UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA

INTEIROS DE GAUSS: UMA ABORDAGEM ELEMENTAR

Icoracy Coutinho da Costa

MANAUS
2016

UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA

Icoracy Coutinho da Costa

INTEIROS DE GAUSS: UMA ABORDAGEM ELEMENTAR

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Alfredo Wagner Martins Pinto

MANAUS
2016

Ficha Catalográfica

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

Costa, Icoracy Coutinho da
C837i INTEIROS DE GAUSS: Uma Abordagem Elementar / Icoracy Coutinho da Costa. 2016
48 f.: il.; 31 cm.

Orientador: Prof. Dr. Alfredo Wagner Martins Pinto
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Amazonas.

1. Números Complexos. 2. Inteiros de Gauss. 3. Norma. 4. Primos de Gauss. I. Pinto, Prof. Dr. Alfredo Wagner Martins II. Universidade Federal do Amazonas III. Título

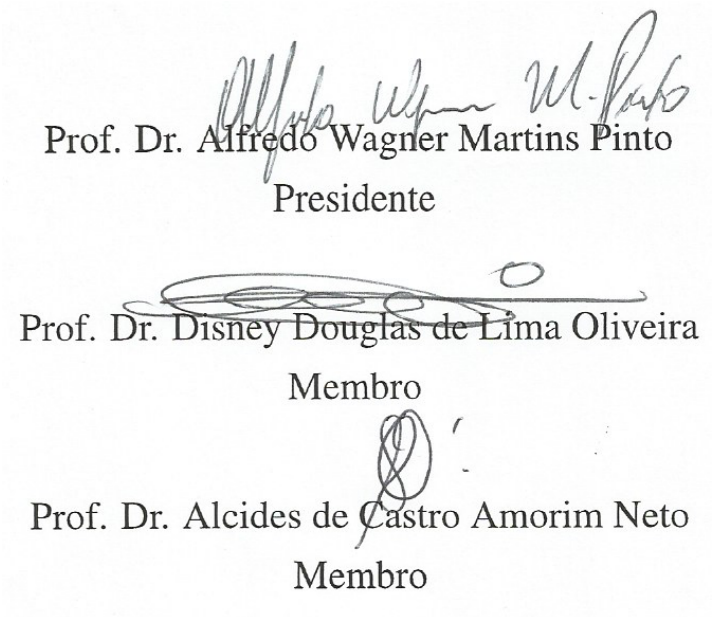
ICORACY COUTINHO DA COSTA

INTEIROS DE GAUSS: UMA ABORDAGEM ELEMENTAR

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em 30 de março de 2016.

BANCA EXAMINADORA



Prof. Dr. Alfredo Wagner Martins Pinto
Presidente

Prof. Dr. Disney Douglas de Lima Oliveira
Membro

Prof. Dr. Alcides de Castro Amorim Neto
Membro

AGRADECIMENTOS

Ao Grande Arquiteto do Universo, pelo dom da vida e bênçãos a mim concedidas por sempre guiar meus passos para realizar com sucesso os meus objetivos.

A minha mãe, Lindalva Coutinho da Costa e, ao meu pai, Coracy Alves da Costa, em memória, que sempre foram minha base forte nesta caminhada, o meu muito obrigado por todos os princípios que me foram passados.

A meus amores Nildes Oliveira da Costa, Giselle Oliveira da Costa e Aline Oliveira da Costa, esposa e filhas, pela dedicação, amor, apoio e principalmente pelo incentivo constante sem o qual eu não estaria concretizando este sonho.

Ao meu orientador Prof. Dr. Alfredo Wagner, pela confiança e dedicação, por toda liberdade no desenvolvimento deste estudo e ter acreditado em meu potencial me conduzindo para esta realização, obrigado pelas horas e apoio disponibilizados.

A todos meus professores do PROFMAT, pela arte de ensinar, por nos desafiar e acreditar em nossa capacidade de aprender sempre mais.

Enfim, agradeço a todos os amigos e, em especial, aos amigos Ramina Samoa Camargo, Yury dos Santos Bezerra, Euderley de Castro Nunes e Roquelane pelo companheirismo nas árduas vitórias conquistadas e todas as pessoas que, direta ou indiretamente, contribuíram para a execução dessa Dissertação de Mestrado.

RESUMO

Este trabalho tem como objetivo contribuir para o aprimoramento dos alunos do Ensino Médio no estudo do Conjunto dos Números Complexos, apresentando-lhes um de seus subconjuntos que possuí uma grande importância no estudo da Álgebra. Este conjunto é denominado de Conjunto dos Inteiros de Gauss.

Inicialmente demonstraremos que o Conjunto dos Inteiros de Gauss é uma estrutura algébrica, mais precisamente um Domínio Fatorial. Na abordagem será feita a comparação entre os esses dois conjuntos definindo as operações de adição, subtração, multiplicação, divisão e potenciação na forma algébrica. Será feita, ainda, um estudo sobre os números primos dentro do Conjunto dos Inteiros de Gauss que serão comparados com os números primos do Conjunto dos Números Inteiros que possibilitará a visualização das diferenças existentes. Por fim, concluiremos com a apresentação de algumas aplicações dos inteiros de Gauss.

Palavras-chave: Números Complexos; Inteiros de Gauss; Norma; Primos de Gauss.

ABSTRACT

The purpose of this research is to help High school students to learn complex number sets. Will be shown one of its subsets that has a great importance in Algebra, the Gaussian integers.

At first, the study will demonstrate that Gaussian integers are an Algebraic structure, a Euclidean domain to be more specific. The study will compare the addition, subtraction, multiplication, division and exponentiation in algebraic form. Then, we will analyze the prime number in the Gaussian integers sets and compare them to prime numbers in the integer sets to show the differences. At last, some Gaussian integers applications will be presented.

Keywords: Complex Numbers; Gauss integers; Norm; Gauss primes.

Sumário

Lista de Figuras

LISTA DE SÍMBOLOS

A^*	Conjunto dos Elementos invertíveis de um Anel A
$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{R}$	Conjunto dos Números Reais
$\mathbb{C}^*$	Conjunto dos Números Complexos
$\mathbb{Z}[i]$	Conjunto dos Inteiros de Gauss
$\left[\frac{a}{b}\right]$	Parte inteira da Divisão Euclidiana

Capítulo 1

Introdução

O estudo dos números complexos ocorre dentro do Ensino Médio, tendo como justificativa a resolução de equações do segundo grau cujo discriminante é menor que zero, sem que seja feita nenhuma referência à sua estrutura de "Corpo", "Anel"ou "Dominio Euclidiano". Nessa fase os alunos passam a conhecer a unidade imaginária $\sqrt{-1}$ e começam o aprendizado das operações de soma, subtração, multiplicação e divisão com esses números. Com base nesse conhecimento básico da álgebra dos números complexos pelos alunos do Ensino Médio e sabendo que a álgebra dos inteiros de Gauss é assemelhada, pretendemos com esse trabalho ampliar esse conteúdo mostrando um pouco da história do desenvolvimento desse conjunto e, apresentar o subconjunto denominado de "Inteiros de Gauss".

Capítulo 2

Um Pouco da História

2.1 Números Complexos

Conforme Cevi e Monteiro [1], a resolução de equações sempre foi um assunto fascinante para os matemáticos ao longo da história. Na antiga Babilônia, os matemáticos resolviam algumas equações do segundo grau através do método hoje chamado "completamento dos quadrados".

Os gregos, de grande importância no desenvolvimento da matemática, utilizavam a régua e o compasso para resolver alguns tipos de equação do segundo grau.

A derrota da Grécia para Roma praticamente acabou com o domínio da matemática Grega. Com o surgimento do cristianismo e a queda do Império Romano, o desenvolvimento da matemática passou para a mão dos Árabes e dos Hindus.

Com o avanço dos matemáticos Hindus nas pesquisas em álgebra e na resolução de equações de 2º grau surge o nome de BASKARA. Entretanto o desenvolvimento do método de resolução das equações de 2º grau que resultam na fórmula de BASKARA é, na verdade de responsabilidade do matemático hindu SRIDHARA, no século II.

Relembrando, dada a equação $ax^2 + bx + c = 0$, com$a \neq 0$, a fórmula de BASKARA mostra que suas raízes são

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad e \quad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

Dependendo da equação, o número $\Delta = b^2 - 4ac$ pode assumir um resultado negativo. Ora, qualquer matemático da época classificaria a equação como absurda, ou seja, sem solução. Nem sequer perdia tempo com ela.

Foi na Itália, no século XVI, que ressurgiu o interesse pelo estudo da matemática na Europa. Lá, e no meio da disputa entre Girolamo Cardano e Nicolo Fontana, vulgo Tartaglia, pela resolução da equação do 3º grau, é que se percebeu que os números reais não eram suficientes e as primeiras ideias da criação do conjunto dos Números Complexos surgiram.

Rememoremos um pouco dessa conturbada história. Girolamo Cardano, nascido em Pávia (1501-1576)¨, era um excepcional cientista, mas não era bem visto pois também era considerado violento, traidor, invejoso e outras qualificações não muito edificantes. Foi o autor de Liber de Ludo Aleae, onde introduziu a ideia de probabilidade e também ensinou maneiras de trapacear nos jogos. Sua maior obra, entretanto,foi o Ars Magna, publicado na Alemanha em 1545, que na época era o maior compêndio algébrico existente.

Nicolo Fontana, o Tartaglia, também tinha talento de matemático e como Cardano era italiano. Nascido em Bréscia em 1500, na sua infância, pobre, foi gravemente ferido por golpes de sabre e, por causa deste incidente, ficou com profunda cicatriz na boca que lhe provocou um permanente defeito na fala. Daí ter sido apelidado de Tartaglia, que significa gago. Ao longo de sua vida publicou diversas obras mas o que o colocou definitivamente nos anais da Matemática foram suas disputas com Cardano.

Consta que, por volta de 1510, um matemático italiano de nome Scipione Del Ferro encontrou uma forma geral de resolver equações do tipo $x^3 + px + q = 0$, mas morreu sem publicar sua descoberta. Seu aluno Antonio Maria Fior conhecia tal solução e tentou ganhar notoriedade com ela. Na época eram comuns os desafios entre sábios. Como Tartaglia era um nome que começava a se destacar nos meios culturais da época, Fior propôs a Tartaglia um desafio. Tartaglia, apesar de não saber resolver ainda tais equações, aceitou o desafio, confiando em seu potencial. Sabendo que Fior conhecia a solução das equações acima citadas, não so deduziu a resolução para este caso, como também resolveu as equações do tipo $x^3 + px^2 = 0$. O resultado deste desafio foi que Fior saiu humilhado.

Nesta época Cardano estava escrevendo a Á Prática Arithmeticae Generalis, que continha ensinamentos sobre álgebra, Aritmética e Geometria. Ao saber que Tartaglia achara a solução geral da equação de 3º grau pediu-lhe que a revelasse, para que fosse publicada em seu próximo livro.

Tartaglia não concordou, alegando que ele mesmo iria publicar sua descoberta. Cardano acusou-o de mesquinho e egoísta, e não desistiu. Após muitas conversas e súplicas este, jurando não divulgar tal descoberta, conseguiu que Tartaglia lhe revelasse a solução. Conforme qualquer um poderia prever, Cardano quebrou todas as promessas e, em 1545, fez publicar Ars Magna a fórmula de Tartaglia. No final, como em muitos outros casos, a posteridade não fez justiça a Tartaglia, sua fórmula é até hoje conhecida como "Fórmula de Cardano".

Observemos essa fórmula que gerou tanta polêmica:

Seja a equação do terceiro grau $ax^3 + bx^2 + cx + d = 0$, com $a \neq 0$.

Tartaglia demonstrou que realizando a substituição $x = y - \dfrac{a}{b}$ elimina-se o termo x^2 da equação.

Na prática, devemos fazer a substituição de variáveis. Considerando $y = x + m$ uma variável de x, temos que $x = y - m$.

Substituindo na equação de terceiro grau:

$a(y - m)^3 + b(y - m)^2 + c(y - m) + d = 0$

$ay^3 - 3ay^2m + 3aym^2 - am^3 + by^2 - 2bym + bm^2 + cy - cm + d = 0.$

$ay^3 - 3ay^2m + by^2 + 3aym^2 - 2bym + cy - am^3 + bm^2 - cm + d = 0$

$ay^3 + (-3am + b)y^2 + (3am^2 - 2bm + c)y - am^3 + bm^2 - cm + d = 0.$

Como queremos que o termo y^2 seja nulo. Então fazemos:

$-3am + b = 0 \Longrightarrow m = \dfrac{b}{3a}$

Substituindo m:

$ay^3 + \left(\dfrac{-b^2}{3a} + c\right)y + \left(\dfrac{2b^3 - 9abc + 27a^2d}{27a^2}\right) = 0$

Como $a \neq 0$, podemos dividir toda a equação por a.

$y^3 + \left(\dfrac{-b^2}{3a^2} + \dfrac{c}{a}\right)y + \left(\dfrac{2b^3 - 9abc + 27a^2d}{27a^3}\right) = 0$

Fazendo:

$-\dfrac{b^2}{3a^2} + \dfrac{c}{a} = p$ e $\dfrac{2b^3 - 9abc + 27a^2d}{27a^3} = q$, temos uma equação na incógnita simplificada y do tipo:

$$y^3 + py + q = 0$$

.

Podemos expressar y na forma de uma soma de dois números os quais são raízes da equação, onde $y = u + v$. Logo:

$(u + v)^3 + p(u + v) + q = 0$

$u^3 + 3u^2v + 3uv^2 + v^3 + pu + pv + q = 0$

$v^3 + u^3 + 3uv(u + v) + p(u + v) + q = 0$

$(v^3 + u^3) + (3uv + p)(u + v) + q = 0$

A equação é verdade para:

$v^3 + u^3 = -q$, e $3uv + p = 0 \Longrightarrow uv = -\dfrac{p}{3} \Longrightarrow u^3v^3 = -\dfrac{p^3}{27}$

Analisando o resultado anterior, vemos que u^3 e v^3 são raízes de uma equação do tipo $w^2 - Sw + P = 0$, onde S e P são respectivamente a soma e o produto das raízes. Logo, podemos escrever tal equação como:

$w^2 + qw - \dfrac{p^3}{27} = 0$

Resolvendo a equação, temos:

$w = \dfrac{-q \pm \sqrt{q^2 - 4\left(\dfrac{-p^3}{27}\right)}}{2}$, onde $w = \dfrac{-q}{2} \pm \sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}}$.

Como u^3 e v^3 são raízes dessa equação e $y = u + v$, então essa fórmula fornece as raízes da equação de 3º grau do tipo $x^3 + px + q = 0$.

Um problema inquietante, que veremos a seguir foi o que levou os matemáticos à descoberta dos números complexos. Na equação $x^3 - 15x - 4 = 0$ é de fácil visualização que 4 é uma das raízes, entretanto aplicando a fórmula de Cardano a solução fornecida é:

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

Parecia haver algo errado com essas soluções. Assim, questões realmente perturbadoras surgiram e não podiam ser ignoradas. Nas equações de grau 2, quando a fórmula de Baskara levava à raiz quadrada de números negativos, era fácil dizer que aquilo indicava a não existência de soluções. Agora, entretanto, notava-se que existiam equações de grau 3 com soluções reais conhecidas, mas cuja determinação passava pela extração de raízes quadradas de números negativos. Isto não ocorria somente com essa equação. Era fácil mostrar que a equação do tipo $x^3 + px + q = 0$ tem 3 raízes reais se, e somente se,

$$\Delta = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 \leq 0$$

.

Não havia como negar que os números reais eram insuficientes para se tratar de equações algébricas. Estava acontecendo no século XVI algo semelhante ao que ocorreu no tempo dos gregos antigos, quando se verificou a insuficiência dos números racionais com a construção do número $\sqrt{2}$, que não era racional: o conceito de número precisava novamente ser estendido.

Foi Rafael Bombelli, italiano, nascido em 1530, quem conseguiu chegar aos novos números. Conforme seu próprio relato em 1572 no livro L'Algebra parte maggiore dell'Arithmética, sua ideia foi supor que os números $\sqrt[3]{2 + \sqrt{-121}}$ e $\sqrt[3]{2 - \sqrt{-121}}$ deveriam ser números da forma $a + \sqrt{-b}$ e $a - \sqrt{-b}$, respectivamente. Com algumas contas ele chegou a conclusão que a=2 e b=1, donde sai que x=4. Logo, os números que viriam a ser chamados Complexos podiam produzir raízes reais. Bombelli reconhece, em sua obra, a existência dos imaginários puros, isto é, complexos da forma bi ou $-bi$, e estabelece as operações entre eles.

Depois de Bombelli, em 1530, outros personagens importantes da História da Matemática deram contribuições ao desenvolvimento da teoria dos Números Complexos, dentre os quais o matemático francês Abraham de Moivre e os irmãos Jacques e Jean Bernoulli. Mas quem fez o trabalho mais importante e decisivo sobre o assunto foi Euler.

Leonhard Euler nasceu em Basileia, Suiça, no ano de 1707. Foi um dos matemáticos que mais produziu e publicou em todos os tempos, além de ter sido muito boa pessoa. Dentre as inúmeras contribuições de Euler, foi notável seu empenho na melhoria da simbologia. Muitas das notações que utilizamos hoje foram introduzidas por ele. Dentre as representações propostas por Euler destacamos o i substituindo $\sqrt{-1}$.

Euler passou a estudar números da forma $z = a + bi$ onde a e b são números reais e $i^2 = -1$.

Esses são os chamados Números Complexos.

2.2 Inteiros de Gauss

O Matemático alemão Carl F. Gauss produziu em todos os ramos da matemática. Mas sabe-se que sentia prazer pela investigação em Aritmética. Foi ele quem lançou os fundamentos

da moderna Teoria dos Números em sua monumental obra "Disquisitiones Arithmeticae"que contém grandes contribuições à Aritmética e à Álgebra, publicada em 1801.

Os inteiros de Gauss ou conjunto dos Inteiros Gaussianos são números complexos da forma $a + bi$, onde a e b são inteiros e $i = \sqrt{-1}$. O conjunto $\mathbb{Z}[i]$ dos inteiros de Gauss surgiu entre os anos de 1808 e 1825, época em que o matemático Carl F. Gauss investigava a reciprocidade cúbica ($x^3 \equiv q$ (mod p), onde p e q são primos) e também a reciprocidade biquadrática ($x^4 \equiv q$ (mod p), onde p e q são primos). Gauss percebeu que essa investigação se tornava mais fácil trabalhando em $\mathbb{Z}[i]$, o anel dos Inteiros de Gauss.

Em 1825, publicou um trabalho em que introduzia os números complexos. Na época Gauss estava investigando questões relacionadas à reciprocidade biquadrática, ou seja, relações entre números primos p e q, tal que o primo q fosse um resto biquadrático do primo p, $x^4 = q(modp)$, quando percebeu que a pesquisa se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$. Desse modo, Gauss estendeu a ideia de Número Inteiro quando definiu $\mathbb{Z}[i]$, pois descobriu que muito da antiga teoria de Euclides sobre fatoração de inteiros poderia ser transportada para esse conjunto com consequências importantes para a Teoria dos Números.

Gauss desenvolveu uma Teoria de Fatorização em primos para esses números Complexos e demonstrou que essa decomposição em primos é única, tal qual no Conjunto dos Números Inteiros. O uso desse estudo foi de fundamental importância para a demonstração do Último Teorema de Fermat.

O desenvolvimento da Teoria dos Números Algébricos foi, em parte, em função das tentativas de solução da equação diofantina, também conhecida como equação de Fermat

$$x^n + y^n = z^n,$$

pois os inteiros algébricos aparecem de maneira natural, como ferramenta para tratar desse assunto.

Essa generalização do Conjunto dos Números Inteiros dá exemplos especiais de desenvolvimento muito mais profundos que chamamos de Teoria dos Números Algébricos. Essa teoria é profunda e poderosa. Além do interesse e fascínio que exerce por suas próprias propriedades, fornece muitas aplicações à Teoria dos Números que permitem uma compreensão de vários fenômenos antes obscuros e misteriosos.

Neste Trabalho estaremos observando alguns desses fenômenos.

Capítulo 3

Números Inteiros

Por muitos milênios os números foram considerados entes intuitivos e algumas de suas propriedades, como a comutatividade e associatividade da adição e da multiplicação, consideradas inerentes à sua própria natureza, sem a necessidade de demonstração.

Com o desenvolvimento da matemática surgiram novos problemas que, para melhor serem compreendidos e solucionados, precisavam de uma fundamentação mais rigorosa do conceito de número. Este trabalho foi realizado pelos matemáticos do século dezenove.

Para os Números naturais prevaleceu a axiomática de Giuseppe Peano, de 1889, que conforme Hefez [8], consiste de quatro axiomas que caracterizam os Números Naturais completamente:

1. Todo Número Natural tem um sucessor, que ainda é um número natural;
2. Números Naturais diferentes têm sucessores diferentes;
3. Existe um único Natural 1 que não é sucessor de nenhum outro natural;
4. Se um conjunto de números naturais contém o número 1 e contém também o sucessor de cada um de seus elementos, então esse conjunto contém todos os números naturais.

Não vamos realizar a construção desse conjunto.

Apresentaremos o estudo dos inteiros de forma axiomática, conforme Hefez [8], a partir de uma lista de propriedades básicas que os caracterizarão completamente, e delas deduziremos as demais propriedades.

3.1 Propriedades Elementares

No conjunto $\mathbb{Z}$ dos números inteiros estão definidas duas operações, uma adição $(+)$ e uma multiplicação $(.)$, além de uma relação de ordem $(\leq)$. Esses elementos se relacionam através de várias propriedades que serão listadas paulatinamente. Esta lista de propriedades caracterizam completamente os números inteiros.

3.2 Anéis

Sejam A um conjunto e $(+)$ e $(.)$ duas operações em A, chamadas de adição e multiplicação. A terna $(A, +, .)$ será chamada de anel se as operações gozarem das seis primeiras propriedades e, de Anel comutativo com unidade se gozar das oito propriedades seguintes. $\forall\ a, b, c \in A$

1. A_1 **(A Adição é Associativa):**

   `(a + b) + c = a + (b + c)`

2. A_2 **(A Adição é Comutativa):**

   `a + b = b + a`

3. A_3 **(Existe um Elemento Neutro para a Adição):**

   Existe $\alpha \in A$ tal que $\alpha + x = x, \forall x \in A$.

4. A_4 **(Todo Elemento de A possui um Simétrico):**

   $\forall a \in A, \exists a' \in A$ tal que $a + a' = 0$.

5. M_1 **(A multiplicação é associativa):**

   Quaisquer que sejam $a, b, c \in A$, tem-se que $(a.b).c = a.(b.c)$.

6. AM **(A multiplicação é distributiva com relação à adição):**

   Quaisquer que sejam $a, b, c \in A$, tem-se que $a.(b + c) = a.b + a.c$; $(a + b).c = a.c + b.c$.

7. M_2 **(A multiplicação é comutativa):**

   Quaisquer que sejam $a, b \in A$, tem-se que $a.b = b.a)$.

8. M_3 **(Existe um elemento neutro para a multiplicação):**

   Existe $\kappa \in A$, com $\kappa \neq 0$, tal que $x.\kappa = x$ para todo $x \in A$.

Observações

Usaremos o símbolo 0 para denotar o elemento neutro da adição que será chamado zero.

Usaremos o símbolo 1 para denotar o elemento neutro da multiplicação que será chamado de *unidade* ou apenas *um*.

O simétrico de a será simbolizado por $-a$ e é único. Note que o simétrico de $-a$ é a.

Usaremos a notação $a - b$ para representar a + (-b). Esta operação em A é chamada de *subtração*.

Um elemento $a \in A$ será dito invertível, se existir um elemento $b \in A$ tal que $a.b = 1$. Esse tal elemento b será chamado de inverso de a. O inverso de um elemento a, se existir, é

único. No caso em que a é invertível, o seu (único inverso) será denotado por a^{-1}. Denotaremos por A^* o conjunto dos elementos invertíveis de um anel A. Observe que se $x, y \in A^*$, então $x.y \in A^*$, isto é, A^* é fechado com respeito a multiplicação de A. Note também que $1 \in A^*$ e que se $x \in A^*$, então $x^{-1} \in A^*$ (pois segue da definição que o inverso de x^{-1} é o próprio x).

Um anel comutativo com unidade A será chamado de *domínio de integridade* ou simplesmente de *domínio* se for verificada uma das seguintes propriedades.

1. M_4 (Integridade)

   Dados $a, b \in A$, se $a \neq 0$ e $b \neq 0$, então $a.b \neq 0$.

   A propriedade acima pode ser escrita da seguinte forma:

2. M_4' (Integridade)

   Dados $a, b \in A$, se $a.b = 0$, então $a = 0$ ou $b = 0$.

O axioma abaixo caracteriza parcialmente o conjunto dos inteiros.

Axioma 3.2.1. $(\mathbb{Z}, +, .)$ *é um domínio de integridade.*

Proposição 3.2.1. *(Lei do cancelamento). Seja A um domínio de integridade. Para todos $a, x, y \in A$ com $a \neq 0$, se $a.x = a.y$, então $x = y$.*

3.3 Anéis Ordenados

Uma relação binária num conjunto A é uma sentença aberta no conjunto A x A.

Um anel A será chamado de *anel ordenado* se existir uma relação binária $x \leq y$, que se lê x é *menor do que ou igual* a y, que goza das seguintes propriedades:

$\mathbb{O}_1$**(Reflexividade)** Para todo $a \in A$, temos $a \leq a$.

$\mathbb{O}_2$**(Antisimetria)** Para todos $a, b \in A$, se $a \leq b$ e $b \leq a$, então $a = b$.

$\mathbb{O}_3$**(Transitividade)** Para todos $a, b, c \in A$, se $a \leq b$ e $b \leq c$, então $a \leq c$.

$\mathbb{O}_4$**(Totalidade)** Dados $a, b \in A$, tem-se que é verdadeira uma das asserções $a \leq b$ ou $b \leq a$.

$\mathbb{OA}$**(Compatibilidade com a Adição)** Para todos $a, b, c \in A$, se $a \leq b$, então $a + c \leq b + c$.

$\mathbb{OM}$**(Compatibilidade com a Multiplicação)** Para todos $a, b, c \in A$, se $a \leq b$ e $0 \leq c$, então $a.c \leq b.c$.

Usaremos a notação $a < b$, que se lê a é *menor do que* b, para indicar que $a \leq b$ com $a \neq b$. Usaremos também as notações $b > a$, que se lê b é *maior do que* a, e $b \geq a$, que se lê b è *maior do que ou igual* a a, significando $a < b$ e $a \leq b$, respectivamente.

Damos mais um passo na axiomatização do conjunto $\mathbb{Z}$ dos inteiros, complementando o Axioma 1 como segue:

Axioma 3.3.1. $(\mathbb{Z}, +, ., \leq)$ *é um domínio ordenado.*

Num anel ordenado define-se o *valor absoluto* de um elemento $a \in A$ como sendo,

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

Segue imediatamente dessa definição que $|a| \geq 0$, para todo $a \in A$ e que vale a igualdade se e somente se $a = 0$.

Proposição 3.3.1. *Sejam A um anel ordenado e $a, b, r \in A$. Temos que*

(i) $|a.b| = |a|.|b|$

(ii) $-|a| \leq a \leq |a|$

(iii) $|a| \leq r$ *se e somente se* $-r \leq a \leq r$

(iv) $|a + b| \leq |a| + |b|$

Corolário 3.3.1. *Sejam A um anel ordenado e $a, b \in A$. Temos que*

$$||a| - |b|| \leq |a \pm b| \leq |a| + |b|.$$

Indicamos [8] para as demonstrações da proposição 3.3.1 e seu corolário.

3.4 Anéis bem ordenados

Um subconjunto S de um anel ordenado A será dito *limitado inferiormente* (respectivamente *superiormente*), se existir um elemento $a \in A$ tal que para todo $x \in S$ se tenha $x \geq a$ (respectivamente $x \leq a$). O conjunto vazio é considerado limitado inferiormente e superiormente.

Diremos que S tem um menor elemento (respectivamente maior elemento), se existir $b \in S$ tal que para todo $x \in S$ se tenha $x \geq b$ (respectivamente, $x \leq b$). Se existir um menor elemento de um subconjunto S de um anel ordenado A, este é único. De fato, se b e b' são menores elementos de S, temos que $b \leq b'$ e $b' \leq b$, logo pela antisimetria da relação de ordem $\leq$, segue que $b = b'$. No caso em que existe o menor elemento de S, ele é denotado por min$S$. A mesma observação vale para o maior elemento que será denotado por max S.

Um domínio ordenado A será chamado de *domínio bem ordenado* se gozar da seguinte propriedade.

PBO (Princípio da Boa Ordenação). Todo subconjunto não vazio de A limitado inferiormente possui um menor elemento.

A propriedade acima é equivalente à seguinte propriedade.

PBO'. Todo subconjunto não vazio de A limitado superiormente possui um maior elemento.

De fato, isto segue das seguintes observações fáceis de verificar.

Seja $\emptyset \neq S \subset A$, defina $S' = \{-b \mid b \in S\}$. Então S é limitado inferiormente se e somente se S' é limitado superiormente. Tem-se também que S possui um menor elemento se e somente se S' possui um maior elemento (neste caso tem-se que min S = -max S').

Daremos a seguir a axiomática completa dos números inteiros.

Axioma 3.4.1. *Axiomas dos números inteiros.*

$(\mathbb{Z}, +, ., \leq)$ *é um domínio bem ordenado.*

A seguir alguns resultados característicos dos domínios bem ordenados.

Proposição 3.4.1. *Sejam A um domínio bem ordenado e $a \in A$. Se $a > 0$, então $a \geq 1$.*

Corolário 3.4.1. *Sejam A um domínio bem ordenado e $a, b \in A$. Se $a > b$, então $a \geq b + 1$.*

Corolário 3.4.2. *Sejam A um domínio bem ordenado e $a, b \in A$ com $b \neq 0$. Então $|a.b| \geq |a|$.*

Proposição 3.4.2. *Seja A um domínio bem ordenado e $a, b \in A$. Se $a.b = 1$, então $a = b = 1$ ou $a = b = -1$.*

A Proposição acima mostra que os únicos elementos invertíveis de um domínio bem ordenado são 1 e -1.

Proposição 3.4.3. ***(Propriedade Arquimediana).*** *Dados elementos a e b de um domínio bem ordenado A com $b \neq 0$, existe um elemento $n \in A$ tal que $n.b > a$.*

Indicamos [8] para demonstrações das proposições e respectivos corolários desta seção.

3.5 Divisão Euclidiana

Teorema 3.5.1. *Dados inteiros d e D com $d \neq 0$, existem inteiros q e r tais que*

$$D = d.q + r \ \ e \ \ 0 \leq r < |d|.$$

Além disso, q e r são unicamente determinados pelas condições acima.

Demonstração. Considere o conjunto limitado inferiormente,

$$S = \{x \in \mathbb{Z}^+ \mid x = D - d.n \ \ para \ \ algum \ \ n \in \mathbb{Z}\}.$$

Este conjunto é não vazio pois pela Propriedade Arquimediana dos Inteiros, (Proposição 3.4.3) existe um inteiro n tal que $n.(-d) \geq D$, portanto $x = D - n.d \in S$.

Pelo Princípio da Boa Ordenação, segue que S possui um menor elemento r. Logo $r = D - d.q$, para algum $q \in \mathbb{Z}$. É claro que $r \geq 0$ pois $r \in S$. Vamos agora provar que $r < |d|$.

Suponha por absurdo que $r \geq |d|$, logo $r = |d| + s$ para algum s tal que $0 \leq s < r$. Portanto

$$D = d.q + |d| + s = d.(q \pm 1) + s,$$

e consequentemente,

$$s = D - d(q \pm 1) \in S.$$

Como $s \in S$ e $s < r$, temos uma contradição pois r era o menor elemento de S.

Para provar a unicidade suponha que

$$D = d.q_1 + r_1 = d.q_2 + r_2,$$

com $0 \leq r_1 < |d|$ e $0 \leq r_2 < |d|$. Por estas últimas desigualdades segue que

$$-|d| < -r_2 \leq r_1 - r_2 \ \ e \ \ r_1 - r_2 < |d| - r_2 \leq |d|,$$

e portanto

$$-|d| < r_1 - r_2 < |d|.$$

Consequentemente, pela Proposição 3.3.1 (iii), temos que $|r_1 - r_2| < |d|$. Como

$$d(q_1 - q_2) = r_2 - r_1,$$

Segue da Proposição 3.3.1 (i), que

$$|d|.|q_1 - q_2| = |r_2 - r_1| < |d|.$$

Isto só é possível se $q_1 = q_2$ e $r_1 = r_2$.

O teorema nos garante portanto que em $\mathbb{Z}$ é possível efetuar a divisão de um número D por outro número $d \neq 0$ com resto pequeno.

Os números D, d, q e r são chamados respectivamente de dividendo, divisor, quociente e resto. □

Observação 3.5.1. *Na divisão euclidiana, se $D \geq 0$ e $d > 0$, então $q \geq 0$. De fato, se valesse $q < 0$, teriamos*

$$D = d.q + r < d.q + d = d(q + 1) \leq 0,$$

Logo $D < 0$, absurdo.

Observação 3.5.2. *Sejam $a, b \in \mathbb{Z}$ com $b > 0$ e q o quociente da divisão de a por b. Denotaremos $\left[\frac{a}{b}\right]$ como o número inteiro q. Esse número é o maior inteiro menor ou igual ao número racional $\frac{a}{b}$. De fato, sendo $a = b.q + r$ com $0 \leq r < b$, segue que $\frac{a}{b} = q + \frac{r}{b}$ com $\frac{r}{b}$ um número*

racional tal que $0 \leq \frac{r}{b} < 1$. *Portanto,*

$$q \leq \frac{a}{b} = q + \frac{r}{b} < q + 1,$$

Logo $q = \left[\frac{a}{b}\right]$.

Observação 3.5.3. *Dado um número racional* c*, existe um número inteiro no intervalo* $(c, c + 1] = \{x \in \mathbb{Q} \mid c < x \leq c + 1\}$.

De fato, suponha $c = \frac{a}{b}$ *com* $a, b \in \mathbb{Z}$ *e* $b > 0$. *Pela observação acima,*

$$[c] = \frac{a}{b} - \frac{r}{b},$$

com $0 \leq \frac{r}{b} < 1$ *e portanto,*

$$0 < ([c] + 1) - c \leq 1,$$

logo $[c] + 1 \in (c, c + 1]$.

3.6 Teorema Fundamental da Aritmética

Este importante teorema mostra que os números primos são os construtores dos inteiros.

Teorema 3.6.1. *(Teorema Fundamental da Aritmética (TFA)). Todo inteiro maior que um se escreve de maneira única como um produto de primos.*

Lema 3.6.1. *(Lema de Euclides) Se p é um primo que divide* $a.b$ *então* p *divide* a *ou* p *divide* b*.*

Indicamos [8] para as demonstrações do Teorema 3.6.1 e Lema 3.6.1.

Capítulo 4

Números Complexos

4.1 O Corpo dos Números Complexos

Nesta seção mostraremos que o Conjunto dos Números Complexos é um Corpo e utilizaremos a definição proposta por GAUSS em 1831 e reforçada por HAMILTON em 1837, conforme Dante [3], na qual o Conjunto dos Números Complexos é um conjunto de pares ordenados de números reais e que sintetizamos abaixo:

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

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

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

Tomemos dois elementos, (a, b) e (c, d), de $\mathbb{R}^2$ para dar as seguintes definições:

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

$$(a, b) = (c, d) \Leftrightarrow a = c \ e \ b = d$$

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

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

A adição acima é simplesmente a adição de vetores em $\mathbb{R}^2$.

- **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 cujo segundo termo é a soma dos produtos do primeiro termo de cada par dado pelo segundo termo do outro.

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

Definição 4.1.1. *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, a adição e a multiplicação conforme secção* 4.1.

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

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

Proposição 4.1.1. *As seguintes propriedades se verificam para quaisquer* $z, w, u \in \mathbb{C}$

1. $(z + w) + u = z + (w + u),\ \forall\ z, w, u \in \mathbb{C}$ (Associatividade da Adição)
2. $z + w = w + z,\ \forall\ z, w\ \in \mathbb{C}$ (Comutatividade da adição)
3. $\exists\ v_0 \in \mathbb{C} \mid z + v_o = z,\ \forall z \in \mathbb{C}$ (Elemento neutro da adição)
4. $\forall\ z \in \mathbb{C},\ \exists\ z' \in \mathbb{C} \mid z + z' = v_0.$ (Elemento simétrico da adição)
5. $(z.w).u = z.(w.u), \forall z, w, u \in \mathbb{C}$ (Associatividade da multiplicação)
6. $z.w = w.z, \forall z, w\ \in \mathbb{C}$ (Comutatividade da multiplicação)
7. $\exists\ m_0 \in \mathbb{C} \mid z.m_o = z,\ \forall z \in \mathbb{C}$ (Elemento neutro da multiplicação)
8. $\forall\ z \in \mathbb{C}^*,\ \exists\ z" \in \mathbb{C} \mid z.z" = m_0$ (Elemento inverso)
9. $z.(w + u) = z.w + z.u, \forall z, w, u \in \mathbb{C}$ (Distributividade da multiplicação em relação a adição)

□

Indicamos [3] para a demonstração das propriedades acima.

Verificadas as propriedades acima, podemos afirmar que as operações de adição e multiplicação definem sobre $\mathbb{C}$ uma estrutura de corpo comutativo; $\mathbb{C}$ é portando o corpo dos números complexos.

- **Subtração**

  Decorre do teorema anterior que, dados os complexos $z = (a, b)$ e $w = (c, d)$, existe um único $z_0 \in \mathbb{C}$ tal que $z + z_0 = w$, pois:

$$z+z_0 = w \Rightarrow z'+(z+z_0) = z'+w \Rightarrow (z'+z)+z_0 = w+z' \Rightarrow v_0+z_0 = w+z' \Rightarrow z_0 = w+z'$$

Esse número z_0 é chamado diferença entre w e z e indicado por $w - z$, portanto:

$$w - z = w + z' = (c, d) + (-a, -b) = (c, -a), (d, -b)$$

- **Divisão**

  Também decorre do teorema anterior que, dados os complexos $z = (a, b) \neq (0, 0)$ e $w = (c, d)$, existe um único $z_0 \in \mathbb{C}$ tal que $z.z_0 = w$ pois:

$$z.z_0 = w \Rightarrow z".(z.z_0) = z".w \Rightarrow (z".z).z_0 = w.z" \Rightarrow m_0.z_0 = w.z" \Rightarrow z_0 = w.z"$$

  Esse número z_0 é chamado quociente entre w e z e indicado por $\frac{w}{z}$, portanto:

$$\frac{w}{z} = w.z" = (c, d).\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) - \left(\frac{c.a + d.b}{a^2 + b^2}, \frac{d.a - c.b}{a^2 + b^2}\right)$$

  Se escrevermos, por abuso de notação, x no lugar de $(x, 0)$ e i no lugar de $(0, 1)$, temos de 4.1 acima que

$$(a, b) = (a, 0) + (b, 0).(0, 1) = a + bi.$$

  A forma acima é chamada *forma algébrica* do número complexo (a, b). Observe que

$$i^2 = (0, 1).(0, 1) = (-1, 0) = -1,$$

  com isso acabamos de construir um corpo que contém o corpo $\mathbb{R}$ e no qual a equação $z^2 + 1 = 0$ admite uma raiz (o número i).

  Na forma algébrica opera-se usando as propriedades de corpo e a informação adicional de que $i^2 = -1$.

Exemplo 1. ***Adição***

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

Exemplo 2. ***Subtração***

$$(a + bi) - (c + di) = (a - c) + (b - d)i$$

Exemplo 3. ***Multiplicação***

$$(a + bi).(c + di) = (ac + bci + adi + bdi^2) = (ac - bd) + (bc + ad)i$$

Exemplo 4. ***Inverso***

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i.$$

Observações:

Os números reais correspondem aos pares em que o segundo elemento é igual a zero. Assim:

- O par (7,0)corresponde ao número real 7;
- O par (-1,0)corresponde ao número real -1;
- O par (0,0)corresponde ao número real 0.

Os pares que tem o segundo elemento diferente de zero correspondem aos complexos que não são reais. Assim:

- O par (0,1)corresponde a um número complexo que não é real;
- O mesmo ocorre com os pares$(3, 5), (1, 3/5), (-2, 4)$ e outros.

4.1.1 Representação gráfica

Sabendo que um Número Complexo $z = a + bi$ é o par ordenado (a, b), podemos representa-lo graficamente como o ponto do plano cartesiano de abscissa a e ordenada b, ou como o vetor que liga a origem desse ponto (Figura 5.1). Nesse contexto chamamos o *Plano Cartesiano* de *Plano Complexo*, o eixo dos x de *Eixo Real* e o eixo dos y de *Eixo Imaginário*.

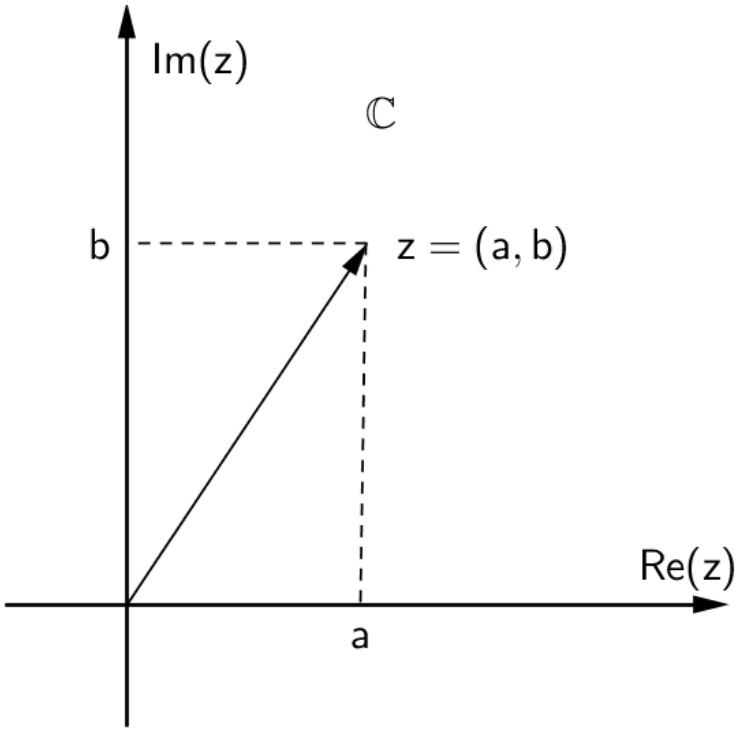


Figura 4.1: Representação Gráfica do Número Complexo

As operações de Soma e Subtração dos Números Complexos também podem ser representadas graficamente no Plano Complexo conforme Figura 5.3 abaixo.

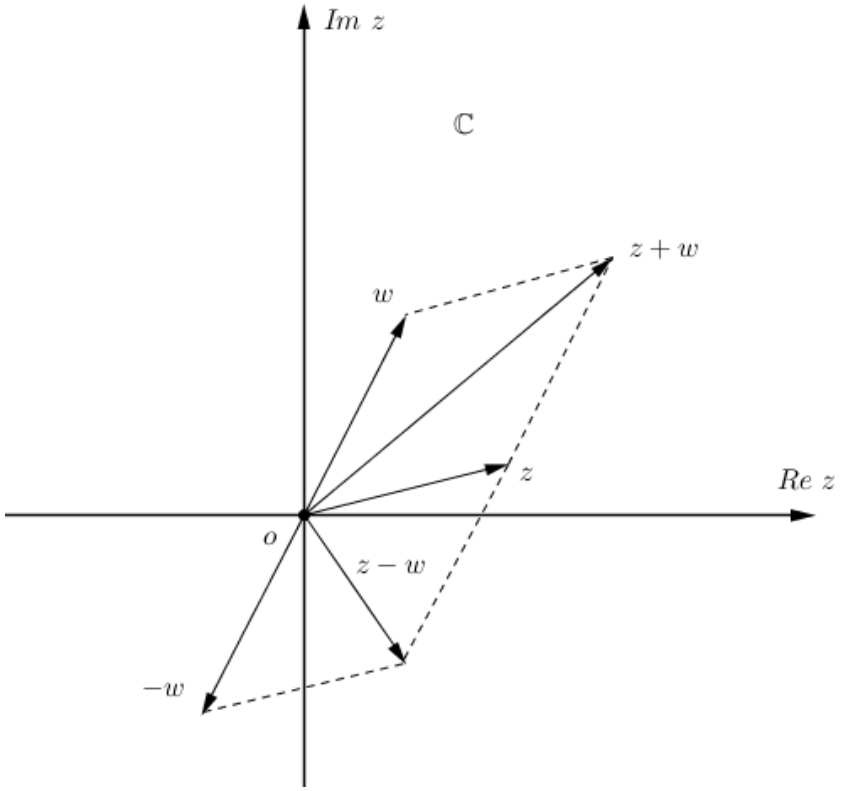


Figura 4.2: Soma e Subtração de Complexos

4.2 Conjugação e Módulo

Seja $z = a + bi \in \mathbb{C}$, com $a, b \in \mathbb{R}$. Define-se o conjugado de z como sendo o complexo $\overline{z} = a - bi$, isto é:

$$z = a + bi \Leftrightarrow \overline{z} = a - bi,$$

e o módulo de z como sendo o número real $|z| = \sqrt{a^2 + b^2}$. A parte real e a parte imaginária de z são respectivamente os números reais Re(z) = a e Im(z) = b.

4.2.1 Propriedades do Conjugado

Teorema 4.2.1. *Para todo $z \in \mathbb{C}$, temos:*

I) $z + \overline{z} = 2.Re(z)$;

II) $z - \overline{z} = 2.Im(z).i$;

III) $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$;

IV) $\overline{z} = 0 \Leftrightarrow z = 0$;

V) $\overline{\overline{z}} = z \; \forall \; z \in \mathbb{C}$;

VI) $\overline{z + w} = \overline{z} + \overline{w}$;

VII) $\overline{z.w} = \overline{z} \; . \; \overline{w}$;

VIII) Se $w \neq 0$, *então* $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$;

IX) Se $z \neq 0$*, então* $(\overline{z})^n = \overline{(z^n)} \forall n \in \mathbb{Z}$*;*
X)$z.\overline{z} = |z|^2, \forall z \in \mathbb{C}$*;*
XI) $|z| = |\overline{z}| = |-z|, \forall z \in \mathbb{C}$*;*
XII) $Re(z) = \dfrac{z+\overline{z}}{2}$ *e* $Im(z) = \dfrac{z-\overline{z}}{2i}$*;*
XIII) $Re(z) \leq |Re(z)| \leq |z|$ *e* $Im(z) \leq |Im(z)| \leq |z|$.

Essas propriedades são fáceis de verificar. A título de ilustração provaremos a propriedade (I).

Sejam $z = a + bi$ *e* $\overline{z} = a - bi$ *a propriedade (I) é consequência das seguintes igualdades:*

$$z + \overline{z} = (a + bi) + (a - bi) = (a + a) + (bi - bi) = 2a + 0 = 2a = 2Rez$$

As seguintes proposições nos fornecerão alguns resultados básicos

Proposição 4.2.1. *Quaisquer que sejam* $z, w \in \mathbb{C}$*, temos que*

$$|z.w| = |z|.|w|$$

Demonstração. Usando as propriedades (VII) e (X) acima, temos que

$$|z.w|^2 = (z.w)\overline{(z.w)} = z.\overline{z}.w.\overline{w} = |z|^2.|w|^2 = (|z|.|w|)^2.$$

Como $|z.w|$ e $|z|.|w|$ são ambos números reais não negativos, extraindo a raiz quadrada de ambos os membros da igualdade $|z.w|^2 = (|z|.|w|)^2$, obtemos que |z.w| = |z|.|w|. □

Proposição 4.2.2. *Quaisquer que sejam* $z, w \in \mathbb{C}$*, temos que*

$$|z + w| \leq |z| + |w|.$$

Demonstração. Usando as propriedades (V) e (VII), verifica-se que $z.\overline{w}$ e $w.\overline{z}$ são conjugados, logo pela propriedade (I) temos que $z.\overline{w} + w.\overline{z} = 2Re(z.\overline{w})$. Como pelas propriedades (XII) e (XIII) e pela Proposição (4.2.1), temos que $z.\overline{w} + w.\overline{z} \leq 2|z|.|w|$, segue pelas propriedades (X) e (VI) que

$$\begin{aligned} |z + w|^2 &= (z + w).\overline{(z + w)} = z.\overline{z} + z.\overline{w} + w.\overline{z} + w.\overline{w} \\ &= |z|^2 + 2Re(z.w) + |w|^2 \leq |z|^2 + 2|z|.|w| + |w|^2 \\ &= (|z| + |w|)^2. \end{aligned}$$

Extraindo a raiz quadrada dos dois extremos das desigualdades acima, obtemos o resultado. □

4.2.2 Conjugados da Soma e do Produto

Teorema 4.2.2. *Se z e w são Números Complexos quaisquer, temos:*

I) $\overline{z+w} = \overline{z} + \overline{w}$

II) $\overline{z.w} = \overline{z}.\overline{w}$

Indicamos [8] para a demonstração do Teorema 4.2.2.

4.2.3 Forma Trigonométrica ou Polar dos Números Complexos

Vejamos agora a representação dos números complexos em coordenadas polares. A relação entre coordenadas cartesianas e coordenadas polares resultou num dos instrumentos mais poderosos na teoria dos números complexos, sem o qual seria praticamente impossível operar com estes números, especialmente no que diz respeito à extração de raízes [8].

Sejam ρ e θ as coordenadas polares do ponto representando z (Figura xxx), onde $\rho \geq 0$. Então

$$x = \rho cos\,\theta \quad e \quad y = \rho sen\,\theta, \tag{4.1}$$

e o número complexo z pode ser escrito na forma polar

$$z = \rho(cos\,\theta + isen\,\theta) \quad (\rho \geq 0) \tag{4.2}$$

O raio vetor ρ é $\sqrt{x^2+y^2}$, isto é,

$$\rho = |z|. \tag{4.3}$$

O ângulo θ é chamado argumento de z denotado por $Arg\,z$. Quando $z \neq 0$, os valores de θ são determinados a partir das equações (4.1) ou da relação

$$tg\,\theta = \frac{y}{x} \tag{4.4}$$

e do quadrante em que o ponto z se encontra.

Entretanto, qualquer θ_0 da forma $\theta + 2k\pi$, com k inteiro, também satisfaz a forma polar, pois $sen\,\theta$ e $cos\,\theta$ são funções periódicas de θ com período 2π radianos, em particular z possui infinitos argumentos. Denotamos o único argumento de z que pertence ao intervalo $(-\pi, \pi]$, como argumento principal e escrevemos $Arg\,z$.

Vejamos agora [8]representações polares para a multiplicação de dois complexos $(z.w)$ e para a divisão de dois complexos $\left(\frac{z}{w}\right)$.

Proposição 4.2.3. *Sejam* $z = \rho_1(cos\theta_1 + isen\theta_1)$ *e* $w = \rho_2(cos\theta_2 + isen\theta_2)$. *Temos que*

$$z.w = \rho_1.\rho_2[cos(\theta_1 + \theta_2) + isen(\theta_1 + \theta_2)]$$

Da Proposição 5.3.1 segue a seguinte regra:

O produto de dois números complexos tem por representação um vetor cujo módulo é o produto dos módulos desses números e cujo ângulo com o eixo $\mathbb{R}$ x $\{0\}$ é a soma dos ângulos(módulo 2π) que as representações destes números formam com o referido eixo.

Proposição 4.2.4. *Sejam* $z = \rho_1(cos\theta_1 + isen\theta_1)$ *e* $w = \rho_2(cos\theta_2 + isen\theta_2) \neq 0$. *Temos que*

$$\frac{z}{w} = \frac{\rho_1}{\rho_2}[cos(\theta_1 - \theta_2) + isen(\theta_1 - \theta_2)]$$

.

Capítulo 5

Inteiros de Gauss

Definição 5.0.1. *Um inteiro de gauss é um número complexo da forma $a+bi$ com a e b inteiros, cujo conjunto denotamos por $\mathbb{Z}[i]$.*

5.1 O anel dos Inteiros Gaussianos

5.1.1 Subanéis

Definição 5.1.1. *Sejam (A,+,.)um anel e L um subconjunto não vazio de A. Diz-se que L é um subanel de A se;*

(i) L é fechado para as operações que dotam A da estrutura de anel;

(ii) (L,+,.) também é um anel.

Proposição 5.1.1. *Sejam A um anel e L um subconjunto não vazio de A. Então L é um subanel de A se, e somente se, as seguintes condições são verificadas:*

(i) $0 \in L$ *(o elemento neutro de A pertence a L)*

(ii) $x, y \in L \Rightarrow x - y \in L$ *(L é fechado para a diferença)*

(iii) $x, y \in L \Rightarrow x.y \in L$ *(L é fechado para o produto).*

Indicamos [7] para a demonstração da proposição 5.1.1.

Proposição 5.1.2. *O conjunto dos Inteiros de Gauss é um Domínio de integridade.*

Demonstração. Com efeito, $0 = 0 + 0i \in \mathbb{Z}[i]$. Como $1 = 1 + 0i$, então $1 \in \mathbb{Z}[i]$.

Sejam $z = a + bi$ e $w = c + di$ dois Inteiros de Gauss, isto é, $a, b, c, d \in \mathbb{Z}$, então $z - w$ e $z.w$ também são Inteiros de Gauss pois

$$z - w = (a - c) + (b - d)i,$$

$$z.w = (ac - bd) + (ad + bc)i,$$

$$w.z = (ca - db) + (da + cb)i = (ac - bd) + (ad + bc)i = zw$$

onde $(a-c), (b-d), (ac-bd)$ e $(ad+cb)$ são inteiros. Logo $\mathbb{Z}[i]$ é um subanel comutativo com unidade de $\mathbb{C}$. Além disso

$$z.w = 0 \Rightarrow |z.w| = 0$$

$$|z|.|w| = 0 \Rightarrow |z| = 0 \ \ ou \ \ |w| = 0$$

$$|z| = 0 \Leftrightarrow z = 0 \ \ e$$

$$|z| = \sqrt{a^2 + b^2}$$

□

O anel dos inteiros gaussianos será denotado por $\mathbb{Z}[i]$.

5.2 Norma

Definiremos também uma função muito importante na aritmética desse conjunto que é chamada de **Norma**, onde:

Definição 5.2.1. *Para $z = a + bi \in \mathbb{Z}[i]$, a Norma é o produto*

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

Por exemplo, $N(3 + 2i) = 3^2 + 2^2 = 13$. Para $m \in \mathbb{Z}, N(m) = m^2$. Em particular, $N(1) = 1$

Pensando em $a + bi$ como um número complexo, sua Norma é o quadrado de seu módulo.

$$|a + bi| = \sqrt{a^2 + b^2}, \ N(a + bi) = a^2 + b^2 = |a + bi|^2.$$

A razão pela qual preferem lidar com Normas em $\mathbb{Z}[i]$ em vez de valores absolutos é que as Normas são inteiros (em vez de raízes quadradas) e as propriedades de divisibilidade em $\mathbb{Z}$ vão fornecer informações importantes sobre as propriedades de divisibilidade em $\mathbb{Z}[i]$. Isto é baseado na seguinte propriedade algébrica da Norma.

Teorema 5.2.1. *A **Norma é multiplicativa**, ou seja, como $\overline{zw} = \overline{z}.\overline{w}$, então $N(z).N(w) = z\overline{z}.w\overline{w} = zw.\overline{zw} = N(zw)$*

Demonstração. Fazendo $z = a + bi$ e $w = c + di$. Então $z.w = (ac - bd) + (ad + bc)i$.
Façamos agora $N(zw)$ e $N(z)N(w)$:

$$N(z)N(w) = (a^2 + b^2)(c^2 + d^2) = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 \tag{5.1}$$

e

$$\begin{aligned} N(zw) &= (ac-bd)^2 + (ad+bc)^2 \\ &= (ac)^2 - 2acbd + (bd)^2 + (ad)^2 + 2adbc + (bc)^2 \\ &= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2. \end{aligned} \tag{5.2}$$

Verificamos que (5.1) e (5.2) tem o mesmo resultados, logo

$$N(zw) = N(z)N(w)$$

□

Determinaremos a seguir os inteiros de Gauss que tem inversos multiplicativos em $\mathbb{Z}[i]$.

5.3 Unidades

5.3.1 Definições

- Elemento invertível: Um elemento $a \in A$ é invertível (em A) se existe $b \in A$ tal que a.b = 1.

  Denotaremos por A^* o conjunto dos elementos invertíveis.

- Elementos associados: Dois elementos $a, b \in A$ são associados (em A) se existe $u \in A^*$,tal que $a = ub$.

Observação 5.3.1. *O produto de invertíveis é invertível, pois se u e v são invertíveis,*

$$(u.v)(v^{-1}.u^{-1}) = u(v.v^{-1}).u^{-1} = u.u^{-1} = 1$$

Proposição 5.3.1. *Ser associado é uma relação de equivalência no seguinte sentido:*

i) z é associado de z;

ii) Se z é associado de w, então w é associado de z;

iii) Se z é associado de w e w é associado de t, então z é associado de t.

Demonstração. Vejamos:

i) $z = 1.z$

ii) Se $z = uw \Rightarrow w = u^{-1}.z$. Como o inverso de um invertível também é invertível, então w é associado de z.

iii) Se $z = u_1 w$ e $w = u_2 t$, então $z = (u_1 u_2)t$

Como o produto de invertíveis é invertível $\Rightarrow z$ é associado de w. □

Proposição 5.3.2. *Seja $\alpha \in \mathbb{Z}[i]$. As seguintes afirmações são equivalentes:*

(i) α *é invertível em* $\mathbb{Z}[i]$*;*

(ii) $N(\alpha) = 1$*;*

(iii) $\alpha \in \{-1, 1, -i, i\}$.

Demonstração.

$(i) \Rightarrow (ii)$: Sendo α invertível, existe $\beta \in \mathbb{Z}[i]$ tal que

$$\alpha.\beta = 1.$$

Consequentemente,

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

Como $N(\alpha) \in \mathbb{Z}^+$, segue das igualdades acima que $N(\alpha) = N(\beta) = 1$.

$(ii) \Rightarrow (iii)$: Suponhamos $N(\alpha) = 1$. Pondo $\alpha = a + bi$, temos que

$$a^2 + b^2 = 1,$$

cujas soluções em $\mathbb{Z}$ x $\mathbb{Z}$ são $(0, \pm 1)$ e $(\pm 1, 0)$. Portanto $\alpha \in \{-1, 1, -i, i\}$.

$(iii) \Rightarrow (i)$: É claro que todo elemento de $\{-1, 1, -i, i\}$ é invertível em $\mathbb{Z}[i]$. □

A Norma de cada Inteiro de Gauss é um número inteiro não negativo, mas não é verdade que cada número inteiro não negativo é Norma de algum elemento de $\mathbb{Z}[i]$. Com efeito, as Normas são os inteiros da forma $a^2 + b^2$ e nem todo inteiro positivo é a soma de dois quadrados. Veremos, por exemplo, que $3, 7, 11, 15, 19$ e 21 não são Normas de nenhum inteiro de Gauss.

5.4 Divisibilidade

Mostraremos que em $\mathbb{Z}[i]$ tem uma divisão com resto "pequeno"semelhante a Divisão Euclidiana em $\mathbb{Z}$ e que o anel dos Inteiros Gaussianos possui propriedades algébricas e aritméticas semelhantes às do Anel dos Inteiros.

5.4.1 Domínios Euclidianos

Definição 5.4.1. *Um domínio Euclidiano (A,+,.,*Υ*) é um domínio de integridade* $(A, +, .)$ *com uma função*

$$\Upsilon : A - \{0\} \to \mathbb{N} = \{0, 1, 2, ...\}$$

Que satisfaz as propriedades seguintes:

1. $\forall a, b \in A,\ b \neq 0$, *existem* $t, r \in A$ *tais que*

$$a = bt + r \ \ com \begin{cases} \Upsilon(r) < \Upsilon(b) \\ \quad ou \quad r = 0. \end{cases}$$

2. $\Upsilon(a) \leq \Upsilon(ab), \forall\ a, b \in A \backslash \{0\}$

Definição 5.4.2. *Seja* $a, b \in \mathbb{Z}[i], b|a$ *(lê-se* b *divide* a*) se* $\exists\, c \in \mathbb{Z}[i]$ *tal que* $a = bc$*. Assim sendo, chamamos* b *de divisor ou fator de* a *e, neste caso, diremos que* a *é multiplo de* b*.*

Exemplo 5. *Se* $8 - i = (1 - 2i)(2 + 3i)$*, então* $1 - 2i$ *e* $2 + 3i$ *dividem* $8 - i$*.*

Exemplo 6. $12 - 5i$ *é divisível por* $1 + 6i$*? Façamos a divisão.*

$$\frac{12 - 5i}{1 + 6i} = \frac{(12 - 5i)(1 - 6i)}{(1 + 6i)(1 - 6i)} = \frac{-18 - 77i}{37} = -\frac{18}{37} - \frac{77}{37}i.$$

Como as partes Real $\left(-\frac{18}{37}\right)$ *e Imaginária* $\left(-\frac{77}{37}\right)$ *não são inteiros,* $1 + 6i$ *não divide* $12 - 5i$ *em* $\mathbf{Z}[i]$*.*

Teorema 5.4.1. *Seja* $z = a + bi \in \mathbb{Z}[i]$ *e* $c \in \mathbb{Z}$*,* $c|z$ *se, e somente se,* $c|a$ *e* $c|b$ *em* $\mathbb{Z}$*.*

Demonstração. Como $c|(a + bi)$ em $\mathbb{Z}[i]$, então $a + bi = c(m + ni)$ para algum $m, n \in \mathbb{Z}$, que é equivalente a dizer que $a = cm$ e $b = cn$, logo $c|a$ e $c|b$. □

Observamos também que a multiplicidade da Norma se transforma em relação de divisibilidade em $\mathbb{Z}[i]$, vejamos,

Teorema 5.4.2. *Para* $z, w \in \mathbb{Z}[i]$*, se* $w|z$ *em* $\mathbb{Z}[i]$*, então* $N(w)|N(z)$ *em* $\mathbb{Z}$*.*

Demonstração. Fazendo $z = wy$ para $y \in \mathbb{Z}[i]$. Pela Norma nos temos que $N(z) = N(w)N(y)$. Como esta equação está em $\mathbb{Z}$, então temos que $N(w)|N(z)$ em $\mathbb{Z}$. □

Corolário 5.4.1. *Um inteiro de Gauss* α *é múltiplo de* $1 + i$ *se, e somente se, sua Norma é par.*

Demonstração. Seja $\alpha = a + bi$ um inteiro de Gauss com Norma par. Então a e b tem a mesma paridade, isso só ocorre se a e b forem ambos ímpares ou ambos pares. Fazendo $a + bi = (1 + i)(x + yi)$ para algum $x, y \in \mathbb{Z}$, temos $a + bi = (x - y) + (x + y)i$, que tem solução $x = \frac{a + b}{2}$ e $y = \frac{b - a}{2}$. Como a e b tem a mesma paridade são números inteiros.

Por outro lado, como $N(1 + i) = 2$, qualquer múltiplo de $1 + i$ também tem Norma par. □

Exemplo 7. *A Norma de* $5 + i$ *é 26, e* $5 + i = (1 + i)(3 - 2i)$*.*

Teorema 5.4.3. ***(divisão com resto)***.

Sejam $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$. Então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que:

$$\alpha = \beta\gamma + \rho, \ \ com \ \ 0 \leq N(\rho) < N(\beta)$$

Demonstração. Trata-se de achar um inteiro gaussiano q tal que

$$N(\alpha - \beta\gamma) < N(\beta).$$

como

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

segue que devemos achar um inteiro gaussiano γ tal que

$$N\left(\frac{\alpha}{\beta} - \gamma\right) < 1.$$

Escrevendo $\dfrac{\alpha}{\beta}$ na forma normal, é fácil ver que existem $x, y \in \mathbb{Q}$ tais que

$$\frac{\alpha}{\beta} = x + yi.$$

Sejam r e s inteiros tais que

$$|x - r| \leq \frac{1}{2} \ \ e \ \ |y - s| \leq \frac{1}{2},$$

(tais inteiros existem em decorrência da Observação 3.5.3.). Pondo $\gamma = r + si$ e $\rho = \alpha - \beta\gamma$, segue que

$$\alpha = \beta.\gamma + \rho,$$

com

$$N(\rho) = N(\beta).N(\frac{\alpha}{\beta} - \gamma) = N(\beta).N(x - r + (y - s)i) =$$

$$= N(\beta)[(x - r)^2 + (y - s)^2] \leq N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}N(\beta) < N(\beta).$$

Corolário 5.4.2. $(\mathbb{Z}[i], +, ., N)$ *é um Domínio Euclidiano.*

Para um melhor entendimento da proposição 5.4.1 mostraremos abaixo alguns exemplos.

Exemplo 8. *Seja* $\alpha = 11 + 10i$ *e* $\beta = 4 + i$*. Então* $N(\beta) = 17$*. Assim*

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{54 + 29i}{17}.$$

Como $\frac{54}{17} = 3, 17...$ *e* $\frac{29}{17} = 1, 70...$*, usamos* $\gamma = 3 + 2i$ *. Então* $\alpha - \beta\gamma = 1 - i$*, por isso definimos* $\rho = 1 - i$*. Note que* $N(\rho) = 2 \leq \left(\frac{1}{2}\right) N(\beta)$*.*

Exemplo 9. *Seja* $\alpha = 41 + 24i$ *e* $\beta = 11 - 2i$*. Então* $N(\beta) = 125$ *e*

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{125} = \frac{403 + 346}{125}$$

Como $\frac{403}{125} = 3, 224...$ *e* $\frac{346}{125} = 2, 768...$ *usamos* $3+3i$ *e encontramos* $\alpha - \beta\gamma = 2 - 3i$*. Definir* $\rho = 2 - 3i$ *e compare* $N(\rho)$ *com* $N(\beta)$*.*

há uma diferença interessante entre o Teorema da Divisão em $\mathbb{Z}[i]$ *e o (usual) Teorema da Divisão em* $\mathbb{Z}$*: é que, em geral, o quociente e o resto não são únicos em* $\mathbb{Z}[i]$

Exemplo 10. *Seja* $\alpha = 1 + 8i$ *e* $\beta = 2 - 4i$*, então*

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{-30 + 20i}{20} = -\frac{3}{2} + i.$$

Como $-\frac{3}{2}$ *encontra-se bem no meio de* -2 *e* -1*, podemos usar* $\gamma = -1 + i$ *ou* $\gamma = -2 + i$*. Utilizando a primeira escolha obtemos*

$$\alpha = \beta(-1 + i) + (-1 + 2i).$$

Usando a segunda escolha,

$$\alpha = \beta(-2 + i) + (1 - 2i).$$

□

5.5 Algoritmo de Euclides para o cálculo do M.D.C

Vamos definir inicialmente os Inteiros de Gauss compostos e primos.

Pelo teorema 5.4.2, se $z|w$ em $\mathbb{Z}[i]$, então $N(z)|N(w)$ em $\mathbb{Z}$, assim $1 \leq N(z) \leq N(w)$ quando $w \neq 0$. Vejamos então quais divisores de w tem Norma igual a 1 ou Norma igual a N(w).

Lema 5.5.1. *Sejam* $w \neq 0$ *e* z *um divisor de* w *tal que* $N(z) = 1$ *ou* $N(z) = N(w)$*, então* z *é uma unidade ou é um associado de* w*.*

Demonstração. Se $N(z) = 1$, então z é uma unidade.

Se $N(z) = N(w)$, fazendo $w = zu \Rightarrow N(w) = N(z).N(u)$, onde fazendo o cancelamento dos iguais, temos que $N(u) = 1$. □

Quando $N(w) > 1$, sempre há oito divisores óbvios de w: $\pm 1, \pm i, \pm w$ e $\pm iw$. Nos chamamos a esses fatores de fatores triviais de w. Eles são análogos aos quatro fatores triviais ± 1 e $\pm n$ de qualquer número inteiro n com $|n| > 1$. Qualquer outro fator de w é chamado de não trivial, os fatores não triviais de w são os fatores com Norma estritamente entre 1 e $N(w)$.

Definição 5.5.1. *Seja w um Inteiro de Gauss. Diremos que w é composto se existirem inteiros de Gauss a e b tais que:*

i) $w = a.b$

ii) $N(a) > 1$ *e* $N(b) > 1$.

Se w não for composto ele é chamado de irredutível.

Proposição 5.5.1. *Se Norma de w é um número primo, então w é irredutível.*

Demonstração. Seja $w = a.b$ com $N(w) = p$, então

$$N(w) = N(a).N(b)$$

então

$$p = N(a).N(b)$$

portanto

$$N(a) = p \ \ e \ \ N(b) = 1 \ \ ou \ \ vice - versa.$$

□

Exemplo 11. $1 + i$ *é irredutível pois tem Norma* 2*.*

Exemplo 12. $2 + i$ *é pois tem Norma irredutível 5.*

Exemplo 13. $1 - 4i$ *é pois tem Norma irredutível 17.*

Definição 5.5.2. *Seja $p \in \mathbb{Z}[i]$ é dito primo, se dados a e b tais que $p|a.b$, então $p|a$ ou $p|b$.*

Vejamos agora a definição de Máximo Divisor Comum em $\mathbb{Z}[i]$.

Definição 5.5.3. *Sejam $z, w \in \mathbb{Z}[i]$, com $z \neq 0$, um Máximo Divisor Comum de z e w é um elemento de $\mathbb{Z}[i]$ tal que:*

i) $d|z$ *e* $d|w$

ii) Se $d'|z$ *e* $d'|w$ *então* $N(d') \leq N(d)$

Definição 5.5.4. *Quando o M.D.C entre z e w é um elemento invertível, dizemos que eles são relativamente primos.*

Teorema 5.5.1. *(ALGORITMO DE EUCLIDES). Sejam z e w em $\mathbb{Z}[i]$ com $w \neq 0$. Então existe um M.D.C entre z e w e além disso se d é um M.D.C entre z e w existem r e s em $\mathbb{Z}[i]$, tais que:*

$$d = rz + sw$$

Demonstração. Aplicando o Teorema da divisão, temos:

$$z = wq_1 + r_1, \ \ onde \ \ r_1 = 0 \ \ ou \ \ N(r_1) < N(w)$$

Se $r_1 = 0 \Rightarrow w|z$ e $w|w \Rightarrow$ que qualquer inteiro de Gauss que divida w e z tem Norma menor ou igual a Norma de w. Logo w é um M.D.C. entre z e w.

Se $r_1 \neq 0$, então

$$w = r_1q_2 + r_2, \ \ onde \ \ r_2 = 0 \ \ ou \ \ N(r_2) < N(r_1)$$

Se $r_2 = 0 \Rightarrow r_1|w$ e como $z = wq_1 + r_1$ e $w = r_1q_2 \Rightarrow z = r_1q_1q_2 + r_1 = r_1(q_2q_1 + 1)$, logo $r_1|z$. Além disso se $d|z$ e $d|w$

$$r_1 = z - wq_1 = dz' - dw'q_1 = d(z' - w'q_1)$$

ou seja, $d|r_1$ e $N(d) \leq N(r_1)$ e portanto r_1 é um M.D.C entre z e w.

Se $r_2 \neq 0$, então

$$r_1 = q_3r_2 + r_3$$

Se $r_3 = 0$, então $r_2|r_1$, além disso

$$w = r_1q_2 + r_2 = r_2q_3q_2 + r_2 = r_2(q_2q_3 + 1)$$

$$z = wq_1 + r_1 = r_2(q_2q_3 + 1)q_1 + r_2q_3 = r_2[(q_2q_3 + 1)q_1 + q_3]$$

portanto

$$r_2|z \ \ e \ \ r_2|w$$

.

Além disso

$$r_2 = w - r_1q_2 = w - (z - wq_1)q_2 = (-q_2)z + (q_1q_2)w$$

Isso mostra que:
i) $r_2|z$ e $r_2|w$
ii) r_2 é uma combinação linear em $\mathbb{Z}[i]$ de z e w
iii) Todo divisor comum entre z e w divide r_2
iv) r_2 é um M.D.C entre z e w.

Prosseguindo o processo o PBO nos diz que existe n tal que $r_{n+1} = 0$. Seguindo o raciocínio acima vemos que o r_n é um M.D.C de z e w e r_n é uma combinação linear em $\mathbb{Z}[i]$ entre z e w.

Isso é chamado Algoritmo de Euclides para o M.D.C. □

Corolário 5.5.1. *Sejam d e d' dois M.D.Cs entre z e w, então eles são associados.*

Demonstração. Com efeito, pela demonstração do Teorema acima temos que $d|d'$ e $d'|d$, portanto eles são associados. □

Corolário 5.5.2. *Seja p tal que $N(p) > 1$. Então p é primo se, e somente se é irredutível.*

Demonstração. ($\Rightarrow$) Por hipótese, p é primo.

Suponha então $p = ab$. Como p é primo, $p|a$ ou $p|b$.

Seja $p|a$. Portanto $p = a'pb \Rightarrow 1 = a'b \Rightarrow b$ é invertível. Portanto p é irredutível.

($\Leftarrow$) Por hipótese p é irredutível.

Seja $p|a.b$ e $p \not| a$ e $d = mdc(a, p)$.

Como $d|p$ então d é invertível ou associado de p.

Como $d|a$ então d não pode ser associado de p, pois p não divide a. Logo d é invertível. Podemos considerar $d = 1$, logo existem r e s tais que $1 = ra + sp \ \ e$

$$b = rab + spb = rkp + sp$$

portanto

$$b = (rk + s)p \Rightarrow p|b.$$

□

Exemplo 14. *Vejamos o cálculo do M.D.C. entre $z = 8 + 12i$ e $w = 4 + 3i$. A Norma de w é 25. Queremos escrever $z = wq_1 + r_1$ onde $N(r_1) = 0 \ \ ou \ \ N(r_1) < 25$, então*

$$\frac{(8 + 12i)(4 - 3i)}{25} = \frac{68}{25} + \frac{24}{25}i.$$

Então, $q_1 = 3 + i \ \ e$

$$r_1 = (7 + 11i) - (3 + i)(4 + 3i) = (8 + 12i) - (9 + 13i) = -1 - i$$

$N(r_1) = 2$ *e* $N(w) = 25$. *Então* $N(r_1) < N(w)$.
Como $N(r_1) \neq 0$, temos que:

$$w = r_1q_2 + r_2 \ \ onde \ \ N(r_2) = 0 \ \ ou \ \ N(r_2) < N(r_1). \ Vejamos,$$

$$\frac{w}{r_1} = \frac{4 + 3i}{-1 - i} = \frac{(4 + 3i)(-1 + i)}{2} = -\frac{7}{2} + \frac{1}{2}i$$

Então,

$$q_2 = -3 + i \ \ ou \ \ -4 + i \ \ ou \ \ -3 \ \ ou \ \ -4$$

.

Podemos utilizar qualquer um dos q_1's encontrados para achar r_2, existindo a possibilidade de quatro soluções diferentes.

Façamos o cálculo de r_2 quando $q_2 = -3 + i$.

$$r_2 = (4 + 3i) - (-1 - i)(-3 + i) = (4 + 3i) - (4 + 2i) = i$$

$N(r_2) = 1$ *e* $N(r_1) = 2$. *Então* $N(r_2) < N(r_1)$.
Como $N(r_2) \neq 0$, *temos que:*

$$r_1 = r_2 q_3 + r_3 \ \ onde \ \ N(r_3) = 0 \ \ pois$$

$$(-1 - i) = i(-1 + i) + 0.$$

Como o último resto diferente de zero é i, que é uma unidade, então z e w são relativamente primos e o M.D.C entre os dois é igual a 1.

Exemplo 15. *Vejamos agora o cálculo do M.D.C. entre $z = -5+10i$ e $w = -1+8i$. A Norma de w é 65. Queremos escrever $z = wq_1 + r_1$ onde $N(r_1) = 0 \ \ ou \ \ N(r_1) < 65$, então*

$$\frac{z}{w} = \frac{-5 + 10i}{-1 + 8i} = \frac{(-5 + 10i)(-1 - 8i)}{65} = \frac{85}{65} + \frac{30}{65}i.$$

Então,

$$q_1 = 1 \ \ e$$

$$r_1 = (-5 + 10i) - (-1 + 8i)(1) = (-5 + 10i) - (-1 + 8i) = -4 + 2i$$

$N(r_1) = 20$ *e* $N(w) = 65$. *Então* $N(r_1) < N(w)$.
Como $N(r_1) \neq 0$, *temos que:*

$$w = r_1 q_2 + r_2 \ \ onde \ \ N(r_2) = 0 \ \ ou \ \ N(r_2) < N(r_1). \ \ Vejamos,$$

$$\frac{w}{r_1} = \frac{-1 + 8i}{-4 + 2i} = \frac{(-1 + 8i)(-4 + 2i)}{20} = \frac{20}{20} - \frac{30}{20}i$$

Então,

$$q_2 = 1 - i \ \ ou \ \ 1 - 2i \ \ e$$

$$r_2 = (-1 + 8i) - (1 - i)(-4 + 2i) = (-1 + 8i) - (-2 + 6i) = 1 + 2i$$

$N(r_2) = 5$ *e* $N(r_1) = 20$. *Então* $N(r_2) < N(r_1)$.

Como $N(r_2) \neq 0$*, temos que:*

$$r_1 = r_2 q_3 + r_3 \ \ onde \ \ N(r_3) = 0 \ \ ou \ \ N(r_3) < N(r_2). \ \ Vejamos,$$

$$\frac{r_1}{r_2} = \frac{-4+2i}{1+2i} = \frac{(-4+2i)(1-2i)}{5} = \frac{0}{5} + \frac{10}{5}i.$$

Então,

$$q_3 = 2i \ \ e$$

$$r_3 = (-4+2i) - (1+2i)(2i) = (-4+2i) - (-4+2i) = 0.$$

Como $r_2 = 1+2i$ *é o último resto diferente de zero, ele é um M.D.C entre* $-5+10i$ *e* $-1+8i$

Logo,

$$(-5+10i) = (3+4i)(1+2i)$$

e

$$(-1+8i) = (1+2i)(3+2i)$$

com $1+2i$ *irredutível.*

5.6 Fatoração Única

Em problemas envolvendo números inteiros, a fatoração única é uma das propriedades mais importantes. Vamos mostrar que ela também é válida para os Inteiros de Gauss. Para isso vamos provar que todo inteiro z de Gauss com norma maior que 1 pode ser escrito como produto de um ou mais primos de Gauss.

Teorema 5.6.1. *(Fatoração Unica). Qualquer* $z \in \mathbb{Z}[i]$ *com* $N(z) > 1$ *tem uma fatoração única em números primos, no seguinte sentido: se*

$$z = p_1 p_2 ... p_n = q_1 q_2 ... q_m,$$

onde os p_j*'s e* q_j*'s são primos em* $\mathbb{Z}[i]$*, então* $n = m$ *e após uma reordenação adequada, cada* p_j *é um associado de* q_j*.*

Demonstração. Por indução na Norma.

1. Se$N(z) = 2$ e $z = a.b$, então $N(a.b) = N(a).N(b) = 2 \Rightarrow N(a) = 1$ e $N(b) = 2$ ou vice-versa. Logo z é primo.

2. Considere $N(z) > 2$.

   (a) Se z é primo a fatoração é imediata.

(b) Se z não é primo, então $z = a.b \Longrightarrow N(z) = N(a).N(b)$, onde $N(a), N(b) > 1$, portanto $N(a), N(b) < N(z)$. Então, se $N(a) < N(z)$. Logo a e b são fatoráveis, e por consequência z é fatorável.

3. Podemos supor agora a existência de duas fatorações para z: $p_1p_2...p_n$ e $q_1q_2...q_m$. Supondo agora, por indução, que $p_1p_2...p_n = \eta q_1q_2...q_m$ sendo η uma unidade, implica que a sequência (p_i) é uma permutação (a menos que sejam multiplicações por unidades) da (q_i). Se max{n;m} = 1, então o resultado é imediato. Supondo que max{$n^{'}$;$m^{'}$} < max{n;m}, pelo lema de Euclides, vemos que para algum i, $p_n|q_j$. Sem perda de generalidade, i = m. Como p_n e q_m são primos, então $q_m = \eta^{'}\ p_n$, onde $\eta^{'}$ é uma unidade. Logo $p_1p_2...p_n = \eta q_1q_2...q_m \Longleftrightarrow p_1p_2...p_{n-1} = \eta\eta^{'}q_1q_2...q_{m-1}$. Por indução $p_1, p_2, ..., p_{n-1}$ é uma permutação (a menos que sejam multiplicações por unidades) de $q_1, q_2, ...q_m$, portanto a fatoração única esta provada.

□

5.7 Congruências em $\mathbb{Z}[i]$

As congruências em $\mathbb{Z}[i]$ também são definidas usando-se a divisibilidade.

Definição 5.7.1. *Sejam z, w números inteiros, e y um inteiro não nulo. Diremos que z é côngruo a w módulo y se $y|(z - w)$, isto é, $z - w = yq$ para um conveniente Inteiro q. Para indicar que z é côngruo a w, módulo y, usa-se a notação*

$$z \equiv w\ (mod\ y)$$

A relação assim definida sobre o Conjunto $\mathbb{Z}$ chama-se congruência módulo y.

Para indicar que $z - w$ não é divisível por y, ou seja, que z não é côngruo a w módulo y, escreve-se

$$z \not\equiv w\ mod\ y$$

Exemplo 16. *Para verificar se $5 + 12i \equiv (2 + i)\ mod\ (5 + i)$, subtraímos e dividimos:*

$$\frac{(5 + 12i) - (2 + i)}{5 + i} = 1 + 2i$$

As congruências em $\mathbb{Z}[i]$, comportam-se bem tanto sob a adição como sob a multiplicação:

Destacamos algumas propriedades básicas da congruência de inteiros:

1. $z \equiv z \ mod \ y$ (reflexidade)

   De fato, $z - z = 0$ é divisível por y.

2. Se $z \equiv w \ mod \ y$, então $w \equiv z \ mod \ y$ (simetria)

   Se $z \equiv w \ mod \ y$, então $y|(z-w)$, ou seja, $z - w = yq$ para algum q. Daí $w - z = y(-q)$ e, portanto, $y|(w - z)$. Logo $w \equiv z \ mod \ y$

3. Se $z \equiv w \ mod \ y$ e $w \equiv s \ mod \ y$, então $z \equiv s \ mod \ y$ (transitividade)

   Por hipótese, $y|(z - w)$ e $y|(w - s)$. Logo, $y|[(z - w) + (w - s)]$, ou seja, $y|(z - s)$. Portanto $z \equiv w \ mod \ y$.

Como congruência módulo zero significa igualdade, nos geralmente assumimos módulo diferente de zero.

Um inteiro de Gauss pode ser reduzido módulo y, se $y \neq 0$, para obter um inteiro de Gauss com Norma reduzida, dividindo-se por y e utilizando-se o resto.

5.7.1 Classes de equivalência

Definimos a classe de equivalência do elemento r na congruência módulo y como sendo o conjunto $\tilde{r} = \{z \in \mathbb{Z}[i]; z \equiv r \ \ mod \ \ y\}$

Observação 5.7.1.
- *Sendo a congruência uma relação de equivalencia, duas classes são iguais ou disjuntas.*
- *O algoritmo da divisão nos diz que todo elemento de $\mathbb{Z}[i]$ é congruente a um elemento r tal que $N(r) < N(y)$*
- *Pela observação acima o número de classes de equivalencia é finito, pois existem um número finito de elementos com norma menor que a norma de um determinado elemento fixo em $\mathbb{Z}[i]$.*

Obsevemos a analize a seguir.
Seja w um inteiro de Gauss com $N(w) > 1$. Vamos analizar

$$z \equiv 0 \ \ mod \ \ w$$

então,

$$z = 0 + kw.$$

Se $k = a + bi$, então

$$z = (a + ib)w = aw + b(iw)$$

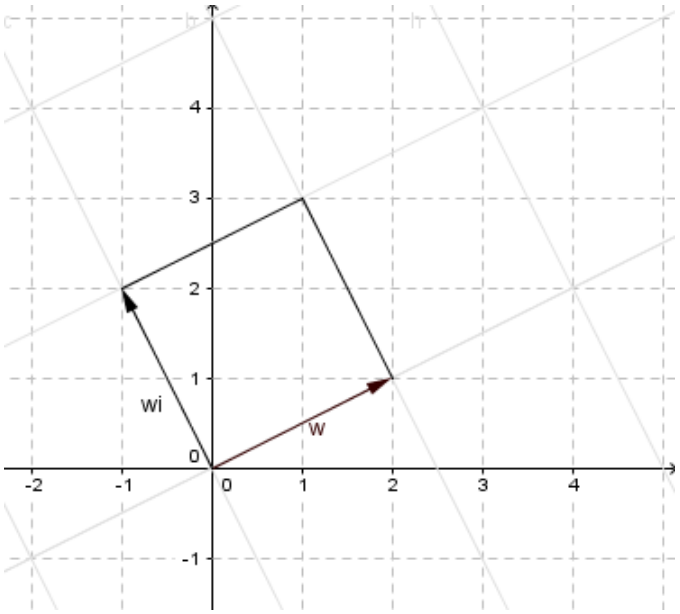


Figura 5.1: Vetores ortogonais w e wi

ou seja, z é uma combinação linear inteira dos vetores ortogonais w e iw (ver Figura 5.1).

No caso da congruência $z \equiv r \mod w$, geometricamente a malha é transladada para o ponto $r = c + di$. Dois números são congruêntes se estiverem na mesma "malha".

Analizemos agora $z \equiv r \mod w$, com $N(r) < N(w)$

Pelo PBO, o subconjunto formado pelas Normas de r é finito, pois $0 \leq N(r) < N(w)$. Então temos:

$$N(r) = N(w) - 1$$

$$N(r) = N(w) - 2$$

$$. \quad .$$

$$. \quad .$$

$$N(r) = 1$$

$$N(r) = 0$$

O conjunto de classes distintas é finito.

A classe de $0 + 0i$ é o conjunto dos múltiplos de y.

Interpretação Geométrica

$$ky = (a + bi)y = ay + b.iy$$

Geometricamente, $\tilde{0}$ é a combinação linear inteira dos vetores ortogonais y e iy.

Exemplo 17. *Façamos a redução de* $1 + 8i \ mod \ 2 - 4i$.

A divisão já foi efetuada no exemplo 10, onde encontramos mais de uma possibilidade:

$$1 + 8i = (2 - 4i)(-1 + i) + (-1 + 2i),$$

e

$$1 + 8i = (2 - 4i)(-2 + i) + (1 - 2i).$$

Portanto, $1 + 8i \equiv -1 + 2i \ mod \ 2 - 4i$ *e* $1 + 8i \equiv (2 - 4i)(-1 + i) + (1 - 2i)$*, e as duas reduções estão corretas.*

Vamos agora observar algebricamente as classes de equivalência para $1 - 2i$.

Como a Norma de $1-2i$ é igual a 5, temos que que as classes de equivalências possíveis são:

$$N(r) = N(w) - 1 = 5 - 1 = 4 \Rightarrow r \in \{\pm 2, \pm 2i\}$$

$N(r) = N(w) - 2 = 5 - 2 = 3$. Não existe elemento de Norma 3.

$$N(r) = N(w) - 3 = 5 - 3 = 2 \Rightarrow r = \{\pm(1 + i), \pm(-1 + i)\}$$

$$N(r) = N(w) - 4 = 5 - 4 = 1 \Rightarrow r = \{(\pm 1), (\pm i)\}$$

$$N(r) = N(w) - 5 = 5 - 5 = 0 \Rightarrow r = \{0\}$$

Temos então, a priori, 13 classes de equivalência. Vamos verificar quais são disjuntas.

$1 \equiv 2i \ \ mod \ \ (1 - 2i)$ e $1 \equiv (-1 - i)$ mod $1 - 2i$, logo 1, $(-1 - i)$ e $2i$ pertencem à mesma classe.

$-1 \equiv -2i \ \ mod \ \ (1 - 2i)$, logo -1 e $-2i$ pertencem à mesma classe.

$i \equiv 1 - i \ \ mod \ \ (1 - 2i)$ e $i \equiv -2 \ \ mod \ \ (1 - 2i)$, logo i, $(1 - i)$ e -2 pertencem à mesma classe.

$-i \equiv (-1+i) \ \ mod \ \ (1-2i)$ e $-i \equiv 2 \ \ mod \ \ (1-2i)$, logo $-i$, 2 e $(-1+i)$ pertencem à mesma classe.disjunta das outras.

Por fim a classe $r = 0$, que representa os múltiplos de $1 - 2i$.

Logo temos, em lugar das 13 classes iniciais, apenas 5 classes que são:

$$1, -1, i, -i, 0.$$

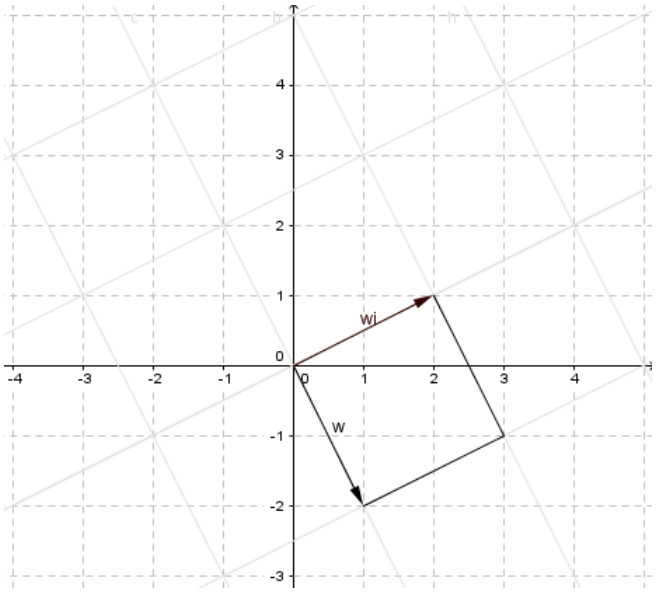


Figura 5.2: Múltiplos de $w = 1 - 2i$ em $\mathbf{Z}[i]$

Capítulo 6

Aplicações

Teorema 6.0.1. *(Fermat).*

Seja p um número primo em $\mathbb{Z}$. Então as afirmações seguintes são equivalentes:
(i) $p = 2$ *ou* $p \equiv 1 \mod 4$.
(ii)Exista $a \in \mathbb{Z}$ *tal que* $a^2 \equiv -1 \mod p$.
(iii) p é irredutível em $\mathbb{Z}[i]$.
(iv) p é a soma de dois quadrados.

Demonstração no Apêndice.

Corolário 6.0.1. *Os elementos irredutíveis de* $\mathbb{Z}[i]$ *são exatamente os elementos do tipo seguinte:*

- $\pm p, \pm ip$ *com p primo em* $\mathbb{Z}$ *tal que* $p \equiv 3 \mod 4$, *por consequência de (iii) do Teorema 6.0.1.*
- $a + bi$ *com* $a^2 + b^2 \equiv 1$ *mod* 4 *igual a um primo de* $\mathbb{Z}$, *por consequência da proposição 5.5.1.*

Demonstração no Apêndice.

Corolário 6.0.2. *Todo inteiro de Gauss pode ser escrito na forma*

$$z = i^k.p_1p_2...p_n.q_1q_2...q_m$$

onde $p_j \equiv 3$ *mod* 4 *é um primo inteiro e* $N(q_j)$ *é um primo inteiro congruênte a* 1 *mod* 4.

Como aplicações da aritmética de $\mathbb{Z}[i]$ para propriedades de $\mathbb{Z}$ iremos abordar:
- O produto de dois números que são soma de dois quadrados também é uma soma de dois quadrados;
- Caracterização dos inteiros que são soma de dois quadrados;
- Um número primo que é soma de dois quadrados é assim em uma única forma;

Exemplo 18. *Vamos determinar a fatoração de* $3+4i$.

Temos que $N(3+4i)=25$. *Essencialmente temos dois primos de Gauss de Norma* 5 *a menos de associados.*

$$2+i \;\; e \;\; 2-i$$

Verificamos que

$$3+4i=(2+i)(2+i)=(2+i)^2$$

Exemplo 19. *Fatoração de* $-6+17i$. *Temos que* $N(-6+17i)=325$. *Vamos procurar um primo de Gauss de Norma* 5 *quew divida* $-6+17i$, *encontramos*

$$-6+17i=(2+i)(1+8i)$$

Seguindo com o mesmo raciocínio vemos que

$$1+8i=(2+i)(2+3i)$$

que são primos $N(5)$ *e* $N(13)$.

Portanto

$$-6+17i=(2+i)^2(2+31).$$

O produto de dois números que são soma de dois quadrados também é uma soma de dois quadrados

Seja

$$r=a^2+b^2 \;\; e \;\; s=c^2+d^2$$

então,

$$r.s=(a^2+b^2)(c^2+d^2)=N[(a+bi)(c+di)]=N([(ac-bd)+(ad+bc)i]$$

então,

$$r.s=(ac-bd)^2+(ad+bc)^2.$$

Caracterização dos inteiros que são soma de dois quadrados

Seja

$$n = 2^k.p_1^{\alpha_1}...p_r^{\alpha_r}.q_1^{\beta_1}...q_s^{\beta_s}$$

fatoração em $\mathbb{Z}$ onde

$$q_j \equiv 1 \ \ mod \ \ 4 \ \ \ e \ \ \ q_j \equiv 3 \ \ mod \ \ 4$$

então n é soma de dois quadrados se, e somente se,

$$\beta_j \ \ for \ \ par \ \ \forall j$$

Se β_j é par $\forall j$, o Teorema de Fermat e a aplicação acima garantem que n é a soma de dois quadrados.

Suponhamos agora que n é a soma de dois quadrados e seja p um primo tal que a maior potência de p que divide n é ímpar. Então,

$$n = a^2 + b^2$$

Consideremos d o mdc entre a e b, teremos

$$n = d^2(a'^2 + b'^2)$$

onde mdc entre a' e b' é igual a 1 a maior potência de p que divide d^2 é par.

Portanto $p|a'^2 + b'^2$. p não pode dividir b' pois senão dividiria também a' contrariando o fato do mdc de a' e b' ser 1. Temos a equação

$$a'^2 + b'^2 = 0$$

no Corpo $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$

$$b'^2.[(a'.b'^{(-1)})^2 + 1] = 0 \ \ em \ \ \frac{\mathbb{Z}}{\mathbb{Z}p}$$

Logo $c^2 + 1 \equiv 0 \ \ mod \ \ p$ tem solução.

Portanto $p \equiv 1 \ \ mod \ \ 4$.

Exemplo 20.

$$765 = 3^2.17.5 =$$

$$= N(3)N(4+i)N(2+i) =$$

$$= N[3.(4+i)(2+i)] =$$

$$= N(21+18i) =$$

$$= 21^2 + 18^2$$

$$765 = 3^2.17.5 =$$

$$= N(3)N(4-i)N(2+i) =$$

$$= N[3.(4-i)(2+i)] =$$

$$= N(27+6i) =$$

$$= 27^2 + 6^2$$

Um número primo que é soma de dois quadrados é assim em uma única forma

Teorema 6.0.2. *Seja p primo tal que $p = a^2 + b^2$, os inteiros a e b são únicos exceto pela ordem e sinais(em particular os quadrados $a^2 + b^2$ são únicos exceto pela ordem).*

Demonstração. Seja $p = a^2 + b^2$, com $a, b \in \mathbb{Z}$. Então, em $\mathbb{Z}[i]$, temos

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

Como $N(a + bi) = p$ e $N(a - bi) = p$ e p é primo em $\mathbb{Z}$, eles são primos em $\mathbb{Z}[i]$ (Teorema 6.0.1). Se houver uma segunda representação $p = c^2 + d^2$, então

$$p = (c + di)(c - di),$$

e $c \pm di$ são primos em $\mathbb{Z}[i]$. Pela fatoração única em $\mathbf{Z}[i]$ devemos ter

$$a + bi = u(c + di) \; ou \; a + bi = u(c - di)$$

para alguma unidade u. A unica diferença entre $c + di$ e $c - di$ é o sinal do coeficiente i, e queremos mostrar que a e b são únicos exceto pela ordem e sinal, por isso, não há mal nenhum em tratar apenas o caso

$$a + bi = u(c + di).$$

Se $u = 1$, então $c = a$ e $d = b$. Se $u = -1$, então $c = -a$ e $d = -b$. Se $u = i$, então $c = b$ e $d = -a$. Se $u = -i$, então $c = -b$ e $d = a$. Assim c e d são iguais a a e b exceto pela ordem e sinais. □

Considerações Finais

Este trabalho foi desenvolvido com o objetivo de tornar mais interessante aos alunos do 3º ano do Ensino Médio, em especial os das escolas públicas, o estudo dos Números Complexos, com a introdução desse estudo sobre o conjunto dos inteiros de Gauss que é um subconjunto dos Complexos de grande importância no estudo da Teoria dos Números.

Cabe ao professor, explorando o assunto, desenvolver nos alunos o hábito da investigação e da pesquisa por meio de situações-problema instigadoras e curiosas.

O trabalho deve ser desenvolvido em sua totalidade pois cada capítulo está entrelaçado com os outros capítulos. Assim, todos os capítulos compõem a Transposição Didática proposta para o estudo dos Inteiros Gaussianos.

Foi abordado inicialmente um pouco da história dos Números Complexos e também dos Inteiros de Gauss e, em seguida, foi feita a construção do conjunto dos Números Inteiros $(\mathbb{Z})$, axiomaticamente, mostrando que o mesmo é um domínio de integridade, em seguida que é um domínio ordenado e, complementando com a demonstração de que o mesmo é um domínio bem ordenado.

O capítulo seguinte, Números Complexos, embasa o desenvolvimento do tema e é de fundamental importância no aprendizado do assunto.

O próximo capítulo, Inteiros de Gauss, culmina no desenvolvimento do tema, mostrando que a aritmética desse conjunto $((\mathbb{Z})[i])$ é semelhante a do conjunto dos Números Inteiros $(\mathbb{Z})$.

Para esse desenvolvimento,sugerimos alguns livros citados nas referências bibliográficas que subsidiarão o trabalho do professor, tais como Garcia[6], Hefez[8], Domingues[4] e Gonçalves[7] que podem contribuir com este tema.

Capítulo 7

Apêndice

Demonstração do Teorema 6.0.1 . (Fermat)

Seja p um número primo. Então as afirmações seguintes são equivalentes:

(i) $p = 2$ ou $p \equiv 1 \ \ mod \ \ 4$.

(ii)Exista $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \ \ mod \ \ p$.

(iii) p é irredutível em $\mathbb{Z}[i]$.

(iv) p é a soma de dois quadrados.

□

Demonstração. (i) $\Rightarrow$ (ii).

Se $p = 2$, basta tomar $a = 1$ e temos que $1^2 \equiv -1 \ \ mod \ \ 2$.

Seja $p = 1 + 4n$, pelo Pequeno Teorema de Fermat,

$$\forall \ x \ \ tal \ \ que \ \ M.D.C(x, p) = 1 \Rightarrow x^{p-1} \equiv 1 \ \ mod \ \ p$$

$$x^{4n} \equiv 1 \ \ mod \ \ p$$

$$x^{4n} - 1 \equiv \ \ 0 \ \ mod \ \ p$$

$$(x^{2n} - 1)(x^{2n} + 1) \equiv \ \ 0 \ \ mod \ \ p.$$

Todas as $4n$ classes $\overline{1}, \overline{2}, ..., \overline{p-1}$ são soluções da equação.

Como $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ é um corpo, o número de raízes de $x^{2n} - 1 = 0$ é $2n$ e o número de raízes de $x^{2n} + 1 = 0$ também é $2n$.

Seja c uma solução de $x^{2n} + 1 = 0$. Tomando $a = c^n$, teremos:

$$a^2 \equiv c^{2n} \ \ mod \ \ p \equiv -1 \ \ modp$$

(ii) $\Rightarrow$ (iii).

Como $a^2 \equiv -1 \mod p \Rightarrow a^2 + 1 = k.p \Rightarrow (a + bi)(a - bi) = kp$,

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

Supondo que $p \nmid a + bi$. Então $(a + i) = rp = (e + fi)p = ep + fip \Rightarrow fp = 1$.

Absurdo, pois p é primo em $\mathbb{Z}$.

Similarmente p não divide $a - bi$ em $\mathbb{Z}[i]$. Logo p não é primo em $\mathbb{Z}[i]$.

(iii) $\Rightarrow$ (iv).

Supondo que p fatore em
$mathbbZ[i]$, então $p = w.z \Rightarrow N(p) = N(w).N(z)$ e como $N(p) = p^2$,

$$p^2 = (a^2 + b^2).(c^2 + d^2) \Rightarrow p^2 = kp(c^2 + d^2) \Rightarrow p = k.(c^2 + d^2)$$

onde, como p é primo em $\mathbb{Z}$, $k = 1$ e $p = (c^2 + d^2)$. Logo p é soma de dois quadrados em $\mathbb{Z}[i]$.

(iv) $\Rightarrow$ (i).

Sendo p um número primo, temos que $p = 2$ ou $p = 4k + 1$ ou $p = 4k + 3$. Vamos mostrar que nenhum inteiro do tipo $4k + 3$ é soma de dois quadrados.

Seja a um inteiro qualquer, então $\overline{a} = \overline{0}, \overline{1}, \overline{2}, \ ou \ \overline{3}$ em $\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)$.

Então, se a e b são dois inteiros quaisquer, as possibilidades para $\overline{a}^2 + \overline{b}^2$ são $\overline{0}, \overline{1}$ ou $\overline{2}$ em $\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)$, e $4n + 3 (= \overline{3}$ em $\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)$) não é soma de dois quadrados.

□

Demonstração do Corolário 6.0.1. Os elementos irredutíveis de $\mathbb{Z}[i]$ são exatamente os elementos do tipo seguinte:

- $\pm p, \pm ip$ com p primo em $\mathbb{Z}$ tal que $p \equiv 3 \mod 4$, por consequência de (iii) do Teorema 6.0.1.
- $a + bi$ com $a^2 + b^2$ igual a um primo de $\mathbb{Z}$, por consequência da proposição 5.5.1.

□

Demonstração. ($\Rightarrow$) Seja um inteiro de Gauss do tipo $\pm p$, $\pm ip$ com p primo em $\mathbb{Z}$, $p \equiv 3 \mod 4$, é irredutível em $\mathbb{Z}[i]$ pelo Teorema 6.0.1.

Um elemento $a + bi \in \mathbb{Z}[i]$, com $a^2 + b^2$ igual a um primo de $\mathbb{Z}$, é irredutível em $\mathbb{Z}[i]$ pois senão, teriamos

$$a + bi = wy \quad com \quad w, y \in \mathbb{Z}[i], \ \ w, y \neq \pm 1, \pm i,$$

logo,

$$a^2 + b^2 = N(a + bi) = N(wy) = N(w)N(y)$$

com $N(w), N(y) \in \mathbb{Z},\ N(w) \neq 1$ e $N(y) \neq 1$. Absurdo, pois por hipótese $a^2 + b^2$ é primo em $\mathbb{Z}$.

($\Leftarrow$) Seja $a + bi$ um elemento irredutível em $\mathbb{Z}[i]$. Se $a^2 + b^2$ não é primo em $\mathbb{Z}$, então $a^2 + b^2 = nm$ com $n, m \in \mathbb{Z}$, $n, m \neq \pm 1$, logo

$$(a + bi)(a - bi) = nm.$$

Pela unicidade da fatoração em $\mathbb{Z}[i]$, temos que $a + bi = un$ e $(a - bi = um)$ com $u \in \{\pm 1, \pm i\}$; logo $a = 0$ ou $b = 0$, ou seja, $a + bi = \pm ic$ ou $a + bi = \pm c$ com $c \in \mathbb{N}$. Entretanto, sendo $a + bi$ irredutível em $\mathbb{Z}[i]$e , por consequencia irredutível em $\mathbb{Z}$.

Pelo Teorema 6.0.1, este elemento c é côngruo a 3 módulo 4. □

Referências Bibliográficas

[1] CEVI, Cristina; MONTEIRO, Martha. *História dos Números Complexos*. São Paulo: IME.USP, 2001.

[2] CONRAD, Keith. *The gaussian integers*. Pre-Print, paper edition,2008.

[3] DANTE, Luiz Roberto. *Matemática*. São Paulo:ÁTICA,2008.

[4] DOMINGUES, Hygino H. *Álgebra Moderna*. São Paulo:ATUAL,2003.

[5] GALLIAN, J. *Contemporary Abstract Algebra*. Heath 1994.

[6] GARCIA, Arnaldo; LEQUAIN, Yves. *Elementos de álgebra*. Rio de Janeiro: IMPA, 2012.

[7] GONÇALVES, Adilson. *Introdução à Álgebra*. Rio de Janeiro: IMPA, 1999.

[8] HEFEZ, Abramo. *Curso de Algebra*. Rio de Janeiro: IMPA,2002.

[9] IEZZI, Gelson.*Fundamentos da Matemática Elementar 6: Complexos, Polinômios e Equações*.São Paulo: Atual 1993.

[10] MARQUES, Cristina M. *Introdução à Teoria dos Anéis*. Minas Gerais: UFMG, 1999.

[11] NETO, Antonio C. M. *Equações Diofantinas*. EUREKA! N 07,2000.

[12] VITORINO, Alfredo; ROLDÃO, Beatriz. *Inteiros de Gauss*. Campinas: 2013.