdot \frac{(c-di)}{(c-di)} \\
&= \frac{ac - adi + bic - (bd)i^2}{c^2 + d^2} \\
&= \frac{(ac+bd)}{c^2+d^2} + \frac{(bc-ad)}{c^2+d^2} \cdot i.
\end{aligned}$$

Exemplo 7. *Seja $z_1 = 1 + 4i$ e $z_2 = 2 - 3i$. Determinar $\frac{z_1}{z_2}$.*
Solução:

$$\begin{aligned}
\frac{z_1}{z_2} &= \frac{z_1}{z_2} \cdot \frac{\bar{z_2}}{\bar{z_2}} \\
&= \frac{(1+4i)}{(2-3i)} \cdot \frac{(2+3i)}{(2+3i)} \\
&= \frac{2 + 3i + 8i + 12i^2}{2^2 + 3^2} \\
&= \frac{2 - 12 + 11i}{4 + 9} \\
&= -\frac{10}{13} + \frac{11}{13} \cdot i
\end{aligned}$$

Do processo prático mencionado acima, temos a seguinte definição:

Definição 1.4.3. *Dado $z \in \mathbf{C}$ sua norma, denotada por $N(z)$, será dada pelo produto de z por $\bar{z}$:*

$$\begin{aligned}
N(z) &= z.\bar{z} \\
&= (x + yi).(x - yi) \\
&= x^2 - x.yi + yi.x + y^2 i^2 \\
&= x^2 + y^2 \\
N(z) &= x^2 + y^2.
\end{aligned}$$

Exemplo 8.

- $N(3-6i) = 3^2 + 6^2 = 9 + 36 = 45.$
- $N(2-2i) = 2^2 + 2^2 = 4 + 4 = 8.$
- $N(5i) = 0^2 + 5^2 = 25.$
- $N(4+i) = 4^2 + 1^2 = 16 + 1 = 17.$

A norma de um complexo apresenta as seguintes propriedades:

P 1. $N(z)$ *é um número não negativo.*
Essa relação é direta, já que a norma é a soma de dois quadrados, portanto é um número não negativo.

P 2. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta),\ para\ qualquer\ \alpha, \beta \in \mathbb{C}.$

Demonstação: Seja α e $\beta \in \mathbb{C}$, com $\alpha = x + yi$ e $\beta = u + vi$, temos:

$$\begin{aligned}
\alpha \cdot \beta &= (x+yi) \cdot (u+vi) \\
&= (xu - yv) + (xv + uy)i \\
N(\alpha \cdot \beta) &= (xu - yv)^2 + (xv + uy)^2 \\
&= x^2u^2 - 2xuyv + y^2v^2 + x^2v^2 + 2xuyv + u^2y^2 \\
&= x^2u^2 + y^2v^2 + x^2v^2 + u^2y^2 \\
&= x^2(u^2 + v^2) + y^2(u^2 + v^2) \\
&= (x^2 + y^2) \cdot (u^2 + v^2) \\
&= N(\alpha) \cdot N(\beta).
\end{aligned}$$

■

P 3. $N(z) = 0$ *se, e somente se,* $z = 0$.
Essa relação também é direta pois a norma é definida por uma soma de dois quadrados, e para essa soma ser nula obrigatorialmente suas parcelas devem ser nulas.

Como mencionado nos inteiros, os complexos abrange uma relação de fechamento, e Euler conseguiu na época demonstrar que qualquer operação efetuada nos complexos terá como resultado ainda um número complexo, tornando assim um conjunto fechado quanto suas operações (BOYER, 1996).

1.5 Inteiros Gaussianos

A percepção que Gauss teve sobre tal conjunto foi no momento em que ele estudava assuntos relacionados a reciprocidade quadrática e verificou que era mais viável trabalhar com números complexos onde a parte real e imaginária são números Inteiros, do que necessariamente com Inteiros, criando assim, com esse formato, um subconjunto dos complexos.

> Gauss chamou a lei da reciprocidade quadrática, que Legendre tinha publicado anos antes, de Theorema aureum, ou a jóia da aritmética. Em obra posterior Gauss tentou achar teorema comparáveis para a congruência $x^n \equiv p(mod\ q)$ para $n = 3\ e\ 4$; mas para estes casos achou entender a palavra inteiro para incluir os chamados inteiros de Gauss.(BOYER, 1996, p.346)

Observou-se que, além de ter essa facilidade de trabalhar com a reciprocidade, as relações aritméticas definidas nos Inteiros poderiam ser enunciadas e definidas de forma análoga para os inteiros gaussianos, ou seja, Gauss observou uma ligação valiosa entre diferentes conjuntos numéricos e que possuem aspectos semelhantes. Essa relação abriu portas para as ramificações dentro da teoria dos números como um avanço no estudo de inteiros algébricos.

A partir da noção inicial de um número complexo, ampliamos a concepção algébrica para definir e conhecer um Inteiro Gaussiano.

Definição 1.5.1. *Os complexo da forma $z = x + yi$, tal que x e y são inteiros, são chamados de Inteiros de Gauss ou Inteiros Gaussianos. O conjunto de todos Inteiros Gaussianos é denotado por $\mathbb{Z}[i]$. Isto é,*

$$\mathbb{Z}[i] = \{x + yi \in \mathbb{C} |\ x, y \in \mathbb{Z}\}.$$

Exemplo 9.

- $z = 2 + 9i,$ é Inteiro Gaussiano, pois $2, 9 \in \mathbb{Z}$.
- $z = -6 - 14i$, é Inteiro Gaussiano, pois $-6, -14 \in \mathbb{Z}$.
- $z = \sqrt{8} + 9i$, não é Inteiro Gaussiano, pois $\sqrt{8} \notin \mathbb{Z}$.
- $z = \pi - 39i$, não é Inteiro Gaussiano, pois $\pi \notin \mathbb{Z}$.
- $z = \frac{5}{2} + \frac{4}{3}.i$, não é Inteiro Gaussiano, pois, $\frac{5}{2}, \frac{4}{3} \notin \mathbb{Z}$.

Como $\mathbb{Z}[i]$ é um subconjunto do conjunto dos números complexos, todas as definições e propriedades vistas em $\mathbb{C}$ são válidas para $\mathbb{Z}[i]$.

Como foi apontado na seção 1.3 sobre os inteiros serem fechados sobre adição, subtração e multiplicação, o mesmo ocorre para os Inteiros Gaussianos.

Teorema 1.5.1. *Dados que* $\alpha = a + bi$ *e* $\beta = c + di$ *sejam Inteiros Gaussianos. Então,* $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ *são Inteiros Gaussianos.*

Demonstração:

Por definição, temos que $a,\ b,\ c,\ d \in \mathbb{Z}$. Logo temos:

1. $\alpha + \beta = (a + bi) + (c + di) = (a + c) + (b + d)i$
2. $\alpha - \beta = (a + bi) - (c + di) = (a - c) + (b - d)i$
3. $\alpha \cdot \beta = (a + bi) \cdot (c + di) = a \cdot c + a \cdot di + bi \cdot c + bi \cdot di = (a \cdot c - b \cdot d) + (a \cdot d + c \cdot b) \cdot i$

De posse dos resultados, temos em ambos itens a soma, subtração e multiplicação de inteiros, que ainda resulta em um inteiro. Assim, os resultados obtidos ainda será um Inteiro Gaussiano. ■

Capítulo 2

Metodologia da pesquisa

2.1 Abordagem metodológica

O trabalho apresenta uma abordagem quantitativa, da qual no âmbito matemático essa abordagem propicia uma descrição dos fundamentos de um determinado fato, assim como um levantamento de relações entre diferentes elementos, condicionando uma ampliação dos fenômenos observados(Fonseca 2002 apud (GERHARDT, 2009) p.20).

Sendo assim a pesquisa buscou a ampliação de conceitos e aplicações do conjunto dos inteiros para o conjunto dos inteiros gaussianos, indo de uma intuição particular para o geral, isto é, tem como ponto de partida as definições, teoremas e proposições dos aspectos aritméticos dos inteiros, estendendo essas relações para os inteiros gaussianos, onde os dados apresentados são mediante a hipótese de que as definições de divisibilidade, números primos e algoritmo da divisão, possam ser enunciados de maneiras semelhantes para os inteiros gaussianos.

A pesquisa segue como estratégia o método explicativo, a qual:

> Vai além do registro, da análise, da classificação e da interpretação dos fenômenos em estudo, procurando identificar quais são os fatores determinantes. Seu objetivo é aprofundar o conhecimento da realidade, indo em busca da razão, do porquê das coisas, estando assim mais sujeitas a erros(MESQUITA, 2007, p.26)

Foram verificadas, mediantes semelhanças, a estrutura dos inteiros gaussianos a partir de interpretação das definições e teoremas demonstrados nos inteiros, a fim de explicar os fatos que são determinantes para o aprofundamento do conhecimento dos

inteiros gaussianos de forma a ser compreendida a relação entre os diferentes corpos numéricos.

As demonstrações foram decorrentes da intuição lógica matemática e propriedades resultantes do conjunto dos inteiros, para esse procedimento técnico foi utilizado o levantamento bibliográfico baseado nas obras de Santos(2020) que tratar os conceitos preliminares dos aspectos aritméticos de divisibilidade, números primos e do algoritmo da divisão nos Inteiros, e Rosen(2011) foi utilizado para estudos dos aspectos mencionados, para os inteiros gaussianos.

2.2 Etapas da pesquisa

A pesquisa apresenta um levantamento bibliográfico sobre os aspectos históricos e preliminares de acordo com as publicações de (BERTONE, 2014), (BOYER, 1996), (FILHO, 1981), (GALDINNO, 2014), (ROONEY, 2012), (ROSEN, 2011) e (SANTOS, 2020). Tendo esse embasamento teórico foi feita a construção da fundamentação teórica a partir do levantamento bibliográfico.

De posse da definição dos Inteiros Gaussianos, é apresentado os aspectos aritméticos relacionados à divisibilidade, números primos e algoritmo da divisão nos Inteiros, para se ter uma base de comparação dos mesmos aspectos para os Inteiros Gaussianos. Com isso, segue alinhado a resultados e teoremas importantes tais, como verificar se um Inteiro Gaussiano é Primo Gaussiano, enuciar e demonstar o Algoritmo da Divisão em $\mathbf{Z}[i]$, apresentando análises à respeito de suas demonstrações e exemplos.

Capítulo 3

Aspectos Aritméticos

3.1 Divisibilidade

3.1.1 Divisibillidade nos Inteiros

Definição 3.1.1. *Se a e b são inteiros, dizemos que a divide b, denotado por $a \mid b$, se existir um inteiro c tal que $b = a \cdot c$. Se a não divide b, denotamos por $a \nmid b$.*

Exemplo 10. *Divisibilidade em $\mathbb{Z}$.*

- Dados $a = 5$, $b = 20$, nesse caso $a \mid b$, pois existe um inteiro $c = 5$ tal que:

$$20 = 4 \cdot 5.$$

- Dados $a = -4$, $b = 100$, nesse caso $a \mid b$, pois existe um inteiro $c = -25$ tal que:

$$100 = (-4) \cdot (-25).$$

- Dados $a = 6$, $b = 13$, nesse caso $a \nmid b$, pois não existe um inteiro c tal que:

$$b = a \cdot c$$

$$13 = 6 \cdot c$$

$$c = \frac{13}{6}$$

pois, $c \notin \mathbb{Z}$.

- Dados $a = -3$, $b = -29$, nesse caso $a \nmid b$, pois não existe um inteiro c tal que:

$$b = a \cdot c$$

$$(-29) = (-3) \cdot c$$

$$c = \frac{29}{3}$$

pois, $c \notin \mathbb{Z}$.

Decorrente da definição, alguns resultados são importantes para a divisibilidade nos Inteiros.

Proposição 3.1.1. *Se a, b e c são inteiros, $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demostração: Por hipótese, $a \mid b$ e $b \mid c$, então existem inteiros k_1 e k_2, com:

$$b = k_1 \cdot a \tag{3.1}$$

$$c = k_1 \cdot b. \tag{3.2}$$

Substituindo a equação 3.1 em 3.2:

$$c = k_1 \cdot k_2 \cdot a.$$

Como mencionado anteriormente, o produto de $k_1 \cdot k_2$, ainda resulta em um inteiro. Logo, fazendo $k_1 \cdot k_2 = k_3$, em que $k_3 \in \mathbb{Z}$, temos:

$$c = k_3 \cdot a.$$

ou seja, $a \mid c$ ■

Exemplo 11.

- Dado que: $4 \mid 16$ e $16 \mid 32$, então $4 \mid 32$.
- Dado que: $6 \mid 18$ e $18 \mid 74$, então $6 \mid 74$.

Proposição 3.1.2. *se a, b, c, m e n são inteiros, tais que $c \mid a$ e $c \mid b$ então $c \mid (m \cdot a + n \cdot b)$.*

Demonstração: se $c \mid a$ e $c \mid b$ então $a = k_1 \cdot c$ e $b = k_2 \cdot c$. Multiplicando-se estas duas equações respectivamente por m e n teremos $m \cdot a = m \cdot k_1 \cdot c$ e $n \cdot b = n \cdot k_2 \cdot c$.

Somando membro a membro obtemos $m \cdot a + n \cdot b = (m \cdot k_1 + n \cdot k_2) \cdot c$, o que nos diz, $c \mid (m \cdot a + n \cdot b)$. Tendo em vista que a operação de $(m \cdot k_1 + n \cdot k_2)$ resultará em um inteiro. ■

Exemplo 12.

- Dado que: $2 \mid 12$ e $12 \mid 24$, então $2 \mid (5 \cdot 12 - 3 \cdot 24)$.
- Dado que: $5 \mid 20$ e $20 \mid 100$, então $5 \mid (3 \cdot 20 - 6 \cdot 100)$.

Teorema 3.1.1. [1] *Dados $a,\ d,\ n \in \mathbb{Z}$. A divisibilidade têm as seguintes propriedades:*

1. $n \mid n$.
2. $d \mid n \quad \Rightarrow \quad a \cdot d \mid a \cdot n$.
3. $ad \mid an \quad e \quad a \neq 0 \quad \Rightarrow \quad d \mid n$.
4. $1 \mid n$.
5. $n \mid 0$.
6. $d \mid n \quad e \quad n \neq 0 \quad \Rightarrow |d| \leq |n|$.
7. $d \mid n \quad e \quad n \mid d \quad \Rightarrow \quad |d| = |n|$.
8. $d \mid n \quad e \quad d \neq 0 \quad \Rightarrow \quad (\frac{n}{d}) \mid n$.

3.1.2 Divisibilidade nos Inteiros Gaussianos

O estudo dos Inteiros Gaussianos segue uma base de comparação com relação aos inteiros, no que diz respeito aos aspectos aritméticos conforme já citado na seção 1.5. Sendo assim, dispondo do método usual da divisão de um complexo e de maneira prática e semelhante, temos:

Definição 3.1.2. *Suponha que α e β são Inteiros Gaussianos. Diz-se que α divide β, se existir um $\gamma \in \mathbb{Z}[i]$, tal que $\beta = \alpha.\gamma$. Se α divide β, denotamos por $\alpha \mid \beta$, caso contrário denotamos por $\alpha \nmid \beta$.*

[1] As demonstrações se encontra na obra de (SANTOS, 2020)

Exemplo 13. *Divisibilidade em* $\mathbb{Z}[i]$.

- Dados $\alpha = 2 + 4i$ e $\beta = 14 - 2i$, temos que $\alpha \mid \beta$, pois existi um $\gamma \in \mathbb{Z}[i]$ para satisfazer a definição:

$$\begin{aligned}
\beta &= \alpha \cdot \gamma \\
\gamma &= \frac{14 - 2i}{2 + 4i} \\
&= \frac{(14 - 2i)}{(2 + 4i)} \cdot \frac{(2 - 4i)}{(2 - 4i)} \\
&= \frac{28 - 56i - 4i + 8i^2}{2^2 + 4^2} \\
&= \frac{28 - 8 - 60i}{20} \\
&= \frac{20 - 60i}{20} \\
&= 1 - 3i
\end{aligned}$$

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

- Dados $\alpha = 4 + i$ e $\beta = 1 + 5i$, temos que $\alpha \mid \beta$ se existir um $\gamma \in \mathbb{Z}[i]$ para cumprir a definição. Vejamos:

$$\begin{aligned}
\beta &= \alpha \cdot \gamma \\
\gamma = &\frac{1 + 5i}{4 + i} \\
&= \frac{(1 + 5i)}{(4 + i)} \cdot \frac{(4 - i)}{(4 - i)} \\
&= \frac{4 - i + 20i - 5i^2}{4^2 + 1^2} \\
&= \frac{4 + 5 + 20i}{17} \\
\gamma = &\frac{9}{17} + \frac{20}{17} \cdot i
\end{aligned}$$

  Nesse caso temos que $\alpha \nmid \beta$, pois $\gamma \notin \mathbb{Z}[i]$.

De posse da definição, temos resultados interressantes sobre a divisibilidade em $\mathbb{Z}[i]$.

Proposição 3.1.3. *Se α, β e γ são Inteiros Gaussianos, tais que $\alpha \mid \beta$ e $\beta \mid \gamma$, então $\alpha \mid \gamma$.*

Demostração: Por hipótese, $\alpha \mid \beta$ e $\beta \mid \gamma$, então existem Inteiros Gaussianos θ_1 e θ_2, com:

$$\beta = \theta_1 \cdot \alpha \tag{3.3}$$

$$\gamma = \theta_1 \cdot \beta. \tag{3.4}$$

Substituindo a equação 3.3 em 3.4:

$$\gamma = \theta_1 \cdot \theta_2 \cdot \alpha.$$

De acordo com o teorema 1.5.1, o produto de $\theta_1 \cdot \theta_2$, ainda resulta em um Inteiro Gaussiano. Logo, fazendo $\theta_1 \cdot \theta_2 = \theta_3$, em que $\theta_3 \in \mathbb{Z}[i]$, temos:

$$\gamma = \theta_3 \cdot \alpha.$$

ou seja, $\alpha \mid \gamma$ ■

Proposição 3.1.4. *Dados $\alpha,\ \beta \in \mathbb{Z}[i]$, se $\alpha \mid \beta$ em $\mathbb{Z}[i]$, então $N(\alpha) \mid N(\beta)$ em $\mathbb{Z}$.*

Demonstração: Se $\alpha \mid \beta$, por definição existe um $\gamma \in \mathbb{Z}[i]$ tal que $\beta = \alpha \cdot \gamma$. Aplicando a norma, $N(\beta) = N(\alpha \cdot \gamma)$, pela propriedade 2, temos:

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

Como a norma é um número real positivo, em especial nos Inteiros Gaussianos, a norma é um Inteiro positivo. Logo, $N(\alpha) \mid N(\beta)$ em $\mathbb{Z}$. ■

Exemplo 14. *Dados $\alpha = 1 - 5i$ e $\beta = 37 - 3i$, temos:*

Verificando, primeiramente, se $\alpha \mid \beta$:

$$\begin{aligned}
\beta &= \alpha \cdot \gamma \\
\gamma &= \frac{37 - 3i}{1 - 5i} \\
&= \frac{37 + 185i - 3i - 15i^2}{1^2 + 5^2} \\
&= \frac{52}{26} + \frac{182i}{26} \cdot i \\
&= 2 - 7i
\end{aligned}$$

Como $\gamma \in \mathbf{Z}[i]$, logo $\alpha \mid \beta$, então pela proposição 3.1.4, $N(\alpha) \mid N(\beta)$. De fato, existe um $k \in \mathbf{Z}$ tal que

$$\begin{aligned} N(\beta) &= N(\alpha) \cdot k \\ 1378 &= 26 \cdot 53. \end{aligned}$$

3.2 Números Primos

3.2.1 Os Inteiros Primos

[2] Tendo hoje suas aplicações, os números primos apresentam uma particularidade devido a sua complexidade em resolução de problemas ainda em abertos na matemática. Os avanços obtidos vêm desde a antiguidade em que a obra os **Elementos** de Euclides relata teoremas e resultados importantes acerca dos números primos.

Definição 3.2.1. *Um número inteiro n ($n > 1$) possuindo apenas dois divisores positivos n e 1 é chamado primo . Se $n > 1$ não é primo dizemos que n é composto.*

Exemplo 15. *Alguns inteiro primos:*

- 2 é primo, pois seus únicos divisores positivos são 2 e 1.
- 17 é primo, pois seus únicos divisores positivos são 17 e 1.
- 29 é primo, pois seus únicos divisores positivos são 29 e 1.
- 47 é primo, pois seus únicos divisores positivos são 47 e 1.
- 8 não é primo, pois possui 2 e 4 como divisores positivos além de 8 e1.

Mediante a definição para inteiros primos, é importante mencionar sobre alguns conceitos que serão tratados mais a frente como **unidades** e **associado**s. As unidades tem como propriedade dividir qualquer número sem alterar seu valor absoluto, nesse caso temos que as unidades nos Inteiros são ± 1. Os associados é definido como o produto pelas unidades, com isso dado um Inteiro p seus associados são $\pm p$.

[2] Os teoremas e demonstrações desta subseção é de acordo com (SANTOS, 2020)

Teorema 3.2.1. ***(Teorema Fundamental da Aritmética)*** *Todo Inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Exemplo 16. *Representação em fatores primos:*

- $28 = 2 \cdot 2 \cdot 7.$
- $18 = 2 \cdot 3 \cdot 3.$
- $27 = 3 \cdot 3 \cdot 3.$
- $42 = 2 \cdot 3 \cdot 7.$

Teorema 3.2.2. *A sequência dos números primos é infinta.*

Demonstração: Suponha que a sequência dos primos seja finita. Seja, $p_1,\ p_2, \ldots, p_n$ a lista de todos os primos. Consideramos $R = p_1 \cdot p_2 \cdot\ \ldots\ \cdot p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa lista e que R é maior do que qualquer p_i. Mas, pelo teorema fundamental da aritmética, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence à nossa lista. Portanto, a sequência dos números primos não pode ser finita. ■

3.2.2 Primos Gaussianos

Sobre a primalidade, será necessário verificar primeiro quem são as unidades em $\mathbb{Z}[i]$.

Definição 3.2.2. *Um Inteiro Gaussiano α é chamado de unidade quando α divide 1. Quando α é uma unidade, $\alpha \cdot \beta$ é dito associado do Inteiro Gaussiano β.*

De forma semelhante aos inteiros, por essa definição podemos extrair resultados importantes para trabalharmos com os Inteiros Gaussianos.

Proposição 3.2.1. *Um Inteiro Gaussiano α é unidade se, e somente se, $N(\alpha) = 1.$*

Demonstração: Suponha que α é unidade, logo $\alpha \mid 1$, então por definição existe um inteiro gaussiano $\beta \neq 0$ tal que $\alpha \cdot \beta = 1$. Aplicando a norma teremos:

$$N(\alpha \cdot \beta) = N(1) \Rightarrow N(\alpha \cdot \beta) = 1.$$

Pela Propriedade 2,

$$N(\alpha) \cdot N(\beta) = 1.$$

Visto que, α e β são Inteiros Gaussianos, suas normas são Inteiros positivos. Logo, $N(\alpha) = N(\beta) = 1$. ■

Proposição 3.2.2. *As unidades nos Inteiros Gaussianos são* $1, -1, i, -i$.

Demonstração: Pelo proposição 3.2.1, temos que dado um $\alpha = (x + yi) \in \mathbb{Z}[i]$, é unidade se $N(\alpha) = 1$, sendo assim:

$$N(x + yi) = 1 \Rightarrow x^2 + y^2 = 1$$

Os únicos valores inteiros possíveis para a solução da equação é de fato:

$$x = \pm 1 \; e \; y = 0 \; ou \; x = 0, \; e \;\; y = \pm 1.$$

Com isso podemos formar os pares e verificar a possibilidades das unidades, $(1,\ 0)$, $(-1,\ 0)$, $(0,\ 1)$, $(0,\ -1)$, nessas configurações para $\alpha = x + yi$ temos ao substituir seus valores as respectivas unidades Gaussianas:

$$\begin{aligned} (1,0) &\Rightarrow \alpha = 1. \\ (-1,0) &\Rightarrow \alpha = -1. \\ (0,1) &\Rightarrow \alpha = i. \\ (0,-1) &\Rightarrow \alpha = -i. \end{aligned}$$

Formalizando assim, as unidades em $\mathbb{Z}[i] :\ 1,\ -1,\ i,\ -i$. ■

Além dos resultados obtidos, o conceito para **associados** de um Inteiro Gaussiano, será verificado mediante ao produto pelas unidades, na qual dado um Inteiro Gaussiano α, seus associados serão $\alpha,\ -\alpha,\ i\alpha,\ -i\alpha$.

Conhecendo a estrutura de um número complexo, é notório que ao ser introduzido uma parte numérica imaginária à mesma pode ter suas unidades, isto é, dado um complexo na forma $x + yi$ temos além de ± 1 como unidades e acrescentamos $\pm i$.

Partindo da hipótese das semelhaças encontradas entre os dois conjuntos, para introduzir o conceito de primalidade em $\mathbb{Z}[i]$, temos que estender a idéia considerada

na primalidade nos Inteiros, ou seja, quando tratamos de números primos nos Inteiros teve como definição um inteiro positivo que possue apenas dois divisores positivos (1 e o próprio número), ou seja, é um número que é divisível pela unidade e ele próprio.

De posse dos resultados iniciais apresentados sobre as unidades e associados em $\mathbb{Z}[i]$, podemos então introduzir a primalidade nos Inteiros Gaussianos.

Definição 3.2.3. *Um Inteiro Gaussiano α não nulo, é dito primo se não é uma unidade e é divisível apenas por unidades e seus associados.*

Ao analisarmos essa definição percebe-se que um primo Gaussiano possuem exatamente 8 divisores, decorrente justamente de suas unidades, ou seja, os únicos divisores de um Primo Gaussiano α são: $1,\ -1,\ i,\ -i,\ \alpha,\ -\alpha,\ i\alpha,\ -i\alpha$.

Percebemos que pelo "aumento" de uma unidade nesse conjunto, consequentemente em relação a primalidade aumentamos então seus divisores, na qual de forma comparativa, os primos Gaussianos tem a mesma características apresentadas para os Inteiros primos, que é o fato de ser dividido apenas pelo os associados e suas unidades, diferindo apenas de suas quantidades de divisores.

Com base na definição, é utilizado um teorema que facilita, na maioria dos casos, a verificação de quando um inteiro Gaussiano é um Primo Gaussiano.

Teorema 3.2.3. *Se θ é um Inteiro Gaussiano e $N(\theta) = p$, em que p é um Inteiro Primo, então θ e $\bar{\theta}$ são Primos Gaussianos.*

Demonstração: Supondo que $\theta = \alpha \cdot \beta$, na qual $\alpha\ , \beta \in \mathbb{Z}[i]$. Aplicando a norma:

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

Aplicando a propriedade 2:

$$\begin{aligned} N(\theta) &= N(\alpha) \cdot N(\beta) \\ p &= N(\alpha) \cdot N(\beta). \end{aligned}$$

Como a $N(\alpha)$ e $N(\beta)$ são Inteiros positivos e p é Inteiro Primo, temos então desse resultado que $N(\alpha) = 1$ e $N(\beta) = p$ ou $N(\alpha) = p$ e $N(\beta) = 1$. O que podemos concluir que de acordo com proposição 3.2.1 que α é uma unidade ou β é uma unidade. Isso significa que θ não pode ser fatorado, em dois Inteiros

Gaussianos, a não ser que um seja unidade. Logo, θ é Primo Gaussiano. Lembrando que, o fato da $N(\bar{\theta}) = p$, temos que $\bar{\theta}$ também é Primo Gaussiano.

■

Exemplo 17.

- $1 - i$ é Primo Gaussiano, pois $N(1 - i) = 1^2 + (-1)^2 = 2$ e 2 é Inteiro Primo.
- $1 + 4i$ é Primo Gaussiano, pois $N(1 + 4i) = 1^2 + 4^2 = 17$ e 17 é Inteiro Primo.

É importante ressaltar que o resultado inverso do Teorema 3.2.3 não é válido, isto é, existem Primos Gaussianos do qual a norma não é Inteiro Primo, vejamos um caso do Inteiro Gaussiano 7, provaremos que é um Primo Gaussiano. Note que a $N(7) = 7^2 = 49$ e 49 não é Inteiro Primo.

Demonstração: Supondo que $7 = (a + bi) \cdot (c + di)$, onde $a,\ b,\ c,\ d \in \mathbb{Z}$, $(a + bi)$ e $(c + di)$ não são unidades. Aplicando a norma:

$$\begin{aligned} N(7) &= N[(a + bi) \cdot (c + di)] \\ 49 &= N(a + bi) \cdot N(c + di) \end{aligned}$$

Pelo fato de $a+bi$ e $c+di$ não serem unidades, logo a $N(a+bi) \neq 1$ e $N(c+di) \neq 1$. Assim, para a igualdade acima temos:

$$N(a + bi) = a^2 + b^2 = 7.$$

O que é um absurdo, pois 7 não é soma de dois quadrados, logo 7 é Primo Gaussiano. ■

Em geral, Inteiros Gaussianos da forma $a + bi$ com a e b não nulos, torna o Teorema 3.2.3 bastante útil para verificar-se a primalidade em $\mathbb{Z}[i]$. Como os Inteiros Gaussianos abrange uma relação com os inteiros e sua definição para primalidade é interligada a dos Inteiros, nos resta complementar a primalidade em $\mathbb{Z}[i]$ verificando quais Inteiros Primos são Primos Gaussianos.

Podemos notar que mediante aos exemplos a respeito dos Primos Gaussianos, existem Inteiros Primos que não são Primos Gaussianos, por outro lado temos Inteiros Primos que são Primos Gaussianos como o caso do número 7.

Os resultados a seguir proporciona uma análise com verificações e generalizações dos Inteiros Primos que são ou não Primos Gaussianos. Assumindo uma observação [3] importante que para todo Inteiro Primo p temos $p \equiv 1(mod\ 4)$ ou $p \equiv 3(mod\ 4)$. O que nos resta então verificar as duas possibilidades para um dado Primo p.

Lema 1. *Seja p primo em $\mathbb{Z}$, as seguintes sentenças são equivalentes[4]:*

1. *p é redutível[5] em $\mathbb{Z}[i]$;*
2. *$p = \theta \cdot \bar{\theta}$, com θ primo em $\mathbb{Z}[i]$;*
3. *p é a soma de dois quadrados.*

Demonstração: $1 \Rightarrow 2$: assuma que p é redutível em $\mathbb{Z}[i]$, por consequência $p = \alpha \cdot \beta$ com $\alpha,\ \beta \in \mathbb{Z}[i]$ e não são unidades. como

$$\begin{aligned} N(p) &= N(\alpha \cdot \beta) \\ p^2 &= N(\alpha) \cdot N(\beta) \end{aligned}$$

temos então que, $N(\alpha) = N(\beta) = p$ tendo assim pelo Teorema 3.2.3, α é primo em $\mathbb{Z}[i]$. Prosseguindo temos que:

$$\begin{aligned} p &= \alpha \cdot \beta \\ \beta &= \frac{p}{\alpha} \\ &= \frac{p \cdot \bar{\alpha}}{N(\alpha)} \\ &= \frac{N(\alpha) \cdot \bar{\alpha}}{N(\alpha)}, \qquad com\ N(\alpha) \neq 0 \\ &= \bar{\alpha}. \end{aligned}$$

Logo $p = \alpha \cdot \beta = \alpha \cdot \bar{\alpha}$.

$2 \Rightarrow 3$: Supondo que $p = \alpha \cdot \bar{\alpha}$. Sendo $\alpha = a + bi$, teremos

$$p = \alpha \cdot \bar{\alpha} = (a + bi) \cdot (a - bi) = a^2 + b^2,$$

segue que p é a soma de dois quadrados.

$3 \Rightarrow 1$:Se $p = a^2 + b^2$, logo $p = (a + bi) \cdot (a - bi)$. Como $p^2 = N(a + bi) \cdot N(a - bi)$

[3] A observação é encontrada em (SANTOS, 2020).

[4] O lema é de acordo com (HEFEZ, 2002)

[5] p pode ser escrito como o produto de dois Inteiros Gaussianos que não são unidades

e como a $N(a+bi) = N(a-bi)$, temos que

$$N(a+bi) = N(a-bi) = p$$

como $(a+bi)$ e $(a-bi)$ não são unidades, ou seja, temos $N(a+bi) \neq 1$, provando assim que p é redutível em $\mathbb{Z}[i]$. ■

O que o lema 1 proporciona, é um resultado importante acerca dos Inteiros Primos que não são Primos Gaussiano, isto é, **todo Inteiro Primo que pode ser escrito como a soma de dois quadrados não é Primo Gaussiano**. Pois, para um dado Inteiro Primo p, podendo ser escrito como a soma de dois quadrados não será Primo Gaussiano, ou seja, pode ser escrito como o produto de dois Inteiros Gaussianos que não são unidades e por consequência terá além das unidades e associados esses dois Inteiros Gaussianos como divisores.

Do qual temos o seguinte Teorema[6] que comprova uma das congruências afirmadas acima com relação aos Inteiros Primos.

Teorema 3.2.4. *Sendo p um primo a equação $a^2 + b^2 = p$ possui solução inteira se, e somente se, $p = 2$ ou $p \equiv 1(mod\ 4)$.*

Do qual podemos obter pelo lema 3.2.2 e do Teorema 3.2.4, uma generalização dos Inteiros Primos que não são Primos Gaussianos.

Exemplo 18. *Inteiro Primo que não é Primo Gaussiano:*

- 13 não é Primo Gaussiano, pois $13 = 2^2 + 3^2 = 4 + 9$.
  Ampliando os resultados, temos que $13 = \alpha \cdot \beta$ com α, $\beta \in \mathbb{Z}[i]$ não sendo unidades, onde $\alpha = a + bi$ e $\beta = c + di$, aplicando a norma

$$\begin{aligned} N(13) &= N(\alpha \cdot \beta) \\ 13^2 &= N(\alpha) \cdot N(\beta) \\ 169 &= (a^2 + b^2) \cdot (c^2 + d^2). \end{aligned}$$

  como α e β não são unidades, logo suas normas são diferentes de 1, ou seja, $a^2 + b^2 \neq 1$ e $c^2 + d^2 \neq 1$ implicando que $a^2 + b^2 = 13$ e $c^2 + d^2 = 13$, como a, b, c, $d \in \mathbb{Z}$, logo seus valores devem corresponder a ± 2 e ± 3, considerando ± 2 para

[6] A demonstração se encontra em (SANTOS, 2020).

a parte real e ± 3 para a parte imaginária, consequentemente temos os possíveis resultados de $2+3i$, $2-3i$, $-2+3i$ e $-2-3i$, após uma inspeção decobrimos que para $\alpha = 2+3i$ e $\beta = 2-3i$ teremos que $\alpha \cdot \beta = 13$, concluindo assim que 13 não é Primo Gaussiano e que $13 = (2+3i) \cdot (2-3i)$.
Notamos que tanto $(2+3i)$ e $(2-3i)$ são Primos Gaussiano, pois como já verificado, sua norma igual a 13, e por 13 ser Inteiro Primo o Teorema 3.2.3 nos garante tal resultado.

O processo é análago para os demais Inteiros Primos que podem ser escrito como soma de dois quadrados, como mostra os exemplos abaixo:

- 2 não é Primo Gaussiano, pois $2 = 1^2 + 1^2 = 1 + 1 \Rightarrow 2 = (1+i) \cdot (1-i)$.
- 5 não é Primo Gaussiano, pois $5 = 2^2 + 1^2 = 4 + 1 \Rightarrow 2 = (2+i) \cdot (2-i)$.
- 17 não é Primo Gaussiano, pois $17 = 4^2 + 1^2 = 16 + 1 \Rightarrow 17 = (4+i) \cdot (4-i)$.
- 37 não é Primo Gaussiano, pois $37 = 1^2 + 6^2 = 1 + 36 \Rightarrow 37 = (1+6i) \cdot (1-6i)$.
- 41 não é Primo Gaussiano, pois $41 = 5^2 + 4^2 = 25 + 16 \Rightarrow 41 = (5+4i) \cdot (5-4i)$.

Como verificamos que Inteiros Primos p da forma $p \equiv 1(mod\ 4)$ não são Primos Gaussianos, o que resta nos então analisar se para um Inteiro Primo p na qual $p \equiv 3(mod\ 4)$ é ou não Primo Gaussiano. Temos o Lema que conclui tal resultado.

Lema 2. *Se $p \in \mathbb{Z}$ é um primo tal que $p \equiv 3(mod\ 4)$ então, p é Primo Gaussiano.*

Demonstração: Dado que $p \equiv 3(mod\ 4)$. Se p pode ser fatorado como $p = \alpha \cdot \beta$ com α, β não sendo unidades,

$$\begin{aligned} p &= \alpha \cdot \beta \\ N(p) &= N(\alpha \cdot \beta) \\ p^2 &= N(\alpha) \cdot N(\beta). \end{aligned}$$

como α e β não são unidades, temos que $N(\alpha) \neq 1$ e $N(\beta) \neq 1$, logo $N(\alpha) = N(\beta) = p$. Escrevendo $\alpha = a + bi$ com $a, b \in \mathbb{Z}$, temos que

$$\begin{aligned} N(\alpha) &= p \\ a^2 + b^2 &= p \\ a^2 + b^2 &\equiv 3(mod\ 4). \end{aligned}$$

chegando em um absurdo, visto que um quadrado perfeito é congruente a 0 ou a 1 módulo 4, portanto $a^2 + b^2$ é congruente a 0, 1 ou 2 módulo 4, mas nunca a 3 módulo 4. Logo p é Primo Gaussiano. ■

Exemplo 19. *Inteiro primos que são Primos Gaussianos:*

- 3 é Primo Gaussiano, pois $3 \equiv 3(mod\ 4)$
- 7 é Primo Gaussiano, pois $7 \equiv 3(mod\ 4)$
- 11 é Primo Gaussiano, pois $11 \equiv 3(mod\ 4)$
- 19 é Primo Gaussiano, pois $19 \equiv 3(mod\ 4)$
- 23 é Primo Gaussiano, pois $23 \equiv 3(mod\ 4)$

Com isso temos uma generalização dos Primos Gaussianos.

Teorema 3.2.5. *Os elementos Primos de $\mathbb{Z}[i]$ são, a menos de associados,*

- *Números Primos p tais que $p \equiv 3(mod\ 4)$;*
- *Números da forma $a + bi$ em que $N(a + bi)$ é primo(necessáriamente igual a 2 ou congruente a 1 módulo 4).*

Assim como apresentados para os Inteiros no teorema 3.2.1, os Inteiros Gaussianos também admitem uma fatoração única.

Teorema 3.2.6. *(Fatoração única[7]) Qualquer elemento $\alpha \neq 0$ de $\mathbf{Z}[i]$ admite uma fatoração*

$$\alpha = \pi_1 \cdot \pi_2 \ldots \pi_n$$

[7] A demonstração se encontra em (MARTINEZ, 2018)

em elementos irredutíveis[8] π_i*. Tal fatoração é única a menos da ordem dos fatores e de multiplicação por unidades, isto é, a menos dos associados.*

Exemplo 20. *Fatorar* 10 *em* $\mathbb{Z}[i]$.

Solução: Como $10 = 2 \cdot 5$. Escrevendo $2 = (1+i) \cdot (1-i)$ e $5 = (2+i) \cdot (2-i)$, temos pelo teorema 3.2.3 que $(1+i),\ (1-i),\ (2+i),\ (2-i)$ são Primos Gaussianos. Sendo assim, $10 = (1+i) \cdot (1-i) \cdot (2+i) \cdot (2-i)$.

Exemplo 21. *Escrever* $\alpha = 1 + 3i$ *como um produto de fatores primos em* $\mathbb{Z}[i]$.

Solução: Se $\theta \in \mathbb{Z}[i]$ é um fator Primo de $1 + 3i$, consequentemente, $1 + 3i = \theta \cdot \theta_1 \cdot \theta_2 \cdot \cdots \cdot \theta_n$, logo $\theta \mid (1 + 3i)$, de acordo com a proposição 3.1.4 temos que $N(\theta) \mid N(1+3i)$, como $N(1+3i) = 10$ e $10 = 2 \cdot 5$, e já sabemos que $2 = (1+i) \cdot (1-i)$ e $5 = (2+i) \cdot (2-i)$ são as fatorações em fatores primos de 2 e 5 em $\mathbf{Z}[i]$ e como $\theta \mid N(\theta)$ e $N(\theta) \mid 10$, então pela proposição 3.1.3 $\theta \mid 10 \Rightarrow \theta \in \{1 \pm i,\ 2 \pm i\}$. Testando as possibilidades, temos ao escolher:

$$1 + 3i = (1+i) \cdot (2+i)$$

é a fatoração procurada.

3.3 Algoritmo da divisão

3.3.1 Algoritmo da divisão - Inteiros

[9] O algoritmo da divisão apresentado no livro **Elementos** de Euclides, dispõe do método usual para a divisão que utilizamos. Para entender a demonstração de tal teorema é necessário ter como base outro teorema, o de Eudoxius:

Teorema de Eudoxius 1. *Dados* a *e* b *Inteiros com* $b \neq 0$ *então* a *é um múltiplo de* b *ou se encontra entre dois múltiplos consecutivos de* b*, isto é, correspondendo a cada par de Inteiros* a *e* $b \neq 0$ *existe um inteiro* q *tal que, para* $b > 0$*,*

$$qb \leq a < (q+1)b$$

[8] São elementos Primos em $\mathbb{Z}[i]$

[9] As definições e toremas dessa subseção é de acordo com (SANTOS, 2020)

e para $b < 0$

$$qb \leq a < (q-1)b.$$

Exemplo 22.

- $a = 13$ e $b = 4$, devemos tomar $q = 3$

$$3.4 \leq 13 < (3+1)4$$

$$12 \leq 13 < 16$$

- $a = -21$ e $b = -5$, devemos tomar $q = 5$

$$5(-5) \leq -21 < (5-1) - 5$$

$$-25 \leq -21 < -20$$

De posse desse resultado podemos então enunciar e demostrar o Algoritmo da divisão em $\mathbb{Z}$.

Teorema 3.3.1. ***(Algoritmo da Divisão em*** $\mathbb{Z}$***)***
Dados dois Inteiros a *e* b*,* $b > 0$*, existe um único par de Inteiros* q *e* r *tal que:*

$$a = qb + r \quad , \quad com \quad 0 \leq r < b \qquad (r = 0 \Rightarrow b \mid a)$$

q *é chamado de quociente e* r *o resto da divisão de* a *por* b*.*

Demonstração: Pelo teorema de Eudoxius, como $b > 0$, existe um q sastisfazendo:

$$qb \leq a < (q+1)b$$

o que implica $0 \leq a - qb$ e $a - qb < b$. Assim, se definirmos $r = a - qb$, teremos, garantida, a existência de q e r. Agora, a fim de mostrarmos a unicidade, Vamos supor a existência de outro par q_1 e r_1 verificando:

$$a = q_1 b + r_1 \qquad com \qquad 0 \leq r_1 < b.$$

Disto temos:

$$a - a = 0$$

$$(qb - r) - (q_1 b - r_1) = 0$$

$$qb - r - q_1 b + r_1 = 0$$

$$qb - q_1 b - r + r_1 = 0$$

$$b(q - q_1) = r - r_1$$

Desse último resultado temos:

$$b \mid (r - r_1).$$

Mas, como $r < b$ e $r_1 < b$, temos que $|r - r_1| < b$, portanto, como $b \mid (r - r_1)$ devemos ter $r - r_1 = 0$ o que implica $r = r_1$.Ora, $(qb - r) - (q_1 b - r_1) = 0$, com $r = r_1$,$qb - q_1 b = 0$

$$qb = q_1 b$$

Pela lei do cancelamento, $q = q_1$, uma vez que temos $b \neq 0$.

E importante ressaltar que os resultados encontrados abrange considerações para $b > 0$, usando valores de $b < 0$, ainda assim, de maneira análoga, pelo teorema de Eudoxius, encontraríamos q e r para $b < 0$. Sendo assim, o seguinte enunciado do Algoritmo da divisão também é válido:

Dados dois inteiros a e b, $b \neq 0$ existe um único par de inteiros q e r tais que $a = qb + r$ com $0 \leq r < |b|$. ■

Exemplo 23.

- Dados $a = 12,\ b = 6$ existe um único par $q = 2,\ r = 0$ que sastisfaz a definição:

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

- Dados $a = 26,\ b = 7$ existe um único par $q = 3,\ r = 5$ que sastisfaz a definição:

$$26 = 7 \cdot 3 + 5$$

Obs: Os valores para q e r em ambos exemplos são únicos que satisfazem a condição $0 \leq r < |b|$.

3.3.2 Algoritmo da divisão - Inteiros Gaussianos

Como mencionado acima, o algoritmo da divisão nos Inteiros estabelece uma divisão de um Inteiro a por um inteiro não nulo b na qual obtemos um único par de inteiros q e r chamados quociente e resto, respectivamente, satisfazendo as condições já mencionadas. O algoritmo da divisão para os Inteiros Gaussianos segue um processo parecido, mas com suas especificações, na qual o quociente e resto não são únicos e utiliza-se a norma como um meio de comparação entre o resto e o divisor.

Observando o fato que para a prova do Algritmo da divisão nos Inteiros, o objetivo era mostrar que existem tais inteiros, quociente e resto, que cumprem determinadas condições, o algoritmo da divisão nos Inteiros Gaussianos segue o mesmo objetivo. Sendo assim temos:

Teorema 3.3.2. ***(Algoritmo da Divisão em*** $\mathbb{Z}[i]$***)*** *Seja* α *e* β *Inteiros Gaussianos com* $\beta \neq 0$*. Então existem Inteiros Gaussianos* γ *e* ρ *tal que:*

$$\alpha = \beta \cdot \gamma + \rho$$

com $0 \leq N(\rho) < N(\beta)$*, em que* γ *é o quociente e* ρ *o resto da divisão.*

Demonstração:

Supondo, inicialmente que, $\frac{\alpha}{\beta} = a + bi$, então $a + bi$ é um complexo que é Inteiro Gaussiano se, e somente se, $\beta \mid \alpha$. Com isso, teremos garantido, pela defnição 3.1.2, um quociente γ e resto ρ nulo.

De forma geral, seja $s = \lfloor a + \frac{1}{2} \rfloor$ e $t = \lfloor b + \frac{1}{2} \rfloor$ na qual s e t são os inteiros mais próximos de a e b, respectivamente, (arredondando para cima quando a parte decimal for a metade ou maior que a metade, arredondando para baixo quando a parte decimal for menor que a metade, como mostra a figura 3.1).

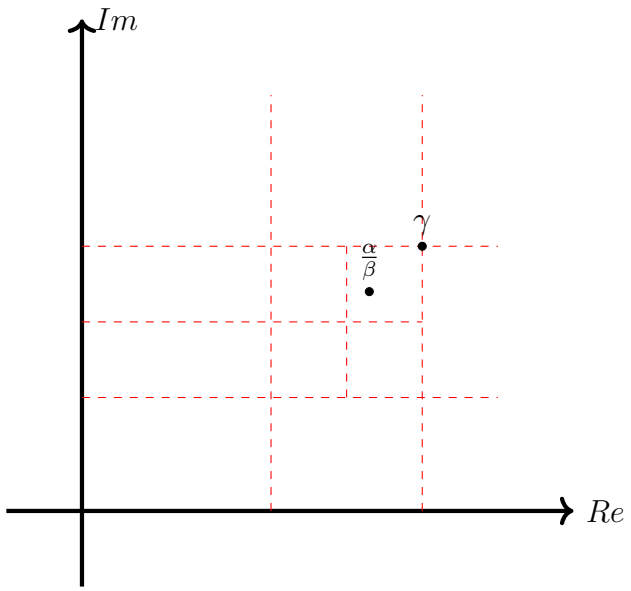


Figura 3.1: Determinando o quociente γ.

Uma vez tomados s e t, obtemos:

$$a + bi = (s + f) + (t + g)i.$$

onde f e g são números reais com $|f| \leq \frac{1}{2}$ e $|g| \leq \frac{1}{2}$ em relação ao seu inteiro mais proximo. Agora temos, como mostra a figura 3.2, analizando somente a parte real temos que, a e f se encontram entre $s - 1$ e s, e qualquer valor real para f teremos:

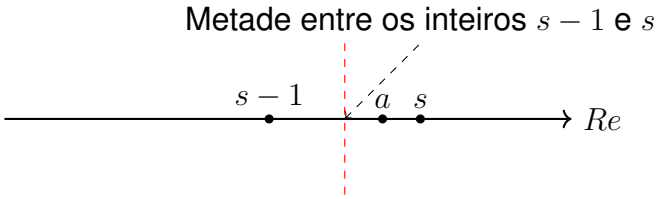


Figura 3.2: Distância de a até o inteiro mais próximo.

De acordo com a definição e interpretação do módulo, observamos que para a teremos com relação ao seu inteiro mais próximo, sempre $|f| \leq \frac{1}{2}$. O processo é análogo para g. Acontecendo isso encontramos γ, pois γ é definido como o inteiro mais próximo de $\frac{\alpha}{\beta}$. Definindo assim $\gamma = s + ti$ e $\rho = \alpha - \beta \cdot \gamma$.

Provando agora que $N(\rho) < N(\beta)$. Do resultado acima temos:

$$\begin{aligned} N(\rho) &= N(\alpha - \beta\gamma) \\ N(\rho) &= N[\beta \cdot (\frac{\alpha}{\beta} - \gamma)] \\ N(\rho) &= N(\beta) \cdot N(\frac{\alpha}{\beta} - \gamma). \end{aligned}$$

Como $\frac{\alpha}{\beta} = a + bi$ e $\gamma = s + ti$, temos:

$$\begin{aligned} N(\rho) &= N(\beta) \cdot N[(a + bi) - (s + ti)] \\ N(\rho) &= N(\beta) \cdot N[(a - s) + (b - t) \cdot i]. \end{aligned}$$

Lembrando que $a + bi = (s + f) + (t + g)i$, logo $a - s = f$, $b - t = g$ e $|f| \leq \frac{1}{2}$, $|g| \leq \frac{1}{2}$.

$$\begin{aligned} N(\rho) &= N(\beta) \cdot N(f + gi)) \\ N(\rho) &= N(\beta) \cdot (f^2 + g^2) \\ N(\rho) &\leq N(\beta) \cdot \left[\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right] \\ N(\rho) &\leq N(\beta) \cdot \left[\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\right] \\ N(\rho) &\leq N(\beta) \cdot \frac{1}{2} \end{aligned}$$

consequentemente temos $N(\rho) \leq N(\beta) \cdot \frac{1}{2} < N(\beta)$. ■

Observamos que na demontração apresentada temos a definição da existência do quociente e resto, porém não nos garantem sua unicidade.

Exemplo 24. *Determinar o quociente γ e resto ρ da divisão de $\alpha = 7+3i$ por $\beta = 4-i$.*

Utilizando o processo da divisão, teremos:

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{7 + 3i}{4 - i} \cdot \frac{(4 + i)}{(4 + i)} \\ &= \frac{25 + 7i + 12i + 3i^2}{4^2 + 1^2} \\ &= \frac{25}{17} + \frac{19}{17} \cdot i \end{aligned}$$

Seguindo como foi definido na demonstração, $\gamma = s + ti$, logo:

$$\begin{aligned} s &= \left\lfloor \frac{25}{17} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{67}{34} \right\rfloor = \left\lfloor 1,97... \right\rfloor = 1 \\ t &= \left\lfloor \frac{19}{17} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{55}{34} \right\rfloor = \left\lfloor 1,61... \right\rfloor = 1. \end{aligned}$$

Com isso, $\gamma = 1 + i$.

Determinando o resto:

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

Verificando a condição para o resto temos:

$$\begin{aligned} N(\rho) &= (2)^2 = 4 \\ N(\beta) &= 4^2 + 1^2 = 17 \\ N(\rho) &< N(\beta) \end{aligned}$$

Logo,

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

Exemplo 25. *Determinar o quociente γ e resto ρ da divisão de $\alpha = 8-2i$ por $\beta = 1+2i$.*

Utilizando o processo da divisão, teremos:

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{8 - 2i}{1 + 2i} \cdot \frac{(1 - 2i)}{(1 - 2i)} \\ &= \frac{8 - 16i - 2i + 4i^2}{1^2 + 2^2} \\ &= \frac{4}{5} - \frac{18}{5} \cdot i \end{aligned}$$

Seguindo como foi definido na demonstração, $\gamma = s + ti$, logo:

$$\begin{aligned} s &= \left\lfloor \frac{4}{5} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{13}{10} \right\rfloor = \left\lfloor 1,3 \right\rfloor = 1 \\ t &= \left\lfloor -\frac{18}{5} + \frac{1}{2} \right\rfloor = \left\lfloor -\frac{31}{10} \right\rfloor = \left\lfloor -3,1 \right\rfloor = -4 \end{aligned}$$

Com isso, $\gamma = 1 - 4i$.

Determinando o resto:

$$\begin{aligned} \alpha &= \beta \cdot \gamma + \rho \\ \rho &= \alpha - \beta \cdot \gamma \\ &= 8 - 2i - (1 + 2i)(1 - 4i) \\ &= 8 - 2i - (1 - 4i + 2i + 8) \\ &= 8 - 2i - 9 + 2i \\ &= -1. \end{aligned}$$

Verificando a condição para o resto temos:

$$\begin{aligned} N(\rho) &= (-1)^2 = 1 \\ N(\beta) &= 1^2 + 2^2 = 5 \\ N(\rho) &< N(\beta) \end{aligned}$$

Logo,

$$\begin{aligned} \alpha &= \beta \cdot \gamma + \rho \\ 8 - 2i &= (1 + 2i) \cdot (1 - 4i) - 1. \end{aligned}$$

Sobre os exemplos acima, verificamos e determinamos o Algoritmo da divisão em $\mathbb{Z}[i]$.

Destacamos que, poderiamos ou não encontrar outro quociente e resto para cumprir o Algoritmo da Divisão, pois não são únicos em $\mathbb{Z}[i]$. O exemplo a seguir detalha mais sobre essa particularidade.

Exemplo 26. *Dados os Inteiros Gaussianos $\alpha = 3 - 2i$ e $\beta = 1 + 2i$, determinar o quociente γ e resto ρ na divisão de α por β.*

Pela definição, o resto deve cumprir a condição $0 \leq N(\rho) < N(\beta)$. Assim, utilizando o processo da divisão, teremos:

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{3-2i}{1+2i} \cdot \frac{1-2i}{1-2i} \\ &= \frac{3-6i-2i+4i^2}{1^2+2^2} \\ &= -\frac{1}{5} - \frac{8}{5} \cdot i. \end{aligned}$$

Nesse momento, usando uma interpretação do que foi feito na demonstração para determinar o quociente devemos tomar inteiros mais próximos (em termos de distância) das partes real e imaginária, ou seja, a parte real $-\frac{1}{5}$ está compreendida entre -1 e 0, analogamente a parte imaginária $-\frac{8}{5}$ se enconta entre -1 e -2. Logo, realizando as combinações com os arredondamentos das partes real e imaginária, levando em consideração todos os valores possíveis, temos os seguintes quocientes γ :

s	t	γ
0	-1	$0-i$
0	-2	$0-2i$
-1	-1	$-1-i$
-1	-2	$-1-2i$

Tabela 3.1: Possíveis quocientes

Dos possíveis valores para o quociente, podemos encontrar os respectivos restos. Com esses valores determinamos então o Algoritmo da Divisão em $\mathbb{Z}[i]$.

(i) Para $\gamma = 0 - i$

$$\begin{aligned} \alpha &= \beta \cdot \gamma + \rho \\ \rho &= \alpha - \beta \cdot \gamma \\ &= 3 - 2i - (1+2i)(-i) \\ &= 3 - 2i - (-i - 2i^2) \\ &= 3 - 2i - (2 - i) \\ &= 3 - 2i - 2 + i \\ &= 1 - i. \end{aligned}$$

Verificando a condição para o resto temos:

$$\begin{aligned} N(\rho) &= 1^2 + (-1)^2 = 2 \\ N(\beta) &= 1^2 + 2^2 = 5 \\ N(\rho) &< N(\beta) \end{aligned}$$

Com isso encontramos um dos quociente e resto da divisão de α por β. Logo,

$$\begin{aligned} \alpha &= \beta \cdot \gamma + \rho \\ 3 - 2i &= (1 + 2i) \cdot (-i) + (1 - i). \end{aligned}$$

(ii) Para $\gamma = 0 - 2i$

$$\begin{aligned} \alpha &= \beta \cdot \gamma + \rho \\ \rho &= \alpha - \beta \cdot \gamma \\ &= 3 - 2i - (1 + 2i)(-2i) \\ &= 3 - 2i - (-2i - 4i^2) \\ &= 3 - 2i - (4 - 2i) \\ &= 3 - 2i - 4 + 2i \\ &= -1. \end{aligned}$$

Verificando a condição para o resto temos:

$$\begin{aligned} N(\rho) &= (-1)^2 = 1 \\ N(\beta) &= 1^2 + 2^2 = 5 \\ N(\rho) &< N(\beta) \end{aligned}$$

Tendo assim um novo quociente e resto da divisão de α por β. Logo,

$$\begin{aligned} \alpha &= \beta \cdot \gamma + \rho \\ 3 - 2i &= (1 + 2i) \cdot (-2i) + (-1). \end{aligned}$$

(iii) Para $\gamma = -1 - i$

$$\begin{aligned}
\alpha &= \beta \cdot \gamma + \rho \\
\rho &= \alpha - \beta \cdot \gamma \\
&= 3 - 2i - (1 + 2i)(-1 - i) \\
&= 3 - 2i - (-1 - i - 2i - 2i^2) \\
&= 3 - 2i - (1 - 3i) \\
&= 3 - 2i - 1 + 3i \\
&= 2 + i.
\end{aligned}$$

Verificando agora a condição para o resto temos:

$$\begin{aligned}
N(\rho) &= 2^2 + (-1)^2 = 5 \\
N(\beta) &= 1^2 + 2^2 = 5 \\
N(\rho) &= N(\beta)
\end{aligned}$$

Observamos que a condição para a norma do resto não foi satisfeita, logo os valores encontrados não são válidos.

(iv) Para $\gamma = -1 - 2i$

$$\begin{aligned}
\alpha &= \beta \cdot \gamma + \rho \\
\rho &= \alpha - \beta \cdot \gamma \\
&= 3 - 2i - (1 + 2i)(-1 - 2i) \\
&= 3 - 2i - (-1 - 2i - 2i - 2i^2) \\
&= 3 - 2i - (1 - 4i) \\
&= 3 - 2i - 1 + 4i \\
&= 2 - 2i.
\end{aligned}$$

Verificando agora a condição para o resto temos:

$$\begin{aligned} N(\rho) &= 2^2 + (-2)^2 = 8 \\ N(\beta) &= 1^2 + 2^2 = 5 \\ N(\rho) &> N(\beta) \end{aligned}$$

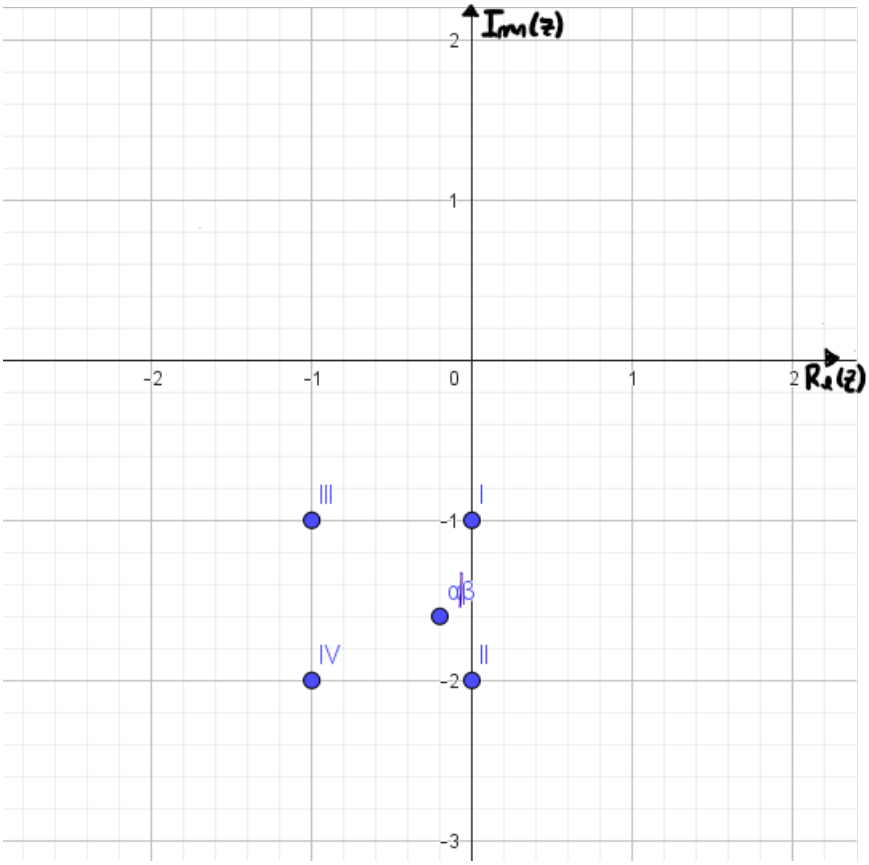
Pelo resultado acima, temos que o quociente e resto não são válidos. Pois, $N(\rho)$ deve ser menor que a $N(\beta)$.

Analizando o exemplo apresentado, podemos retirar algumas observações:

- O Algoritmo da Divisão em $\mathbb{Z}[i]$, o quociente e resto não são únicos como mostra o caso (i) e o caso (ii) nos quais obtemos quociente e resto que sastifazem as condições do Algoritmo da Divisão em $\mathbb{Z}[i]$, diferindo do Algoritmo da Divisão em $\mathbf{Z}$ no qual o quociente e resto são únicos.

- O processo para determinar γ. De acordo com a demonstração, para determinar o quociente devemos tomar os interios mais próximos do resultado da divisão de $\frac{\alpha}{\beta}$ e assim definir tal quociente e seu respectivo resto que satisfaz a condição para sua existência e assim concluir o Algoritmo da Divisão em $\mathbb{Z}[i]$. E nesse processo temos que em um caso geral, o resultado de tal divisão $\frac{\alpha}{\beta}$ se encontra entre quatro Inteiros Gaussianos, tal fato é apresentado na figura 3.1.
  Mediante o exemplo, no caso (i) e (ii) os quocientes e seus respectivos restos satisfizeram as condições do algoritmo, e de fato esses dois casos representam os Inteiros Gaussianos mais próximos (em temos de distância) do resultado da divisão, enquanto os casos (iii) e (iv) apresentam quocientes que são resultados de um arredondamento que é feito para Interios Gaussinos que se encontram mais distantes (em termos de distância) do resultado da divisão. Como ilustra a figura 3.3.

Figura 3.3: Representação gráfica dos inteiros mais próximos da divisão de α por β



Fonte: Do Autor(2023)

É possível ver geometricamente que de fato a divisão de α por β se encontra mais próximo dos Inteiros Gaussianos considerados nos casos (i) e (ii).

Considerações Finais

Nesta pesquisa, realizamos uma abordagem introdutória ao conjunto dos Inteiros Gaussianos, partindo da hipótese de semelhança com o conjunto dos Inteiros nos quais são válidos definições e demonstrações de caráter análogo. Com o fim da pesquisa, observa-se uma sustentação do propósito inicial e um alcance do objetivo da pesquisa na qual se refere que é possível compreender o conjunto dos Inteiros Gaussianos realizando uma analogia com os Inteiros.

De acordo com a pesquisa, é possível observar alguns tópicos mencionados que possibilitam uma reflexão e base para outras pesquisas relacionadas a temáticas, como por exemplo os números primos, tal aspecto trabalhado na pesquisa possibilita uma compreensão dos Primos Gaussianos e que pode ser utilizada como base para trabalhos que diz respeitos a primalidades em diferentes estruturas numéricas.

O Algoritmo da divisão em $\mathbb{Z}[i]$, é possível observar uma particularidade neste aspecto na qual o quociente e resto não são únicos. Com isso, verifica-se uma particularidade em relação ao quociente e resto em um divisão dependendo da estrutura e ambiente matemático que se está trabalhando. E essa reflexão pode servir como base para trabalhos que levem a temática em questão com perguntas relacionadas à, como a quantidade de quociente e resto está relacionada com a aritmética que se está trabalhando?

Com tudo, a pesquisa apresentada contribui para o conhecimento de um conjunto pouco mencionado, até mesmos em livros nacionais, e esse contato com assuntos desse ramo matemático nos possibilita um pensamento investigativo em especial acerca da teoria dos números e que serve como apoio para assuntos mais complexos como os Inteiros Algébricos que necessitam de um conhecimento prévio.

Referências Bibliográficas

BERTONE, A. ***Introdução a teoria dos números***. Uberlândia - MG: UFU, 2014.

BOYER, C. ***Históra da matemática***. 2. ed. São Paulo: Blucher, 1996.

FILHO, E. ***TEORIA ELEMENTAR DOS NÚMEROS.*** São Paulo: Nobel, 1981.

GALDINNO, U. ***Teoria dos números e criptografia com aplicações básicas***. 2014. Disponível em:⟨http://tede.bc.uepb.edu.br/jspui/bitstream/tede/2266/5/PDF%20-%20Uelder%20Alves%20Galdino.pdf⟩. Acesso em: 07 de julho de 2022.

GERHARDT, T. ***Métodos da pesquisa***. Porto Alegre: Editora da UFRGS, 2009.

HEFEZ, A. ***Curso de Ágebra, volume 1***. 3. ed. Rio de Janeiro: IMPA, 2002.

IEZZI, G. ***Fundamentos de matemática elementar: complexos, polinômios, equações.*** 8. ed. São Paulo: Atual, 2013.

MARTINEZ, F. B. E. A. ***Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro***. 4. ed. Rio de Janeiro: IMPA, 2018.

MESQUITA, M. ***A pesquisa e a construção do conhecimento científico: do planejamento aos textos, da escola à academia.*** 3. ed. São Paulo: Rêspel, 2007.

ROONEY, A. ***A Históra da matemática - desde a criação da pirâmedes até a exploração do infinito***. São Paulo: M. Books do Brasil, 2012.

ROSEN, K. ***Elementary number theory***. 6. ed. Boston: Pearson, 2011.

SANTOS, J. ***Introdução a teoria dos números***. São Paulo: IMPA, 2020.