Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

A Teoria Elementar dos Inteiros de Gauss

Paulo Henrique Alves Batista

Goiânia

2019

sistema de bibliotecas ufg

PRPG
PRÓ-REITORIA DE PÓS-GRADUAÇÃO

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[x] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação:

Nome completo do autor: Paulo Henrique Alves Batista

Título do trabalho: A Teoria Elementar dos Inteiros de Gauss

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.

Paulo Henrique Alves Batista
Assinatura do(a) autor(a)[2]

Ciente e de acordo:

Assinatura do(a) orientador(a)[2] Data: 29 / 11 / 2019

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

[2] A assinatura deve ser escaneada.

Paulo Henrique Alves Batista

A Teoria Elementar dos Inteiros de Gauss

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração: Matemática do Ensino Básico.
Orientadora: Profª. Drª. Ivonildes Ribeiro Martins Dias.

Goiânia

2019

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Alves Batista , Paulo Henrique
A Teoria Elementar dos Inteiros de Gauss [manuscrito] / Paulo Henrique Alves Batista . - 2019.
v, 79 f.: il.

Orientador: Profa. Dra. Ivonildes Ribeiro Martins Dias.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), PROFMAT - Programa de Pós graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2019.
Bibliografia.
Inclui lista de figuras.

1. Inteiros. 2. Inteiros de Gauss. 3. Ternos pitagóricos. I. Ribeiro Martins Dias, Ivonildes , orient. II. Título.

CDU 51

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº **13** da sessão de Defesa de Dissertação de Paulo Henrique Alves Batista, que confere o título de Mestre em Matemática.

Aos oito dias do mês de novembro de dois mil e dezenove, a partir das 14**horas**, no **laboratório do IME/UFG**, realizou-se a sessão pública de Defesa de Dissertação intitulada **"A Teoria Elementar dos Inteiros de Gauss"**. Os trabalhos foram instalados pela Orientadora, Professora Doutora Ivonildes Ribeiro Martins Dias - IME/UFG com a participação dos demais membros da Banca Examinadora: Professor Doutor Paulo Henrique de Azevedo Rodrigues - IME/UFG e membro titular externo; Daiane Soares Veras - IFGoiâno. Durante a arguição os membros da banca **não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, tendo sido o candidato **aprovado** pelos seus membros. Proclamados os resultados pelo Professora Doutora Ivonildes Ribeiro Martins Dias, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, ao oito dias do mês de novembro de dois mil e dezenove.

TÍTULO SUGERIDO PELA BANCA

Documento assinado eletronicamente por **Ivonildes Ribeiro Martins**, **Professor do Magistério Superior**, em 11/11/2019, às 16:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Paulo Henrique De Azevedo Rodrigues**, **Professor do Magistério Superior**, em 11/11/2019, às 17:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Daiane Soares Veras**, **Usuário Externo**, em 13/11/2019, às 13:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0961297** e o código CRC **B320875E**.

Referência: Processo nº 23070.039517/2019-89 SEI nº 0961297

Paulo Henrique Alves Batista graduou em Licenciatura em Matemática pela Universidade Estadual de Goiás(UEG Campus Cora Coralina) em 2014, especializou-se em Neuropedagogia aplicada à Educação pela Faculdade Brasileira de Educação e Cultura e também Especialista em Pesquisa em Educação Matemática pela UEG - Campus Cora Coralina. Atuou na rede particular de ensino no Colégio Monteiro Lobato - Itapuranga e Cooperativa de Ensino da Cidade de Goiás - COOPECIGO - Cidade de Goiás, no Instituto Federal de Goiás - Campus Cidade de Goiás. Atualmente, professor efetivo da Secretaria de Educação do Estado de Goiás (SEDUC) no CEPMG-Deputado José Alves de Assis e professor temporário da UEG - Campus Cora Coralina.

Dedicatória

A Deus, minha mãe, meu pai, minha irmã e a minha parceira de viagem e estudos Daianne Naier por todo apoio e tolerância em dias difíceis. A turma PROFMAT 2017/1, em especial a Dulcicléa, Lorena, Ilga; ao Curso de Licenciatura em Matemática da UEG-Campus Cora Coralina; a todos meus amigos, professores e alunos que de alguma forma contribuíram para a realização desta conquista.

Agradecimentos

Primeiramente, agradeço a Deus por ter me concedido sabedoria para finalizar essa etapa tão importante para minha vida acadêmica, aos meus familiares, em especial a minha Mãe Josefa Alves Vieira Batista, a minha Irmã Jessica Lorrana Alves Batista e ao meu Pai Paulo Jacinto de Oliveira Batista, vocês foram fundamentais para que pudesse encontrar forças para esta conquista.

A minha Orientadora Drª. Ivonildes Ribeiro Martins Dias, me faltam palavras para expressar o quanto foi importante durante este processo, desde a disciplina MA 14, a qual descobri meu fascínio pela Matemática Pura. Suas contribuições, compreensão e confiança foram primordiais para finalização desta pesquisa e o que me resta é agradecer por toda a cooperação, apoio e amizade.

Agradeço aos professores Dr. Paulo Henrique de Azevedo Rodrigues e Drª. Daiane Soares Veras por aceitar o convite para composição da banca e por todas as contribuições e sugestões feitas para o aprimoramento da minha pesquisa, rendo os mais sinceros agradecimentos pelo empenho e disposição de todos vocês.

Não poderia deixar de ressaltar, o quanto os professores do PROFMAT foram fundamentais no desenvolvimento de habilidades para a realização deste trabalho, neste caso foram eles: Dr. Eduardo Arbieto Alarcon, Dr. Paulo Henrique de Azevedo Rodrigues, Drª. Rosângela Maria da Silva, Drª. Kélem Gomes Lourenço, Dr. Ewerton Rocha Vieira, Dr. Maria Bethânia S. dos Santos e Dr. Elisabeth Cristina de Faria. Minha evolução foi incalculável e considero que tive o privilégio de estudar disciplinas ministradas por vocês, rendo os meus mais sinceros agradecimentos pelo empenho em instruir com tamanha qualidade e dedicação.

Foram muitos que cooperaram direta e indiretamente para a minha inserção no PROFMAT e finalização do mesmo, no entanto, em nome da Ms. Geórgia Clarice, professora que sempre acreditou em meu potencial e me encorajou diante dos maiores desafios, a minha eterna gratidão a todos vocês.

Ao meu coordenador de Curso Rodrigo Bastos Daude e também em nome do Major Agmar Pereira Soares e sua esposa Elizabete Soares a todos da Equipe Gestora do CEPMG-DJAA rendo os mais sinceros agradecimentos pelo apoio e compreensão durante esse processo de finalização deste curso.

Gratidão a todos os meus alunos e meus amigos professores do Colégio Monteiro Lobato, IFG: Campus Cidade de Goiás, Cooperativa de Ensino da Cidade de Goiás - COOPECIGO, Pré - ENEM Raça e em especial, a Licenciatura em Matemática da UEG - Campus Cora Coralina e CEPMG - Deputado José Alves de Assis, grato por todo o apoio e compreensão.

Resumo

O trabalho refere-se a importância das propriedades aritméticas dos Inteiros na compreensão de novas estruturas abstratas, como os Inteiros de Gauss ($\mathbb{Z}[i]$), subconjunto dos Números Complexos ($\mathbb{C}$). Esta pesquisa é de cunho bibliográfico a fim de promover um levantamento teórico perante aos principais resultados que estão em torno dos conjuntos $\mathbb{Z}$ e $\mathbb{Z}[i]$. O trabalho vem com o intuito de mobilizar os professores de matemática que é fundamental ter domínio matemático sobre as propriedades aritméticas de $\mathbb{Z}$, por que elas possibilitará a ele e aos discentes a capacidade de estabelecer um paralelo entre $\mathbb{Z}$ e $\mathbb{Z}[i]$ e consequentemente, descrever as diferenças e semelhanças entre as estruturas analisadas. A pesquisa foi dividida em três capítulos. Inicialmente, foram expostos os principais resultados referentes ao conjunto $\mathbb{Z}$ e a priori de propriedades que serão válidas para o conjunto $\mathbb{Z}[i]$. Em seguida, será feita uma abordagem minuciosa sobre as características de $\mathbb{Z}[i]$ e enfim uma sugestão de aplicação matemática de $\mathbb{Z}[i]$ que pode ser desenvolvida no Ensino Básico, 3ª série do Ensino Médio, referente a determinação de todos os possíveis ternos pitagóricos a partir de um valor previamente fixado para a hipotenusa de um triângulo retângulo. Durante todo o trabalho, é perceptível o busca intensa mediante rigor matemático, fato este realizado de forma intencional, a fim de promover aos professores de Matemática a oportunidade de conhecer e/ou aprofundar o conhecimento matemático mediante outras estruturas abstratas, neste caso, o conjunto $\mathbb{Z}[i]$.

Palavras-chave: Inteiros; Inteiros de Gauss; Ternos pitagóricos.

Abstract

This work refers to the importance of the arithmetic properties of the integers in the comprehension of the abstracts structures as Gauss integers $\mathbb{Z}[i]$ subset of complex numbers($\mathbb{C}$) a alarm information is the little relevance that this topic receives by math teachers of elementary school, This research is a bibliographic work in order to promote a theoretical survey by the main results which are around the sts $\mathbb{Z}$ and $\mathbb{Z}[i]$, This work has the intention of mobilise the math teachers who might have math dominium on $|z$ arithmetic properties, because they will give them the possibilities to estabilish a parallel between $\mathbb{Z}$ and $\mathbb{Z}[i]$ and consequently to describe the equalities and differences between the analysed structures, The research was divided in three chapters, Initially were exposed the main results referents to the set $\mathbb{Z}$ and a priori of properties that will be valid to the set $\mathbb{Z}[i]$,then it will be done a detailed approach about the characteristics of $\mathbb{Z}[i]$ and a suggestion of math application of $\mathbb{Z}[i]$ that could be developed at the elementary education , in high school third grade concerning to the determination of all possible Pythagoras theorems derived from a value previously fixed to the hypotenuse right triangule , During al the work its visible the intense search on a strict mathematical achieved by intentional form, in order to promote to the math teachers the opportunity if knowing or deepen the math knowledges through other abstracts structures, in this case the set $\mathbb{Z}[i]$.

Key words:Integers, Gauss integers, Phytagoream theorems.

Lista de Figuras

2.1 $-1+2i$ *e* $-2-i$ 59
2.2 $-1+2i$ *e* $-2-i$ 60
2.3 $\mathbb{Z}[i]$-*múltiplos de* $-1+2i$ 61
2.4 $-1+2i$ *e* $-2-i$ 61

3.1 $\Delta(ABC)$ é retângulo em Â. 64

Sumário

Introdução **1**

1 Introdução à Teoria dos Números Inteiros **6**

1.1 Uma Apresentação Axiomática dos Inteiros 6

1.2 A Ordenação em $\mathbb{Z}$ 8

1.2.1 Principio da Boa Ordenação 10

1.3 Valor Absoluto 11

1.4 Divisibilidade em $\mathbb{Z}$ 13

1.5 Divisão Euclideana 14

1.6 Máximo Divisor Comum 16

1.7 Números Primos 19

1.7.1 Teorema Fundamental da Aritmética 19

1.8 A Aritmética dos Restos em $\mathbb{Z}$ 21

1.8.1 Congruência 21

2 A aritmética dos Inteiros de Gauss **25**

2.1 Anel dos Inteiros de Gauss 25

2.2 A Norma de $\mathbb{Z}[i]$ 27

2.3 Divisibilidade em $\mathbb{Z}[i]$ 30

2.4 Divisão Euclideana em $\mathbb{Z}[i]$ 34

2.5 Primos em $\mathbb{Z}[i]$ 39

2.6 Máximo Divisor Comum em $\mathbb{Z}[i]$ 46

2.7 Fatoração Única em $\mathbb{Z}[i]$ 53

2.8 Congruência em $\mathbb{Z}[i]$ 57

3 Os lados inteiros de um triângulos retângulos e sua relação com os Inteiros de Gauss **63**

3.1 Os Ternos Pitagóricos 64

3.2 Determinação de Triângulos Retângulos a Partir de um Valor Fixo para a Hipotenusa 68

Considerações finais **76**

Referências bibliográficas **78**

Introdução

O Brasil, em pesquisa Matemática, tem reconhecimento internacional. Em 2018 ele foi promovido ao Grupo V, considerado a "Elite", da International Mathematical Union-IMU, veja [14]. A IMU é uma entidade que congrega 76 países e tem por objetivo fomentar a cooperação internacional nessa área de conhecimento. Agora, no ranking da IMU, o país está ao lado de países como a Alemanha, Canadá, China, Estados Unidos, Israel, Itália, Japão, Reino Unido e Rússia no que se refere à qualidade da pesquisa em matemática. Assim, reconhecida pelo padrão de excelência mundial.

Por outro lado, vale ressaltar que tal padrão de excelência não se estende aos demais níveis educacionais, principalmente nas séries iniciais. Os resultados do Brasil no Programme for International Student Assessment-Pisa em 2018, mostram que no ranking mundial o país ficou na 70ª colocação em matemática dentre 79 países avaliados. O que aponta uma grande discrepância entre a pesquisa e o ensino/aprendizagem de matemática no país conforme aponta Suely Druck, uma das idealizadoras da Olimpíadas de Matemática das Escolas Públicas-OBMEP:

> "Atualmente, pesquisa e ensino em matemática compõem mundos distintos e distanciados. O primeiro cumpre com competência o seu papel de produzir conhecimento e formar recursos humanos para pesquisa. Já o segundo vem cumprindo muito mal o seu papel de transferir conhecimento e formar cidadãos, e ainda se debate com questões primárias e até surrealistas que dizem respeito à sua missão". [12]

Diante de tais resultados chega nos a seguinte reflexão "Qual o motivo de tamanho distanciamento entre pesquisa e ensino/aprendizagem em matemática? O que necessitamos para que o ensino no país esteja equiparado ao ensino em outros países participantes do mesmo grupo da IMU?"

Por um lado, a pesquisa matemática é abordada de modo criterioso com muito

rigor matemático, leva-se em consideração os axiomas, teoremas, proposições, propriedades entre outros, já o ensino é abordado, de um modo geral, formulaíco (até mesmo mágico) e com procedimentos mecânicos, como se o educando fosse um software desenvolvendo algum algoritmo pronto, deixando de explorar o seu potencial e limitando-o no desenvolvimento do seu raciocínio.

Assim, diante dos resultados, acreditamos que o ensino de matemática deve ser mais rigoroso no que tange as utilizações de propriedades e determinadas demonstrações, mesmo no ensino básico, e que o estudo dessa área será mais prazeroso se existir entendimento dos processos que foram seguidos nas obtenções de resultados.

Diante da necessidade de ações e políticas educacionais (efetivas) que buscam aperfeiçoar o ensino de matemática no Brasil, principalmente em escolas públicas, surgiram vários projetos, dentre eles destaca-se o PROFMAT-Mestrado Profissional em Matemática em Rede Nacional. De acordo com a apresentação, veja [13], o programa visa trazer o professor para o conhecimento da matéria que vai ensinar e habilitá-lo a empregar esses conhecimentos em situações da vida real e das ciências, de maneira a poder dar aos jovens a convicção de que a Matemática, além de bela e educativa, é também um instrumento poderoso para resolver problemas, elucidar situações e fornecer respostas. Além disso, surgiu por

> "Parte da constatação de que o professor de Matemática do ensino básico público possui formação deficiente, chegando à sala de aula despreparado e ignorando o conteúdo do que deve ensinar." [13, PROFMAT]

Portanto, o conhecimento rigoroso e aprofundado dos assuntos estudados deve ser de suma importância tanto para o educando quanto para o educador. Pensando nisso, a presente pesquisa busca resgatar o formalismo matemático durante o estudo de certas estruturas: O anel dos Inteiros $\mathbb{Z}$ e o anel dos Inteiros de Gauss $\mathbb{Z}[i]$.

No Ensino Fundamental o conjunto dos inteiros $\mathbb{Z}$ é iniciado e utilizado para resolver problemas aritméticos e situações problemas envolvendo dívidas, desconto e outros. Mas, a omissão das características dessa estrutura, discussão referente as propriedades, geralmente, inviabilizam a compreensão dos estudantes e a persistência de alguma dúvida referente a esse conjunto. Isso nos motivou a realizar um estudo detalhado sobre $\mathbb{Z}$, desde a definição até os principais resultados que cercam essa estrutura. Com o objetivo de intensificar o rigor matemático, mostrando que tal formalismo é indispensável para a compreensão e aplicação das propriedades de $\mathbb{Z}$. O intuito é sensibilizar

o professor de quão importante é a compreensão dos objetos e das propriedades e que tal percepção possibilite a incrementação de suas aulas.

O estudo de $\mathbb{Z}[i]$, que geralmente não é citado no Ensino Básico, tem como objetivo oferecer aos professores um contato mais aprofundado com outras estruturas similares ao conjunto dos inteiros. Mostrando que admitindo certas propriedades também nessas estruturas podem ser desenvolvidas teorias tão importantes quanto as estudas em $\mathbb{Z}$. Além disso, compreender outras estruturas abstratas fornecerá ao professor novas ferramentas para a elaboração de suas aulas, promovendo maior autonomia, inclusive em seus estudos, pois irá se encontrar mais preparado para estabelecer links entre conteúdos e as respectivas aplicações.

A propósito, é de suma importância a formação continuada para o professor da Educação Básica, inclusive para ajuda-lo na sua pratica em sala de aula. Quem conhece bem o conteúdo tem mais ferramentas para desenvolver métodos mais eficazes para o ensino. Apesar que a vida deste profissional consiste em uma série de obstáculos, dentre elas: carga horária excessiva, salários baixos e outros.

Não é objetivo dessa pesquisa ressaltar a mazelas da educação, no entanto, a carga horária excessiva impede o profissional da educação em desenvolver pesquisas e buscar, por meio delas, a oportunidade de alcançar novos conhecimentos, e consequentemente, os discentes recebem de forma direta ou indireta as contribuições advindas dos estudos realizados pelo professor, e essa concepção é confirmada por Freire:

> "[...] se convença definitivamente de que ensinar não é transferir conhecimento, mas criar as possibilidades para a sua produção ou a sua construção." [6, Freire]

A intenção é basicamente essa, possibilitar ao professor conhecer e/ ou aprimorar o seu conhecimento e consequentemente, oferecer aos discentes a possibilidade de construir suas próprias concepções e despertar o interesse em descobrir outras estruturas.

A compreensão de $\mathbb{Z}[i]$ está correlacionada as propriedades de $\mathbb{Z}$, e estas, contribuem significativamente para o entendimento de $\mathbb{Z}[i]$, e durante a pesquisa poderão observar diversas semelhanças existentes entre esses conjuntos. Assim, haverá uma discussão teórica em relação a cada uma, afim de oferecer ao leitor um olhar amplo mediante as propriedades de ambas as estruturas e o quanto uma discussão teórica bem estruturada do conjunto $\mathbb{Z}$ pode: desenvolver o raciocínio logico matemático, prepara-los para o contato com novas estruturas abstratas, propiciar aos discentes a chance de alçar novos conhecimentos e até mesmo aplicação prática.

Embora este trabalho prioriza uma discussão matemática intensa, em nenhum momento houve a intensão de esquecer ou menosprezar as áreas metodologias que por sua vez, são extremamente relevantes para um bom desenvolvimento das aulas. Mas acredita-se que a valorização do conhecimento matemático possibilitará ao professor a oportunidade de estabelecer conexões entre os conteúdos e um melhor aproveitamento das diversas metodologias existentes, pois por mais didático que seja o professor de matemática, suas aulas podem ser comprometidas caso haja uma limitação em seu conhecimento teórico.

O conjunto do Inteiros Gaussianos $\mathbb{Z}[i]$, introduzido por Gauss em 1825 veja [16], é o conjunto dos números complexos da forma $a + bi$, onde a e b são números inteiros, e é assim denominado em homenagem ao seu criador. Ele foi definido enquanto Gauss investigava questões relacionadas à reciprocidade biquadrática, quando percebeu que a pesquisa se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$. Desse modo, Gauss estendeu a ideia de números inteiros 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.

Essa generalização do conjunto dos números inteiros dá exemplos especiais de desenvolvimentos muito mais profundos que chamamos de Teoria dos Números Algébricos. 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.

Assim, neste trabalho faremos uma abordagem elementar mediante aos conceitos iniciais para o entendimento desta estrutura, no que tange, desde a sua origem e, principalmente, com sua semelhança com os Inteiros e, inclusive, a sua presença na determinação de Ternos Pitagóricos.

Existem poucos trabalhos relacionados ao tema, no entanto, a intenção desta pesquisa é proporcionar a oportunidade de conhecer e/ou aprimorar o saber mediante a versatilidade de $\mathbb{Z}[i]$ e o quanto o conhecimento das propriedades de $\mathbb{Z}$ pode auxiliar para tal compreensão. Além disso, os resultados importantes de cada conjunto serão explorados e a priori os que apresentam similaridades, sendo que alguns casos, conforme ilustrado na pesquisa, serão totalmente análogos, para confirmar o quanto apresentam características semelhantes.

No que diz respeito a sua estruturação, o trabalho constituí-se por três capítulos. O primeiro capítulo, trata-se de descrever os principais resultados do conjunto dos inteiros, e dentre estes, os que podem ser generalizados em $\mathbb{Z}[i]$, afim de proporcionar

ao leitor o paralelo entre essas estruturas.

Já no segundo capítulo será realizada uma discussão sobre os Inteiros de Gauss, com o intuito de descrever propriedades já apresentadas, e sempre em busca de destacar os resultados apresentados no Capítulo 1.

E finalmente, no Capítulo 3, optamos em expor uma aplicação sobre Terno Pitagórico, estes determinados através dos Inteiros de Gauss e podem ser desenvolvidas na 3° série do Ensino médio.

Capítulo 1

Introdução à Teoria dos Números Inteiros

Neste capítulo, será abordado o conjunto dos números Inteiros, denotado por $\mathbb{Z}$. Suas definições, proposições e teoremas contribuirão para o desenvolvimento deste trabalho. Essa seção será construída a fim de priorizar as propriedades aritméticas com o intuito de proporcionar aos professores de Matemática um aperfeiçoamento em sua prática em sala de aula e/ou desenvolvimentos de futuras pesquisas sobre a temática.

É importante frisar que a construção do conjunto dos Números Naturais ($\mathbb{N}$) e dos Números Inteiros ($\mathbb{Z}$) não será feita, pelo fato de não ser objetivo desta pesquisa. Isto porque o intuito é realizar demonstrações e por meio delas mostrar a formalidade matemática necessária para os resultados expostos e, além disso, recorrer a eles, durante outras seções a fim de estabelecer um paralelo entre as estruturas (no caso $\mathbb{Z}$ e $\mathbb{Z}[i]$). Indicamos ao caro leitor [5], [7] e [15] para mais informações sobre esses conjunto ou até mesmo algum questionamento referente a ele ou suas propriedades.

1.1 Uma Apresentação Axiomática dos Inteiros

A origem e a formulação do número ocorreu simultaneamente com o nascimento e o desenvolvimento da Matemática. A necessidade de contar objetos e as exigências da própria Matemática foram determinantes no desenvolvimento desse conceito. Houve

durante séculos a discussão sobre a existência de números negativos, mas segundo [5, p. 88]: "Coube também aos hindus a introdução dos números negativo. O objetivo era indicar o débito". Além disso, afirma que:

> "[...]O primeiro registro do uso de números negativos de que se tem notícia foi feito pelo matemático e astrônomo hindu Brahmagupta (598-?), que já conhecia inclusive as regras para as operações com números negativos.[...]" [5, p.88]

Neste registro, é possível destacar que o primeiro a manusear elementos deste conjunto foi um matemático hindu, saliento ainda que este não foi o único matemático hindu a discutir sobre os inteiros, pois Bhaskara por volta do século XII já realizavam discussões sobre resultados positivos e negativos de uma raiz quadrada e, mais importante ainda, relatava sobre a impossibilidade de determinar o resultado de uma raiz quadrada cujo o radicando fosse um número inteiro negativo.

Ao se tratar de um conjunto cujas propriedades eram polêmicas, muitos até desconsideravam sua existência como F. Viete (1540-1603) ([5, p.88]). Diante dessas afirmações, é fácil perceber que houveram inúmeras incertezas e discussões para chegar a estrutura atual dos inteiros, mas é certo que todas elas foram primordiais para o desenvolvimentos de diversos estudos, inclusive, para o desenvolvimento deste trabalho.

A problemática arraigada em $\mathbb{N}$ é o fato de $a - b$, com $a,\ b \in \mathbb{N}$ ser definida apenas para $a \geq b$. Os inteiros é o conjunto responsável para dar significado a todas as expressões $a - b$, com $a,\ b \in \mathbb{N}$.

É de fundamental importância as propriedades básicas dos inteiros, porém destaco ao leitor que elas foram admitidas como verdadeiras neste estudo. Para mais informações sobre essas propriedades como suas respectivas demonstrações recomendo a leitura de [5], [7] e [9].

Segundo [7], o conjunto $\mathbb{Z}$ é fechado em relação as operações de adição e multiplicação. Isso significa que, dados a, $b \in \mathbb{Z}$, então $a + b \in \mathbb{Z}$ e $a \cdot b \in \mathbb{Z}$.

A seguir, apresentaremos as propriedades básicas dos inteiros em relação as duas operação em que este conjunto está munido, observe:

Propriedade 1.1 (Propriedades Básicas da Aritmética)**.** *Para c, d, $e \in \mathbb{Z}$. as seguintes propriedades são válidas:*

i. (Comutativa da adição) $c + d = d + c$.

ii. (Associativa da adição) $(c + d) + e = c + (d + e)$.

iii. (Existência do elemento neutro da adição) $c + 0 = 0 + c = c$.

iv. (Existência do elemento simétrico da adição) *Para cada* c, *existe* $c' \in \mathbb{Z}$, $(c' = -c)$ *tal que* $c + c' = c' + c = 0$.

v. (Comutativa da multiplicação) $c \cdot d = d \cdot c$.

vi. (Associativa da multiplicação) $(c \cdot d) \cdot e = c \cdot (d \cdot e)$.

vii. (Existência do elemento neutro da multiplicação) $c \cdot 1 = 1 \cdot c = c$.

viii. (Distributiva). $c \cdot (d + e) = c \cdot d + c \cdot e$.

Proposição 1.2 (Lei do Cancelamento)**.** *Para quaisquer* $a,\ b,\ c \in \mathbb{Z}$, *se* $a + c = b + c$, *então* $a = b$. *Além disso, se* $x \in \mathbb{Z}$, $x \neq 0$ *é tal que* $ax = bx$ *então* $a = b$.

1.2 A Ordenação em $\mathbb{Z}$

A ordenação dos inteiros é responsável em nos sensibilizar do quanto é importante conhecer a organização deste conjunto. Mesmo sendo uma estrutura relativamente "simples", nela encontra-se propriedades valiosas para a matemática e além de ser vista como uma característica ímpar desta estrutura, justamente ao definir sua ordenação. Nesta perspectiva, pode-se destacar [5], [7] e [15] os responsáveis pelo respaldo teórico para as demonstrações utilizadas nesta seção e novamente, faço menção ao leitor interessado em detalhes de algumas demonstrações omitidas, ou seja, assumidas como verdadeiras, estes autores contribuirão para tal entendimento.

Dados $a,\ b \in \mathbb{Z}$. Dizemos que a é *menor ou igual a* b (analogamente, b é *maior ou igual* a a), indicado por $a \leq b$ (da mesma forma, $a \geq b$), se existir um $k \in \mathbb{N}$ tal que $b = a + k$, segundo [15, p. 72].

A seguir algumas propriedades importantes sobre este tópico:

Propriedade 1.3. *Sejam* $a,\ b,\ c \in \mathbb{Z}$, *então:*

i. (Reflexiva) $a \leq a$.

ii. (Antissimétrica) *Se* $a \leq b$ *e* $a \geq b$, *então* $a = b$.

iii. (Transitiva) *Se* $a \leq b$ *e* $b \leq c$, *então* $a \leq c$.

iv. *Apenas uma das afirmações é verdadeira:* $a \leq b$ *ou* $b \leq a$.

v. (Compatível e cancelativa com respeito à soma) *Temos que,* $a \leq b$ *se, e somente se,* $a + c \leq b + c$.

vi. *Se* $a \leq b$ *e* $c \geq 0$, *então* $ac \leq bc$.

vi. *Se* $a \leq b$ *e* $c \leq 0$, *então* $ac \geq bc$.

Para a e $b \in \mathbb{Z}$ denotaremos $a + (-b) = a - b$). Observe que, com essa notação, se $a \leq b$, então $b - a \in \mathbb{N}$[1] Assim, podemos reescrever os itens (i) e (iv) da Propriedade 1.3, e obtemos a *Lei da Tricotomia* em $\mathbb{Z}$: "Se $a,\ b \in \mathbb{Z}$, uma, e apenas uma, das possibilidades seguintes é válida:

$$a - b = 0,\ b - a \in \mathbb{N} \text{ ou } -(b - a) = a - b \in \mathbb{N}."$$

Diremos que a é *menor do que* b e representamos por $a < b$, quando $b - a \in \mathbb{N}$. Com essa notação, podemos reescrever a Lei da Tricotomia:

Proposição 1.4 (Tricotomia)**.** *Se* $a,\ b \in \mathbb{Z}$, *uma, e apenas uma, das possibilidades seguintes é válida:*

i. $a = b$;

ii. $a < b$;

iii. $b < a$.

Usaremos a notação $b > a$ que indica b *maior que* a, para representar $a < b$. Com respeito a essa relação entre números inteiros podemos generalizar os itens (iii), (v), (vi) e (vii) da Propriedade 1.3. Além disso, a multiplicação é compatível e cancelativa com respeito à desigualdade:

$$a, b, c \in \mathbb{Z},\ c > 0,\ a < b \Rightarrow ac < bc.$$

[1] Aqui consideramos $0 \in \mathbb{N}$.

1.2.1 Principio da Boa Ordenação

O conjunto dos inteiros apresenta um diferencial em sua composição que é a propriedade denominada por *Princípio da Boa ordenação*. Este tópico foi baseado em [7].

Definição 1.5. *Diremos que um subconjunto não vazio S de $\mathbb{Z}$ é limitado inferiormente, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in S$. Neste caso, diremos que c é uma cota inferior para S.*

Por convenção o conjunto vazio será denominado limitado inferiormente.

Diremos que $b \in \mathbb{Z}$ é o menor elemento de S, se b é uma cota inferior de S e $b \in S$, neste caso denotaremos $b = min\ S$. Pelo Item $(ii.)$ da Propriedade 1.3 podemos mostrar que, caso exista um menor elemento em S, então ele é único.

Uma das principais propriedades dos números inteiros é o *Princípio da Boa Ordenação*, enunciado a seguir, não a demonstraremos mas esse resultado será fundamental na demonstração da Proposição 1.7.

Proposição 1.6 (Principio da Boa ordenação)**.** *Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.*

De modo análogo, diremos que um subconjunto T de $\mathbb{Z}$ é *limitado superiormente* se for vazio[2] ou se existir um número $d \in \mathbb{Z}$ tal que $x \leq d$ para todo $x \in T$. Neste caso, d é uma *cota superior* para T. E ainda, diremos que $b \in \mathbb{Z}$ é o *maior elemento* de T, se b é uma cota superior de T com $b \in T$, sendo denotado por $max\ T = b$.

Proposição 1.7. *Se T é um subconjunto de $\mathbb{Z}$ não vazio e limitado superiormente, então T possui um maior elemento.*

Demonstração. Considere d uma cota superior de T, assim, $x \leq d$ para todo $x \in T$. Seja $S = \{y \in \mathbb{Z} :\ y \leq d - x,\ \text{com } x \in T\}$. O conjunto S é não vazio e limitado inferiormente pelo zero. Logo, pelo Principio da Boa Ordenação, ele possui um menor elemento $d - b$, com $b \in T$. Para todo $x \in T$, temos que $d - x \in S$, assim

$$\begin{aligned} d - x &\geq d - b \text{ (como } d - b \text{ é o menor elemento de } S) \\ -x &\geq -b \text{ (Pelo Item } (v) \text{ da Propriedade 1.3)} \\ x &\leq b \text{ (Pelos item } (vi) \text{ da Propriedade 1.3)} \end{aligned}$$

[2]por convenção

Logo $b = max\ T$. □

Uma das principais consequências do Principio da Boa ordenação é o *Principio de Indução Matemática*. Ele consiste em uma importante ferramenta matemática para demonstrar propriedades sobre o conjunto dos números inteiros. Segue a sua apresentação.

Teorema 1.8 (Principio de Indução Matemática)**.** *Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que:*

(i) $a \in S$.

(ii) *S é fechado com respeito à operação de "somar 1" a seus elementos, ou seja, se $n \in S$, então $n + 1 \in S$.*

Então, $\{x \in \mathbb{Z} : x \geq a\} \subset S$.

A partir do Teorema 1.8, podemos estabelecer uma maneira de demonstrar afirmações válidas para todo o número inteiro maiores ou iguais a um dado $a \in \mathbb{Z}$: "Considere $p(n)$ uma sentença aberta em $n \in \mathbb{Z}$. Suponha que, $p(a)$ é verdadeira, e que sempre que $p(n)$ é verdadeira, para algum $n \geq a$, implica que $p(n + 1)$ é verdadeira. Então, $p(n)$ é verdadeira para todo $n \geq a$". De fato, basta considerar $S = \{x \in \mathbb{Z} : p(n) \text{ é verdadeira}\}$. Observe que, $a \in S$. Além disso, se $n \in S$, então $n + 1 \in S$. Logo, pelo Teorema 1.8, $\{x \in \mathbb{Z} : x \geq a\} \subset S$, ou seja, $p(n)$ é verdadeira para todo $n \geq a$.

1.3 Valor Absoluto

Para a Geometria, o valor absoluto, denotado por $|a|$ é a distância do número analisado à origem, no caso dos inteiros, ao 0, por isso o valor positivo para ambas as situações. A seguir, será descrita a definição de valor absoluto, vejamos:

Definição 1.9. *Para $a \in \mathbb{Z}$ o valor absoluto, também designado de módulo de a e denotado por $|a|$ é definido por*

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

Observe, por exemplo, que $|-15| = -(-15) = +15$.

Proposição 1.10. *Para quaisquer* $a,\ b \in \mathbb{Z}$, *tem-se:*

i. $|a| = |-a|$;

ii. $-|a| \leq a \leq |a|$;

iii. $|ab| = |a|.|b|$;

iv. (Desigualdade Triangular) $|a+b| \leq |a| + |b|$.

A demonstração desta proposição será omitida, caso tenha dúvidas sobre a mesma, consulte [5, p. 97, 1991].

O resultado a seguir será demonstrado detalhadamente para ilustrar o formalismo mencionado anteriormente.[3]

Corolário 1.11. *Sejam* $a,\ b \in \mathbb{Z}$, *então tem-se*

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

Demonstração. Sabemos que $a = (a-b)+b$, aplicando módulo em ambos os membros dessa igualdade, temos que $|a| = |(a-b)+b|$. Assim,

$$|a| = |(a-b)+b| \leq |(a-b)| + |b| = |a-b| + |b|, \text{ (pelo Item } (iv) \text{ da Proposição 1.10)}$$

ou seja,

$$\begin{aligned}
|a| &\leq |a-b| + |b| \\
|a| + (-|b|) &\leq (|a-b| + |b|) + (-|b|) \text{ (pelo Item } (v) \text{ da Propriedade 1.3)} \\
|a| - |b|) &\leq |a-b| + (|b| + (-|b|)) \text{ (pelo Item } (ii) \text{ da Propriedade 1.1)} \\
|a| - |b| &\leq |a-b| + 0 \text{ (pelo Item } (iv) \text{ da Propriedade 1.1)} \\
|a| - |b| &\leq |a-b| \text{ (pelo Item } (iii) \text{ da Propriedade 1.1)}
\end{aligned}$$

[3] Deixaremos outras demontrações mais detalhadas para o próximo capítulo.

Além disso, como $|a-b| = |a+(-b)|$, temos que

$$\begin{aligned} |a-b| &\leq |a| + |-b|)) \text{ (pelo Item } (iv) \text{ da Propriedade 1.10)} \\ &\leq |a| + |b| \text{ (pelo Item } (i) \text{ da Propriedade 1.10)} \end{aligned}$$

Portanto $|a| - |b| \leq |a-b| \leq |a| + |b|$, como queríamos demonstrar. □

1.4 Divisibilidade em $\mathbb{Z}$

Nesta seção, abordaremos a divisibilidade em $\mathbb{Z}$ e suas propriedades. Estas são de estimada relevância para fundamentação deste trabalho. É importante frisar que este assunto é comentado frequentemente no ensino básico, de forma mais específica nas séries iniciais do Ensino Fundamental II no 6º ano.

Essa discussão se intensifica no momento em que as operações usuais em $\mathbb{Z}$ são apresentadas, porém por mais seguros e consistentes que sejam os resultados, devido ao fato do fechamento na adição e multiplicação, existem situações as quais podem ser submetidas que só o entendimento efetivo das operações permitirá um tomada de decisão coerente. A seguir, vejamos a definição de divisibilidade em $\mathbb{Z}$.

Definição 1.12. *Sejam $a,\ b \in \mathbb{Z}$. Dizemos que a divide b, e escrevemos $a|b$, se existir $c \in \mathbb{Z}$ tal que $b = ac$. Caso contrário, diremos que a não divide b, e usamos a notação $a \nmid b$. Se $a|b$ dizemos ainda que a é divisor (ou fator) de b, ou ainda, que b é múltiplo de a ou que b é divisível por a*

É importante frisar que a notação $a|b$ não descreve nenhuma operação em $\mathbb{Z}$ e tampouco uma representação de fração, pois ela representa uma sentença na qual verifica se existe algum $c \in \mathbb{Z}$ tal que $b = ac$. Se existe $c \in \mathbb{Z}$ tal que $b = ac$, com $b \neq 0$, c será denominado a *razão* entre a e b e será denotada por $\frac{a}{b}$. Observe, por exemplo, que $\frac{11}{5}$ não faz nenhum sentido em $\mathbb{Z}$ já que não existe um inteiro c tal que $11 = 5 \cdot c$.

Neste momento, serão apresentadas as propriedades de divisibilidade de $\mathbb{Z}$. Vale destacar que serão demonstradas apenas as propriedades que apresentarem peculiaridades.

Proposição 1.13. *Dados $a,\ b,\ c\ d \in \mathbb{Z}$. Tem-se*

i) $1 \,|\, a$, $a \,|\, a$ *e* $a \,|\, 0$.

ii) $0 \mid a$ *se, e somente se,* $a = 0$.

iii) $a \mid b$ *se, e somente se,* $|a| \mid |b|$.

iv) (Reflexiva) $\forall\ a \in \mathbb{Z}$, $a|a$.

v) (Antissimétrica) *Se* $a|b$ *e* $b|a$ *, então* $a = \pm b$.

vi) (Transitividade) *Sejam* $a,\ b,\ c \in \mathbb{Z}$, *se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

vii) Se $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$.

A demonstração da Proposição 1.13 pode ser encontradas em [7] e [5].

A seguinte proposição é de extrema utilidade para as próximas seções.

Proposição 1.14. *Sejam* $a,\ b,\ c \in \mathbb{Z}$ *tais que* $a|b$ *e* $a|c$, *então para* $\forall\ x,\ y \in \mathbb{Z}$

$$a|(bx + cy).$$

Demonstração. Como $a|b$ e $a|c$, então existem $k,\ l \in \mathbb{Z}$ tais que $b = ak$ e $c = al$. Então,

$$\begin{aligned} bx + cy &= x(ak) + y(al) \\ &= a(xk) + a(yl) \text{ (pelos itens } (v) \text{ e } (vi) \text{ da Propriedade 1.1)} \\ &= a(xk + yl) \text{ (pelo Item } (vii) \text{ da Propriedade 1.1)} \end{aligned}$$

Portanto, $a|(bx + cy)$. □

Como consequência imediata da Proposição 1.14 temos que, dados $a,\ b,\ c \in \mathbb{Z}$ tais que $a|(b \pm c)$, então

$$a|b \text{ se, e somente se, } a|c.$$

1.5 Divisão Euclideana

Sem dúvida, este tópico é um dos principais resultados mediante a conclusões realizadas em diversos resultados de Teoria dos Números e também fundamental para este trabalho. Certamente a divisão euclideana é de suma importância, inclusive desempenha papel fundamental em diversas demonstrações.

É explícito que a apresentação da divisão euclideana no ensino básico é realizada minimamente e de forma simples (ou informal ou sem rigor da sua definição), motivo este também, devido ao seu nível de complexidade, a carga de conhecimentos prévios necessários para seu entendimento. Isso restringe, principalmente, uma apresentação formal para esses discentes, em especial às séries finais do ensino fundamental. Graças a esse tópico, a determinação do máximo divisor comum e soluções equações diofantinas são imediatas e eficazes.

A divisão euclidiana, enunciada no livro *Os Elementos* de Euclides para números naturais, é um resultado central da aritmética. Para sua demonstração utilizaremos a *Propriedade Arquimediana* uma importante propriedade dos números inteiros que é uma consequência imediata do princípio da boa ordenação. Não demonstraremos essa propriedade mas sua demonstração pode ser encontrada em [7]. É importante lembrar que nesta seção, as demonstrações foram baseada nas obras [7], [11] e [15].

Proposição 1.15 (Propriedade Arquimediana)**.** *Sejam $a, b \in \mathbb{N}$, com $b \neq 0$. Então existe $x \in \mathbb{N}$ tal que $xb > a$.*

Teorema 1.16 (Divisão Euclideana)**.** *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Existem dois únicos números $q, r \in \mathbb{Z}$,*

$$a = bq + r, \ \textit{com } 0 \leqslant r \leqslant |b|.$$

Demonstração. Seja $S = \{a - xy : y \in \mathbb{Z}\} \cap \mathbb{N}$. Note que, pela Propriedade 1.15, S não é vazio. Além disso, S é limitado inferiormente por zero. Pela Proposição 1.6, S possui um menor elemento r.

Consideremos que $r = a - bq$ para certo $q \in \mathbb{Z}$. Como $r \geqslant 0$, basta mostrar que $r < |b|$. Suponhamos por absurdo que $r \geqslant |b|$. Portanto existe um $s \in \mathbb{N}$ tal que $r = |b| + s$, logo $0 \leqslant s < r$. Além disso, $s = r - |b| = a - bq - |b| = a - (q \pm 1)b \in S$, o que contradiz o fato de r ser o menor elemento do conjunto S. Logo, $r < |b|$.

Unicidade. Suponha que $a = bq + r = bq_1 + r_1$, onde $q, q_1, r, r_1 \in \mathbb{Z}, 0 \leqslant r < |b|$ e $0 \leqslant r_1 < |b|$. Suponha ainda, sem perda de generalidade, que $r_1 > r$. Assim, $0 < r_1 - r < |b|$. Além disso, $r_1 - r = (a - bq) - (a - q_1 b) = (q_1 - q)b$, ou seja, $b | r_1 - r$ o que só é possível se $r_1 - r = 0$ isto é, $r_1 = r$ e $q_1 = q$. □

Observação 1.17. *A partir da divisão Euclideana, no Teorema 1.16, podemos determinar q_1, $r_1 \in \mathbb{Z}$ com $0 \leq |r_1| \leq \dfrac{|b|}{2}$ tais que $a = bq_1 + r_1$. De fato, suponha que $a = bq + r$ onde $0 \leq r < |b|$. Se $r \leq \dfrac{|b|}{2}$ tome $q = q_1$ e $r = r_1$. Assim,*

$a = bq_1 + r_1$, *onde* $0 \leq |r_1| \leq \dfrac{|b|}{2}$. *Agora, se* $r > \dfrac{|b|}{2}$, *considere* $r' = |b| - r$. *Então* $a = bq + r = bq + |b| - r' = b(q \pm 1) + (-r')$. *Basta tomar* $q_1 = q \pm 1$ *e* $r_1 = -r'$. *Assim,* $a = bq_1 + r_1$, *onde* $0 \leq |r_1| = |-r'| = |b| - r \leq |b| - \dfrac{|b|}{2} \leq \dfrac{|b|}{2}$.

No Teorema 1.16 q, $r \in \mathbb{Z}$ são denominados como *quociente* e *resto* respectivamente. Caso $r = 0$, então a é um múltiplo de b. Observe que, se $a = 0$, então $q = r = 0$. Mais ainda, se $a > 0$ e $a < b$ então $q = 0$ e $r = a$.

Exemplo 1.18. *Determine o resto e o quociente da divisão euclideana de* 27 *por* 5.

Demonstração. De acordo com Teorema 1.16, devemos determinar r e $q \in \mathbb{Z}$ tais que $27 = 5q + r$, com $0 \leq r < 5$. Como, $27 = 5 \cdot 5 + 2$, temos que $r = 2$ e $q = 5$ são o resto e o quociente, respectivamente. □

1.6 Máximo Divisor Comum

Definiremos agora o máximo divisor comum entre a e b.

Definição 1.19. *O inteiro positivo* d *é dito o máximo divisor comum entre* a *e* b *se*

(i) d *é divisor comum de* a *e* b*;*

(ii) qualquer divisor de a *e* b *é divisor de* d.

Seguindo [9], utilizaremos como notação (a, b) para o máximo divisor comum entre a e b. Como é uma exigência que o máximo divisor comum de a e b seja positivo, temos

$$(a, b) = (-a, b) = (a, -b) = (-a, -b).$$

Além disso, o máximo divisor comum entre dois números inteiros é único. De fato, sejam d, $d' \in \mathbb{Z}$ satisfazendo $(a, b) = d$ e $(a, b) = d'$. Pelo Item (ii) da Definição 1.19 tem-se que $d|d'$ e $d'|d$. Pela Proposição 1.13 segue que $d = \pm d'$. Como $d > 0$ e $d' > 0$ segue que $d = d'$. Segundo [9], temos que

Lema 1.20. *Se* a, $b \in \mathbb{Z}$, *não ambos nulos, então existe* $(a, b) = d$. *Além disso, podemos encontrar inteiros* x_0 *e* y_0 *tais que* $d = ax_0 + b_0$.

Demonstração. Seja $C = \{ax + by : \text{ com } x,\ y \in \mathbb{Z}\}$. Primeiramente observe que $C \neq \{0\}$, já que a ou b é diferente de zero e $a = 1 \cdot a + 0 \cdot b \in C$ e $b = 0 \cdot a + 1 \cdot b \in C$. Mais que isso, se $m = ax + by \in C$, então $-m = a(-x) + b(-y) \in C$, ou seja, existem inteiros positivos em C. Portanto, pela Proposição 1.6, existe um menor inteiro positivo d que é minimo em C. Assim, $d = ax_0 + by_0$, para certos $x_0, y_0 \in \mathbb{Z}$.
Afirmamos que $d = (a, b)$. De fato, dado $m = ax + by \in C$, pelo Teorema 1.16, existem $q, r \in \mathbb{Z}$ tais que $m = dq + r$, com $0 \leq r < d$, isto é,

$$ax + by = t(ax_0 + by_0) + r \text{ onde } r = (x - tx_0)a + (y - ty_0)b.$$

Logo $r \in C$, como $0 \leq r < d$ e d é o mínimo de C, então $r = 0$. Assim, $m = td$, ou seja, $d|m$, para $\forall m \in C$. Em particular, $d|a$ e $d|b$. Além disso, se $c|a$ e $c|b$, então, pela Proposição 1.14, $c|ax_0 + by_0 = d$. □

Lema 1.21. *Dados $a,\ b,\ n \in \mathbb{Z}$. Se $d = (a, b - an)$, então, $d = (a, b)$, em outras palavras,*

$$(a, b - an) = (a, b).$$

Demonstração. Como $d = (a, b - an)$, então $d \mid a$ e $d \mid (b - an)$. De acordo com Proposição 1.14 temos que $d \mid an + (b - an) = b$. Assim, $d|a$ e $d|b$ segue, por definição, que $d|(a, b) = c$. Analogamente, como $c = (a, b)$, $c|a$ e $c|b$ e, pela Proposição 1.14, temos que $c \mid b - an$. donde $c|d$. Como $c, d > 0$, segue que $d = c$. □

Em particular, se $a = bq + r$, então

$$(b, a) = (b, a - bq) = (b, r).$$

Considere $a,\ b \in \mathbb{Z}$. Nestas condições, pode-se definir o conjunto

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by :\ x,\ y \in \mathbb{Z}\}.$$

Se a e b ambos não nulos, então o conjunto $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N} \neq \emptyset$, pois $a^2 + b^2 = a \cdot a + b \cdot b \in (a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}$.

Denotaremos o conjunto $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}$ por $I(a, b)$. Defina também o conjunto

$$d\mathbb{Z} = \{td :\ t \in \mathbb{Z}\}$$

Segue o seguinte teorema, que não será demonstrado, para formalizar uma série de critérios importantes e também particularidades do Máximo Divisor Comum.

Teorema 1.22. *Dados* $a,\ b \in \mathbb{Z}$, *com* $a \neq 0$ *e* $b \neq 0$. *Se* $d = minI(a,b) \cap \mathbb{N}$, *então*

(i) $d = (a,b)$;

(ii) $I(a,b) = d\mathbb{Z}$.

O Teorema 1.22 nos diz que todos os múltiplos de d podem ser escritos como combinação linear de a e b. O Teorema de Bèzout é um corolário desse resultado como veremos a seguir e não será demonstrado.

Corolário 1.23. *Dados quaisquer* $a,\ b \in \mathbb{Z}$ *não nulos, e* $n \in \mathbb{N}$, *temos que*

$$(na, nb) = n(a,b).$$

Corolário 1.24. *Sejam* $a,\ b \in \mathbb{Z}$, *ambos não nulos, então*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

Demonstração. Seja $d = (a,b)$. Então pode-se reescrever a sentença em função de d da forma

$$(a,b) = (d \cdot \frac{a}{d}\ ,\ d \cdot \frac{b}{d}).$$

De acordo com o Corolário 1.23, a sentença pode ser descrita da forma:

$$d = (a,b) = (d \cdot \frac{a}{d}\ ,\ d \cdot \frac{b}{d}) = d \cdot (\frac{a}{d}\ ,\ \frac{b}{d}).$$

Como $d \neq 0$, então, ao aplicar a Proposição 1.2, obtemos

$$d \cdot (\frac{a}{d}\ ,\ \frac{b}{d}) = d \cdot 1 \Rightarrow (\frac{a}{d}\ ,\ \frac{b}{d}) = 1$$

□

Definição 1.25. *Dados* $a, b \in \mathbb{Z}$, *se* $(a,b) = 1$ *diremos que* a *e* b *são coprimos ou primos entre si ou ainda relativamente primos.*

A seguir apresentaremos um resultado muito importante sobre elementos relativamente primos. A demonstração deste resultado será omitida.

Teorema 1.26 (Lema de Gauss)**.** *Dados* $a,\ b,\ c \in \mathbb{Z}$. *Se* $a \mid bc$ *e* $(a,b) = 1$, *então* $a \mid c$.

Além disso, se $a,\ b,\ c \in \mathbb{Z}$, com b e c não nulos, temos que

$$b \mid a \text{ e } c \mid a \text{ se, e somente se, } \frac{bc}{(b,c)} \mid a.$$

1.7 Números Primos

Uma parte significativa de resultados elegantes na Teoria dos Números é atribuída aos estudos direcionados para os números primos. Devido a singularidade de sua definição, essa categoria numérica ocupa lugar privilegiado na matemática. Segundo [15], o conceito de *primo*, palavra que se origina do grego e cujo significado original é *primeiro*.

Realmente, existem vários relatos históricos sobre a existência do conceito de primos, já que até mesmo no papiro de Rhind havia registros, porém a civilização grega é a responsável pela demonstração sobre a existência de infinitos primos e também pela configuração atual da Teoria dos Números.

Embora os números primos seja um conceito trabalhado no ensino básico com pouca enfase, porém de suma importância, por esse motivo, faremos uma seção direcionado ao estudo detalhado desde a definição até as principais propriedades a fim de sensibilizar a relevância da temática para o ensino. Esta seção segue baseada nos autores [7] e [11].

1.7.1 Teorema Fundamental da Aritmética

Definição 1.27. *Seja* $p \in \mathbb{Z}$ *com* $p \neq 0$ *e* $p \neq \pm 1$. *Se os únicos divisores de* p *são* ± 1 *e* $\pm p$ *diremos que* p *é primo.*

Um número $n \in \mathbb{Z}$ *(*$n \neq 0$ *e* $n \neq \pm 1$*) que não é primo é denominado composto.*

Veja, por exemplo, que o número $2 \in \mathbb{Z}$ é um primo, pois se $k > 0$, com $k|2$, então $0 < k \leq 2$. Logo, existem duas possibilidades: $k = 1$ ou $k = 2$, sendo assim, 2 é primo. Vale ressaltar que é o único primo par, pois todos os outros números inteiros pares são múltiplos de 2. Os números 0 e ± 1 não são primos e nem compostos.

Proposição 1.28 (Lema de Euclides). *Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Para $a = 0$ e $b = 0$ o resultado é imediato. No entanto, vamos provar para $a \neq 0$ e $b \neq 0$. Suponha que $p \not| a$, então $(p, a) = 1$. Como, por hipótese, $p \mid ab$, segue, pelo Teorema 1.26, que $p \mid b$. □

Como resultado imediato desse teorema segue que, se $p,\ p_1,\ \cdots, p_n$ são primos e, $p \mid p_1 \cdots\ p_n$, então $p = \pm p_i$ para algum $1 \leq i \leq n$.

Teorema 1.29 (Teorema Fundamental da Arimética). *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.*

Demonstração. A demonstração será apresentada primeiro a existência da decomposição e depois a unicidade, vejamos:
Existência: Por hipótese, $n > 1$. Suponhamos por absurdo que
$X = \{n \in \mathbb{N} - \{0\} :$ n não pode ser decomposto como produto de números primos$\}$, seja não vazio. Então, pela Proposição 1.6, X tem um menor elemento, digamos $n_0 = minX$. Observe que, n_0 não pode ser primo, visto que n_0 é igual a ele mesmo, estaria na sua forma mais elementar. Então, considere $n_0 = ab$, com $a,\ b > 1$, logo

$$a = \frac{n}{b} < n = minX \Rightarrow a < n.$$

Analogamente,

$$b = \frac{n}{a} < n = minX \Rightarrow b < n.$$

Portanto, $a,\ b \notin X$, o que implica que $a,\ b$ podem ser escritos em produto de números primos, isto é:

$$a = p_1 \cdots p_k \text{ e } b = q_1 \cdots q_r \tag{1.1}$$

nos quais p_i, q_j são primos, com $1 \leq i \leq k$ e $1 \leq j \leq r$. Então, a partir da Equação (1.1), n pode escrito por

$$n = p_1 \cdots p_k \cdot q_1 \cdots q_r,$$

contradizendo o fato de que $n \in X$.
Unicidade: Vamos provar por indução sobre n. Suponha que n possa ser decomposto

das seguintes formas como o produto de fatores primos

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r,$$

então $p_1 \,|\, q_1 q_2 \cdots q_r$. Segue, pela Proposição 1.28, que $p_1 = p_j$ para algum $1 \leq j \leq r$. Podemos supor, sem perda de generalidade, que $p_1 = q_1$ (como vale a propriedade comutativa da multiplicação, basta reindexar os índices de q_j). Assim, pela Proposição 1.2, $p_2 \cdots p_k = q_2 \cdots q_r$. Como $p_2 \cdot p_3 \cdots p_k < n$, por hipótese de indução, implica que $k = s$ e os pares p_i e q_j são iguais. □

Uma prova clássica realizada pela civilização grega, pode até ser considerada um legado deixado por esse povo, foi a existência de infinitos números primos, a seguir, realizaremos a demonstração inspirada em Euclides.

Teorema 1.30 (Teorema de Euclides)**.** *Existem infinitos números primos.*

Demonstração. Suponha, por absurdo, que existe um número finito de primos, digamos $p_1,\ p_2,\ \cdots, p_n$. Considere

$$N = p_1 \cdot p_2 \cdots p_n + 1 \Rightarrow N > 1. \tag{1.2}$$

Então, pelo Teorema 1.29, temos que existe p_j com $1 \leq j \leq n$, tal que $p_j \,|\, N \Rightarrow p_j \,|\, N - p_1 \cdot p_2 \cdots p_n = 1$. Absurdo, pois p_j é primo, logo é maior do que 1. □

1.8 A Aritmética dos Restos em $\mathbb{Z}$

Agora realizaremos uma discussão de suma importância a partir dos restos da divisão de um dado número previamente fixado. Este tópico é baseado na obra [7].

1.8.1 Congruência

Definição 1.31. *Seja $m \in \mathbb{Z}$ e $m > 1$. Dois números a e b são ditos côngruos módulo m se $m \,|\, b - a$. Este caso será denotado por $a \equiv b \pmod{m}$.*

Se $m \nmid b - a$ denotaremos por $a \not\equiv b \pmod{m}$.

A definição estabelece a restrição para $m \neq 1$ pelo simples fato que o resto da divisão de qualquer número inteiro por 1 será igual a 0. Isso torna-se irrelevante mediante aos objetivos almejados para aritmética dos restos, pois o intuito é observar a variação nos restos da divisão euclideana a partir de um número fixo, por isso, $m > 1$.

Uma consequência imediata da Definição 1.31 é uma relação de equivalência e de maneira bem sutil. Vejamos:

Proposição 1.32. *Dado $m \in \mathbb{N}$. Para quaisquer $a,\ b,\ c \in \mathbb{Z}$, tem-se que*

i. (Reflexiva) $a \equiv a \pmod{m}$.

ii. (Simétrica) *Se* $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$.

iii. (Transitiva) *Se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$.

Pode-se mostrar que, dados $a,\ b,\ m \in \mathbb{Z}$, com $m > 1$. Então $a \equiv b \pmod{m}$ se, e somente se, a e b deixam o mesmo resto na divisão euclideana por m.

Por ser uma relação de equivalência torna-se mais forte e consistência quando associada as operações de adição e multiplicação, como verificaremos a seguir.

Proposição 1.33. *Dados $a,\ b,\ c,\ d,\ m\ n \in \mathbb{Z}$, com m e $n > 1$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então*

i. $a + c \equiv b + d \pmod{m}$;

ii. $ac \equiv bd \pmod{m}$.

iii. $a^n \equiv b^n \pmod{m}$.

Antes de demonstrar o próximo teorema vamos determinar os coeficientes da expressão $(1+x)^n$, onde x é uma variável e $n \in \mathbb{N}$.
Para $n = 1$ temos $(1+x)^1 = 1 + x$;
Para $n = 2$ temos $(1+x)^2 = (1+x)(1+x) = 1 + 2x + x^2$;
Para $n = 3$ temos que $(1+x)^3 = (1+x)^2(1+x) = (1 + 2x + x^3) = 1 + 3x + 3x^2 + x^3$;
Assim, $(1+x)^n = a_0 + a_1x + ... + a_nx^n$.
O termo a_i será denotado por $a_i = \binom{n}{i}$ e denominado de *número binominal*. Observe que $a_0 = 1 = a_n$, logo $\binom{n}{0} = \binom{n}{n} = 1$. Além disso, como $a_{n+r} = 0$ para todo $r \geq 1$,

segue que $\binom{n}{i} = 0$ se $i > n$. Pode-se provar, por indução, que para todos $n, i \in \mathbb{N}$ com $1 \leq i \leq n$,

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}, \tag{1.3}$$

onde, para $n \in \mathbb{N}$, $n!$ é definido, por

$$n! = \begin{cases} 1, \text{ se } n = 0 \text{ ou } n = 1; \\ n(n-1)!, \text{ se } n > 1. \end{cases}$$

Lema 1.34. *Para p primo e $1 \leq i \leq p-1$, então $p|\binom{p}{i}$.*

Demonstração. Se $i = 1$ ou $i = p-1$, pela Equação (1.3),

$$\binom{p}{1} = \frac{p!}{1!(p-1)!} = p,$$

o resultado é verdadeiro. Podemos supor então que $1 < i < p-1$. Pela Equação (1.3)

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p.(p-1)...(p-(i-1))(p-i)!}{i!(p-i)!} = \frac{p.(p-1)...(p-i+1)}{i!} \in \mathbb{N}.$$

Logo, $i!|p.(p-1)...(p-i+1)$. Como $1 < i < p-1$, $(i!, p) = 1$ e $i!|(p-1)...(p-i+1)$. Portanto,

$$\binom{p}{i} = p\frac{(p-1)...(p-i+1)}{i!}.$$

□

Teorema 1.35 (Pequeno Teorema de Fermat)**.** *Dado um número primo p e $a \in \mathbb{Z}$ então $a^p \equiv a \mod p$.*

Demonstração. Se $p = 2$, então $a^2 - a = a(a-1)$ é um número par e $p|a^2 - a$. Suponhamos então que $p > 2$ e $a \geqslant 0$. Vamos provar por indução sobre a. Para $a = 0$, o resultado é verdadeiro pois $p|0 = a^p - a$. Suponhamos que o teorema é verdadeiro

para $a > 0$. Provaremos para $a + 1$.

$$(a+1)^p - (a+1) = a^p + \binom{p}{1} a^{p-1} + ... + \binom{p}{p-1} a - a - 1 = (a^p - a) + \binom{p}{1} a^{p-1} + ... + pa.$$

Logo, utilizando a hipótese de indução e o Lema 1.34, o resultado é verdadeiro para $a > 0$. Agora, se $a < 0$, então $-a > 0$ e pelo passo anterior $(-a)^p = -a^p \equiv -a \mod p$, já que p é ímpar. O resultado segue da Proposição 1.33 item (ii). □

Como consequência imediado do Teorema 1.35 temos que se $p \nmid a$ e $a \in \mathbb{Z}$, então

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

.

Capítulo 2

A aritmética dos Inteiros de Gauss

Esse trabalho fará um estudo entre as propriedades aritméticas dos conjuntos: Inteiros e Inteiros de Gauss. Nele, constará uma série de extensões que comprovam a validade e aplicabilidade dos Inteiros de Gauss. Dentre elas, serão discutidas em $\mathbb{Z}[i]$: a norma, divisibilidade e outras.

Sabemos que embora não seja a finalidade da pesquisa estabelecer um estudo sobre anéis, porém é válido ressaltar o fato que $\mathbb{Z}[i]$ é um anel, ou seja, um conjunto munido por duas operações, que generalizam as propriedades básicas da aritmética, Propriedade 1.1. A seguir a exposição de adição e multiplicação em $\mathbb{Z}[i]$, vejamos:

É importante lembrar ao leitor que a construção deste capítulo foi baseada nas obras [2], [3], [8], [9] e [10].

2.1 Anel dos Inteiros de Gauss

O conjunto do Inteiros Gaussianos $\mathbb{Z}[i]$, introduzido por Gauss em 1825 veja [16], é o conjunto dos números complexos da forma $a + bi$, onde a e b são números inteiros, e é assim denominado em homenagem ao seu criador. Ele foi definido enquanto Gauss investigava questões relacionadas à reciprocidade biquadrática, quando percebeu que a pesquisa se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$. Desse modo, Gauss estendeu a ideia de números inteiros 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.

Traremos agora a definição mais rigorosa desse conjunto e sua estrutura algébrica. Considere o conjunto definido por

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

onde $i^2 = -1$. Sejam $\alpha = a + bi$ e $\beta = c + di \in \mathbb{Z}[i]$ diremos que $\alpha = \beta$, se $a = c$ e $b = d$. Em $\mathbb{Z}[i]$ podemos estabelecer uma estrutura de anéis definindo as seguintes operações[1]:

i. (Adição) $\alpha \oplus \beta = (a + c) + (b + d)i$.

ii. (Multiplicação) $\alpha \odot \beta = (ac - bd) + (ad + bc)i$.

onde as operações $+$ e $\cdot$ no lado direito de cada uma dessas igualdades são as operações usuais de $\mathbb{Z}$.

Podemos mostrar que essas operações em $\mathbb{Z}[i]$ satisfazem propriedades análogas à Propriedade 1.1.

Propriedade 2.1 (Propriedades Básicas da Aritmética em $\mathbb{Z}[i]$)**.** *Para α, β, $\delta \in \mathbb{Z}[i]$. as seguintes propriedades são válidas:*

i. (Comutativa da adição) $\alpha \oplus \beta = \beta \oplus \alpha$.

ii. (Associativa da adição) $(\alpha \oplus \beta) \oplus \delta = \alpha \oplus (\beta \oplus \delta)$.

iii. (Existência do elemento neutro da adição) *Existe* $\mathbf{0} = 0 + 0i \in \mathbb{Z}[i]$ *tal que* $\alpha \oplus \mathbf{0} = \mathbf{0} \oplus \alpha = \alpha$.

iv. (Existência do elemento simétrico da adição) *Para cada* $\alpha = a + bi$, *existe* $\alpha' \in \mathbb{Z}[i]$, $(\alpha' = -a + (-b)i)$ *tal que* $\alpha \oplus \alpha' = \alpha' \oplus \alpha = \Theta$.

v. (Comutativa da multiplicação)$\alpha \odot \beta = \beta \odot \alpha$.

vi. (Associativa da multiplicação) $(\alpha \odot \beta) \odot \delta = \alpha \odot (\beta \odot \delta)$.

vii. (Existência do elemento neutro da multiplicação) *Existe* $\mathbf{1} = 1 + 0i \in \mathbb{Z}[i]$ *tal que* $\alpha \odot \mathbf{1} = \mathbf{1} \odot \alpha = \alpha$.

viii. (Distributiva). $(\alpha \oplus \beta) \odot \delta = \alpha \odot \delta \oplus \beta \odot \delta$.

[1] essas operações são as induzidas do conjunto dos números complexos $\mathbb{C}$.

Denotaremos as operações $\oplus$ e $\odot$ em $\mathbb{Z}[i]$ simplesmente por $+$ e $\cdot$, respectivamente. Observe que $\mathbb{Z} \subset \mathbb{Z}[i]$, além disso, o elemento neutro da adição $\mathbf{0} = 0$ e o elemento neutro da multiplicação $\mathbf{1} = 1$. Podemos também, em $\mathbb{Z}[i]$ generalizar a Lei do Cancelamento, Proposição 2.2.

Proposição 2.2 (Lei do Cancelamento em $\mathbb{Z}[i]$)**.** *Para quaisquer α, β, $\delta \in \mathbb{Z}[i]$, se $\alpha + \delta = \beta + \delta$, então $\alpha = \beta$. Além disso, se $x \in \mathbb{Z}[i]$, $x \neq 0$ é tal que $\alpha x = \beta x$ então $\alpha = \beta$.*

O conjunto $\mathbb{Z}[i]$ com essas operações é denominado *Anel dos Inteiros de Gauss.* A seguir, faremos um estudo referentes a sua estrutura e os principais resultados que este conjunto pode oferecer.

2.2 A Norma de $\mathbb{Z}[i]$

A finalidade desta seção é estabelecer um paralelo entre os conjuntos dos Inteiros e Inteiros de Gauss. Podemos observar no conjunto $\mathbb{Z}$ que o comprimento de cada elemento é representado pelo valor absoluto, conforme a Definição 1.9. Já no conjunto de $\mathbb{Z}[i]$, o comprimento de cada elemento é representado pela norma. A partir deste momento, será descrita com mais detalhes, observe:

Definição 2.3. *Seja $z = a + bi \in \mathbb{Z}[i]$, o conjugado de z é o elemento $\overline{z} = a - bi \in \mathbb{Z}[i]$.*

Exemplo 2.4. *Observe:*

1. $z = 1 + 2i \Rightarrow \overline{z} = 1 - 2i$
2. $z = -5i \Rightarrow \overline{z} = 5i$
3. $z = -8 \Rightarrow \overline{z} = -8$

Definição 2.5. *Considere $z = a + bi \in \mathbb{Z}[i]$ então a norma de z é denotada por $N(z)$ é dada por*

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

Um fato importante é que a norma de z ou também denominado por módulo de z é um número natural, ou seja, $N(z) \in \mathbb{N}$.

Exemplo 2.6. $z = 8 + 7i \Rightarrow N(z) = 8^2 + 7^2 = 64 + 49 = 113$

É notável a existência de uma relação direta entre a norma do número complexo z e o valor absoluto do número $z \in \mathbb{Z}[i]$, definido acima, observe:

$$|z| = |a + bi| = \sqrt{a^2 + b^2} \text{ e } N(z) = a^2 + b^2 = |a + bi|^2$$

O que motiva os estudos em tratar da norma de $N(z)$ e não $|z|$, é por que a $N(z) \in \mathbb{Z}$ enquanto $|z| \in \mathbb{R}^2$. Além disso, por meio da norma de $\mathbb{Z}[i]$ é possível obter resultado importantes graças as propriedades de divisibilidade nas normas em $\mathbb{Z}$ para as normas de $\mathbb{Z}[i]$.

Observe que, como $N(z) \leq \mathbb{Z}$ **unidades** de um conjunto são os elementos invertíveis E a partir deste resultado, podemos definir o conjunto das unidades de $\mathbb{Z}[i]$, dado por

Proposição 2.7. *O conjunto $U = \{\pm 1, \pm i\}$ são as unidades de $\mathbb{Z}[i]$.*

Demonstração. Assim como o conjunto $\mathbb{Z}$, as unidades em $\mathbb{Z}[i]$, são todos os elementos $z \in \mathbb{Z}[i]$ que possuem inverso multiplicativo, isso significa que existe $\mathbb{Z}' \in \mathbb{Z}[i]$ tal que $z \cdot z' = 1$. Deste modo, se $z = a + bi$ é uma unidade, então segue

$$1 = z \cdot z' \Rightarrow 1 = N(z \cdot z') = N(z) \cdot N(z') \Rightarrow N(z) = 1.$$

Mas

$$N(z) = 1 \Rightarrow a^2 + b^2 = 1 \Leftrightarrow a = \pm 1 \; e \; b = 0 \; ou \; a = 0 \; e \; b = \pm 1.$$

Logo as unidades em $\mathbb{Z}[i]$ são ± 1 e $\pm i$. □

Esta justificativa é fundamentada na propriedade algébrica a seguir, pois seu resultado comprova que a norma em $\mathbb{Z}[i]$ é multiplicativa.

Teorema 2.8. *Seja $\alpha,\ \beta \in \mathbb{Z}[i]$ então $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.*

Demonstração. Sejam $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha = a + bi$ e $\beta = m + ni$, com $a, b, m, n \in \mathbb{Z}$. Note que

$$\alpha \cdot \beta = (a + bi) \cdot (m + ni) = (am - bn) + (an + bm)i. \tag{2.1}$$

[2]conjunto dos números reais

Aplicando a Definição 2.5, as normas de α e β são dadas respectivamente, por

$$N(\alpha) = N(a+bi) = (a+bi)(a-bi) = a^2 + b^2, \tag{2.2}$$

$$N(\beta) = N(m+ni) = (m+ni)(m-ni) = m^2 + n^2. \tag{2.3}$$

Queremos mostrar $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$. Das Equação (2.2) e (2.3) obtemos:

$$N(\alpha) \cdot N(\beta) = (a^2 + b^2) \cdot (m^2 + n^2),$$

$$N(\alpha) \cdot N(\beta) = (am)^2 + (bn)^2 + (an)^2 + (bm)^2. \tag{2.4}$$

Por outro lado, de (2.1), temos

$$N(\alpha\beta) = (am - bn)^2 + (an + bm)^2,$$

$$N(\alpha\beta) = (am)^2 + (bn)^2 + (an)^2 + (bm)^2. \tag{2.5}$$

Donde concluímos que $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$. □

Uma consequência imediata do Teorema 2.8 é mostrar que existem os inteiros de Gauss possuem inverso multiplicativo em $\mathbb{Z}[i]$. O intuito é utilizar o conceito de norma para a questão da inversibilidade em $\mathbb{Z}$.

Proposição 2.9. *Dado $\alpha \in \mathbb{Z}[i]$. As afirmações a seguir são equivalentes:*

1. *α é invertível em $\mathbb{Z}[i]$;*
2. *$N(\alpha) = 1$;*
3. *$\alpha \in \{-1, 1, -i, i\}$.*

Demonstração. (1) $\Rightarrow$ (2): Seja $\alpha \in \mathbb{Z}[i]$ invertível, então existe $\beta \in \mathbb{Z}[i]$ tal que

$$\alpha \cdot \beta = 1 \tag{2.6}$$

Ao aplicar a Teorema 2.8 em (2.6), então

$$N(\alpha) \cdot N(\beta) = N(\alpha \cdot \beta) = N(1) = 1 \tag{2.7}$$

Como $N(\alpha) \in \mathbb{Z}_+$ então conclui-se que $N(\alpha) = 1$.

(2) $\Rightarrow$ (3): Seja $\alpha = a + bi$ com $N(z) = 1$. Assim,

$$N(\alpha) = N(a + bi) = a^2 + b^2 = 1. \tag{2.8}$$

Logo, os possíveis valores para a e b podem ser 0, 1 ou -1. Graça a este resultado, obtemos que $\alpha \in \{-1, 1, -i, i\}$.

(3) $\Rightarrow$ (1): É fácil ver todos os elementos do conjunto $\{-1, 1, -i, i\}$ são invertíveis em $\mathbb{Z}[i]$. □

Vale observar que $N(z) \in \mathbb{Z}_+$. Mas $\mathbb{Z}_+ \not\subset N(z)$, por exemplo, os inteiros como: $3, 7, 11, 15, 19$ e 21 não pertencem a $N(z)$, pois não podem ser escritos como soma dos quadrados. Veremos mais detalhes sobre isso nas seções que seguem.

O segundo fato importante é identificar as unidade de $\mathbb{Z}[i]$.

Em síntese, é importante salientar que o conjunto $\{-1, 1, -i, i\}$ é composto por todas as unidades de $\mathbb{Z}[i]$, ou seja, cada elemento desse conjunto possui inverso multiplicativo.

2.3 Divisibilidade em $\mathbb{Z}[i]$

A divisibilidade em $\mathbb{Z}[i]$ pode ser definida por

Definição 2.10. *Sejam α, $\beta \in \mathbb{Z}[i]$, diz-se que β divide α, e denota-se por $\beta \,|\, \alpha$, se existir algum $\gamma \in \mathbb{Z}[i]$ tal que $\alpha = \beta\gamma$.*

Então β é divisor de α ou fator de α, ou ainda, α é múltiplo de β. Neste momento, serão apresentadas as propriedades de divisibilidade de $\mathbb{Z}[i]$ e suas respectivas demonstrações são análogas a $\mathbb{Z}$. A seguir, algumas propriedades importantes

Proposição 2.11. *Dados a, b, $c \in \mathbb{Z}[i]$. Tem-se*

i) $a|a$.

ii) Se $a|b$ *e* $b|a$ *, então* $a = b$.

iii) Se $a \,|\, b$ *e* $b \,|\, c \Rightarrow a \,|\, c$.

iv) Se $a \,|\, b$ *e* $a \,|\, c \Rightarrow a \,|bx + cy$, *para todo* $x, y \in \mathbb{Z}[i]$.

Neste momento, será exposto um exemplo baseado na Definição 2.10.

Exemplo 2.12. *Sejam* $\alpha = 4 + 3i$, $\beta = -2 + 11i$ *e* $\gamma = 1 + 2i$, *então* $-2 + 11i = (4 + 3i) \cdot (1 + 2i)$. *Logo,* $4 + 3i$ *divide* $-2 + 11i$, *ou seja,* $(4 + 3i) \,|\, (-2 + 11i)$.

Se $\alpha, \beta \in \mathbb{Z}[i]$, e $\alpha|\beta$, então $\dfrac{\alpha}{\beta} \in \mathbb{Z}[i]$? Considerando α e β dos Exemplo 2.12 obtemos:

$$\frac{\alpha}{\beta} = \frac{(-2 + 11i)}{(4 + 3i)} \cdot \frac{(4 - 3i)}{(4 - 3i)} = \frac{25 + 50i}{25} = \frac{25}{25} + \frac{50}{25}i = 1 + 2i.$$

Por outro lado, $\beta = 14 + 3i$ e $\alpha = 4 + 5i$ então tome

$$\frac{(14 + 3i)}{(4 + 5i)} \cdot \frac{(4 - 5i)}{(4 - 5i)} = \frac{71 - 58i}{41} = \frac{71}{41} - \frac{58}{41}i \notin \mathbb{Z}[i].$$

Busca-se por meio dessa pesquisa solucionar essas e outras questões importantes, já que no conjunto $\mathbb{Z}$ a divisão não consta nas propriedades de fechamento, e nos inteiros de Gauss, sob quais condições $\dfrac{\alpha}{\beta} \in \mathbb{Z}[i]$?

Teorema 2.13. *Dado* $z = a + bi \in \mathbb{Z}[i]$, $c \in \mathbb{Z}$. *Então* $c \,|\, z$ *se, e somente se,* $c \,|\, a$ *e* $c \,|\, b$.

Demonstração. Por hipótese, $c \,|\, z$, então, $z = cx$ para algum $x \in \mathbb{Z}[i]$. Como $z = a + bi$ e $x = m + ni$, assim

$$z = cx \Rightarrow a + bi = c(m + ni) \tag{2.9}$$

Desenvolvendo as operações do segundo membro da Equação (2.9), obtém-se que

$$a + bi = (cm) + (cn)i \Rightarrow a = cm \text{ e } b = cn \Rightarrow c \,|\, a \text{ e } c \,|\, b.$$

Reciprocamente suponha que $c \,|\, a$ e $c \,|\, b$, então

$$a = cm \text{ e } b = cn, \text{ para algum } m,\ n \in \mathbb{Z}.$$

Agora $z = a + bi$. Então $z \in \mathbb{Z}[i]$ e

$$z = a + bi \Rightarrow z = (cm) + (cn)i = c(m + ni), \text{ para algum } c \in \mathbb{Z} \text{ e } x = m + ni \in \mathbb{Z}[i].$$

Portanto, $c \mid z$. □

Teorema 2.14. *Considere α, $\beta \in \mathbb{Z}[i]$. Se $\alpha \mid \beta$, então $N(\alpha) \mid N(\beta)$.*

Demonstração. Como $\alpha \mid \beta$, então

$$\beta = \alpha\gamma, \text{ para algum } \gamma \in \mathbb{Z}[i]. \tag{2.10}$$

Ao aplicar o Teorema 2.8 na Equação (2.10), teremos

$$N(\beta) = N(\alpha) \cdot N(\gamma) \Rightarrow N(\alpha) \mid N(\beta).$$

□

Corolário 2.15. *Seja α um inteiro de Gauss, α é múltiplo de $1+i$ se, e somente se, $N(\alpha)$ é par.*

Demonstração. Seja α é múltiplo de $1+i$ se, e somente se, existe $x+yi \in \mathbb{Z}[i]$ tal que $\alpha = (1+i) \cdot (x+yi)$ ou equivalentemente

$$\begin{cases} x - y = a \\ x + y = b \end{cases}.$$

Assim, α é múltiplo de $1+i$ se, e somente se, o sistema linear acima possui solução em $\mathbb{Z}$. Agora, a solução desse sistema é dada por $x = \left(\frac{a+b}{2}\right)$ e $y = \left(\frac{b-a}{2}\right)$. E $x, y \in \mathbb{Z}$ se, e somente se, a e b possuem a mesma paridade. Logo,

Caso 1 Dado $a,\ b \in \mathbb{Z}$ e ambos pares , logo

$$a = 2k_1 \text{ e } b = 2k_2 \tag{2.11}$$

Então, substituindo em $N(\alpha)$ a Equação (2.11), obtemos

$$N(\alpha) = a^2 + b^2 = (2k_1)^2 + (2k_2)^2 = 4k_1^2 + 4k_2^2 = 2[2k_1^2 + 2k_2^2] \Rightarrow N(\alpha) \text{ é par.}$$

O processo é análogo ao caso 2, vejamos:

Caso 2 Sejam a e $b \in \mathbb{Z}$ e ambos ímpares, por conseguinte,

$$a = 2k_1 + 1 \text{ e } b = 2k_2 + 1 \tag{2.12}$$

Dessa forma, substituindo em $N(\alpha)$ a Equação (2.12), obtemos

$$N(\alpha) = a^2 + b^2 = (2k_1+1)^2 + (2k_2+1)^2 = [4k_1^2 + 4k_1 + 1] + [4k_2^2 + 4k_2 + 1] \tag{2.13}$$

Aplicando as Propriedades Associativa e Comutativa na Equação (2.13), assim

$$N(\alpha) = (4k_1^2 + 4k_2^2) + (4k_1 + 4k_2) + (1 + 1)$$

$$N(\alpha) = 2 \cdot (2k_1^2 + 2k_2^2) + 2 \cdot (2k_1 + 2k_2) + 2(1)$$

$$N(\alpha) = 2 \cdot [(2k_1^2 + 2k_2^2) + (2k_1 + 2k_2) + 1] \Rightarrow N(\alpha) \text{ é par.}$$

Observe que, se a e b possuem paridades distintas, suponha sem perda de generalidade a par e b ímpar. Então, $a = 2k_1$ e $b = 2k_2 + 1$, então:

$$N(\alpha) = a^2 + b^2 = (2k_1)^2 + (2k_2 + 1)^2 = 4k_1^2 + 4k_2^2 + 4k_2 + 1,$$

ou seja, $N(\alpha)$ é ímpar. □

observe que a demonstração do Corolário anterior nos fornece uma formula explicita para determinar $\gamma \in \mathbb{Z}[i]$ tal que $\alpha = (1 + i)\gamma$.

Exemplo 2.16. *Seja $\alpha = 6 + 8i$ se $N(\alpha) = 6^2 + 8^2 = 100$, então $6 + 8i$ é múltiplo de $(1 + i)$. De acordo com o Corolário 2.15, $\gamma \in \mathbb{Z}[i]$ é dado por*

$$\gamma = \Big(\frac{6+8}{2}\Big) + \Big(\frac{6-8}{2}\Big)i = 7 - i \in \mathbb{Z},$$

isto é, $6 + 8i = (1 + i)(7 - i)$.

Exemplo 2.17. *Dado $\alpha = 5 + 3i$, se $N(\alpha) = 5^2 + 3^2 = 34$, então $5 + 3i$ é múltiplo de*

$(1+i)$. *De fato*

$$\gamma = \Big(\frac{5+3}{2}\Big) + \Big(\frac{5-3}{2}\Big)i = 4+i \text{ e } 5+3i = (1+i)(4+i).$$

2.4 Divisão Euclideana em $\mathbb{Z}[i]$

Os inteiros de Gauss podem estabelecer condições para a divisão não exata denominada Divisão com resto. A seguir, será discutida e representada pelo teorema.

Teorema 2.18. *Sejam $\alpha, \beta \in \mathbb{Z}[i]$, com $\beta \neq 0$. Então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que*

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

Demonstração. Por hipótese, $\beta \neq 0$ e assim pode-se escrever o seguinte quociente

$$\frac{\alpha}{\beta} = \frac{\alpha \cdot \overline{\beta}}{\beta \cdot \overline{\beta}}$$

Como $N(\beta) = \beta\overline{\beta}$, sendo assim

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{m+ni}{N(\beta)} = \frac{m}{N(\beta)} + \frac{n}{N(\beta)}i \tag{2.14}$$

Como $m,\ n,\ N(\beta) \in \mathbb{Z}$, temos a Observação 1.17 que

$$m = N(\beta)q_1 + r_1 \text{ e } n = N(\beta)q_2 + r_2. \tag{2.15}$$

Onde r_1 e r_2 satisfazem

$$0 \leq |r_1| \leq \frac{1}{2}N(\beta) \text{ e } 0 \leq |r_2| \leq \frac{1}{2}N(\beta). \tag{2.16}$$

Substituindo a Equação (2.15) e (2.14),

$$\frac{\alpha}{\beta} = \frac{N(\beta)q_1 + r_1}{N(\beta)} + \frac{N(\beta)q_2 + r_2}{N(\beta)}i$$

$$\frac{\alpha}{\beta} = \frac{N(\beta)q_1 + N(\beta)q_2 i}{N(\beta)} + \frac{r_1 + r_2 i}{N(\beta)} = \frac{N(\beta)[q_1 + q_2 i]}{N(\beta)} + \frac{r_1 + r_2 i}{N(\beta)}$$

$$\frac{\alpha}{\beta} = q_1 + q_2 i + \frac{r_1 + r_2 i}{N(\beta)} \tag{2.17}$$

Ao tomar $\gamma = q_1 + q_2 i$, então a Equação (2.17) será descrita da forma

$$\frac{\alpha}{\beta} = \gamma + \frac{r_1 + r_2 i}{N(\beta)} \tag{2.18}$$

Multiplicando ambos os membros da Equação (2.18) por β teremos

$$\alpha = \beta\gamma + \frac{r_1 + r_2 i}{\overline{\beta}} \Rightarrow \alpha - \beta\gamma = \frac{r_1 + r_2 i}{\overline{\beta}}. \tag{2.19}$$

Ao utilizar a Definição 2.5 e o Teorema 2.8 na Equação (2.19), desta forma temos que

$$N(\alpha - \beta\gamma) = \frac{r_1^2 + r_2^2}{N(\overline{\beta})}. \tag{2.20}$$

Como $N(\beta) = N(\overline{\beta})$ e ao aplicar a condição da Desigualdade (2.16), teremos

$$N(\alpha - \beta\gamma) \leq \frac{\frac{1}{4}N(\beta)^2 + \frac{1}{4}N(\beta)^2}{N(\beta)} \leq \frac{1}{2}N(\beta) < N(\beta).$$

Desta forma, com $\rho = \alpha - \beta\gamma$, então

$$N(\rho) < N(\beta).$$

□

A seguir, de forma prática, será realizada uma série de exemplos referente ao Teo-

rema 2.18 a fim de promover um melhor entendimento do resultado provado anteriormente.

Exemplo 2.19. *Dados* $\alpha = 23 + 6i$ *e* $\beta = 2 + 3i$. *Assim*

$$\frac{\alpha}{\beta} = \frac{\alpha \cdot \overline{\beta}}{\beta \cdot \overline{\beta}} = \frac{(23+6i)(2-3i)}{(2+3i)(2-3i)} = \frac{64-57i}{13} = \frac{64}{13} - \frac{57}{13}i.$$

Considere $\alpha = \beta \cdot \gamma + \rho$, *com* $N(\rho) < N(\beta)$. *Sabe-se que* $N(\beta) = 2^2 + 3^2 = 4 + 9 = 13$. *Agora vamos determinar* γ. *Sua determinação será baseada na parte inteira que mais aproxima o valor da parte real e imaginária, conforme o procedimento utilizado a seguir:*

$$\frac{64}{13} = 4,923076923\cdots \Rightarrow 4 < \frac{64}{13} < 5$$

e

$$-\frac{57}{13} = -4,384615385\cdots \Rightarrow -5 < \frac{57}{13} < -4$$

Mediante aos extremos do intervalo, vamos estabelecer todas as combinações possíveis entre os extremos do intervalo, devido a isso obteremos 4 *possíveis valores de* γ, *observe:*

Caso 1 $\gamma_1 = 4 - 5i$

$$\rho = \alpha - \beta\gamma_1 = (23 + 6i) - [(2 + 3i)(4 - 5i)] = 4i \Rightarrow N(\rho) = 16. \tag{2.21}$$

Este caso não satisfaz a condição pois $N(\rho) < N(\beta)$, *por que* $16 > 13$.

O processo é análogo para γ_2, γ_3 *e* γ_4, *vejamos.*

Caso 2 $\gamma_2 = 4 - 4i$

$$\rho = \alpha - \beta\gamma_1 = (23 + 6i) - [(2 + 3i)(4 - 4i)] = 3 + 2i \Rightarrow N(\rho) = 13. \tag{2.22}$$

Este caso não satisfaz a condição, visto que $N(\rho) < N(\beta)$, *pois* $13 = 13$.

Caso 3 $\gamma_3 = 5 - 5i$

$$\rho = \alpha - \beta\gamma_1 = (23 + 6i) - [(2 + 3i)(5 - 5i)] = -2 + i \Rightarrow N(\rho) = 5 \qquad (2.23)$$

Este caso satisfaz a condição de $N(\rho) < N(\beta)$, *pois* $5 < 13$.

Caso 4 $\gamma_3 = 5 - 4i$

$$\rho = \alpha - \beta\gamma_1 = (23 + 6i) - [(2 + 3i)(5 - 4i)] = 1 - i \Rightarrow N(\rho) = 2 \qquad (2.24)$$

Este caso satisfaz a condição de $N(\rho) < N(\beta)$, *porque* $2 < 13$.

O objetivo em resolver o exemplo anterior em etapas é com intuito de descrever uma distinção entre a Divisão Euclideana (Teorema 1.16) e a Divisão com resto em $\mathbb{Z}[i]$ e ressaltar que a divisão em $\mathbb{Z}[i]$ não é única, ou seja, como o exemplo mostrou tanto o caso 3 quanto o caso 4 são resultados possíveis, enquanto a Divisão Euclideana temos a unicidade dos restos para um dado divisor.

Nesta perspectiva, ambos os casos 3 ou 4 poderiam ser solução para o problema proposto, uma vez que foi solicitado o quociente entre α e β e não exigiram a exposição de todas as possíveis soluções.

Exemplo 2.20. *Sejam* $\alpha = 45 + 25i$ *e* $\beta = 11 - 2i$, *como* $N(\beta) = 125$, *então:*

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{(43 + 20i)(11 - 2i)}{(11 + 2i)(11 + 2i)} = \frac{433 + 310i}{125} = \frac{433}{125} + \frac{310}{125}i$$

Considere $\alpha = \beta \cdot \gamma + \rho$, *com* $N(\rho) < N(\beta)$. *A parte inteira que mais aproxima o valor da parte real e imaginária, escolhida conforme o procedimento utilizado é*

$$\frac{433}{125} = 3,464 \Rightarrow 3 < \frac{433}{125} < 4 \qquad (2.25)$$

e

$$\frac{310}{125} = 2,48 \Rightarrow 2 < \frac{310}{125} < 3 \qquad (2.26)$$

Por meio dos extremos dos intervalos reais (2.25) e (2.26) determinamos γ_1, γ_2, γ_3, γ_4. *São eles*

$$\gamma_1 = 3 + 2i,\ \gamma_2 = 3 + 3i,\ \gamma_3 = 4 + 2i,\ \gamma_4 = 4 + 3i. \qquad (2.27)$$

Diante da determinação dos possíveis valores para γ_i com $1 \leq i \leq 4$ e $i \in \mathbb{N}$. a seguir será desenvolvido o quociente explorando cada caso e destacando se o mesmo satisfaz a condição do Teorema 2.18.

Caso 1 $\gamma_1 = 3 + 2i$

$$\rho = \alpha - \beta\gamma_1 = (45 + 25i) - [(11 - 2i)(3 + 2i)] = 8 - 9i \Rightarrow N(\rho) = 145$$

Como $N(\rho) < N(\beta)$, então ρ não satisfaz por que $145 > 125$.

Caso 2 $\gamma_2 = 3 + 3i$

$$\rho = \alpha - \beta\gamma_1 = (45 + 25i) - [(11 - 2i)(3 + 3i)] = 6 - 2i \Rightarrow N(\rho) = 40$$

Portanto $N(\rho) < N(\beta)$, pois $40 < 125$.

Caso 3 $\gamma_4 = 4 + 2i$

$$\rho = \alpha - \beta\gamma_1 = (45 + 25i) - [(11 - 2i)(4 + 2i)] = -3 + 11i \Rightarrow N(\rho) = 130$$

Contudo, se $N(\rho) < N(\beta)$, então não satisfaz por que $130 > 125$.

Caso 4 $\gamma_3 = 4 + 3i$

$$\rho = \alpha - \beta\gamma_1 = (45 + 25i) - [(11 - 2i)(4 + 3i)] = -5 \Rightarrow N(\rho) = 25$$

Então $N(\rho) < N(\beta)$, pois $25 < 125$.

Portanto, apenas $\gamma_2 = 3 + 3i$ e $\gamma_4 = 4 + 3i$ satisfez as condição do Teorema 2.18.

É possível observar na resolução dos exemplos uma diferença relevante n Após a resolução destes exemplos podemos destacar uma diferença curiosa e relevante entre Teorema da Divisão com Resto em $\mathbb{Z}[i]$ (Teorema 2.18) e a Divisão euclideana em $\mathbb{Z}$ (Teorema 1.16), pois na estrutura algébrica de $\mathbb{Z}[i]$, geralmente, o quociente e o resto da divisão não são únicos, como é possível ser observado nos exemplos anteriores.

Uma observação importante nesta seção é a relevância em realizar uma discussão deste tópico no Ensino Básico porque, geralmente, os discentes do Ensino Médio estão habituados em se deparar com problemas nos quais o resto e o quociente são únicos, já em $\mathbb{Z}[i]$ isso não acontece e a partir disso, os professores de matemática podem aproveitar problemas assim para mostrar que a unicidade de resultados de uma operação em uma estrutura podem não preservar a unicidade em outras e além de ser oportunidade de instigar os estudantes para desenvolver pesquisas em relação as essas novas estruturas, isso contribuiria no aprimoramento de seus conhecimentos matemáticos.

2.5 Primos em $\mathbb{Z}[i]$

É indiscutível a importância dos números primos, conforme foi destacado no Capitulo 1 na Seção 1.7. Além disso, diversos resultados mais sofisticados da matemática são advindos dos números primos em $\mathbb{Z}$, pode-se questionar: como é caracterizado a primalidade de $\alpha \in \mathbb{Z}[i]$? São satisfeitas as mesmas condições existentes em $\mathbb{Z}$? Os números primos em $\mathbb{Z}$ também são considerados números primos em $\mathbb{Z}[i]$? A seguir serão apresentadas definições, proposições e teoremas que caracterizam esta classe numérica em $\mathbb{Z}[i]$ a fim de possibilitar ao leitor a oportunidade de responder estes e outros questionamentos em relação os primos em $\mathbb{Z}[i]$.

Definição 2.21. *Sejam $\alpha, \beta \in \mathbb{Z}[i]$. São eles chamados de **associados** se $\alpha = u\beta$ sendo que u é uma unidade.*

Lema 2.22. *Dados $w \neq 0$ e z um divisor de w tal que $N(z) = 1$ ou $N(z) = N(w)$, então z é uma unidade ou um associado de w.*

Demonstração. Para a demonstração foi realizado por meio de dois casos, então:

Caso 1. $N(z) = 1$.

Se $N(z) = 1$,então z é uma unidade.

Caso 2. $N(z) = N(w)$

Como $w,\ z \in \mathbb{Z}[i]$. Por hipótese, $w \neq 0$ e z é múltiplo de w, então:

$$w = uz,$$

para algum $u \in \mathbb{Z}[i]$. Tendo em vista que a Norma em $\mathbb{Z}[i]$ é multiplicativa, conforme

ilustrado no Teorema 2.8, assim teremos:

$$N(w) = N(uz) \Rightarrow N(w) = N(u) \cdot N(z).$$

Como, por hipótese $N(z) = N(w)$, logo:

$$N(w) = N(u) \cdot N(z) \Rightarrow N(w) = N(u) \cdot N(w). \tag{2.28}$$

Sabemos que $w \neq 0$, então a Equação 2.28 pode ser representada da forma:

$$N(u) \cdot N(w) - N(w) = N(w) \cdot (N(u) - 1) = 0 \Rightarrow N(u) = 1. \tag{2.29}$$

Portanto, z é associado de w pois a $N(u) = 1$ conforme ilustrado em (2.28). □

É importante esclarecer o Lema 2.22 não afirma que existem apenas $\pm\alpha$ ou $\pm\alpha i$ cuja a norma é igual a $N(\alpha)$. Os números $1 - 8i$ e $-4 + 7i$ possuem normal igual a 65 e ambos não são associados. Em outras palavras, o Lema 2.22 indica que $\pm\alpha$ ou $\pm\alpha i$ são os únicos inteiros de Gauss que divide α e tem normal igual a $N(\alpha)$.

Em $\mathbb{Z}[i]$ podemos direcionar o olhar aos divisores de um dado $w \in \mathbb{Z}[i]$, pois quando $N(w) > 1$ é possível elencar oito divisores triviais de w, são eles: ± 1, $\pm i$, $\pm w$ e $\pm wi$. Agora, dado qualquer outro fator de w é denominado não trivial. Seja x um divisor não trivial de w, então $1 < N(x) < N(w)$.

Definição 2.23. *Seja $\alpha \in \mathbb{Z}[i]$. Diremos que α é composto se existirem β, $\gamma \in \mathbb{Z}[i]$ tais que:*

i. $\alpha = \beta\gamma$

ii. $N(\beta) > 1$ *e* $N(\gamma) > 1$

Caso o α não esteja sob estas restrições da Definição 2.23 então ele é dito *irredutível*, conforme a seguinte definição:

Definição 2.24 (Irredutível)**.** *Um elemento não nulo α de $\mathbb{Z}[i]$ é chamado de irredutível se α não for uma unidade e sempre quando $\alpha = \beta\gamma$ com β, $\gamma \in \mathbb{Z}[i]$, então β ou γ é uma unidade.*

Proposição 2.25. *Se $N(w)$ é um primo em $\mathbb{Z}$, então w é irredutível.*

Demonstração. Seja $w \in \mathbb{Z}[i]$ e $N(w) = p$, com p primo em $\mathbb{Z}$. Se existirem β, $\gamma \in \mathbb{Z}[i]$ tais que

$$w = \beta\gamma, \tag{2.30}$$

então β ou γ é unidade em $\mathbb{Z}[i]$.

Além disso,

$$N(w) = N(\beta\gamma) = N(\beta)N(\gamma) \Rightarrow N(\beta)N(\gamma) = p. \tag{2.31}$$

Como p é primo em $\mathbb{Z}$, temos que $N(\beta) = p$ e $N(\gamma) = 1$ ou $N(\beta) = 1$ e $N(\gamma) = p$, mostrando que γ é unidade ou β é a unidade. □

Exemplo 2.26. *$\alpha = 1 - i$ é irredutível, pois $N(\alpha) = 1^2 + (-1)^2 = 2$, que é primo.*

Exemplo 2.27. *$\alpha = 1 + 2i$ é irredutível, pois $N(\alpha) = 1^2 + (2)^2 = 5$, visto que 5 é primo.*

Exemplo 2.28. *$\alpha = -2 + 3i$ é irredutível, pois $N(\alpha) = (-2)^2 + (3)^2 = 13$, visto que 13 é primo.*

Para enfatizar a definição $\alpha = 23 - 2i$, por meio de uma fatoração trivial pode ser descrito da forma:

$$23 - 2i = i \cdot (-23i - 2).$$

Mas pode ser fatorado de forma não trivial, veja:

$$23 - 2i = (2 - 3i) \cdot (4 + 5i).$$

Um fato interessante que envolve a fatoração não trivial de 5 é $(2 + i) \cdot (2 - i)$. É notável 5 é um número primo em $\mathbb{Z}$, no entanto é composto em $\mathbb{Z}[i]$, existem outros casos, conforme os exemplos a seguir:

Exemplo 2.29. *A fatoração não trivial do $13 = (3 + 2i)(3 - 2i)$.*

Isso mostra o quanto o estudo torna-se a cada vez mais relevante, já que as propriedades dos $\mathbb{Z}$ entrelaça com $\mathbb{Z}[i]$ demonstrando assim diferenças não observadas geralmente. Entretanto, não acontece para todos os primos em $\mathbb{Z}$, o 7 é um exemplo de

primo em ambos os conjuntos. Suponhamos que 7 é composto, então pode ser escrito $7 = \alpha\beta$. Tomando a norma em ambos os membros temos: $N(\alpha)N(\beta) = 49$. Como a fatoração é não trivial por isso é sabido que $N(\alpha) > 1$ e $N(\beta) > 1$. Por isso, $N(\alpha) = 7$, sendo $\alpha = m + ni$, então: $N(\alpha) = a^2 + b^2 = 7$. Está equação não é solúvel, pois não existem a, $b \in \mathbb{Z}$ assim obtemos uma contradição. Portanto, 7 possui apenas fatores triviais em $\mathbb{Z}[i]$, então 7 é primo em $\mathbb{Z}[i]$.

Conforme o objetivo desta pesquisa que consiste em estabelecer um paralelo entre as propriedades válidas em $\mathbb{Z}$ e $\mathbb{Z}[i]$. Acompanhe a definição de primos em $\mathbb{Z}[i]$.

Definição 2.30 (Primos em $\mathbb{Z}[i]$)**.** *Dizemos que $\pi \in \mathbb{Z}[i]$ é primo, se a e b são tais que $\pi \mid ab$, então $\pi \mid a$ ou $\pi \mid b$.*

Lema 2.31. *Seja $\pi \in \mathbb{Z}[i]$. Se $\alpha_1, \alpha_2, \cdots \alpha_r \in \mathbb{Z}[i]$, com $\pi \mid \alpha_1\alpha_2 \cdots \alpha_r$, então $\pi \mid \alpha_j$, com $1 \leq j \leq r$ e $r \in \mathbb{N}$.*

Demonstração. A verificação deste resultado será feita para $r = 2$, visto que para $r > 2$ é um processo simples de indução. Suponha $\pi \mid \alpha_1\alpha_2$, mas $\pi \nmid \alpha_1$, logo π e α_1 são relativamente primos, pode-se concluir pelo Corolário 2.51 se $\pi \nmid \alpha_1$ então $\pi \mid \alpha_2$. □

Neste momento é possível demonstrar a fatoração única em $\mathbb{Z}[i]$. A seguir faremos uma discussão sobre a impossibilidade de estabelecer a demonstração por intermédio da igualdade dos fatores conforme é realizada na demonstração do Teorema Fundamental da Aritmética em $\mathbb{Z}$. Observe:

$$\pi_1\pi_2 \cdots \pi_r = \pi'_1\pi'_2 \cdots \pi'_s \tag{2.32}$$

com $1 \leq j \leq r$ e $1 \leq k \leq s$, com $r, s \in \mathbb{N}$.

Nota-se que na Equação (2.32) os números π_j e π_k são primos em $\mathbb{Z}[i]$, sendo que $r = s$ e $\pi_j = \pi_k \cdot i$, isso acontecerá após a realização dos ajustes adequados para tal acontecimento se efetivar. Para compreender melhor, esse relato, considere:

$$17 = (4 + i) \cdot (4 - i) = (1 + 4i) \cdot (1 - 4i) \tag{2.33}$$

Os fatores $(4 + i)$, $(4 - i)$, $(1 + 4i)$ e $(1 - 4i)$ são primos em $\mathbb{Z}[i]$, pela Proposição 2.25, porque ambos apresentam norma igual a 17. Porém mesmo que a igualdade se estabeleça, porém os dois primos em um membro não aparece no outro, então este fato

impede a existência da fatoração única? Não, inclusive pode-se observar que fatores são associados, vejamos:

$$1 + 4i = (4 - i)i \text{ e } 1 - 4i = (4 + i)(-i) \tag{2.34}$$

Situação similiar acontece em $\mathbb{Z}$, conforme o exemplo a seguir:

$$6 = 2 \cdot 3 = (-2) \cdot (-3) \tag{2.35}$$

Entretanto, saliento que não significa a ausência da fatoração única em $\mathbb{Z}$, visto que o direcionamento das análise concentram-se em números positivos e também primos positivos, com a finalidade de evitar problemas com sinais.

Tendo em vista que não há positividade em $\mathbb{Z}[i]$ e não é o objetivo discutir sobre tal condição. Por isso optamos em considerar nossas fatorações a igualdade entre associados.

Lema 2.32. *Considere $p \in \mathbb{Z}$ um número primo. As afirmações a seguir são equivalentes:*

1. *p é redutível em $\mathbb{Z}[i]$.*

2. *$p = \alpha \cdot \overline{\alpha}$ com α primo em $\mathbb{Z}[i]$.*

3. *p é soma de dois quadrados.*

Demonstração. A prova deste lema será realizada por etapas, observe:

$(1 \Rightarrow 2)$ Suponha que p é redutível em $\mathbb{Z}[i]$, então

$$p = \alpha \cdot \beta$$

com $\alpha, \beta \in \mathbb{Z}[i]$ não invertível. Por outro lado:

$$p^2 = N(p) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta),$$

concluímos que $N(\alpha) = N(\beta) = p$, pela Proposição 2.25, logo α é irredutível em $\mathbb{Z}[i]$, assim:

$$\beta = \frac{p}{\alpha} = \frac{p \cdot \overline{\alpha}}{\alpha \cdot \overline{\alpha}} = \frac{p \cdot \overline{\alpha}}{N(\alpha)} = \overline{\alpha},$$

portanto $p = \alpha \cdot \beta = \alpha \cdot \overline{\alpha}$.

$(2 \Rightarrow 3)$ Considere $p = \alpha \cdot \overline{\alpha}$. Seja $\alpha = a + bi$, deste modo:

$$p = \alpha \cdot \overline{\alpha} = (a + bi) \cdot (a - bi) = a^2 + b^2, \tag{2.36}$$

então p é soma de dois quadrados.

$(3 \Rightarrow 1)$ Seja $p = a^2 + b^2$, então:

$$p = (a + bi) \cdot (a - bi). \tag{2.37}$$

Assim:

$$p^2 = N(p) = N(a + bi) \cdot N(a - bi), \tag{2.38}$$

$N(a + bi) = N(a - bi) = p$, logo não são invertíveis e p é redutível em $\mathbb{Z}[i]$. □

O teorema 2.33 e os lemas 2.35 e 2.36 indicamos [8].

Teorema 2.33. *Os elementos irredutíveis de* $\mathbb{Z}[i]$ *são:*

1. $\pm p$, $\pm pi$ *com* p *primo em* $\mathbb{N}$ *tal que* $p \equiv 3 \pmod 4$.

2. $a + bi$ *com* $a^2 + b^2 = p$, p *primo em* $\mathbb{N}$.

Proposição 2.34. *Sejam* π *um primo ímpar e* a *um inteiro não divisível por* π *; dizemos que* a *é um resíduo (ou resto) quadrático módulo* π *se*

$$X^2 \equiv a \pmod p,$$

tem solução em $\{0,\ 1,\ \ldots,\ p - 1\}$.

Lema 2.35. *Dado um inteiro* p *com* $p > 2$, *existe um inteiro* $\mathbb{Z}$ *que não é resíduo quadrático módulo* p.

Lema 2.36. *Seja* p *um número primo, com* $p > 2$ *e* a *um inteiro não resíduo quadrático módulo* p. *Então:*

$$a^{\frac{p-1}{2}} \equiv -1 (mod\, p)$$

Teorema 2.37 (Fermat)**.** *Considere* $p \in \mathbb{N}$ *um número primo. As afirmações a seguir são equivalentes:*

1. $p = 2$ *ou* $p \equiv 1 \pmod 4$.

2. p *não é irredutível em* $\mathbb{Z}[i]$.

3. p *é soma de dois quadrados.*

Demonstração. (1) $\Rightarrow$ (2): Seja $p = 2$, então $-1 \equiv 1 \pmod 2$, logo, -1 é resíduo quadrático módulo 2. Agora, vamos analisar para $p \equiv 1(mod\,4)$. Segundo Lema 2.35 existe um $a \in \mathbb{Z}$ tal que a não é resíduo quadrático módulo p. Tome um $b = a^{\frac{p-1}{4}} \in \mathbb{Z}$, conforme o Lema 2.36, obtêm-se:

$$b^2 \equiv [a^{\frac{p-1}{4}}]^2 \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

então -1 é resíduo quadrático módulo p.

(2) $\Rightarrow$ (3): Suponha que existe $b \in \mathbb{Z}$ tal que $b^2 \equiv -1 \pmod p$, então consequentemente:

$$p \,|\, (b^2 + 1) \Rightarrow p \,|\, (b + i) \cdot (b - i). \tag{2.39}$$

Mediante ao resultado obtido na Equação (2.39), nota-se que $p \,|\, (b \pm i) \pmod 2$, pois caso não satisfaça essa afirmação, teríamos algum $\theta = m + ni \in \mathbb{Z}[i]$ tal que:

$$p(m + ni) = b \pm i \Rightarrow pm + pni = b \pm i \tag{2.40}$$

Já nos deparamos com um absurdo, por que ao estabelecermos a igualdade, teríamos:

$$pm = b \text{ e } pn = \pm 1, \tag{2.41}$$

pois $pn = \pm 1$, sendo que $b,\ n \in \mathbb{Z}$, logo só haveria duas possibilidades, sendo elas: $p = n = 1$ ou $p = n = -1$, mas p é primo por hipótese, logo p deve ser diferente de ± 1.

(3) $\Rightarrow$ (1): Seja $p > 2$ e suponha que $p = a^2 + b^2$. Como p não é par, a e b possuem paridades diferentes. A nossa intenção é provar que $p \equiv 1 \pmod 4$. Suponha que $a = 2c + 1$ e $b = 2d$, $c, d \in \mathbb{Z}$. Então

$$p = a^2 + b^2 = (2c + 1)^2 + (2d)^2 = 4c^2 + 4c + 1 + 4d^2 = 4(c^2 + d^2 + c) + 1, \tag{2.42}$$

então:

$$p \equiv a^2 + b^2 \equiv 4(c^2 + d^2 + c) + 1 \equiv 1 \pmod 4.$$

□

2.6 Máximo Divisor Comum em $\mathbb{Z}[i]$

A seguir realizaremos a descrição do Máximo Divisor Comum ou comumente tratado por MDC no conjunto dos Inteiros de Gauss. Indicaremos por (α, β) o máximo divisor comum de α e β.

Definição 2.38. *Dados* $\alpha,\ \beta \in \mathbb{Z}[i]$, *com* $z \neq 0$, *o* $(\alpha, \beta) = \delta \in \mathbb{Z}[i]$, *assim:*

i. $\delta \mid \alpha$ *e* $\delta \mid \beta$

ii. *Se* $\delta' \mid \alpha$ *e* $\delta' \mid \beta$ *então* $N(\delta') \leq N(\delta)$.

Mesmo sendo análogo o conceito de máximo divisor comum em relação a $\mathbb{Z}$ não existe um valor fixo para (α, β). Seja δ o máximo divisor comum de α e β, neste caso, indica que são (pelo menos) $-\delta$, $i\delta$ e $-i\delta$. Devido a isso, há a possibilidade de existir maiores divisores; nós apenas não sabemos ainda (descobriremos no Proposição 2.43). Este raciocínio nos permite meditar na existência de um máximo divisor comum, porém não sobre o maior divisor comum.

Definição 2.39. *Sejam* α *e* $\beta \in \mathbb{Z}[i]$. *Diremos que* α *e* β *são relativamente primos quando seus fatores comuns são apenas as unidades* $-1, 1, -i, i$.

Lema 2.40. *Dados* a, b *e* $c \in \mathbb{Z}[i]$. *Então:*

$$(a, b) = (a, b - ac).$$

Demonstração. Considere agora $\delta = (a, b - ac)$, de acordo com a Definição 2.38, por isso:

$$\delta | a \text{ e } \delta | b - ac.$$

Por outro lado,

$$\delta | a \Rightarrow \delta | ac.$$

Dessa forma, $\delta | b$, pois

$$b = ac + (b - ac).$$

□

Teorema 2.41 (Algoritmo de Euclides)**.** *Seja α e $\beta \in \mathbb{Z}[i]$ e ambos diferentes de zero. De maneira recursiva, aplicando o teorema 2.18, iniciando com este par, α e β, e posteriormente o divisor e o resto desta equação, propiciará a origem de uma nova equação, sendo que eles serão o dividendo e o divisor nesta próxima, desde que o resto seja diferente de zero:*

$$\alpha = \beta\gamma_1 + \rho_1,\ N(\rho_1) < N(\beta).$$

$$\beta = \rho_1\gamma_2 + \rho_2,\ N(\rho_2) < N(\rho_1).$$

$$\rho_1 = \rho_2\gamma_3 + \rho_3,\ N(\rho_3) < N(\rho_2).$$

$$\vdots$$

O último resto diferente de zero é divisível por todos os divisores comuns de α e β, sendo assim ele é um divisor comum, fato este que indica-o a ser um máximo divisor comum.

Demonstração. A demonstração deste teorema é análoga ao Algoritmo de Euclides em $\mathbb{Z}$. Fica a cargo do leitor a respectiva demonstração, recomendo a leitura [15]. □

Exemplo 2.42. *Determine o máximo divisor comum de $\alpha = 32 + 9i$ e $\beta = 4 + 11i$.*

Resolução. Os detalhes relacionados a divisão euclideana em $\mathbb{Z}[i]$ em cada etapa do Algoritmo de Euclides serão omitidos. Então:

$$32 + 9i = (4 + 11i) \cdot (2 - 2i) + (2 - 5i)$$

$$4 + 11i = (2 - 5i) \cdot (-2 + i) + (3 - i)$$

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

$$3 - i = (-i) \cdot (1 + 3i) + 0$$

Portanto, o $(\alpha, \beta) = -i$ isso indica que os mesmo são relativamente primos. □

Proposição 2.43. *Dados α e $\beta \in \mathbb{Z}[i]$ e $\delta = (\alpha, \beta)$ obtido pelo Algoritmo de Euclides. Qualquer máximo divisor comum é associado a δ.*

Demonstração. Suponha que δ' é um máximo divisor comum de α e β. Como $\delta|\alpha$ e $\delta|\beta$, segue que:

$$\delta|\delta' \Rightarrow N(\delta) \leq N(\delta'). \tag{2.43}$$

Por outro lado, como $\delta = (a, b)$ e $\delta'|a$ e $\delta'|b$ então

$$\delta'|\delta \Rightarrow N(\delta') \leq N(\delta). \tag{2.44}$$

De (2.43) em (2.6), temos que

$$N(\delta) = N(\delta'),$$

assim, δ e δ' são associados, segundo o Lema 2.22. □

A seguir, vamos observar o máximo divisor comum diferente de unidade e comprovado pelo Teorema 2.43 será exemplificado a seguir:

Exemplo 2.44. *O máximo divisor comum nem sempre é uma unidade. Agora, veja o caso $\alpha = 11 + 3i$ e $\beta = 1 + 8i$. Então:*

Resolução.

$$11 + 3i = (1 + 8i) \cdot (1 - i) + (2 - 4i)$$

$$1 + 8i = (2 - 4i) \cdot (-1 + i) + (-1 + 2i)$$

$$2 - 4i = (-1 + 2i) \cdot (-2) + 0$$

Agora, vamos utilizar a outra possibilidade na segunda equação e através dela é possível determinar uma equação com resto diferente de zero, logo:

$$11 + 3i = (1 + 8i) \cdot (1 - i) + (2 - 4i)$$

$$1 + 8i = (2 - 4i) \cdot (-2 + i) + (1 - 2i)$$

$$2 - 4i = (1 - 2i) \cdot (2) + 0$$

Ambos os casos não há nenhuma inconsistência, pois ambos estão adequados as condições necessárias e assim obtemos dois máximos divisor comum -1+2i e 1-2i, respectivamente. Uma particularidade importante é o fato de serem associados, observe

$$-1 + 2i = (-1) \cdot (1 - 2i).$$

□

Teorema 2.45 (Bachet-Bèzout)**.** *Se $\delta = (\alpha, \beta)$ então existem r e $s \in \mathbb{Z}[i]$, tais que $\delta = \alpha r + \beta s$.*

Demonstração. Sabe-se que é possível escrever $\delta \in \mathbb{Z}[i]$ como combinação linear de α e β por meio Algoritmo de Euclides. A demonstração é análoga a realizada para o conjunto $\mathbb{Z}$. □

Agora, será apresentado resultados referentes a consequências imediatas da Proposição 2.47. Aqui estão algumas delas:

Corolário 2.46. *Se α e β são relativamente primos então:*

$$\alpha r + \beta s = 1,$$

para algum r e $s \in \mathbb{Z}[i]$.

Demonstração. Basta utilizar o Teorema 2.47 e tomar $\delta \in \{\pm 1, \pm i\}$. □

Proposição 2.47 (Bachet-Bèzout)**.** *Se $\delta = (\alpha, \beta)$ então existem r e $s \in \mathbb{Z}[i]$, tais que $\delta = \alpha r + \beta s$.*

Demonstração. Sabe-se que é possível escrever $\delta \in \mathbb{Z}[i]$ como combinação linear de α e β por meio Algoritmo de Euclides. A demonstração é análoga a realizada para o conjunto $\mathbb{Z}$ e deixarei a cargo do leitor. □

Agora, será apresentado resultados referentes a consequências imediatas da Proposição 2.47. Aqui estão algumas delas:

Corolário 2.48. *Se α e β são relativamente primos então:*

$$\alpha r + \beta s = 1,$$

para algum r e $s \in \mathbb{Z}[i]$.

Demonstração. Por hipótese α e β são relativamente primos, então o máximo divisor comum é uma unidade, seja $\delta = (\alpha, \beta) = 1$, pois será utilizado o número 1 como representa das unidades $\{\pm 1, \pm i\}$. Sendo assim, segundo a Proposição 2.47 existe r e s tal que:

$$\alpha r + \beta s = 1.$$

□

Exemplo 2.49. *Aplique o Teorema 2.47 no Exemplo 2.44.*

Resolução. Seja $\alpha = 11 + 3i$ e $\beta = 1 + 8i$, e através das equações já determinada no Exemplo 2.44 podemos reescrevê -lás da forma:

$$-1 + 2i = (1 + 8i) - (2 - 4i) \cdot (-1 + i) \cdot (-1 + i), \tag{2.45}$$

$$2 - 4i = (11 + 3i) - (1 + 8i) \cdot (1 - i). \tag{2.46}$$

Ao Substituir a Equação (2.45) na Equação (2.46), temos:

$$-1 + 2i = (1 + 8i) - [(11 + 3i) - (1 + 8i) \cdot (1 - i)] \cdot (-1 + i). \tag{2.47}$$

Como $\alpha = 11+3i$ e $\beta = 1+8i$, então a Equação (2.47) pode ser descrita da seguinte maneira:

$$\begin{aligned} -1 + 2i &= \beta - [\alpha - (1 - i)\beta] \cdot (-1 + i). \\ -1 + 2i &= \beta - [(-1 + i)\alpha - (1 - i)(-1 + i)\beta] \\ -1 + 2i &= \beta - [(-1 + i)\alpha - (2i)\beta] \\ -1 + 2i &= \beta - (-1 + i)\alpha + (2i)\beta \\ -1 + 2i &= (1 - i)\alpha + (1 + 2i)\beta \end{aligned} \tag{2.48}$$

Portanto, na Equação (2.48) verifica-se a Proposição 2.47, que consiste em escrever como combinação linear de α e β. □

Exemplo 2.50. *Aplique o Teorema 2.47 no Exemplo 2.42.*

Resolução. Seja $\alpha = 32 + 9i$ e $\beta = 4 + 11i$, então:

$$-i = (2 - 5i) - (3 - i) \cdot (1 - i) \tag{2.49}$$
$$3 - i = (4 + 11i) - (2 - 5i) \cdot (-2 + i) \tag{2.50}$$
$$2 - 5i = (32 + 9i) - (4 + 11i) \cdot (2 - 2i) \tag{2.51}$$

Substituindo a Equação (2.50) na Equação (2.49), temos:

$$-i = (2 - 5i) - [(4 + 11i) - (2 - 5i) \cdot (-2 + i)] \cdot (1 - i)$$

Lembre-se que durante as resoluções e afim de facilitar as manipulações algébricas faremos a substituição de $\alpha = 32 + 9i$ e $\beta = 4 + 11i$ e este procedimento será realizado durante toda a resolução. Sendo assim:

$$\begin{aligned} -i &= (2 - 5i) - [\beta(1 - i) - (2 - 5i) \cdot (-2 + i) \cdot (1 - i)] \\ -i &= -\beta(1 - i) + (2 - 5i) + (2 - 5i) \cdot (-2 + i) \cdot (1 - i) \\ -i &= -\beta(1 - i) + (2 - 5i) \cdot [1 + (-2 + i) \cdot (1 - i)] \\ -i &= -\beta(1 - i) + 3i(2 - 5i) \end{aligned} \tag{2.52}$$

Agora vamos substituir a Equação (2.51) na Equação (2.52), teremos:

$$\begin{aligned} -i &= -\beta(1 - i) + 3i(2 - 5i) \\ -i &= -\beta(1 - i) + 3i \cdot [(32 + 9i) - (4 + 11i) \cdot (2 - 2i)] \\ -i &= -\beta(1 - i) + (3i)\alpha - \beta(3i) \cdot (2 - 2i) \\ -i &= (3i)\alpha - \beta[(1 - i) + (6 + 6i)] \\ -i &= (3i)\alpha - (7 + 5i)\beta \\ -i &= (3i)\alpha + (-7 - 5i)\beta \end{aligned}$$

Portanto, existe $r = 3i$ e $s = -7 - 5i$ de tal forma que a combinação linear com α e β, pode ser dada por:

$$(3i)\alpha + (-7 - 5i)\beta = -i$$

Corolário 2.51. *Se $\alpha \mid \beta\gamma$ e α e β são relativamente primos, então $\alpha \mid \gamma$.*

Demonstração. Por hipótese $\alpha \mid \beta\gamma$, então:

$$\beta\gamma = \alpha m, \text{ para algum } m \in \mathbb{Z}[i]. \tag{2.53}$$

Sendo que α e β são relativamente primos segundo a hipótese, então pela Proposição 2.47, teremos:

$$\exists\ r,\ s \in \mathbb{Z}[i] \text{ tal que } \alpha r + \beta s = 1. \tag{2.54}$$

Para obtermos o resultado esperado basta multiplicar a Equação (2.54) por γ, assim:

$$\begin{aligned} \gamma\alpha r + \gamma\beta s &= \gamma \cdot 1 \\ \gamma\alpha r + \gamma\beta s &= \gamma. \end{aligned} \tag{2.55}$$

Sendo que $\beta\gamma = \alpha m$ na Equação (2.55), então:

$$\begin{aligned} \gamma\alpha r + \alpha m s &= \gamma \\ \alpha(\gamma r + m s) &= \gamma. \end{aligned} \tag{2.56}$$

Logo, pela Equação (2.56), podemos afirmar que $\alpha \mid \gamma$. □

Corolário 2.52. *Seja α e β relativamente primos, se $\alpha \mid \gamma$ e $\beta \mid \gamma$ em $\mathbb{Z}[i]$, então $\alpha\beta \mid \gamma$.*

Demonstração. De imediato, já sabe-se que:

$$\gamma = \alpha p, \text{ para algum } p \in \mathbb{Z}[i], \tag{2.57}$$

$$\gamma = \beta m, \text{ para algum } m \in \mathbb{Z}[i]. \tag{2.58}$$

Igualando as Equações (2.57) e (2.58), temos:

$$\alpha p = \beta m. \tag{2.59}$$

Como α e β são relativamente primos, logo pela Equação (2.59):

$$\alpha \not| \beta.$$

Então:

$$\alpha \,|\, m. \tag{2.60}$$

Multiplicando por β a Equação (2.60), teremos:

$$\beta\alpha \,|\, \beta m \Rightarrow \beta\alpha \,|\, \gamma.$$

□

2.7 Fatoração Única em $\mathbb{Z}[i]$

Diante das discussões realizada na Seção 2.5 referentes a primalidade em $\mathbb{Z}[i]$ que iniciou em sua definição até na nomeação dos fatores trivial de um dado $\alpha \in [i]$ e alguns resultados importantes. Neste momento, iremos retomar a discussão referente a alguns outros resultados que compõem a definição dos números inteiros de Gauss compostos e primos, posteriormente, provar uma única fatoração. Ressalto novamente que a construção da subseção foi baseada em [2].

Teorema 2.53 (Teorema da Unicidade da Fatoração)**.** *Seja $\alpha \in \mathbb{Z}[i]$ com $N(\alpha) > 1$ e $\alpha \neq 0$ uma não unidade de $\mathbb{Z}[i]$. Suponhamos que*

$$\alpha = \pi_1\pi_2 \cdots \pi_n = \pi_1'\pi_2' \cdots \pi_m'$$

onde os π_i e π_j' são elementos primos de $\mathbb{Z}[i]$. Então, $n = m$ e cada π_i, $1 \leq i \leq n$ é

associado de algum π'_j, $1 \leq j \leq m$ *e reciprocamente, cada* π'_j *é um associado de algum* π_i.

Demonstração. Inicialmente, direcionaremos para a hipótese que:

$$\alpha = \pi_1\pi_2 \cdots \pi_n = \pi'_1\pi'_2 \cdots \pi'_m. \tag{2.61}$$

De imediato, ao observar que $\pi_1 \,|\, \pi_1\pi_2 \cdots \pi_n$, logo $\pi_1 \,|\, \pi'_1\pi'_2 \cdots \pi'_m$. De acordo com Lema 2.31, π_1 divide algum π'_j; como π_1 e π'_j são primos em $\mathbb{Z}[i]$ e $\pi_1 \,|\, \pi'_j$ pelo fato de serem associados e $\pi'_j = u\pi_1$, onde u é uma unidade de $\mathbb{Z}[i]$. Então, podemos reescrever a Equação (2.61), da seguinte maneira:

$$\begin{aligned} \pi_1\pi_2 \cdots \pi_n = \pi'_1\pi'_2 \cdots \pi'_m &= u\pi_1\pi'_2 \cdots \pi'_m \\ \Rightarrow \pi_1\pi_2 \cdots \pi_n &= u\pi_1\pi'_2 \cdots \pi'_m \end{aligned} \tag{2.62}$$

Ao cancelar π_1 em ambos os membros da Equação (2.62), tem-se:

$$\pi_2 \cdots \pi_n = u\pi'_2 \cdots \pi'_{j-1}\pi'_{j+1} \cdots \pi'_m \tag{2.63}$$

Ao realizar o mesmo argumento agora em relação a π_2. Depois de alguns passos, utilizando essa argumentação, o primeiro membro ficará 1, e o segundo membro, consequentemente, é um produto de um dado número π' isso descreve o excedente de m sobre n, ou seja, $n \leq m$, porém é importante enfatizar que estes fatores excedentes não são unidades de $\mathbb{Z}[i]$. Analogamente, $m \leq n$, desta forma $n = m$. Nota-se que no decorrer da demonstração todo π_i possui um dado π_j associado e reciprocamente. □

De maneira abstrata foi mostrado que existe uma fatoração primária para os Inteiros de Gauss, porém é diferente quando exibimos este resultado na prática. Não há um método prático para tal feito, mas como todo o trabalho esta baseado em um paralelo com os Inteiros, agora olharemos para a Norma e assim por intermédio do método prático da fatoração dos Inteiros na Norma de uma dado número em $\mathbb{Z}[i]$. Nosso intuito não é de forma alguma expor um método prático para fatoração de um número inteiro de Gauss, mas sim expor uma exemplificação do teorema anteriormente provado.

Exemplo 2.54. *A fatoração primária de* $\alpha = 5 + 3i$.

Resolução. Como $\alpha = 5 + 3i$, então aplicando a Definição 2.5, temos que:

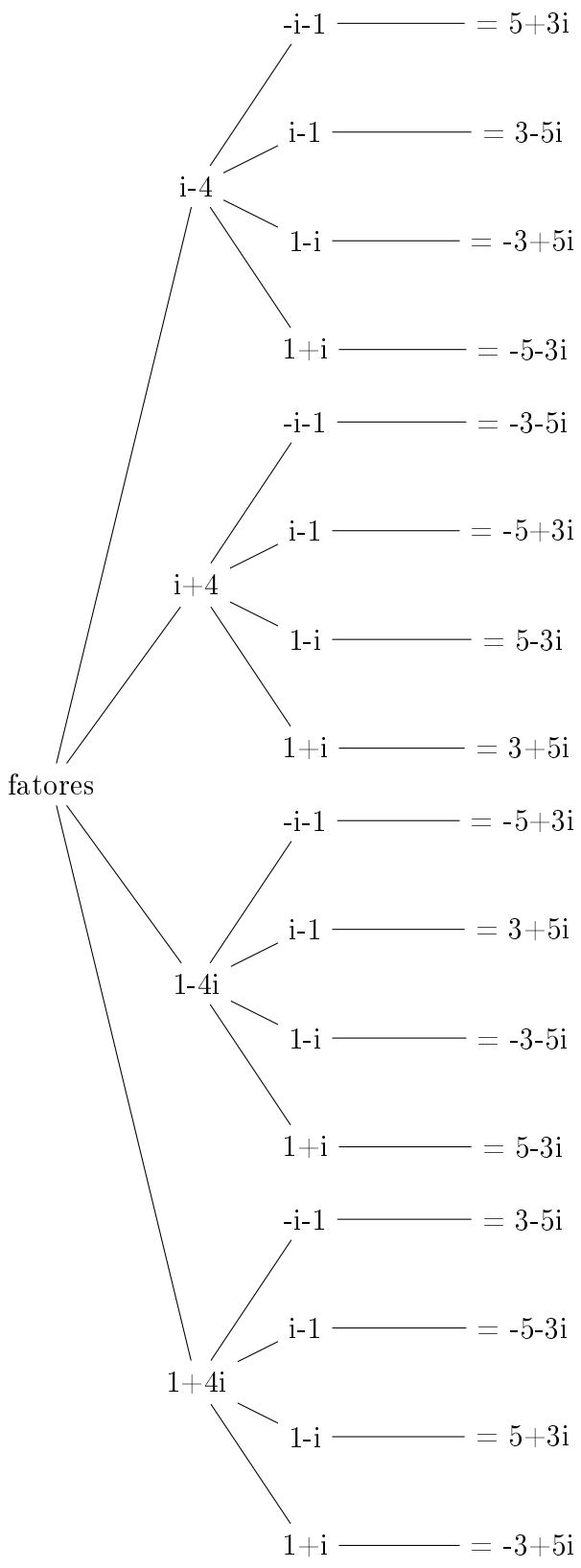
$$N(\alpha) = N(5 + 3i) = 34 = 2 \cdot 17$$

Em seguida, vamos determinar Inteiros de Gauss que possuem norma igual a 2 e 17, uma maneira simples de visualizar origina-se por meio da soma de quadrados, então: $2 = 1^2 + 1^2$ e $17 = 1^2 + 4^2$. Em seguida, logo:

$$2 = (1 + i)(1 - i) = (-i - 1)(i - 1) \tag{2.64}$$

$$17 = (1 + 4i)(1 - 4i) = (4 + i)(4 - i) \tag{2.65}$$

De forma mais didática, utilizarei o diagrama em Árvore, para descrever todas as possibilidades, lembrando que os resultados são obtidos por meio do produto dos respectivos nó do diagrama. Vejamos o diagrama a seguir:


fatores
i-4
-i-1 = 5+3i
i-1 = 3-5i
1-i = -3+5i
1+i = -5-3i
i+4
-i-1 = -3-5i
i-1 = -5+3i
1-i = 5-3i
1+i = 3+5i
1-4i
-i-1 = -5+3i
i-1 = 3+5i
1-i = -3-5i
1+i = 5-3i
1+4i
-i-1 = 3-5i
i-1 = -5-3i
1-i = 5+3i
1+i = -3+5i

Ao observamos todas as combinações uma delas condiz com a fatoração esperada é ela:

$$(1+4i)\cdot(i-1) = 5+3i \tag{2.66}$$

Portanto, temos que $\alpha = 5+3i$ possui uma fatoração primária como $(1+4i)\cdot(i-1)$. □

2.8 Congruência em $\mathbb{Z}[i]$

A congruência já foi apresentada em $\mathbb{Z}$ e agora, este tópico, será descrito com o intuito de concretizar nosso objetivo de possibilitar ao leitor a oportunidade de visualizar as semelhanças existentes entre a congruência em ambos os conjuntos. É importante destacar que embora trataremos deste conceito em $\mathbb{Z}[i]$ diversas proposições são análogas a $\mathbb{Z}$ e devido a este fato as demonstrações serão omitidas. Este tópico foi baseado nas obras [2] e [3].

Definição 2.55. *Sejam α, β, $\gamma \in \mathbb{Z}[i]$, com γ não nulo. Diremos que α e β são côngruos módulo γ, se $\gamma \mid \alpha-\beta$, ou seja, $\alpha-\beta = \gamma k$ para algum $k \in \mathbb{Z}[i]$*

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

Caso contrário, se $\gamma \nmid \alpha-\beta$ diremos que α e β são incôngruos módulo m e denotaremos por:

$$\alpha \not\equiv \beta (mod\, \gamma)$$

Exemplo 2.56. *Verifique que $1+12i \equiv 2-i\ (mod\,(3+i))$.*

Resolução. Segundo a Definição 2.55, tem-se:

$$\frac{(1+12i)-(2-i)}{3+i} = \frac{-1+13i}{3-i} = \frac{(-1+13i)(3-i)}{N(3+i)} = \frac{10+40i}{10} = 1+4i.$$

Portanto, $1+12i \equiv 2-i\ (mod\,(3+i))$. □

Em vista da Definição 2.55, pode-se descrever de maneira imediata a proposição a seguir, é importante relatar que esta caso tem demonstração análoga ao conjunto $\mathbb{Z}$, veja:

Proposição 2.57. *Dados $\gamma \in \mathbb{Z}[i]$. Para quaisquer α, β e $\delta \in \mathbb{Z}[i]$, tem-se que:*

i. (Reflexiva) $\alpha \equiv \alpha (mod\, \gamma)$.

ii. (Simétrica) Se $\alpha \equiv \beta (mod\, \gamma)$, então $\beta \equiv \alpha (mod\, \gamma)$.

iii. (Transitiva) Se $\alpha \equiv \beta (mod\, \gamma)$ e $\beta \equiv \delta (mod\, \gamma)$, então $\alpha \equiv \delta (mod\, \gamma)$.

No entanto, as propriedades de congruência não se resume nas citadas anteriormente, agora elencaremos uma série de proposições e teoremas válidas para $\mathbb{Z}[i]$ e reafirmo que as demonstrações serão realizadas apenas nos casos que não são análogas a $\mathbb{Z}$, caso o leitor tenha alguma dúvida referente a sua demonstração, recomendo ao mesmo retornar ao Capítulo 1 na Seção 1.8. Então segue o estudos os principais resultados válidos para $\mathbb{Z}[i]$, observe:

Proposição 2.58. *Sejam α, β, γ, δ, $\theta \in \mathbb{Z}[i]$, com γ não nulo. Se $\alpha \equiv \beta (mod\, \gamma)$ e $\delta \equiv \theta (mod\, \gamma)$, então $\alpha + \delta \equiv \beta + \theta (mod\, \gamma)$.*

Proposição 2.59. *Sejam α, β, γ, δ, $\theta \in \mathbb{Z}[i]$, com γ não nulo. Se $\alpha \equiv \beta (mod\, \gamma)$ e $\delta \equiv \theta (mod\, \gamma)$, então $\alpha \cdot \delta \equiv \beta \cdot \theta (mod\, \gamma)$.*

Exemplo 2.60. *Determinar possíveis valores para k tal que $(4+5i)^2 \equiv k (mod\, (2-i))$.*

Resolução. De fato, podemos apropriar do Teorema 2.18, vale ressaltar que os cálculos da divisão entre $(4+5i)^2$ e $2-i$ serão omitidos, mas caso tenha alguma dúvida sobre a obtenção dos resultados, retorne aos Exemplos 2.19 ou 2.20 para maiores esclarecimentos.

Sabendo que

$$(4+5i)^2 = -9+40i,$$

então observe:

1. $-9+40i = (2-i)\cdot(-12+14i)+1 \Rightarrow (4+5i)^2 \equiv 1 (mod\, (2-i))$.

2. $-9+40i = (2-i)\cdot(-12+15i)+(-2i) \Rightarrow (4+5i)^2 \equiv -2i (mod\, (2-i))$.

3. $-9+40i = (2-i)\cdot(-11+14i)+(-1+i) \Rightarrow (4+5i)^2 \equiv -1+i (mod\, (2-i))$.

Portanto, k pode assumir os valores: 1, $-2i$ e $-1+i$. □

Destaco a importância do Exemplo 2.60, já que k poderá assumir qualquer valor citado, pelo fato de todos estarem nas condições, ou seja, nenhum deles detém maior relevância.

Exemplo 2.61. *Reduza* $5+12i \ mod\ 4+i$.

Resolução. Inicialmente, vamos efetuar a divisão entre $5+12i$ por $4+i$, logo:

1. $5+12i = (4+i)(2+2i)+(-1+2i) \Rightarrow 5+12i \equiv -1+2i(mod\,(4+i))$

2. $5+12i = (4+i)(2+3i)+(-1+2i) \Rightarrow 5+12i \equiv -2i(mod\,(4+i))$

Portanto, $5+12i \equiv -1+2i(mod\,(4+i))$ e $5+12i \equiv -2i(mod\,(4+i))$, qualquer um é um bom representante para tal redução, pois ambos funcionam. □

É possível aproveitar o resultado Exemplo 2.61 para vislumbrarmos de mais um item importante o conjunto $\mathbb{Z}[i]$ nos proporciona, que é o fato de plotar os $\mathbb{Z}[i]$-múltiplos dado. Vale lembrar que o Exemplo 2.61 direcionará a análise para $\mathbb{Z}[i]$-múltiplos de $-1+2i$. Seja $\alpha = p+qi \in \mathbb{Z}[i]$, então sua representação algébrica é dada:

$$(-1+2i)\cdot\alpha = (-1+2i)\cdot(p+qi) = (-1+2i)p+(-1+2i)qi = (-1+2i)p+(-2-i)q. \quad (2.67)$$

Logo, a Equação (2.67) é a combinação entre $-1+2i$ e $-2-i$. Para a representação geométrica de $-1+2i$ e $-2-i$ em $\mathbb{R}^2$ é denominado por *plano de Argand - Gauss*. No plano Argand - Gauss, o eixo das abscissas é chamado de *eixo real*, denotado por (Re) e o eixo das ordenadas chamado por *eixo imaginário*, denotado por (Im). Considere $z = a+bi \in \mathbb{Z}[i]$ e sua representação geométrica no plano de Argand - Gauss é dada por $P(a,b)$, então, veja a figura a seguir que descreve os representantes $-1+2i$ e$-2-i$ cujas coordenadas são $(-1,2)$ e $(-2,-1)$ em $\mathbb{R}^2$, como representado na Figura 2.1.

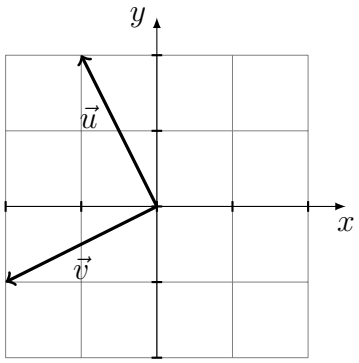


Figura 2.1: $-1+2i$ *e* $-2-i$

Entretanto, por meio da Figura 2.1 é fácil visualizar o esboço de um quadrado através de suas arestas, conforme a Figura 2.2.

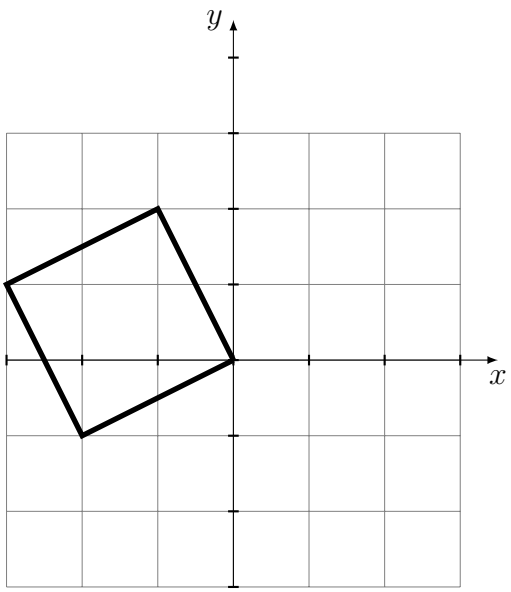


Figura 2.2: $-1+2i$ *e* $-2-i$

No entanto, por meio do quadrado esboçado na Figura 2.2 podemos fracionar todo a malha do plano cartesiano em quadrados congruentes e relativamente posicionado a ele, veja este argumento na Figura 2.3. A Figura 2.3 tem um significa de extrema relevância para aritmética modular pois os inteiros de Gauss côngruos $-1+2i$ são todos aqueles que estão em quadrados diferentes, porém com a mesma posição relativa daqueles situados na Figura 2.2, pelo simples fato de cada quadrado compartilhar seu lado com os demais quadrados e isso geometricamente significa adicionar $-1+2i$, $2-i$ e seus opostos.

Entretanto, não é este o principal resultado que está pesquisa busca descrever, mas um deles é observar o envolvimento da aritmética modular de $\mathbb{Z}[i]$ em elencar os representantes do conjunto $\mathbb{Z}[i]/-1+2i$, ou seja, os representantes dos $\mathbb{Z}[i]$-múltiplos. Então, inicialmente para determinar $\mathbb{Z}[i]/-1+2i$ iremos determinar a norma do vetor $-1+2i$, logo:

$$N(-1+2i) = (-1)^2 + 2^2 = 1 + 4 = 5 \tag{2.68}$$

Posteriormente, como a estrutura analisada é $\mathbb{Z}[i]$, para nomear os representantes do conjunto $\mathbb{Z}[i]/-1+2i$ basta utilizar o quadrado da Figura 2.2 e elencar todos os vetores possíveis que podem ser formados por um vértice do quadrado e qualquer ponto interno dele(é sabido que estes vetores estão representandos por pontos no plano cartesiano com coordenadas inteiras), enfatizo que o ponto do vértice uma vez escolhido

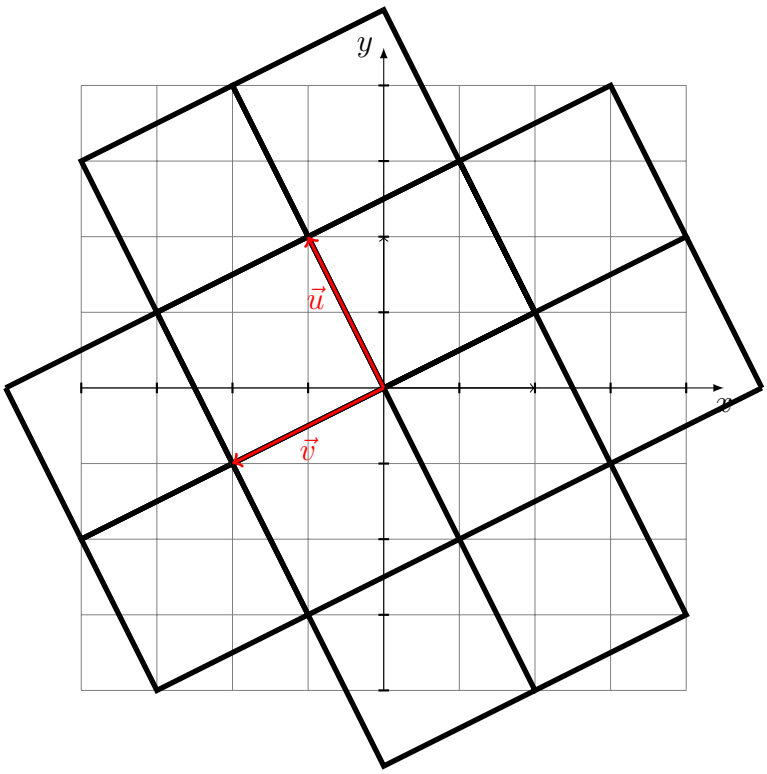


Figura 2.3: $\mathbb{Z}[i]$-*múltiplos de* $-1+2i$

é fixada com o intuito de determinar os demais vetores. Observe a Figura 2.4 com os possíveis representantes (vetores) e ainda que a origem $O(0,0)$ é o vértice fixado para este caso.

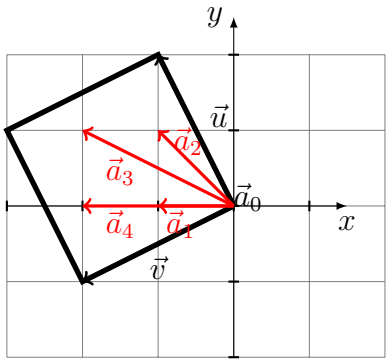


Figura 2.4: $-1+2i$ *e* $-2-i$

É importante descrever que a origem é o ponto escolhido e na Figura 2.4 os repre-

sentantes são:

$$0,\ i,\ 2i,\ -1+i,\ -2+i. \tag{2.69}$$

Agora, mais um item importante refere-se a quantificação dos representantes. Essa quantidade condiz com a norma de $-1+2i$. Essa discussão assemelha-se ao sistema completo de restos de $\mathbb{Z}$, o permite-nos visualizar para esta estrutura mais uma característica bem semelhante aos Inteiros.

Capítulo 3

Os lados inteiros de um triângulos retângulos e sua relação com os Inteiros de Gauss

Nesta pesquisa, pode-se observar as principais características que o conjunto $\mathbb{Z}[i]$ possui, no entanto, quando trata-se de números complexos, a priori é buscar uma aplicação deste conceito, e esta seção é responsável por descrever uma aplicabilidade dos Inteiros de Gauss na Geometria. Mesmo que independentemente da sua aplicação prática o conceito desempenha papel fundamental na compreensão das propriedades algébricas e aritméticas que frequentemente estamos manuseando durante resoluções de problemas no geral.

Um questionamento comum é a ausência de aplicação em situações problemas envolvendo os Números Complexos na 3ª série do Ensino Básico. Eventualmente, as aplicações consiste em: representar geometricamente um dado número, descrever sua forma trigonométrica e entre outros, embora os livros didáticos explorem vagamente as diversas aplicações. Esta pesquisa busca nesta Seção discorrer sobre uma possibilidade de aplicação de Números Complexos por meio de um subconjunto $\mathbb{Z}[i]$, pois Ternos pitagóricos são usados frequentemente e a sua determinação não é simples de ser feita, caso a determinação seja através das cálculos manuais, em alguns casos podem ser dificilmente concluídas. Agora com ferramentas corretas, como as propriedades de $\mathbb{Z}[i]$

essa atividade pode se tornar mais tranquila. É importante descrever que essa seção é baseada na obra [1] e [4].

Conforme a Geometria Euclideana o triângulo é uma figura geométrica plana que possui inúmeros resultados importantes e um caso particular é o triângulo retângulo, tipo este de triângulo que satisfaz uma série de resultados importantes e inclusive ele é a figura que satisfaz um dos teoremas mais conhecidos que é o teorema de Pitágoras. A seguir, um triângulo retângulo ABC, denotado por $\Delta(ABC)$, observe:

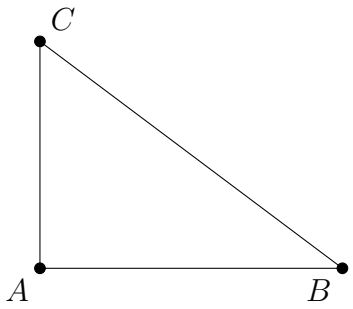


Figura 3.1: $\Delta(ABC)$ é retângulo em Â.

Em um triângulo retângulo os lados recebem nomes especiais, catetos e hipotenusa. A hipotenusa é o maior lado do $\Delta(ABC)$, na figura 3.1 está representado por $\overline{BC} = z$ e os demais $\overline{AC} = x$ e $\overline{AB} = y$ são os catetos desse triângulo. Esse tipo de triângulo apresenta um regularidade ímpar que pode ser descrita pelo teorema a seguir:

Teorema 3.1. *O triângulo ABC é retângulo se, e somente se, a hipotenusa ao quadrado é igual a soma dos quadrados dos catetos.*

Definição 3.2. *Sejam x, y, z inteiros positivos que satisfazem a relação $z^2 = x^2 + y^2$ são denominados ternos pitagóricos ou números pitagóricos.*

Em torno deste resultado é possível observar que existem os chamados ternos pitagóricos primitivos, e essa seção é responsável de possibilitar a determinação de todos os ternos pitagóricos primitivos a partir de um valor fixo para a hipotenusa.

3.1 Os Ternos Pitagóricos

Definição 3.3. *Seja (x, y, z) um terno pitagórico. Quando $((x, y), y) = 1$ diremos que (x, y, z) é um Terno Pitagórico Primitivo.*

Denotaremos o máximo divisor comum entre x, y, z por $((x, y), y)$. Se (x, y, z) é um terno pitagórico e $t \in \mathbb{Z}$, com $t = ((x, y), y)$, então (tx, ty, tz), este novo terno também é denominada como um terno pitagórico, porém não é primitivo, e por isso ele satisfaz o teorema de Pitágoras, conforme ilustrado a seguir:

$$(tx)^2 + (ty)^2 = t^2x^2 + t^2y^2 = t^2 \cdot (x^2 + y^2) = t^2z^2 = (tz)^2. \tag{3.1}$$

Essa situação descreve que podemos multiplicar ou dividir os Ternos Pitagóricos Primitivos e obter todos os outros. Por isso, $(5, 12, 13)$ é um Terno Pitagórico Primitivo e $(10, 24, 26)$, $(15, 36, 39)$ também são ternos pitagóricos.

Neste instante, após esse breve comentário sobre Terno Pitagórico, apresentaremos a seguir alguns resultados importantes para nos auxiliar na compreensão desta aplicação, então vejamos.

Teorema 3.4. *(x, y, z), é um terno pitagórico se, e somente, se existir $r,\ s \in \mathbb{Z}$ tais que $r > s > 0$, r e s possui a mesma paridade, rs é um quadrado perfeito, com:*

$$x = \sqrt{rs},\ y = \frac{r - s}{2} \ \text{e}\ z = \frac{r + s}{2}.$$

Demonstração. Seja (x, y, z) um terno pitagórico. Assim temos:

$$x^2 + y^2 = z^2 \Rightarrow x^2 = z^2 - y^2 = (z + y) \cdot (z - y). \tag{3.2}$$

Suponha que:

$$r = z + y \tag{3.3}$$

$$s = z - y, \tag{3.4}$$

então:

$$x^2 = (z + y) \cdot (z - y) \Rightarrow x^2 = rs \Rightarrow x = \pm\sqrt{rs}, \tag{3.5}$$

como x é um lado de um triângulo, utilizaremos apenas

$$x = \sqrt{rs},$$

por hipótese $r,\ s \in \mathbb{Z}$, tais que $r > s > 0$, r e s possuem a mesma paridade, então, é possível obter relações para y e z. Para y, basta subtrair as Equações (3.3) e (3.4), logo:

$$r - s = (z + y) - (z - y) \Rightarrow r - s = z + y - z + y \Rightarrow 2y = r - s \Rightarrow y = \frac{r - s}{2}, \quad (3.6)$$

para determinar um relação para z basta adicionar as Equações(3.3) com (3.4), assim:

$$r + s = (z + y) + (z - y) \Rightarrow r + s = z + y + z - y \Rightarrow 2z = r + s \Rightarrow z = \frac{r + s}{2}. \quad (3.7)$$

Portanto, $x = \sqrt{rs}$, $y = \dfrac{r - s}{2}$ e $z = \dfrac{r + s}{2}$.

Reciprocamente, suponha $r,\ s \in \mathbb{Z}$ estejam conforme as condições do teorema. É sabido que $r, s \in \mathbb{Z}$, tais que $r > s > 0$ e possuem2 a mesma paridade, então vamos considerar $y = \dfrac{r - s}{2}$ e $z = \dfrac{r + s}{2}$, ambos positivos. Por outro lado, seja rs um quadrado perfeito, então $x = \sqrt{rs}$ é um inteiro positivo. Desta forma, verifica-se que:

$$x^2 + y^2 = (\sqrt{rs})^2 + \left(\frac{r - s}{2}\right)^2 = rs + \frac{(r - s)^2}{4} = rs + \frac{r^2 - 2rs + s^2}{4} = \left(\frac{r + s}{2}\right)^2 = z^2. \quad (3.8)$$

Assim, pode-se concluir que (x, y, z) é um terno pitagórico. □

A Proposição 3.5 é de suma importância durante a exposição dos exemplos que serão exposto nessa seção, então, segue enunciada:

Proposição 3.5. *Se $x \geq 3$, existe um triângulo retângulo com cateto x.*

Demonstração. Considere $r,\ s \in \mathbb{Z}$, tais que $r > s > 0$ e possuem a mesma paridade, além disso, rs é quadrado perfeito e conforme o Teorema 3.4 temos que:

$$x = \sqrt{rs},\ y = \frac{r - s}{2} \text{ e } z = \frac{r + s}{2}.$$

Nessas condições, queremos provar que x pode ser um cateto de um triângulo retângulo. No entanto, há duas possibilidades para x, sendo ele par ou ímpar. Então:

(x é par) Seja $r = x^2$ e $s = 1$, utilizando o Teorema 3.4, no qual:

$$x = \sqrt{rs} = \sqrt{x^2 \cdot 1} = \sqrt{x^2} = x \text{ e } y = \frac{x^2 - 1}{2}$$

e

$$z^2 = x^2 + y^2 = (x)^2 + \left(\frac{x^2 - 1}{2}\right)^2 = x^2 + \left(\frac{x^4 - 2x^2 + 1}{4}\right), \tag{3.9}$$

Ao desenvolvendo a expressão da Equação (3.9), temos que:

$$\frac{4x^2 + x^4 - 2x^2 + 1}{4} = \left(\frac{x^2 + 1}{2}\right)^2 = (z)^2 = z^2.$$

x é ímpar Este caso é análogo ao anterior, basta considerar $r = \frac{x^2}{2}$ e $s = 2$, então:

$$x = \sqrt{rs} = \sqrt{\frac{x^2}{2} \cdot 2} = \sqrt{x^2} = x \text{ e } y = \frac{\frac{x^2}{2} - 2}{2} = \frac{x^2 - 4}{4},$$

e

$$z^2 = x^2 + y^2 = (x)^2 + \left(\frac{x^2 - 4}{4}\right)^2 = x^2 + \left(\frac{x^4 - 8x^2 + 16}{4}\right) = \left(\frac{x^2 + 4}{4}\right)^2.$$

□

Teorema 3.6. *Sejam $x,\ y,\ z \in \mathbb{Z}^+$. As asserções a seguir são equivalentes:*

1. $(x, y) = 1$ *e* $x^2 + y^2 = z^2$

2. $x = 2ab$, $y = a^2 - b^2$ *ou vice-versa e* $z = a^2 + b^2$, *com a e b inteiros positivos, tais que* $a > b > 0$, $(a, b) = 1$ *e a e b possuem paridades distintas.*

Indicamos ao caro leitor a obra [1] e [4] para mais informações sobre o Teorema 3.6.

Mediante aos resultados importantes apresentados na Subseção 3.1, sabemos que por meio deles, poderíamos discutir a determinação de triângulos retângulos com cateto

ou hipotenusa em um dado valor fixo, no entanto, somente, quando há um valor fixo para a hipotenusa para determinação de todos os ternos possíveis que será explorada, pois a finalidade desta Subseção 3.2 é explorar o conhecimento já discorrido neste trabalho que é o conjunto $\mathbb{Z}[i]$ e por meio dele, possibilitar a chance de encontrar triângulos retângulos a partir de um valor dado para a hipotenusa.

3.2 Determinação de Triângulos Retângulos a Partir de um Valor Fixo para a Hipotenusa

Neste momento, determinaremos os números inteiros positivos z que são hipotenusa de um dado triângulo retângulo. Deste modo, iremos determinar todos os possíveis triângulos retângulos com z para a hipotenusa e a quantidade de triângulos possíveis com o valor fixo da hipotenusa e tudo isso, será realizado por meio da decomposição de z em fatores primos.

Seja $x,\ y,\ z \in \mathbb{Z}$. z é o valor fixo da hipotenusa de um triângulo retângulo, fato interessante que não é possível determinar z^2 como um produto de dois inteiros x e y, e a alternativa encontrada é utilizar os conjunto $\mathbb{Z}[i]$ para nos auxiliar nesta determinação, então:

$$z^2 = x^2 + y^2 = (x + yi) \cdot (x - yi) \text{ com } x, y \in \mathbb{Z}.$$

Teorema 3.7. *Seja z um número inteiro positivo. Então existe um triângulo retângulo com hipotenusa z se, e somente se, z é divisível por um número primo p tal que $p \equiv 1 \pmod 4$.*

Demonstração. ($\Leftarrow$) Considere p um número primo. Seja $z \in \mathbb{Z}$, como z é divisível por p, então:

$$z = p \cdot z_1, \text{ com } p \equiv 1 \pmod 4.$$

Pelo Teorema 2.37, sabemos que $a,\ b \in \mathbb{Z}^+$ tais que $p = a^2 + b^2 = N(a + bi)$. Portanto:

$$p^2 = (N(a + bi))^2 = N[(a + bi)^2] = N[(a^2 - b^2) + (2ab)i] = (a^2 - b^2)^2 + (2ab)^2.$$

Suponha que $a > b > 0$, consequentemente:

$$a^2 - b^2 > 0 \text{ e } 2ab > 0.$$

Assim, pode-se observar que:

$$z^2 = p^2 z_1^2 = (a^2 - b^2)^2 \cdot z_1^2 + (2ab)^2 \cdot z_1^2 = ((a^2 - b^2) \cdot z_1)^2 + ((2ab) \cdot z_1)^2.$$

($\Rightarrow$) Caso z não seja divisível por p, com $p \equiv 1 \pmod 4$ e, sendo que, $x^2 + y^2 = z^2$, com $x,\ y \in \mathbb{N}$ e $x > y > 0$. Nesta perspectiva, podemos observar a fatoração de z, que por sinal é descrita da forma:

$$z = 2^v \cdot \pi_1^{s_1} \cdots \pi_k^{s_k} \Rightarrow z = 2^{2v} \cdot \pi_1^{s_1} \cdots \pi_k^{s_k}, \tag{3.10}$$

com $\pi_j \equiv 3 \pmod 4$.

Sabe-se que $z^2 = (x + yi) \cdot (x - yi)$, logo $N(x + yi) = N(x - yi)$. Uma observação importante é o fato que $N(1 + i) = 2$ usaremos esse item na fatoração de $x + yi$, assim, podemos fatorar z^2 em elementos irredutíveis de $\mathbb{Z}[i]$, conforme a ilustrado a seguir:

$$z^2 = u \cdot (1 + i)^{2v} \cdot \pi_1^{s_1} \cdots \pi_k^{s_k} = u \cdot (2i)^v \cdot \pi_1^{s_1} \cdots \pi_k^{s_k},$$

u é um elemento invertível em $\mathbb{Z}[i]$.

Portanto, $x + yi$ é um numero real ou um imaginário puro, isso implica em $x = 0$ ou $y = 0$, uma contradição, já que x e y são catetos de um dado triângulo retângulo. $\square$

Lema 3.8. *Sejam $p_1,\ p_2,\ \cdots,\ p_k$ números primos distintos tais que $p_j \equiv 1 \pmod 4$. Suponha que $p_j = a_j^2 + b_j^2$, com $a_j, b_j \in \mathbb{Z}$, e $\alpha = x + yi = (a_1 + b_1)^{n_1} \cdot (a_2 + b_2)^{n_2} \cdots (a_k + b_k)^{n_k}$. Então x e y são primos entre si em $\mathbb{Z}[i]$.*

Teorema 3.9. *Seja $z = p_1^{t_1} \cdot p_2^{t_2} \cdots p_k^{t_k} \cdot w$. Suponha p_j números primos distintos e $p_j \equiv 1 \pmod 4$ e ainda que w não é divisível por nenhum primo $p \equiv 1 \pmod 4$. Então existem:*

$$\sum_{m=1}^{k} 2^{m-1} \Big(\sum_{1 \le j_1 < j_2 < \cdots < j_m \le k} t_{j_1} t_{j_2} \cdots t_{j_m} \Big)$$

triângulos retângulos com hipotenusa igual a z e não semelhantes.

Demonstração. Considere $z = z_1 \cdot z_2$, com p_j primos de sendo que $p_j \mid z_1$ tais que $p_j \equiv 1 \pmod 4$ e todos aqueles q_j que dividem z_2 são tais que $q_j = 2$ ou $q_j \equiv 3 \pmod 4$. Sabe-se que na prova do Teorema 3.7 e por consequências do Teoremas (2.33) e (2.53), pois x e y devem ser múltiplos de z_2. É relevante, neste contexto é que p_j divida z_1.

Seja d um divisor de z_1, $z = dz_3$. Queremos determinar x_1, y_1 primos entre si tais que $x_1^2 + y_1^2 = d^2$ e sendo que $x = x_1 z_3$ e $y = y_1 z_3$, logo:

$$\begin{aligned} x^2 + y^2 &= (x_1 z_3)^2 + (y_1 z_3)^2 \\ &= (x_1)^2 (z_3)^2 + (y_1)^2 (z_3)^2 \\ &= ((x_1)^2 + (y_1)^2)(z_3)^2 \\ &= d^2 (z_3)^2 \\ &= (d(z_3))^2 \\ &= z^2 \end{aligned} \tag{3.11}$$

No entanto, suponhamos que $z = p_1^{t_1} \cdot p_2^{t_2} \cdots p_k^{t_k} \cdot w$ com $p_j \equiv 1 \pmod 4$ e vamos determinar x e y primos entre si de tal forma que $x^2 + y^2 = d^2$.

Por outro lado, vamos analisar um caso particular para $k = 1$. Considere $z = p^t$, como $p = a^2 + b^2 = (a + bi)(a - bi)$. Portanto:

$$z^2 = p^{2t} = N(p^t) = N[(a+bi)^t]N[(a-bi)^t] = N[(a+bi)^t]N[(a+bi)^t] = N[(a+bi)^{2t}]. \tag{3.12}$$

Contudo, se $(a + bi)^{2t} = x + yi$, assim como $N(a + bi)^{2t} = N(x + yi) = x^2 + y^2$, então $z^2 = x^2 + y^2$ e, segundo o Lema 3.8 x e y são primos entre si. Neste sentido, podemos concluir que se x ou y serem negativos, é necessário trocar o sinal para obter o valor do cateto. Pode-se escolher:

$$z^2 = p^{2t} = N(p^{2t}) = N[(a+bi)^t]N[(a-bi)^t] = N[(a-bi)^t]N[(a-bi)^t] = N[(a-bi)^{2t}]. \tag{3.13}$$

Conforme a propriedade do conjugado complexo $(a - bi)^{2t} = x - yi$, teremos o mesmo triângulo retângulo.

Tome $k > 1$. Seja $p_j = a_j^2 + b_j^2 = (a + bi)(a - bi)$ e $\alpha_j = a_j + b_j i$. De imediato, $\alpha = x + yi$ é um dos números complexos $\beta_1 \beta_2 \cdots \beta_k$ na qual $\beta_j = \overline{\alpha_j}^{2t_j}$ ou $\beta_j = {\alpha_j}^{2t_j}$. É importante destacar que $N(\alpha) = z^2 = x^2 + y^2$ e de acordo com Lema 3.8 então x

e y são primos entre si. Ao contar a quantidade de triângulos, sabemos que existem 2^k para escolha de α, no entanto, sabe-se que esta havendo uma contagem dupla pois esta incluso o conjugado, no qual gera o mesmo triângulo retângulo, então o total de triângulos retângulos será:

$$\frac{2^k}{2} = 2^{k-1}, \tag{3.14}$$

com catetos x e y são primos entre si, tais que $x^2 + y^2 = z^2$. Lembrando que $k = 1$ possui apenas um triângulo retângulo com catetos primos entre si não semelhantes ao obtido. Entretanto, vamos determinar a quantidade de triângulos possui a hipotenusa k, sendo que $z = p_1^{t_1} \cdot p_2^{t_2} \cdots p_k^{t_k}$ com $p_j \equiv 1 \pmod 4$.

Admita um divisor $d = p_{j_1}^{s_{j_1}} \cdot p_{j_2}^{s_{j_2}} \cdots p_{j_k}^{s_{j_k}}$ com expoentes positivos, $z = dz_1$. Sabe-se que há 2^{m-1} triângulos retângulos com hipotenusa d e catetos primos entre si. Multiplicando d por z_1, então:

$$z = d \cdot z_1 = p_{j_1}^{s_{j_1}} \cdot p_{j_2}^{s_{j_2}} \cdots p_{j_k}^{s_{j_m}} z_1, \tag{3.15}$$

assim, concluímos que 2^{m-1} triângulos retângulos com hipotenusa z. Um fato importante que os primos $p_{j_1} p_{j_2} \cdots p_{j_m}$ são $t_{j_1} t_{j_2} \cdots t_{j_m}$ divisores. Ao variar $j_1 j_2 \cdots j_m$ com $1 \leq j_1 \leq j_2 \leq \cdots \leq j_m \leq k$, então podemos representar da forma:

$$\sum_{1 \leq j_1 < j_2 < \cdots < j_m \leq k} t_{j_1} t_{j_2} \cdots t_{j_m}, \tag{3.16}$$

com divisores possuindo exatamente m primos distintos, assim fazendo variar do m de 1 a k. □

Uma observação importante é mediante ao resultado apresentado pelo Teorema 3.9, para facilitar a compreensão da notação utilizada por intermédio de um somatório duplo, observe:

$$\sum_{m=1}^{k} 2^{m-1} \Big(\sum_{1 \leq j_1 < j_2 < \cdots < j_m \leq k} t_{j_1} t_{j_2} \cdots t_{j_m} \Big) =$$

$$= 2^0 \cdot \sum_{j=1}^{k} t_{j_1} + 2^1 \cdot \sum_{1 \leq j_1 < j_2 \leq k} t_{j_1} t_{j_2} + \cdots + 2^{k-1} \cdot \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq k} t_{j_1} t_{j_2} \cdots t_{j_k} \tag{3.17}$$

Corolário 3.10. *Considere* $z = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k} \cdot w$ *e obedecendo as condições do Teorema 3.9 e sendo elas satisfeitas, logo existem:*

$$\sum_{m=1}^{k} 2^{m-1} \binom{k}{m} \tag{3.18}$$

triângulos retângulos não semelhantes com hipotenusa z *e catetos inteiros.*

Indicamos [4] para mais informações referentes as demonstrações do Lema 3.8 e Corolário 3.10.

Agora, veremos na prática com utilizar estes resultados apresentados anteriormente.

Exemplo 3.11. *Quantos triângulos retângulos não semelhantes existem com a hipotenusa igual a* 5602350.

Resolução. Primeiramente, vamos determinar a decomposição em fatores primos do número 5602350, e ela é dada por:

$$z = 2 \cdot 3 \cdot 5^2 \cdot 13^3 \cdot 17. \tag{3.19}$$

Em seguida, identificar os primos $p_j \equiv 1 \pmod 4$, então:

$$2 \not\equiv 1 \pmod 4 \tag{3.20}$$
$$3 \not\equiv 1 \pmod 4 \tag{3.21}$$
$$5 \equiv 1 \pmod 4 \tag{3.22}$$
$$13 \equiv 1 \pmod 4 \tag{3.23}$$
$$17 \equiv 1 \pmod 4 \tag{3.24}$$

Seja $t_{j_1} = 2$, $t_{j_2} = 3$ e $t_{j_3} = 1$, ao aplicar o Teorema 3.9, obtêm-se:

$$\sum_{m=1}^{3} 2^{m-1}\Big(\sum_{1\le j_1<j_2<j_3\le 3} t_{j_1}t_{j_2}t_{j_3}\Big) = 2^{1-1}\cdot\sum_{j=1}^{3} t_{j_1} + 2^{2-1}\cdot\sum_{1\le j_1<j_2\le 3} t_{j_1}t_{j_2} + 2^{3-1}\cdot\sum_{1\le j_1<j_2<j_3\le 3} t_{j_1}t_{j_2}t_{j_3} \tag{3.25}$$

Desenvolvendo os somatórios da Equação (3.25), assim:

$$2^{1-1} \cdot \sum_{j=1}^{3} t_{j_1} = 2^0 \cdot (2+3+1) = 6, \tag{3.26}$$

$$2^{2-1} \cdot \sum_{1 \leq j_1 < j_2 \leq 3} t_{j_1} t_{j_2} = 2^1 \cdot (2 \cdot 3 + 2 \cdot 1 + 3 \cdot 1) = 2 \cdot 11 = 22 \tag{3.27}$$

e

$$2^{3-1} \cdot \sum_{1 \leq j_1 < j_2 < j_3 \leq 3} t_{j_1} t_{j_2} t_{j_3} = 2^2 \cdot 2 \cdot 3 \cdot 1 = 4 \cdot 6 = 24. \tag{3.28}$$

Portanto, o número total de triângulos retângulos não semelhantes é a soma das Equações (3.26), (3.27) e (3.28), então:

$$\sum_{m=1}^{3} 2^{m-1} \Big(\sum_{1 \leq j_1 < j_2 < j_3 \leq 3} t_{j_1} t_{j_2} t_{j_3} \Big) = 6 + 22 + 24 = 52.$$

□

Neste momento estamos preparados para determinar os triângulos não semelhantes a partir de um valor fixo da hipotenusa z.

Exemplo 3.12. *Determinar todos os possíveis triângulos retângulos não semelhantes com hipotenusa igual a* $z = 325$ *e catetos inteiros.*

Resolução. Utilizando o Teorema 3.9, inicialmente, $z = 325 = 5^2 \cdot 13$. É notável que ambos os fatores primos 5 e 13 deixam resto 1 quando divididos por 4. Então:

$$\sum_{m=1}^{2} 2^{m-1} \Big(\sum_{1 \leq j_1 < j_2 \leq 2} t_{j_1} t_{j_2} \Big) = 2^{1-1} \cdot \sum_{j=1}^{2} t_{j_1} + 2^{2-1} \cdot \sum_{1 \leq j_1 < j_2 \leq 2} t_{j_1} t_{j_2} = 7$$

triângulos retângulos não semelhantes com hipotenusa igual a $z = 325$.

Pode-se observar que:

$$5 = 2^2 + 1^2 \text{ e } 13 = 3^2 + 2^2 \tag{3.29}$$

e ao escrever 5 e 13 em fatores primos irredutíveis em $\mathbb{Z}[i]$, teremos:

$$5 = (2+i)(2-i) \text{ e } 13 = (3+2i)(3-2i). \tag{3.30}$$

A seguir vamos descrever cada um dos ternos pitagóricos, vejamos as possibilidades de acordo com o Lema 3.8, então:

$$\begin{aligned}
\alpha_1 &= (2+i)^4 \cdot (3+2i)^2 = -323 + 36i \\
\alpha_2 &= (2+i)^4 \cdot (3-2i)^2 = 253 + 204i \\
\alpha_3 &= 5 \cdot (2+i)^2 \cdot (3+2i)^2 = -165 + 280i \\
\alpha_4 &= 5 \cdot (2+i)^2 \cdot (3-2i)^2 = 315 - 80i \\
\alpha_5 &= 13 \cdot (2+i)^4 = -91 + 312i \\
\alpha_6 &= 25 \cdot (3+2i)^2 = 125 + 300i \\
\alpha_7 &= 25 \cdot (3+2i)^2 = 195 + 260i
\end{aligned}$$

Então, agora, basta verificar se de fato todos os $\alpha_j \in \mathbb{Z}[i]$, com $j \in \mathbb{N}$ e $1 \leq j \leq 7$. Como $N(\alpha_j) = 325^2 = 105625$, então obtêm-se:

$$\begin{aligned}
N(\alpha_1) &= (323)^2 + (36)^2 = 325^2 = 105625 \\
N(\alpha_2) &= (253)^2 + (204)^2 = 325^2 = 105625 \\
N(\alpha_3) &= (165)^2 + (280)^2 = 325^2 = 105625 \\
N(\alpha_4) &= (315)^2 + (80)^2 = 325^2 = 105625 \\
N(\alpha_5) &= (91)^2 + (312)^2 = 325^2 = 105625 \\
N(\alpha_6) &= (125)^2 + (300)^2 = 325^2 = 105625 \\
N(\alpha_7) &= (195)^2 + (260)^2 = 325^2 = 105625
\end{aligned}$$

Então, por intermédio de $\mathbb{Z}[i]$ determinamos os 7 triângulos retângulos não seme-

lhantes cujos ternos pitagóricos são:

$$(36, 323, 325)$$
$$(80, 315, 325)$$
$$(91, 312, 325)$$
$$(125, 300, 325)$$
$$(165, 280, 325)$$
$$(195, 260, 325)$$
$$(204, 253, 325)$$

Os cálculos foram realizados por tentativa e não por intermédio de softwares, visto que durante a realização da pesquisas não foi encontrado nenhum software que desenvolvesse essa aplicação, porém aqui fica uma aplicação simples que pode ser explorada com alunos do Ensino Médio, pois representa uma aplicação dos complexos na Geometria Plana e além de estar associada a uma série de conceitos importantes como Teorema de Pitágoras, ternos pitagóricos.

Não é fácil determinar triângulos retângulos não semelhantes e graças aos Inteiros de Gauss podemos alçar resultados consistentes de forma simples e eficaz.

Considerações finais

A formação continuada do docente é de suma importância para uma melhor prática em sala de aula. Aqui, mediante aos estudos realizados nos conjuntos $\mathbb{Z}$ e $\mathbb{Z}[i]$ espera-se que os professores de Matemática explorem com maior intensidade estes conjuntos e estabeleçam que este tópico é indispensável para o bom desempenho para discente do Ensino Básico.

As propriedades aritméticas foram priorizadas e descritas com detalhes a fim de proporcionar o paralelo existente entre os conjuntos e o quanto o entendimento de $\mathbb{Z}$ coopera para a compreensão dos principais resultados de $\mathbb{Z}[i]$ e além disso, $\mathbb{Z}$ apresenta resultados totalmente análogos a $\mathbb{Z}[i]$, o que comprova a semelhança existente entre essas estruturas.

Este estudo foi direcionado ao aperfeiçoamento profissional de um professor de Matemática com o intuito de propiciar uma abordagem elementar das propriedades que sustentam essas estruturas e auxiliar-o com uma pesquisa referente a um assunto, geralmente, discutido de forma sucinta.

Existem inúmeros questionamentos mediante a utilidade prática dos números complexos, e após a leitura, poderão vislumbrar de uma aplicabilidade de $\mathbb{Z}[i]$ na Geometria. Ela consiste na determinação dos catetos de um triângulo retângulo com valor de uma hipotenusa fixa e ainda, estes ternos encontrados são ternos pitagóricos. Vale mencionar que determinar esse terno pitagórico por tentativa, dependendo do valor fixado pode se tornar inviável o cálculo.

Espera-se que esta pesquisa seja um respaldo teórico para os professores de matemática que ainda não conhecia o tema, assim como eu e para aqueles que ja conhecem a temática, possibilite um aprofundamento matemático sobre os Inteiros de Gauss.

Portanto, que o leitor tenha verificado a importância de conhecer essa estrutura e o quanto o conjunto $\mathbb{Z}$ cooperara na compreensão de $\mathbb{Z}[i]$, com intuito de ampliar o conhecimento e oportunizar aos professores outros horizontes em relação a outras

estruturas, as vezes, não imaginamos intersecção entre ambas as estruturas, mas esta pesquisa descreve claramente, o quanto são semelhantes e além de ser extremamente importante na descoberta de novas estruturas.

Sabe-se que este trabalho foi direcionado aos professores de Matemática com o intuito de aprimorar seu conhecimento sobre o conjunto $\mathbb{Z}[i]$, e consequentemente, permitir que eles, correlacionem o conjunto $\mathbb{Z}$ a outras estruturas e compreendam o quanto o conjunto $\mathbb{Z}$ é importante durante este estudo. Embora, o conjunto $\mathbb{Z}$ auxilia no entendimento de outras estruturas, um exemplo disso, foi feito pelo matemático Kummer que considerou um subanel $\mathbb{Z}[\sqrt{5}i]$, descrito por:

$$\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i;\ a,\ b \in \mathbb{Z}\}$$

este anel apresenta particularidades interessantes assim como $\mathbb{Z}[i]$ e a partir deste, surgiu questionamentos como: " Os elementos primos e irredutíveis coincidem como em $\mathbb{Z}[i]$? "; "$\mathbb{Z}[\sqrt{5}i]$ apresenta unicidade em sua fatoração?". Então, estas e outras indagações podem ser conduzidas após esta pesquisa, porém esta estrutura ficará para os próximos estudos.

Referências Bibliográficas

[1] ANDRADE, José F., *Triângulos retângulos com lados inteiros: Procurando as hipotenusas*. Matemática Universitária. n° 41. Dezembro/2006.

[2] CONRAD, Keith, *The gaussian integers*. 2008. Pre-Print, paper edition. Disponível em: https://pdfs.semanticscholar.org/7472/6a271df1591d01f1dae66ae57b421cc758df.pdf

[3] COSTA, Icoracy Coutinho da, *Inteiros de Gauss: uma abordagem elementar*. 2016. Dissertação (Mestrado Profissional em Matemática - ProfMat) - Instituto de Ciências Exatas, Universidade Federal do Amazonas. Manaus, 2016.

[4] CUNHA, Johny Andrade da, *Somas de quadrados e triângulos retângulos com lados inteiros*. 2019. Dissertação (Mestrado Profissional em Matemática - ProfMat) - Departamento de Matemática, Universidade Federal de Sergipe. Itabaiana, 2019.

[5] DOMINGUES, Hygino H., *Fundamentos da aritmética*. Atual, São Paulo, 1991.

[6] Freire, Paulo., *Pedagogia da autonomia: saberes necessários à pratica educativa/ Paulo Freire*, Paz e Terra (Coleção Leitura), São Paulo, 1996.

[7] Hefez, Abramo., *Aritmética/ Abramo Hefez* , SBM, Coleção PROFMAT, Volume único, 2ª Edição, Rio de Janeiro, 2016.

[8] Hefez, Abramo., *Curso de Álgebra, volume 1 (3º edição)* , IMPA, Coleção Matemática Universitária, Volume 1, 3ª Edição, Rio de Janeiro, 2002.

[9] Herstein, I. N., *Tópicos de Álgebra*; Tradução de Adalberto P. Bergamasco e L. H. Jacy Monteiro, Editora da Univ. e Polígono; São Paulo, 1970.

[10] LIMA, Luciana Sequeira Cury e, *O Anel dos Inteiros de Gauss*. 2016. Dissertação (Mestrado Profissional em Matemática - ProfMat) - Centro de Ciências Exatas e Tecnologias, Universidade Federal do Estado do Rio de Janeiro. Rio de Janeiro, 2016.

[11] MARTINEZ, Fabio E. Brochero. et al., *Um passeio com os primos e outros números familiares pelo mundo inteiro*, Livraria Virtual IMPA, 3ª Edição, Rio de Janeiro, (2013).

[12] M. A. Filho, *Entrevista com a Professora Suely Druck*, Jornal da Unicamp, pg 6–7, 14–27 de Fevereiro de 2005.

[13] Mestrado Profissional em Matemática em Rede Nacional-PROFMAT, http://www.profmat-sbm.org.br/organizacao/apresentacao/, acesso em 02/12/2019.

[14] Programa de Iniciação Científica e Mestrado IME-UFG https://picme.mat.ufg.br/, acesso em 02/12/2019.

[15] SILVA, Jhone Caldeira ; GOMES, Olimpio Ribeiro., *Estruturas algébricas para licenciatura: Elementos da Aritmética superior/ Jhone Caldeira Silva, Olimpio Ribeiro Gomes*, Blucher, São Paulo, 2018.

[16] https://www.somatematica.com.br/coluna/gisele/27102006.php, acesso em 02/12/2019.