INSTITUTO FEDERAL
Goiás
Câmpus Valparaíso

Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Câmpus Valparaíso
Licenciatura em Matemática

Inteiros que são soma de dois quadrados

Natã Amarante Passos

Trabalho de Conclusão de Curso – Licenciatura em Matemática

Orientador: Prof. Dr. Silvio Sandro Alves de Macedo

VALPARAÍSO DE GOIÁS - GO
2025

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

Identificação da Produção Técnico-Científica

[ ] Tese	[ ] Artigo Científico
[ ] Dissertação	[ ] Capítulo de Livro
[ ] Monografia – Especialização	[ ] Livro
[x] TCC - Graduação	[ ] Trabalho Apresentado em Evento
[ ] Produto Técnico e Educacional - Tipo: _____	

Nome Completo do Autor: Natã Amarante Passos
Matrícula: 20201150040385
Título do Trabalho:

Autorização - Marque uma das opções

1. (x) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. ( ) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data ___/___/_____ (Embargo);
3. ( ) Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

( ) O documento está sujeito a registro de patente.
( ) O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.
( ) Outra justificativa: _____

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
ii. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

_____Brasília_____, __11__/__07__/_2025___.
Local Data

Documento assinado digitalmente
gov.br
NATA AMARANTE PASSOS
Data: 14/07/2025 12:56:46-0300
Verifique em https://validar.iti.gov.br

_____
Assinatura do Autor e/ou Detentor dos Direitos Autorais

Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Câmpus Valparaíso
Licenciatura em Matemática

Inteiros que são soma de dois quadrados

Natã Amarante Passos

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia de Goiás (IFG), Câmpus Valparaíso de Goiás, como parte dos requisitos para a conclusão do Curso e obtenção do título de licenciado em Matemática.

Orientador: Prof. Dr. Silvio Sandro Alves de Macedo

Dados Internacionais de Catalogação na Publicação (CIP)

P289i

Passos, Natã Amarante

Inteiros que são somas de dois quadrados [recurso eletrônico] / Natã Amarante Passos.
2025.
Dados eletrônicos (1 arquivo).
74 f. : il. color.

Orientador: Prof. Dr. Sílvio Sandro Alves de Macedo.
Trabalho de conclusão de curso (Licenciatura em Matemática) – Instituto Federal de Educação, Ciência e Tecnologia de Goiás, câmpus Valparaíso, 2025.
Modo de acesso: World Wide Web.
Arquivo de texto em formato PDF.
Disponível em: https://repositorio.ifg.edu.br.

1. Anéis Euclidianos. 2. Inteiros Gaussianos. 3. Primos gaussianos. 4. Números primos - Soma de quadrados. I. Título. II. Macedo, Sílvio Sandro Alves de, orient.

CDD 512.5

Bibliotecário: Lourenildo Targino Pedrosa – CRB-1/2264.

Termo de Aprovação

NATÃ AMARANTE PASSOS

INTEIROS QUE SÃO SOMA DE DOIS QUADRADOS

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia de Goiás – Câmpus Valparaíso de Goiás, como parte dos requisitos para a obtenção do título de Licenciado em Matemática.

Monografia defendida e aprovada em 14 de março de 2025 pela banca examinadora constituída pelos seguintes membros:

BANCA EXAMINADORA

Prof. Dr. Silvio Sandro Alves de Macedo
Presidente da banca / Orientador
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Prof. Dr. Agenor Freitas de Andrade
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Profa. Dra. Daiane Soares Veras
Instituto Federal de Educação, Ciência e Tecnologia de Goiás

Valparaíso de Goiás – GO

2025

Documento assinado eletronicamente por:

- **Daiane Soares Veras**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 01/06/2025 18:56:52.
- **Agenor Freitas de Andrade**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 24/04/2025 08:33:06.
- **Silvio Sandro Alves de Macedo**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 23/04/2025 16:45:08.

Este documento foi emitido pelo SUAP em 13/03/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifg.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 626895
Código de Autenticação: ff7536b767

Dedico este trabalho a Deus, minha família e meus professores.

RESUMO

O objetivo principal desta monografia é dar uma caracterização dos inteiros que podem ser escritos como soma de dois quadrados. Esse é um resultado clássico da Teoria dos Números, cuja descoberta é atribuída a Fermat (1601-1665). A parte essencial da demonstração consiste em caracterizar os primos que são soma de dois quadrados, mais precisamente, se $p > 2$ é um primo que é soma de dois quadrados, então p é da forma $4k+1$. Esse último enunciado foi enviado em uma carta de Fermat para Mersenne (1588-1648) em 1640. O matemático Euler (1707-1783) daria uma demonstração desse resultado em 1754. Nesta monografia daremos uma demonstração moderna desse resultado de Fermat, seguindo a abordagem clássica de usar certas propriedades do anel dos inteiros gaussianos, que são números complexos da forma $z = a + bi$ com a, b inteiros e $i^2 = -1$.

Palavras-chave: anéis euclidianos; inteiros gaussianos; primos gaussianos; números primos; soma de quadrados.

ABSTRACT

The main objective of this monograph is to characterize the integers that can be written as the sum of two squares. This is a classical result in Number Theory, whose discovery is attributed to Fermat (1601–1665). The essential part of the proof consists in characterizing the prime numbers that are sums of two squares; more precisely, if $p > 2$ is a prime and can be expressed as the sum of two squares, then p is of the form $4k + 1$. This statement was sent by Fermat to Mersenne (1588–1648) in a letter dated 1640. The mathematician Euler (1707–1783) provided a proof of this result in 1754. In this monograph, we present a modern proof of this result, following the classical approach based on properties of the ring of Gaussian integers, which are complex numbers of the form $z = a + bi$, where a and b are integers and $i^2 = -1$.

Keywords: Euclidean rings; Gaussian integers; Gaussian primes; prime numbers; sum of squares.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Dizemos que um terno (a,b,c) de inteiros positivos é pitagórico quando $a^2+b^2=c^2$. Por exemplo, $(3,4,5)$ é um terno pitagórico, pois $3^2+4^2=5^2$. O terno $(5,12,13)$ também é pitagórico porque $5^2+12^2=13^2$. O significado geométrico da igualdade $3^2+4^2=5^2$ é que existe um triângulo retângulo com hipotenusa medindo 5 unidades e catetos medindo 3 e 4 unidades.

Desde a Grécia antiga, já se sabia que há infinitos triângulos retângulos cujas medidas são números inteiros, isto é, sabiam como gerar todos os inteiros positivos a,b e c tais que $a^2+b^2=c^2$ [1].

Observe que igualdades como $2=1^2+1^2$ ou $5=2^2+1^2$ representam triângulos retângulos cujos catetos têm medidas inteiras mas cujas hipotenusas têm medidas irracionais uma vez que $\sqrt{2}$ e $\sqrt{5}$ são números irracionais.

Aqui surge uma pergunta natural: quais inteiros positivos n são tais que $n=a^2+b^2$ com a e b inteiros positivos? É bem conhecido que, se n não for um quadrado perfeito, então $\sqrt{n}$ é um número irracional. Assim, quando n não é um quadrado perfeito, a igualdade $n=a^2+b^2$ representa um triângulo retângulo com hipotenusa $\sqrt{n}$ (irracional) e catetos de medidas inteiras a e b.

Voltando à pergunta feita anteriormente: se n for um inteiro tal que $n=a^2+b^2$, então, considerando todos os casos possíveis para os valores de a e b, temos: a = par e b = par; a = par e b = ímpar; a = ímpar e b = ímpar, não é difícil verificar que n é da forma $4k$, $4k+1$ ou $4k+2$.

Não é difícil verificar que, em cada um desses casos, n será congruente a 0, 1 ou 2 módulo 4, isto é, n será da forma $4k$, $4k+1$ ou $4k+2$.

A identidde a seguir aparece em um livro de Fibonacci [2] (sem os créditos), mas já era conhecida muito tempo antes pelos árabes (Shokranian, 2010):

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2.$$

Essa identidade implica que, se dois inteiros podem ser escritos como soma de dois quadrados, então o seu produto também pode ser representado como soma de dois quadrados.

Da afirmação acima decorre o seguinte: como todo inteiro n pode ser decomposto como um produto de fatores primos (Teorema Fundamental da Aritmética), se todos os primos nos quais n se decompõe forem soma de dois quadrados, então n também será uma soma de dois quadrados.

---

[1] Os ternos pitagóricos (a,b,c) são gerados pelas relações $a=m^2-n^2, b=2mn$ e $c=m^2+n^2$, com $m>n>0$.

[2] Fibonacci (cerca de 1180-1250) ou "filho de Bonaccio" é o nome pelo qual Leonardo de Pisa, matemático e comerciante italiano, era conhecido.

Assim, a pergunta inicial pode ser refinada: quais primos p são soma de dois quadrados? Esses primos que são soma de dois quadrados vão "gerar" todos os inteiros que são soma de dois quadrados.

Como os inteiros da forma $4k$ ou $4k+2$ são sempre pares, concluímos o seguinte:

Se p é um primo que é soma de dois quadrados, então
$p = 2$ (pois $2 = 1^2 + 1^2$) ou p é da forma $p = 4k+1$. (1)

Examinando uma pequena lista dos primeiros números primos, observamos que, de fato, apenas os primos da forma $4k+1$ (e o número 2) podem ser escritos como soma de dois quadrados. Os primos da forma $4k+3$ não admitem tal representação.

$2 = 1^2 + 1^2$	$19 = 4\times 4 + 3$	$47 = 4\times 11 + 3$	$79 = 4\times 19 + 3$
$3 = 4\times 0 + 3$	$23 = 4\times 5 + 3$	$53 = 7^2 + 2^2$	$83 = 4\times 20 + 3$
$5 = 1^2 + 2^2$	$29 = 5^2 + 2^2$	$59 = 4\times 14 + 3$	$89 = 8^2 + 5^2$
$7 = 4\times 1 + 3$	$31 = 5^2 + 2^2$	$61 = 5^2 + 6^2$	$97 = 9^2 + 4^2$
$11 = 4\times 2 + 3$	$37 = 6^2 + 1^2$	$67 = 4\times 16 + 3$	$101 = 10^2 + 1^2$
$13 = 2^2 + 3^2$	$41 = 5^2 + 4^2$	$71 = 4\times 17 + 3$	$103 = 4\times 25 + 3$
$17 = 1^2 + 4^2$	$43 = 4\times 10 + 3$	$73 = 8^2 + 3^2$	$107 = 4\times 26 + 3$

Aqui surge uma pergunta natural, cuja resposta positiva, juntamente com a conclusão em (1), caracterizaria os primos que são soma de dois quadrados:

Todo primo da forma $4k+1$ é uma soma de dois quadrados?

Em 1640, Pierre de Fermat (1601-1665), um advogado e conselheiro do parlamento francês, que em seu tempo livre se dedicava à matemática, escreveu uma carta destinada a Mersenne contendo o seguinte enunciado: "Um primo da forma *4k+1* pode ser representado como a soma de dois quadrados." (Eves (2011, p. 391)).

Figura 1 – Pierre de Fermat

Fonte: Smith (1906)

Uma vez caracterizados os primos que são soma de dois quadrados, pode-se estender a pergunta para um inteiro qualquer e buscar alguma caracterização dos inteiros n tais que $n = a^2 + b^2$.

Como já dissemos acima, como todo inteiro pode ser escrito como um produto de fatores primos, segue que uma caracterização de $n = a^2 + b^2$ está relacionado com o problema da caracterização dos primos que são soma de dois quadrados. De fato, o cerne do problema foi resolvido por Fermat em sua carta a Mersenne.

Fermat publicou pouco durante sua vida, porém os principais matemáticos da época mantinham diversas correspondências científicas com ele. Dentre as contribuições de Fermat, a fundação da moderna teoria dos números é destacada por Eves (2011, p. 390) como a mais importante.

O apreço de Fermat pela teoria dos números teria surgido através do livro *Aritmética*, de Diofanto. Muitas contribuições de Fermat à teoria dos números foram feitas por notas e enunciados às margens desse livro (Eves, 2011, p. 390).

Ainda, segundo Eves (2011, p. 391), a primeira demonstração do enunciado de Fermat, juntamente com a prova da unicidade da representação dos primos da forma $4k+1$ como soma de dois quadrados, foi apresentada por Euler em 1754.

Os métodos de prova de Fermat foram completamente perdidos até 1879, quando um documento intitulado *Relation des découvertes en la science des nombres*[3] foi encontrado entre os manuscritos de Huygens na biblioteca de Leyden; parece que Fermat usou um método indutivo, chamado por ele de *la descente infinie ou indefinie*[4] (Cajori, 1909, p. 211). André Weil [5] sugeriu plausivelmente que a prova de Fermat teria sido muito semelhante àquela que Euler mais tarde reivindicaria (Gray, 2018, p. 1).

O objetivo principal desta monografia é caracterizar os inteiros que podem ser escritos como soma de dois quadrados (Teorema 3.4.4). Para provar esse resultado principal, é crucial a caracterização dos primos que são soma de dois quadrados (Teorema 3.4.2).

Para provar que os primos da forma $4k+1$ são soma de dois quadrados, seguiremos a prova apresentada por Herstein (2005). Essa prova usa o chamado anel dos inteiros gaussianos, denotado por $\mathbb{Z}[i]$, que são números complexos da forma $\alpha = a + bi$ com a e b inteiros.

O anel $\mathbb{Z}[i]$ possui propriedades análogas àquelas de $\mathbb{Z}$, o anel dos inteiros. Uma propriedade crucial em $\mathbb{Z}$ é que se p é um primo que divide o produto ab, então p divide a ou p divide b.

Em $\mathbb{Z}[i]$ há a noção de primo gaussiano, e vale uma propriedade análoga: Se α é um primo gaussiano que divide o produto $\beta\gamma$, então α divide β ou α divide γ.

[3] "Relação das des-cobertas na ciência dos números". (tradução nossa).

[4] "a descida infinita ou indefinida". (tradução nossa)

[5] André Weil (1906-1998) foi um matemático francês conhecido pelas suas obras sobre teoria dos números e geometria algébrica.

Apenas para ilustrar como certas propriedades em $\mathbb{Z}$ se comportam ao serem estendidas para $\mathbb{Z}[i]$, observe o seguinte: se $p = a^2 + b^2$ é um primo em $\mathbb{Z}$, então $p = a^2 + b^2 = (a + bi)(a - bi)$. Logo p não é um primo gaussiano em $\mathbb{Z}[i]$.

Esta monografia está dividida em três capítulos. No primeiro, apresentaremos a definição de anel e provaremos algumas de suas propriedades fundamentais. Em seguida, introduziremos os chamados anéis euclidianos, que são anéis com propriedades análogas àquelas do anel dos inteiros $\mathbb{Z}$. O objetivo principal deste capítulo é provar que se π é um elemento primo em um anel euclidiano A e π divide ab, então π divide a ou π divide b.

No segundo capítulo estudaremos alguns teoremas importantes no anel $\mathbb{Z}$ dos inteiros como o Pequeno Teorema de Fermat (Proposição 2.2.7), o Teorema de Wilson (Proposição 2.2.8) e um teorema de Euler (Teorema 2.3.1). Como esses resultados são geralmente expressos usando a notação de congruência, abordaremos brevemente esse conceito. O resultado mais importante deste capítulo é o teorema de Euler, que fornece uma caracterização dos primos da forma $p = 4k + 1$ em termos da existência de solução para certas equações em $\mathbb{Z}$.

No terceiro capítulo provaremos o Teorema 3.4.4, que é o resultado principal desta monografia: um inteiro n pode ser representado como soma de dois quadrados se, e somente se, ele tiver uma fatoração em primpos da forma

$$n = 2^{\alpha} {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r} {q_1}^{\beta_1} {q_2}^{\beta_2} \cdots {q_s}^{\beta_s}$$

onde cada p_i é um primo da forma $4k + 1$, cada q_j é um primo da forma $4k + 3$, α e cada α_i são inteiros não negativos e todos os β_j são inteiros pares.

Para provar esse resultado, vamos estudar, nesse capítulo, algumas propriedades do anel dos inteiros gaussianos $\mathbb{Z}[i]$, incluindo a prova de que $\mathbb{Z}[i]$ é um anel euclidiano. Isso garantirá a validade da Proposição 1.1.30 nesse anel. Essa proposição, juntamente com o Teorema de Euler (Teorema 2.3.1), nos permitirá provar o Lema 3.4.1, o resultado chave para provar o nosso resultado principal.

1 ANÉIS

Neste capítulo estudaremos algumas propriedades de anéis euclidianos, que são anéis com propriedades análogas àquelas do anel dos inteiros $\mathbb{Z}$. A propriedade mais importante de um primo p em $\mathbb{Z}$ é que se p divide ab, então p divide a ou p divide b.

O objetivo principal deste capítulo é estender esse resultado à anéis euclidianos quaisquer, isto é, vamos mostrar a seguinte propriedade: se π é um elemento primo em um anel euclidiano A e π divide ab, então π divide a ou π divide b.

1.1 ANÉIS EUCLIDIANOS

Vamos começar definindo um anel. Em todo o texto o conjunto dos números naturais será denotado por $\mathbb{N} = \{1,2,3,...\}$.

Definição 1.1.1. *Um anel $(A,+,\cdot)$ é um conjunto A, munido de uma operação $+$ (chamada adição) e de uma operação $\cdot$ (chamada multiplicação) que satisfazem as seguintes propriedades:*

(1) A adição é associativa, isto é

$$(a+b)+c = a+(b+c), \text{ para quaisquer } a,b,c \in A.$$

(2) Existe um elemento neutro com respeito à adição, denotado por 0, tal que

$$a+0 = a = 0+a, \text{ para qualquer } a \in A.$$

(3) Todo elemento $a \in A$ possui um inverso com respeito à adição, denotado por $-a$, tal que

$$a+(-a) = 0 \; e \; (-a)+a.$$

(4) A adição é comutativa, isto é

$$a+b = b+a, \text{ para quaisquer } a,b \in A.$$

(5) A multiplicação é associativa, isto é

$$(a\cdot b)\cdot c = a\cdot(b\cdot c), \text{ para quaisquer } a,b,c \in A.$$

(6) A adição é distributiva relativamente à multiplicação, isto é

$$a\cdot(b+c) = a\cdot b + a\cdot c \;\; e \;\; (a+b)\cdot c = a\cdot c + b\cdot c, \text{ para quaisquer } a,b,c \in A.$$

Um anel A é comutativo se $a \cdot b = b \cdot a$, para quaisquer $a, b \in A$.

Um anel A é com unidade se existir o elemento $1 \in A$ (chamado elemento unidade) tal que $1 \cdot a = a = a \cdot 1$ para todo $a \in A$.

Observe que se um anel possuir elemento unidade, ele é único. De fato, se 1 e $1'$ são unidades de uma anel A, então $1 = 1 \cdot 1' = 1'$.

Seja M_2 o conjunto de todas as matrizes 2×2 com entradas em $\mathbb{R}$, o conjunto dos números reais. A operação de soma de duas matrizes $a = (a_{ij})$ e $b = (b_{ij})$ em M_2 é definida por

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}.$$

E a operação de multiplicação é definida por

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} \cdot b_{11} + a_{12} \cdot b_{21} & a_{11} \cdot b_{12} + a_{12} \cdot b_{22} \\ a_{21} \cdot b_{11} + a_{22} \cdot b_{21} & a_{21} \cdot b_{12} + a_{22} \cdot b_{22} \end{pmatrix}.$$

Pode-se mostrar que essas operações de soma e multiplicação de matrizes satisfazem as propriedades (1)-(6) da Definição 1.1.1, logo M_2 é um anel.

Fixemos a seguinte notação para estas matrizes especiais:

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ e } e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Observe que $e_{12} \cdot e_{21} = e_{11}$, porém $e_{21} \cdot e_{12} = e_{22}$. Portanto M_2 não é um anel comutativo.

A matriz $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o elemento unidade do anel pois

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} e \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Portanto M_2 é um anel com unidade. Esse anel com unidade (e não comutativo) é chamado de anel das matrizes 2×2.

De modo análogo defini-se o anel das matrizes $n \times n$ (com entradas em $\mathbb{R}$), denotado por M_n. As operações desse anel e algumas de suas propriedades costumam ser estudadas no segundo ano do Ensino Médio.

Exemplo 1.1.2. *O conjunto dos números inteiros* $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ *munido das operações usuais de adição e multiplicação é um anel comutativo com unidade.*

O anel $\mathbb{Z}$ é chamado anel dos inteiros e o estudo das suas propriedades inicia-se no Ensino Fundamental. Neste trabalho faremos um estudo mais aprofundado do anel $\mathbb{Z}$, necessários à demonstração do nosso resultado principal.

Exemplo 1.1.3. *Pode-se mostrar que o conjunto* $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$, *onde* $i^2 = -1$, *munido das operações de adição e multiplicação, definidas por*

$$(a+bi)+(c+di) = (a+c)+(b+d)i, \tag{1.1}$$

$$(a+bi)(c+di) = ac-bd+(ad+bc)i \tag{1.2}$$

é um anel comutativo com unidade. Ele é chamado de anel dos inteiros gaussianos.

Um inteiro gaussiano $\alpha = a+bi \in \mathbb{Z}[i]$ é um caso particular de número complexo $z = a+bi$ com $a,b \in \mathbb{R}$ e $i^2 = -1$. Os números complexos costumavam ser estudados no último ano do Ensino Médio, juntamente com as equações algébricas.

É um trabalho rotineiro mostrar que as operações de soma e multiplicação sobre $\mathbb{Z}[i]$, definidas em (1.1) e (1.2), satisfazem as propriedades (1)-(6) da Definição 1.1.1.

Para ilustrar a maneira como se demonstra essas propriedades, vamos apenas mostrar que a multiplicação definida em $\mathbb{Z}[i]$ é comutativa e que ela tem unidade.

De fato, dados $\alpha = a+bi$ e $\beta = c+di$ em $\mathbb{Z}[i]$, temos

$$\alpha\beta = (a+bi)(c+di) = ac-bd+(ad+bc)i.$$

Por outro lado

$$\beta\alpha = (c+di)(a+bi) = ca-db+(cb+da)i.$$

Comparando as duas igualdades acima, temos $\alpha\beta = \beta\alpha$. Portanto a operação definida em (1.2) é comutativa.

Observe que

$$(1+0i)\cdot(a+bi) = (1\cdot a-0\cdot b)+(1\cdot b+0\cdot a)i = a+bi,$$

$$(a+bi)(1+0i) = (a\cdot 1-b\cdot 0)+(b\cdot 1+a\cdot 0) = a+bi.$$

Logo $1 = 1+0i$ é o elemento unidade do anel $\mathbb{Z}[i]$.

Definição 1.1.4. *Dizemos que um anel* A *é de integridade quando ele é comutativo e vale a seguinte propriedade: se* $ab = 0$, *então* $a = 0$ *ou* $b = 0$, *para quaisquer* $a,b \in A$.

Observe que $\mathbb{Z}$ é um anel de integridade. De fato, $\mathbb{Z}$ é um anel comutatitvo no qual $ab = 0$ implica $a = 0$ ou $b = 0$. Como veremos adiante (Corolário 3.2.4), $\mathbb{Z}[i]$ também é um anel de integridade.

O anel das matrizes M_2 não é de integridade por dois motivos: primeiro, a operação de multiplicação não é comutativa (como já vimos acima); segundo, $e_{11}e_{22} = 0$, onde $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ é a matriz nula de M_2.

Proposição 1.1.5. *Seja* A *um anel qualquer e* a,b *elementos quaisquer de* A. *As seguintes propriedades são satisfeitas:*

(i) $0 \cdot a = 0$ *e* $a \cdot 0 = 0$ *para todo* $a \in A$.

(ii) $-(ab) = (-a)b = a(-b)$.

Demonstração.

(i) Se $a \in A$, então $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$, está equação implica que $a \cdot 0 = 0 + 0 = 0$, então $a \cdot 0 = 0$.

(ii) Observe que

$$ab + a(-b) = a(b + (-b)) = a(b - b) = a \cdot 0 = 0.$$

Então $ab + a(-b) = 0 \Rightarrow a(-b) = -(ab)$.

Observe ainda que

$$0 = a(b + (-b)) = ab + a(-b) = b(a + a(-1)) = b(a + (-a)) = ba + b(-a).$$

Então temos $-(ab) = (-a)b$. Portanto $-(ab) = (-a)b = a(-b)$. □

Definição 1.1.6. *Dizemos que um anel de integridade* A *é euclidiano se para todo* $a \in A$ *não nulo está definido um inteiro não negativo* $d(a)$ *tal que*

(i) Para quaisquer $a, b \in A$*, ambos não nulos, existem* $q, r \in A$ *tais que* $a = bq + r$*, onde* $r = 0$ *ou* $d(r) < d(b)$

(ii) Para quaisquer $a, b \in A$*, ambos não nulos,* $d(a) \leq d(ab)$.

Veremos mais adiante que $\mathbb{Z}$ é um anel euclidiano (Proposição 1.1.11). No Capítulo 2 veremos que $\mathbb{Z}[i]$ também é um anel euclidiano (Proposição 3.2.5).

Definição 1.1.7. *Sejam* a *e* b *elementos de um anel comutativo* A*. Dizemos que* a *divide* b *se existir* $c \in A$ *tal que* $b = ac$.

No anel $\mathbb{Z}$, 4 divide -12 pois $-12 = 4 \cdot (-3)$; ainda, 0 divide 0 pois $0 = 0 \cdot 1$.
No anel $\mathbb{Z}[i]$, $2 + 3i$ divide $-1 + 5i$ pois $-1 + 5i = (1 + i)(2 + 3i)$.

Em um anel A, quando a divide b, escrevemos $a \mid b$. Quando a divide b também dizemos que b é múltiplo de a.

Sejam a, b elementos de um anel A. A operação de subtração é definida por

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

Proposição 1.1.8. *Sejam* a*,* b*,* c*,* d *elementos de um anel comutativo* A.

(i) Se $a \mid b$ *e* $a \mid c$ *então* $a \mid (b \pm c)$.

(ii) Se $a \mid b$ *e* $c \mid d$ *então* $ac \mid bd$.

(iii) Se $a \mid b$ então $a \mid bd$.

(iv) Se $a \mid b$ então $a^n \mid b^n$ para todo $n \in \mathbb{N}$.

Demonstração.

(i) Se $a \mid b$ e $a \mid c$ temos que, $b = am$ e $c = an$, onde $m\ e\ n \in A$. Se somarmos b e c, então $b + c = am + an = a(m + n)$; onde temos $a \mid (b + c)$. Se subtrairmos c de b, então $b - c = am - an = a(m - n)$; onde temos $a \mid (b - c)$. Logo $a \mid (b \pm c)$.

(ii) Se $a \mid b$, tomando e $c \mid d$ temos que; $b = am$ e $d = cn$, onde $m\ e\ n \in A$. E então $bd = (am)(cn)$, e pela propriedade associativa e comutativa da multiplicação, $bd = (ac)(mn)$. Logo $ac \mid bd$.

(iii) Se $a \mid b$, tomando $c = 1$ no item anterior temos que $a \mid bd$.

(iv) Se $a \mid b$ temos pelo item (ii) que $aa \mid bb$, isto é $a^2 \mid b^2$. Aplicando novamente o item (ii) temos que $a^2 \mid b^2$ implica $(a^2)a \mid (b^2)b$, isto é $a^3 \mid b^3$. Prosseguindo assim, vemos que $a^n \mid b^n$ para cada $n \in \mathbb{N}$. □

1.1.1 O ANEL DOS INTEIROS

Nesta seção vamos mostrar que o anel dos inteiros $\mathbb{Z}$ é um anel euclidiano, ou seja, que em $\mathbb{Z}$ vale o Algoritmo da Divisão. É esse resultado que fundamenta o "algoritmo da chave", que é ensinado já no Ensino Fundamental.

Definição 1.1.9. *Seja B um subconjunto de $\mathbb{Z}$.*

(i) Dizemos que B é limitado inferiormente se existir um inteiro $k \in \mathbb{Z}$ tal que $k \leq b$, para todo inteiro $b \in B$.

(ii) Dizemos que $b_0 \in B$ é o mínimo de B se $b_0 \leq b$, para todo $b \in B$. O mínimo de B é denotado por $b_0 = \min(B)$.

Como exemplo, o mínimo do conjunto $\mathbb{N}$ dos números naturais é 1. O conjunto $B = \{\ldots, -3, -2, -1\}$ dos inteiros negativos não possui mínimo.

Agora podemos enunciar o Principio da Boa Ordem.

Proposição 1.1.10 (Princípio da Boa Ordem)**.** *Todo conjunto não vazio de inteiros limitado inferiormente tem mínimo.*

Pode-se provar que o Princípio da Boa Ordem é equivalente ao Princípio de Indução Finita, que não abordaremos aqui. Ao leitor interessado, sugerimos o Capítulo 1 de Lima (2014).

Uma consequência do Princípio da Boa Ordem é o Algoritmo da Divisão.

Proposição 1.1.11 (Algoritmo da Divisão)**.** *Dados dois inteiros a e b, com $b \neq 0$, existem e são únicos os inteiros q e r tais que*

$$a = bq + r \text{ onde } 0 \leq r < |b|.$$

Demonstração. Vamos demonstrar primeiro a existência desses números. Começaremos estudando o caso em que $b > 0$. Considere o conjunto

$$S = \{a - bk \mid k \in \mathbb{Z},\ a - bk \geq 0\}.$$

Observe que S é não vazio: se $a \geq 0$ então $a - b \cdot 0 \in S$; se $a < 0$ então $a - (2a)b = a(1 - 2b) > 0$ (pois $1 - 2b < 0$), donde $a - (2a)b \in S$.

Pelo princípio da Boa Ordem existe um elemento mínimo $r \in S$, com $r = a - qb \geq 0$ para algum $q \in \mathbb{Z}$.

Temos que $a = bq + r$ de modo que, para demonstrar que estes inteiros estão nas condições do enunciado basta provar que $r < b$. Suponha por absurdo que $r \geq b$. Então

$$a - b(q + 1) = bq + r - b(q + 1) = r - b \geq 0,$$

logo $a - b(q + 1)$ também pertenceria a S. Mas $a - b(q + 1) = a - bq - b = r - b < r$, que é o mínimo de S, uma contradição.

Se $b < 0$, como $-b > 0$, pelo resultado anterior, existem q_1 *e* r_1 tais que $a = (-b)q_1 + r_1$ e $0 \leq r_1 < -b$. Escrevendo $a = b(-q_1) + r_1$ vemos que, neste caso, os inteiros $-q_1$ *e* r_1 estão nas condições do enunciado.

Vamos imaginar, que se pudesse determinar outro par de inteiros q_1 e r_1, tais que $a = bq_1 + r_1$, com $0 \leq r_1 < b$. Então $qb + r = bq_1 + r_1$ e, portanto, $b(q - q_1) = r_1 - r$. Se $r = r_1$, então $b(q - q_1) = 0$ donde $q - q_1 = 0$ e temos também que $q = q_1$. Suponhamos que $r \neq r_1$, digamos $r > r_1$. Daí, o segundo membro da última igualdade seria estritamente negativo e, como $b > 0$, então $q - q_1$ também seria estritamente negativo e, portanto, $q_1 - q > 0$, ou seja, $q_1 - q \geq 1$. Mas de $b(q - q_1) = r_1 - r$ segue que

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

Levando-se em conta que $b > 0$, $r_1 \geq 0$ e $q_1 - q \geq 1$, da última igualdade seguiria que $r \geq b$, o que é absurdo. Da mesma forma, prova-se que a desigualdade $r_1 > r$ também é impossível. □

Corolário 1.1.12. *Dados dois inteiros a e b, com $b > 0$, existem inteiros q e r tais que $a = bq + r$ e $|r| \leq \frac{b}{2}$.*

Demonstração. O Algoritmo da Divisão garante a existência de inteiros q *e* r tais que $a = bq + r$ com $0 \leq r < b$. Se $0 \leq r < \frac{b}{2}$, não há o que provar. Se $\frac{b}{2} \leq r < b$, basta observar

que $a = (q+1)b + (r-b)$ e $-\frac{b}{2} \leq r - b < 0$. □

A Proposição 1.1.11 mostra que $\mathbb{Z}$ é um anel euclidiano. De fato, $|a|$ é o valor absoluto do número a, que é definido por

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

A parte (i) da Definição 1.1.6 está mostrada na Proposição 1.1.11. A parte (ii) da Definição 1.1.6 é válida devido à seguinte propriedade do valor absoluto: $|ab| = |a||b|$.

Veremos mais adiante (Proposição 3.2.5) que $\mathbb{Z}[i]$ também é um anel euclidiano.

1.1.2 MÁXIMO DIVISOR COMUM

Nesta seção vamos estender o conceito de máximo divisor comum à aneis euclidianos quaisquer. Para fazer isso precisamos introduzir o conceito de ideal.

Definição 1.1.13. *Seja A um anel. Dizemos que um subconjunto $I \subseteq A$ é um ideal de A se as seguintes propriedades são satisfeitas:*

(i) $0 \in I$.

(ii) *Se* $x, y \in I$ *então* $x + y \in I$.

(iii) *Se* $x \in I$ *então* $-x \in I$.

(iv) *Se* $x \in I$ *e* $a \in A$ *então* $ax \in I$ *e* $xa \in I$.

O significado das propriedades (i)-(iii) da definição acima é que se I é um ideal de um anel A, então I contém 0, o elemento neutro do anel A; e $x, y \in I \Rightarrow x \pm y \in I$. Em outras palavras:

$0 \in I$

I é fechado para as operações de soma e subtração.

O significado da propriedade (iv) é que um ideal I "absorve" produtos no anel. Vejamos alguns exemplos de ideais.

Dado $d \in \mathbb{Z}$, seja $J = \{dk \mid k \in \mathbb{Z}\}$. Vamos mostrar que J é um ideal de $\mathbb{Z}$:

(i) Como $0 = d \cdot 0$, temos $0 \in J$.

(ii) Sejam $x = dm$ e $y = dn$ em J. Então $x + y = (m+n)d \in J$.

(iii) Seja $x = dm \in J$. Então $-x = -(dm) = d(-m)$; logo $-x \in J$.

(iv) Dados $x = dk \in J$ e $m \in \mathbb{Z}$, temos $mx = m(dk) = d(mk) \in J$ e $xm = (dk)x = d(kx) \in J$.

Assim J possui as propriedades (i)-(iv) da Definição 1.1.13, e portanto é um ideal de $\mathbb{Z}$.

Em um anel qualquer A, não é difícil verificar que o subconjunto $\{0\}$ e o próprio A satisfazem as propriedades (i)-(iv) da Definição 1.1.13. Portanto $\{0\}$ e A são ideais de A; eles são chamados de *ideais triviais* de A.

Nosso objetivo a seguir é mostrar que os únicos ideais do anel M_2 das matrizes 2×2 são os triviais. Mas antes, voltemos às matrizes

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ e } e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Vamos chamá-las de *matrizes básicas*. Se pusermos $\delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$, pode-se verificar que a seguinte igualdade é verdadeira:

$$e_{ij}e_{kl} = \delta_{jk}e_{il}. \tag{1.3}$$

A relação 1.3 nos fornece uma maneira prática de calcular o produto de duas *matrizes básicas*. Ela também pode ser usada para calcular o produto de duas matrizes quaisquer de M_2.

Seja $a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ em M_2. Observe que

$$\begin{aligned} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} &= \begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a_{21} & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_{22} \end{pmatrix} \\ &= a_{11}\cdot\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + a_{12}\cdot\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + a_{21}\cdot\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + a_{22}\cdot\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Assim $a = a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22}$. Vejamos um cálculo específico que usaremos mais adiante:

$$\begin{aligned} e_{11}ae_{11} &= e_{11}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{11} = (a_{11}e_{11} + a_{12}e_{12})e_{11} = a_{11}e_{11} \\ e_{11}ae_{21} &= e_{11}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{21} = (a_{11}e_{11} + a_{12}e_{12})e_{21} = a_{12}e_{11} \\ e_{12}ae_{11} &= e_{12}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{11} = (a_{21}e_{11} + a_{22}e_{12})e_{11} = a_{21}e_{11} \\ e_{12}ae_{21} &= e_{12}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{21} = (a_{21}e_{11} + a_{22}e_{12})e_{21} = a_{22}e_{11}. \end{aligned}$$

Também podemos observar

$$\begin{aligned} e_{21}ae_{12} &= e_{21}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{12} = (a_{11}e_{21} + a_{22}e_{12})e_{12} = a_{11}e_{22} \\ e_{21}ae_{22} &= e_{21}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{22} = (a_{11}e_{21} + a_{22}e_{12})e_{22} = a_{12}e_{22} \\ e_{22}ae_{12} &= e_{22}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{12} = (a_{21}e_{11} + a_{22}e_{12})e_{12} = a_{21}e_{22} \\ e_{22}ae_{22} &= e_{22}(a_{11}e_{11} + a_{12}e_{12} + a_{21}e_{21} + a_{22}e_{22})e_{22} = (a_{21}e_{11} + a_{22}e_{12})e_{22} = a_{22}e_{22}. \end{aligned}$$

Os cálculos acima mostram que se $a = (a_{ij})$ então

$$e_{1i} \cdot a \cdot e_{j1} = a_{ij} \cdot e_{11} \text{ e } e_{2i} \cdot a \cdot e_{j2} = a_{ij} \cdot e_{22}. \tag{1.4}$$

Agora estamos em condições de mostrar que os únicos ideais de M_2 são os triviais.

Seja I um ideal de M_2 e vamos assumir que $I \neq \{0\}$. Assim I contém uma matriz a não nula, isto é, a possui algum elemento não nulo $a_{rs} \neq 0$. Segue das relações em 1.4 e da definição de ideal que

$$e_{1r} \cdot a \cdot e_{s1} = a_{rs} e_{11} \in I \text{ e } e_{2r} \cdot a \cdot e_{s2} = a_{rs} e_{22} \in I.$$

Daí concluimos que

$$\begin{pmatrix} a_{rs} & 0 \\ 0 & a_{rs} \end{pmatrix} = \begin{pmatrix} a_{rs} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_{rs} \end{pmatrix} \in I,$$

assim

$$\begin{pmatrix} a_{rs}^{-1} & 0 \\ 0 & a_{rs}^{-1} \end{pmatrix} \cdot \begin{pmatrix} a_{rs} & 0 \\ 0 & a_{rs} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I.$$

Como $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o elemento unidade do anel M_2 segue que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I$$

para quaisquer $a, b, c, d \in \mathbb{R}$, isto é, $I = M_2$. Acabamos de provar que se I é um ideal de M_2 então $I = \{0\}$ ou $I = M_2$.

O exemplo seguinte será importante para os nossos objetivos.

Exemplo 1.1.14. *Seja A um anel comutativo e $a \in A$. O conjunto $\langle a \rangle = \{ax \mid x \in A\}$ é um ideal de A.*

De fato, vamos mostrar que o conjunto $\langle a \rangle$ satisfaz as propriedades (i)-(iv) da Definição 1.1.13.

(i) Como $0 = a \cdot 0$ (Proposição 1.1.5 (i)), temos que $0 \in \langle a \rangle$.

(ii) Sejam $b, c \in \langle a \rangle$. Assim $b = ax$ e $c = ay$ com $x, y \in A$. Como $b + c = ax + ay = a(x + y)$ (Definição 1.1.1 (6)) segue que $b + c \in \langle a \rangle$.

(iii) Dado $b \in \langle a \rangle$, temos $b = ax$ com $x \in A$. Como $-b = -(ax) = a(-x)$ (Proposição 1.1.5 (ii)), segue que $-b \in \langle a \rangle$.

(iv) Dados $b \in \langle a \rangle$ e $c \in A$, temos $b = ax$ com $x \in A$. Como $bc = (ax)c = a(xc)$ (Definição 1.1.1 (5)) temos que $bc \in \langle a \rangle$. Nesta segunda parte, usaremos a comutatividade: $cb = c(ax) = (ca)x = (ac)x = a(cx)$; logo $cb \in \langle a \rangle$. □

Proposição 1.1.15. *Todo ideal de $\mathbb{Z}$ é da forma $\langle d\rangle = \{dn \mid n \in \mathbb{Z}\}$ para algum $d \in \mathbb{Z}$.*

Demonstração. Seja J um ideal de $\mathbb{Z}$. Se $J = \{0\}$ então $J = \langle 0\rangle$. Suponhamos que $J \neq \{0\}$. Assim existe $a \in J$ com $a \neq 0$, e temos $-a \in J$. Portanto o conjunto $S = \{a \in J \mid a > 0\}$ é não vazio. Pelo Principio da Boa Ordem (Proposição 1.1.10) o conjunto J possui mínimo $d > 0$. Vamos provar que $J = \langle d\rangle$.

Notamos que $\langle d\rangle \subseteq J$ porque se $d \in J$ e $n \in \mathbb{Z}$ então $dn \in J$ pois J absorve produtos à direita. Assim é suficiente provarmos que $J \subseteq \langle d\rangle$.

Seja $b \in J$ um elemento qualquer. Pelo Algoritmo da Divisão (Proposição 1.1.11) existem $q, r \in \mathbb{Z}$ tais que

$$b = qd + r \text{ onde } 0 \leq r < d.$$

Daí segue que $0 \leq r = b - qd < d$. Como b e $q \cdot d$ pertencem a J segue que $r \in J$ com $0 \leq r < d$.

Pela minimalidade de d segue que $r = 0$ e portanto $b = qd \in J$. Portanto $J \subseteq \langle d\rangle$ e consequentemente $J = \langle d\rangle$ □

A Proposição 1.1.15 nos dá uma forma para todos os ideais de $\mathbb{Z}$. Note que a chave da demonstração está no uso do Algoritmo da Divisão, ou seja, está fato de $\mathbb{Z}$ ser um anel euclidiano.

De fato, a demonstração da Proposição 1.1.15 pode ser estendida para anéis euclidianos quaisquer, usando a função $d : A \longrightarrow \mathbb{N}$ dada na Definição 1.1.6 no lugar do valor absoluto $d(a) = |a|$, que aparece na Proposição 1.1.11.

Se a é um elemento de um anel comutativo A, fixemos a seguinte notação:

$$\langle a\rangle = \{ax \mid x \in A\}.$$

Proposição 1.1.16. *Seja A um anel euclidiano e I um ideal de A. Então $I = \langle a\rangle$ para algum $a \in A$.*

Demonstração. Se $I = \{0\}$, como $0 = 0 \cdot x$ para todo $x \in A$ (Proposição 1.1.5 (i)), temos que $I = \langle 0\rangle$. Assim podemos admitir que $I \neq \{0\}$, isto é, que existe $a \in I$ não nulo. Seja $a \in I$ tal que $d(a)$ seja mínimo. Esse elemento existe porque a função d assume valores em $\mathbb{N}$ e a Proposição 1.1.10 pode ser aplicada no conjunto dos valores $d(x)$ com $x \in I$.

Seja $b \in I$. Existem $q, r \in A$ tais que $b = aq + r$ onde $r = 0$ ou $d(r) < d(a)$ (Definição 1.1.6 (i)). Como $a, b \in I$ e I é um ideal de A, segue que $r = b - aq$ pertence a I. Pela minimalidade de $d(a)$ não podemos ter $d(r) < d(a)$, logo deve ser $r = 0$, e portanto $b = aq$. Assim $I = \langle a\rangle$.□

Agora estamos prontos para introduzir o conceito de máximo divisor comum em anéis euclidianos quaisquer. Vamos começar com a definição de máximo divisor comum no anel $\mathbb{Z}$ dos inteiros.

Definição 1.1.17. *Sejam a e b inteiros quaisquer. Um inteiro $d > 0$ chama-se máximo divisor comum de a e b se as duas condições abaixo são satisfeitas:*

(i) $d \mid a$ *e* $d \mid b$*;*

(ii) Se $c \mid a$ *e* $c \mid b$*, então* $c \mid d$*.*

Note que as condições (i) e (ii) da definição acima implicam que d é de fato o maior inteiro positivo que divide a e b.

Para ver isso, observe que se um inteiro c é tal que $c \mid a$ e $c \mid b$, então, pela condição (ii) da Definição 1.1.17 devemos ter $c \mid d$. Logo $d = cc_1$, e isso implica que $c \leq d$.

Note também que um máximo divisor comum de a e b, se existir, é único.

Para ver isso observe que se d e d' forem máximos divisores comuns de a e b, então

$$d \mid a \text{ e } d \mid b \Rightarrow d \mid d' \text{ e } d' \mid a \text{ e } d' \mid b \Rightarrow d' \mid d.$$

Como $d \mid d'$ implica $d \leq d'$ e $d' \mid d$ implica $d' \leq d$, temos $d = d'$.

Porém a Definição 1.1.17 não garante a existência do máximo divisor comum. Vamos provar isso como uma consequência do fato de que todo ideal de $\mathbb{Z}$ ser da forma $\langle d \rangle = \{dn \mid n \in \mathbb{Z}\}$ para algum $d \in \mathbb{Z}$ (Proposição 1.1.15). Comecemos com o

Exemplo 1.1.18. *Para quaisquer* $a, b \in \mathbb{Z}$ *o conjunto* $J = \{ma + nb \mid m, n \in \mathbb{Z}\}$ *é um ideal* $\mathbb{Z}$*.*

Vamos mostrar que J possui as propriedades (i)-(iv) da Definição 1.1.13.

(i) $0 \in J$ pois $0 = 0 \cdot a + 0 \cdot b$.

(ii) Se x e y pertencem a J, então $x = ma + nb$ e $y = m'a + n'b$. Assim

$$x + y = (ma + nb) + (m'a + n'b) = (m + m')a + (n + n')b,$$

e portanto $x + y$ pertence a J.

(iii) Se $x = ma + nb$ pertence a J então

$$-x = -(ma + nb) = (-1)(ma + nb) = (-1)(ma) + (-1)(nb) = (-m)a + (-n)b.$$

Logo $-x$ pertence a J.

(iv) Dados $x = ma + nb \in J$ e $c \in \mathbb{Z}$ temos que $xc = (ma + nb)c = m(ac) + n(bc) \in J$. Como $\mathbb{Z}$ é um anel comutativo, $xc = cx \in J$.

Proposição 1.1.19. *Quaisquer dois inteiros* a *e* b *em* $\mathbb{Z}$ *possui máximo divisor comum* d*. Mais ainda, existem inteiros* r *e* s *tais que* $d = ra + sb$*.*

Demonstração. Pela Proposição 1.1.15 o ideal $J = \{ma + nb \mid m, n \in \mathbb{Z}\}$ é da forma $J = \langle d \rangle$ para algum $d \in \mathbb{Z}$. Agora observe que $a = 1a + 0b \in J$ e $b = 0a + 1b \in J$. Assim a e b são múltiplos de d, consequentemente $d \mid a$ e $d \mid b$. Agora observe que $J = \langle d \rangle$ implica a existência inteiros r e s tais que $d = ra + sb$. Se $c \mid a$ e $c \mid b$ então $c \mid ra$ e $c \mid sb$ (Proposição 1.1.8 (iii)), logo c divide $ra + sb = d$ (Proposição 1.1.8 (i)). Mostramos, portanto, a existência do máximo divisor comum de dois inteiros quaisquer. □

Lema 1.1.20. *Para quaisquer a e b em um anel comutativo A, o conjunto $J = \{\lambda a + \mu b \mid \lambda, \mu \in A\}$ é um ideal de A.*

A demostração de que $J = \{\lambda a + \mu b \mid \lambda, \mu \in A\}$ é um ideal de A é a mesma do Exemplo 1.1.18, bastando trocar os símbolos m e n por λ e μ, respectivamente.

Trataremos a seguir do máximo divisor comum em anéis euclidianos quaisquer.

Definição 1.1.21 (Máximo Divisor Comum)**.** *Sejam a e b elementos de um anel euclidiano A. Dizemos que $d \in A$ é máximo divisor comum de a e b, denotado por $d = (a, b)$, quando as duas condições abaixo forem satisfeitas:*

(i) $d \mid a$ *e* $d \mid b$.

(ii) Se $c \mid a$ *e* $c \mid b$, *então* $c \mid d$.

Proposição 1.1.22. *Se A é um anel euclidiano, então A possui elemento unidade.*

Demonstração. Seja A um anel euclidiano. Como A é um ideal de A, segue da Proposição 1.1.16 que $A = \langle u_0 \rangle$ para algum $u_0 \in A$. Assim todo elemento em A é um múltiplo de u_0. Portanto, em particular, $u_0 = u_0 c$ para algum $c \in R$. Se $a \in A$, então $a = x u_0$ para algum $x \in A$, donde $ac = (x u_0)c = x(u_0 c) = x u_0 = a$. Vemos assim que c é o elemento unidade requerido. □

A proposição seguinte garante a existência de máximo divisor comum entre dois elementos quaisquer de um anel euclidiano.

Proposição 1.1.23. *Seja A um anel euclidiano. Então quaisquer elementos a e b em A possui um máximo divisor comum d. Mais ainda, existem $\lambda, \mu \in A$ tais que $d = \lambda a + \mu b$.*

Demonstração. Seja $J = \{xa + yb \mid x, y \in A\}$. Como J é um ideal A (Lema 1.1.20), segue da Proposição 1.1.16 que existe um elemento $d \in A$ tal que $J = \langle d \rangle$. Logo $d = \lambda a + \mu b$ para certos $\lambda, \mu \in A$. Ora, pela Proposição 1.1.22, A possui elemento unidade 1, assim $a = 1a + 0b \in J$ e $b = 0a + 1b \in J$. Como $J = \langle d \rangle$, segue que $d \mid a$ e $d \mid b$.

Suponhamos, finalmente, que $c \mid a$ e $c \mid b$, então $c \mid \lambda a$ e $c \mid \mu b$ (Proposição 1.1.8 (iii)), de modo que c divide $\lambda a + \mu b = d$ (Proposição 1.1.8 (i)). Portanto d satisfaz as duas condições da Definição 1.1.21 e assim d é o máximo divisor comum de a e b. □

1.1.3 ELEMENTOS PRIMOS

Nesta seção vamos estender o conceito de número primo à anéis euclidianos quaisquer. A propriedade mais importante de um primo p em $\mathbb{Z}$ é que se p divide ab, então p divide a ou p divide b.

Veremos que essa propriedade pode ser estendida para um anel euclidiano qualquer.

Definição 1.1.24. *Seja A um anel comutativo com elemento unidade. Um elemento $a \in A$ é uma unidade em A se existir um elemento $b \in A$ tal que $ab = 1$.*

Por exemplo, as unidades do anel $\mathbb{Z}$ são 1 e -1. De fato, a equação $ab = 1$ admite soluções em $\mathbb{Z}$ apenas quando $a = \pm 1$.

Veremos, como uma consequência da Proposição 3.3.1, que as unidades do anel dos inteiros gaussianos $\mathbb{Z}[i]$ são $1, -1, i$ e $-i$.

Note que *unidade* e *elemento unidade* são conceitos diferentes. Por exemplo, já vimos, no início deste capítulo, que se um anel possuir elemento unidade ele é único. Como vimos nos exemplos acima, um anel pode possuir mais de uma unidade.

Definição 1.1.25. *Em um anel euclidiano A dizemos que $\pi \in A$ é um elemento primo se π não for uma unidade e se $\pi = ab$ implicar que a ou b são unidades.*

Assim, dizemos que um elemento é primo quando não puder ser fatorado de maneira não trivial.

Como as unidades de $\mathbb{Z}$ são ± 1, segue da Definição 1.1.25 que p é um elemento primo de $\mathbb{Z}$ se $p \neq \pm 1$ e os únicos divisores de p são ± 1 e $\pm p$. Aqui está uma pequena lista de elementos primos de $\mathbb{Z}$: $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29$ *e* ± 31.

Como observado por Herstein, na fatoração, os primos negativos não introduzem diferenças essenciais (Herstein, 2005, p. 22). De fato, observe, por exemplo, que $10 = 2 \cdot 5 = (-2) \cdot (-5)$.

Assim, seguindo Herstein (2005), daremos a seguinte definição para elemento primo em $\mathbb{Z}$, que chamaremos apenas de primo:

Definição 1.1.26. *Um inteiro $p \in \mathbb{Z}$ é primo se $p > 1$ e os únicos divisores positivos de p são 1 e o próprio p. Se um inteiro não é primo, diremos que ele é composto.*

Aqui está a lista dos primeiros 20 primos inteiros:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.$$

Note que 5 é primo em $\mathbb{Z}$ mas não é primo em $\mathbb{Z}[i]$. De fato $5 = 2^2 + 1^2 = (2+i)(2-i)$, que é uma fatoração não trivial de 5 em $\mathbb{Z}[i]$.

Mais geralmente, se p é um inteiro primo e $p = a^2 + b^2$ com a, b inteiros, então $p = (a+bi)(a-bi)$. Logo p não é um primo em $\mathbb{Z}[i]$. Veremos, no Corolário 3.3.3, que um primo $p \in \mathbb{Z}$ é primo em $\mathbb{Z}[i]$ se, e somente se, $p = 4k + 3$, para algum $k \in \mathbb{Z}$.

Se um inteiro primo p não divide a, então $(p, a) = 1$, isto é, o máximo divisor comum de p e a é 1. Segue da Proposição 1.1.19 que existem inteiros r e s tais que $pr + as = 1$. Vamos escrever esse resultado na forma do

Lema 1.1.27. *Se p é um inteiro primo que não divide um inteiro a, então existem inteiros r e s tais que $pr + as = 1$.*

Agora estamos em condição de provar o principal resultado sobre inteiros primos deste capítulo.

Proposição 1.1.28. *Seja p um inteiro primo e a, b inteiros quaisquer. Se $p \mid ab$ então $p \mid a$ ou $p \mid b$.*

Demonstração. Suponha que p divida ab mas que p não divida a; vamos mostrar que p divide b. De p não dividir a segue do Lema 1.1.27 que existem inteiros r e s tais que $pr + as = 1$. Multiplicando ambos os membros dessa igualdade por b, temos que

$$p(rb) + (ab)s = b.$$

Como $p \mid ab$ e $p \mid p$, segue da Proposição 1.1.8 (iii) que p divide prb e p divide abs. Logo p divide a soma $p(rb) + (ab)s$ (Proposição 1.1.8 (i)). Assim $p \mid b$. □

Agora estamos em condições de estender a Proposição 1.1.28 para anéis euclidianos quaisquer. Usaremos um lema análogo ao Lema 1.1.27:

Lema 1.1.29. *Seja A um anel euclidiano com $a, b, c \in A$. Se $a \mid bc$ e $(a, b) = 1$ então $a \mid c$.*

Demonstração. Como vimos na Proposição 1.1.23, o máximo divisor comum de a e b pode ser escrito na forma $\lambda a + \mu b$ com $\lambda, \mu \in A$. Como supomos $(a, b) = 1$, segue que existem $\lambda, \mu \in A$ tais que $\lambda a + \mu b = 1$. Multiplicando ambos os membros dessa igualdade por c, obtemos $\lambda ac + \mu bc = c$. Com $a \mid bc$, por hipótese, e $a \mid a$, segue da Proposição 1.1.8 que $a \mid \lambda ac$ e $a \mid \mu bc$. Portanto a divide a soma $\lambda ac + \mu bc = c$, provando o lema. □

Proposição 1.1.30. *Seja π um elemento primo em um anel euclidiano A. Se $\pi \mid ab$, onde $a, b \in A$, então $\pi \mid a$ ou $\pi \mid b$.*

Demonstração. Se π não divide a então $(\pi, a) = 1$. Pelo Lema 1.1.29 segue que $\pi \mid b$.

2 ALGUNS TEOREMAS SOBRE NÚMEROS PRIMOS

Neste capítulo, à menos que o contrário seja explicitado, estaremos trabalhando no anel $\mathbb{Z}$ dos inteiros. Continuaremos estudando algumas propriedades desse anel.

O objetivo principal deste capítulo é demostrar o Teorema de Euler, que é o seguinte: Seja p um número primo ímpar. Então a congruência $x^2 \equiv -1 \pmod{p}$ tem uma solução se, e somente se, $p \equiv 1 \pmod{4}$.

Para provarmos esse Teorema de Euler utilizaremos o Pequeno Teorema de Fermat e o Teorema de Wilson.

2.1 A INFINIDADE DOS NÚMEROS PRIMOS

Tomando um inteiro qualquer $n > 1$, notamos que n é primo ou não é primo. Se ele não for primo, então ele é composto, isto é $n = ab$ onde $a > 1$ e $b > 1$. Por exemplo:

$$4 = 2 \cdot 2,\ 18 = 3 \cdot 6,\ 105 = 3 \cdot 35.$$

Prosseguindo, perguntamos se a ou b são ou não primos. Se algum deles for primo, cessamos a fatoração. Se algum deles for composto, então o escrevemos como um produto de dois inteiros maiores do que 1:

$$4 = 2 \cdot 2,\ 18 = 3 \cdot 3 \cdot 2,\ 105 = 3 \cdot 5 \cdot 7.$$

Assim, começando com um inteiro qualquer $n > 1$, podemos sempre escrevê-lo como um produto de fatores primos. Mais ainda, essa decomposição de n em fatores primos é única. Esse é o conteúdo do Teorema Fundamental da Arimética.

Proposição 2.1.1 (Teorema Fundamental da Aritmética)**.** *Todo inteiro maior do que* 1 *pode ser decomposto em fatores primos de maneira única, a menos da ordem dos fatores.*

Demonstração. Vamos provar primeiramente que todo inteiro $n > 1$ pode ser decomposto em um produto de fatores primos. Se n é primo não há nada a ser demonstrado. Suponha que n seja composto. Seja $p_1 > 1$ o menor dos divisores positivos de n (que existe, pelo Princípio da Boa Ordenação). Afirmamos que p_1 é primo. De fato, se p_1 fosse composto, então existiria $m > 1$ tal que $m \mid p_1$ com $1 < m < p_1$. Assim $m \mid n$ com $1 < m < p_1$, o que contraria a minimalidade de p_1. Logo $n = p_1 \cdot n_1$ com p_1 primo.

Se n_1 for primo terminamos. Caso contrário, tomanos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$ com p_1 e p_2 primos.

Repetindo esse procedimento, obtemos uma fatoração completa $n = p_1 p_2 p_3 \ldots p_r$ onde $p_1, p_2, \ldots, p_r$ são primos (não necessariamente distintos).

Agora vamos provar a unicidade dessa decomposição de n em fatores primos.

Chamamos de *anormais* os inteiros positivos que podem ser fatorados em primos de mais de uma maneira. Seja n o menor inteiro anormal. Um mesmo primo p não pode aparecer em duas fatorações diferentes de n, caso contrário, n dividido por p (que chamaremos de m) seria anormal com $m < n$, contrariando a minimalidade de n. Temos então que

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s,$$

onde os p_i e q_j são primos, nenhum p_i é igual a qualquer q_j e vice-versa.

Podemos tomar p_1 como o menor dos primos p_i. Como n é composto, temos $p_1^2 \leq n$. Similarmente, se q_1 é o menor dos primos q_j, então $q_1^2 \leq n$. Assim

$$p_1^2 q_1^2 \leq nn \Rightarrow (p_1 q_1)^2 \leq n^2 \Rightarrow p_1 q_1 \leq n.$$

Afirmamos que $p_1 q_1 < n$. Com efeito, se fosse $n = p_1 q_1$, então

$$p_1^2 \leq n = p_1 q_1 \Rightarrow p_1 \leq q_1 \text{ e } q_1^2 \leq n = p_1 q_1 \Rightarrow q_1 \leq p_1.$$

Assim teríamos $p_1 = q_1$, o que não é possível. Definindo $N = n - p_1 q_1$, como $0 < N < n$ segue que N não é anormal.

Agora, como $p_1 \mid n$, temos que $p_1 \mid N$. Do mesmo modo, $q_1 \mid N$. Portanto, p_1 e q_1 aparecem na fatoração única de N e portanto $p_1 q_1 \mid N$. Disso, segue-se que $p_1 q_1 \mid n$ e, consequentemente, q_1 divide o inteiro $\dfrac{n}{p_1} = p_2 \dots p_r$.

Mas $\dfrac{n}{p_1}$ é menor que n e, portanto, tem fatoração única em primos. Como q_1 não é igual a nenhum dos p_i, temos uma contradição. Logo, não pode haver números anormais e isso demonstra a unicidade da decomposição de n em fatores primos. □

O matemático grego Euclides (300 a.C) foi o primeiro a provar que a lista dos números primos é infinita.

Proposição 2.1.2 (Euclides)**.** *O conjunto dos números primos é infinito.*

Demonstração. Suponha o contrário, que $p_1, p_2, p_3, ..., p_n$ seja a lista finita de todos os primos existentes. Consideremos o número $N = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$. Observe que N é maior do que qualquer dos primos dessa lista, logo N deve ser um número composto. Pelo Teorema Fundamental da Aritmética, N pode ser escrito como um produto de fatores primos. Como todos os primos existentes estão na lista $p_1, p_2, \dots, p_n$, segue que existe um primo p_i dessa lista que divide N. Mas isso é uma contradição porque a igualdade $N = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$ implica que N dividido por p_i deixa resto 1. Portanto a lista dos números primos é infinita. □

2.2 ALGUNS RESULTADOS DE FERMAT

O *Princípio da Boa Ordem* também é conhecido como *método da descida de Fermat* e foi a ferramenta usada por ele para estabelecer uma porção de resultados curiosos; entre eles está a proposição seguinte (Guzmán, 1991).

Proposição 2.2.1. *A equação $x^2 + y^2 = 3z^2$ admite apenas a solução nula em $\mathbb{Z}$.*

Demonstração. Suponha que a equação $x^2 + y^2 = 3z^2$ admita uma solução não nula (x, y, z). Vejamos quais propriedades teria essa solução. Se x for múltiplo de 3, isto é, $x = 3q_1$, então

$$y^2 = 3z^2 - (3q_1)^2 = 3(z^2 - 3{q_1}^2)$$

isto é, y^2 é multiplo de 3, e isso implica, pela Proposição 1.1.28, que y é múltiplo de 3. Segue que se x ou y forem múltiplo de 3, então x *e* y serão múltiplos de 3. Observe que se um número não é múltiplo de 3, então ele pode ser escrito como $3q + 1$ ou $3q - 1$ (Corolário 1.1.12), e seus respectivos quadrados são

$$(3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1,$$
$$(3q - 1)^2 = 9q^2 - 6q + 1 = 3(3q - 2) + 1.$$

Então, se ambos x *e* y não são múltiplos de 3, temos

$$x^2 + y^2 = (3q + 1) + (3q' + 1) = 3(q + q') + 2$$

que não é múltiplo de 3. Mostramos que se (x, y, z) é uma solução da equação $x^2 + y^2 = 3z^2$, então x *e* y são múltiplos de 3. Sejam então $x = 3x_1$, $y = 3y_1$, e assim podemos escrever

$$3z^2 = x^2 + y^2 = 3^2{x_1}^2 + 3^2{y_1}^2 = 9({x_1}^2 + {y_1}^2)$$

Portanto, ${z}^2 = 3({x_1}^2 + {y_1}^2)$, o que mostra que z^2 é múltiplo de 3 e isso implica que z também é múltiplo de 3. Pondo $z = 3z_1$ e substituindo na última igualdade,temos

$$3^2{z_1}^2 = 3({x_1}^2 + {y_1}^2),$$

ou seja

$$3{z_1}^2 = ({x_1}^2 + {y_1}^2)$$

Portanto, se (x, y, z) for uma solução da equação $x^2 + y^2 = 3z^2$ então $x = 3x_1, y = 3y_1$ *e* $z = 3z_1$ com ${x_1}^2 + {y_1}^2 = 3{z_1}^2$. Agora, observe que se (x, y, z) for uma solução não nula da equação então $x \neq 0$ *ou* $y \neq 0$. Podemos supor, sem perca de generelidade, que $x \neq 0$. Como $(-x, y, z)$ também é uma solução da equação, $x^2 + y^2 = 3z^2$ segue que existe uma solução (x, y, z) com $x > 0$. Segue do Princípio da boa ordem que dentre todas as soluções da equação existe uma solução (x_1, y_1, z_1) com $x_1 > 0$ e x_1 o menor possível. Mas pelo que vimos no argumento acima, $x_1 = 3x_2, y_1 = 3y_2$ *e* $z_1 = 3z_2$ onde (x_2, y_2, z_2) é

uma solução da equação; e isso viola a minimalidade de x_1. Logo a equação $x^2 + y^2 = 3z^2$ não admite solução além de $(0,0,0)$. □

Uma consequência da proposição acima é que $\sqrt{3}$ é irracional. De fato, se existisse inteiros a e b tais que, $\sqrt{3} = \frac{a}{b}$ então $3 = \frac{a^2}{b^2} \Rightarrow a^2 + 0^2 = 3b^2$, o que não é possível pois $(a,0,b)$ seria uma solução não nula da equação $x^2 + y^2 = 3z^2$.

O seguinte resultado é atribuido a Fermat, veja Eves (2011, p. 391), Boyer (1974, p. 249) ou Cajori (1909, p. 210).

Proposição 2.2.2. *Todo primo ímpar pode ser expresso de maneira única como a diferença de dois quadrados.*

Demonstração. Se $p = a^2 - b^2$, então $p = (a+b)(a-b)$. Mas, como p é primo, os únicos fatores de p são 1 e p; daí, $a+b = p$ e $a-b = 1$. Somando membro à membro $a+b = p$ e $a-b = 1$, temos $2a = p+1$. Como p é ímpar podemos escrever

$$a = \frac{p+1}{2}.$$

Agora, subtraindo membro à membro $a+b = p$ e $a-b = 1$, temos

$$a+b-(a-b) = p-1 \Rightarrow 2b = p-1 \Rightarrow b = \frac{p-1}{2}.$$

Portanto todo primo p se escreve que maneira única como $p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$. □

A proposição acima dá uma resposta para o seguinte problema: quais números primos podem ser escritos como uma diferença de dois quadrados? A resposta: todos os primos ímpares.

Observe que o primo 2 não pode ser a diferença de dois quadrados. De fato, se fosse $2 = a^2 - b^2 = (a-b)(a+b)$, então temos as duas possibilidades:

$$a-b = 1 \text{ e } a+b = 2 \text{ ou ainda } a-b = 2 \text{ e } a+b = 1.$$

Somando membro à membro em qualquer dos dois casos acima temos $2a = 3$, que não possui solução inteira.

A proposição abaixo nos dá uma condição necessária para que um inteiro seja uma soma de dois quadrados.

Proposição 2.2.3. *Se um primo p é soma de dois quadrados então $p = 2$ ou $p = 4k+1$.*

Demonstração. Seja n um inteiro que é uma soma de dois quadrados, isto é $n = a^2 + b^2$ com $a, b \in \mathbb{Z}$. Se a e b forem pares, digamos $a = 2r$ e $b = 2s$, então

$$a^2 + b^2 = (2r)^2 + (2s)^2 = 4r^2 + 4s^2 = 4(r^2 + s^2).$$

Se a for par e b for ímpar, digamos $a = 2r$ e $b = 2s+1$, então

$$a^2 + b^2 = (2r)^2 + (2s+1)^2 = 4r^2 + 4s^2 + 4s + 1 = 4(r^2 + s^2 + s) + 1.$$

Se a e b forem ímpares, digamos $a = 2r+1$ e $b = 2s+1$, então

$$a^2 + b^2 = (2r+1)^2 + (2s+1)^2 = 4r^2 + 4r + 1 + 4s^2 + 4s + 1 = 4(r^2 + k + s^2 + s) + 2.$$

Então em qualquer dos casos n é da forma $4k, 4k+1$ *ou* $4k+2$, onde $k \in \mathbb{Z}$. Em particular, se n é primo, então $n = 2$ ou $n = 4k+1$. □

Veremos que se um primo p é da forma $p = 4k+1$ então p é uma soma de dois quadrados (Teorema 3.4.2). Como $2 = 1^2 + 1^2$, esse teorema mostra que a recíproca da Proposição 2.2.3 é verdadeira.

A definição seguinte introduz a noção de congruência entre números inteiros. Alguns teoremas clássicos sobre inteiros são apresentados com esta notação de congruência.

Definição 2.2.4. *Sejam a, b, n inteiros com $n > 0$. Dizemos que a é congruente a b módulo n, denotado por $a \equiv b \pmod{n}$, se $n \mid (a-b)$, isto é, se $a - b = nq$ para algum inteiro q.*

Por exemplo, $10 \equiv 2 \pmod{4}$ pois 4 divide a diferença $10 - 2 = 8$. A relação de congruência $\equiv$ permite estabelecer propriedades análogas àquelas do anel $\mathbb{Z}$.

Proposição 2.2.5. *Se a, b, c, d e n são inteiros com $n > 1$ e tais que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então*

(i) $a + c \equiv b + d \pmod{n}$

(ii) $a - c \equiv b - d \pmod{n}$

(iii) $ac \equiv bd \pmod{n}$

Demonstração.

(i) De $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ temos $a - b = nk_1$ e $c - d = nk_2$. Somando membro a membro obtemos $(a+c) - (b+d) = n(k_1 + k_2)$ e isto implica que $a + c \equiv b + c \pmod{n}$.

(ii) Como $a - c = a + (-c)$ e $b - d = b + (-d)$, segue do item (i) que $a - c \equiv b - d \pmod{n}$.

(iii) Multiplicando ambos os membros de $a - b = nk_1$ por c e ambos os membros de $c - d = nk_2$ por b, obtemos $ac - bc = nk_1 c$ e $bc - bd = nbk_2$. Agora, somando membro a membro essas duas últimas igualdades, obtemos $ac - bc + bc - bd = nk_1 c + nbk_2$, isto é $ac - bd = n(ck_1 + bk_2)$, o que implica $ac \equiv bd \pmod{n}$. □

A notação de congruência também é útil para estabelecer equações. O resultado seguinte será usado nas demonstrações de dois teoremas clássicos sobre os inteiros: o Pequeno Teorema de Fermat e o Teorema de Wilson.

Proposição 2.2.6. *Seja p um primo que não divide a. Então a congruência $ax \equiv 1 \pmod{p}$ possui uma única solução no conjunto $\{1,2,\ldots,p-1\}$.*

Demonstração. Como $(p,a) = 1$, segue do Lema 1.1.27 que existem inteiros k e b tais que $pk + ab = 1$. Assim $ab - 1 = p(-k)$, isto é, p divide $ab-1$ e portanto $ab \equiv 1 \pmod{p}$. Note que essa última congruência também implica que p não divide b (porque se p dividisse b então p também dividiria ab). Assim b é solução da equação $ax \equiv 1 \pmod{p}$.

Por outro lado, segue do Algoritmo da Divisão (Proposição 1.1.11) que existem únicos inteiros q e r tais que $b = pq + r$ com $0 \leq r < p$. Como p não divide b, segue que b é congruente módulo p a exatamente um dos inteiros $1,2,\ldots,p-1$. □

Proposição 2.2.7 (Pequeno Teorema de Fermat)**.** *Seja p um número primo. Se p não divide a então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração. Considere a lista de números $a, 2a, 3a, \ldots, (p-1)a$. Como $(a,p) = 1$, segue da Proposição 1.1.28 que nenhum destes números ja, $1 \leq j \leq p-1$ é divisível por p, ou seja, nenhum deles é congruente a zero módulo p.

Agora considere dois números quaisquer aj e ak na lista $a, 2a, 3a, \ldots, (p-1)a$. Se fosse $aj \equiv ak \pmod{p}$, então p dividiria $aj - ak = a(j-k)$. Mas isso não é possível porque p não divide a e p não divide $j-k$. Assim cada um dos números $a, 2a, 3a, \ldots, (p-1)a$ é congruente a exatamente um dentre os números $1,2,3,\ldots,p-1$.

Assim podemos aplicar a Proposição 2.2.5 (iii) e obter a congruência

$$(2a)(3a)\ldots(p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p},$$

ou seja $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Então p divide $a^{p-1}(p-1)! - (p-1)! = (a^{p-1}-1)(p-1)!$. Como p não divide $(p-1)!$ segue da Proposição 1.1.28 que p divide $a^{p-1}-1$, isto é $a^{p-1} \equiv 1 \pmod{p}$, o que conclui a demonstração. □

Proposição 2.2.8 (Teorema de Wilson)**.** *Se p é um número primo, então*

$$(p-1)! \equiv -1 \pmod{p}.$$

Demonstração.

Como $(2-1)! \equiv 1 \equiv -1 \pmod{2}$ o resultado é válido para $p = 2$. Segue da Proposição 2.2.6 que, para cada $a \in \{1,2,3,\ldots,p-1\}$, a congruência $ax \equiv 1 \pmod{p}$ possui uma única solução $x \in \{1,2,3,\ldots,p-1\}$.

Observe que se $a = 1$ então a solução de $ax \equiv 1 \pmod{p}$ é $x = 1$. Se $a = p-1$, então a solução de $ax \equiv 1 \pmod{p}$ é $x = p-1$ pois $(p-1)^2 = p^2 - 2p + 1$, que é congruente a 1 módulo p.

Afirmamos que $a = 1$ e $a = p-1$ são os únicos valores de a para os quais $a^2 \equiv 1 \pmod{p}$. De fato, se $a^2 \equiv 1 \pmod{p}$ então $p \mid (a^2-1)$, isto é $p \mid (a-1)(a+1)$. Assim $p \mid a-1$ ou $p \mid a+1$. Se $p \mid (a-1)$ então $a-1 = pk$, que implica $a \equiv 1 \pmod{p}$. Se $p \mid (a+1)$ então $a+1 = pk$, que implica $a \equiv -1 \equiv p-1 \pmod{p}$.

Assim podemos agrupar os números $2,3,\ldots,p-2$ em pares a,b de números distintos tais que $ab \equiv 1 \pmod{p}$. Pela Proposição 2.2.5 (iii) podemos multiplicar todos esse pares e obter $2\cdot 3\cdot 4\cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$. Multiplicando-se ambos os lados dessa congruência por $p-1$, temos

$$2\cdot 3\cdot 4\cdot \ldots \cdot (p-2)(p-1) \equiv (p-1) \pmod{p},$$

isto é $(p-1)! \equiv -1 \pmod{p}$. Uma vez que $p-1 \equiv -1 \pmod{p}$, obtemos finalmente que $(p-1)! \equiv -1 \pmod{p}$. □

2.3 UM TEOREMA DE EULER

Estamos prontos para demonstrar o resultado mais importante deste capítulo.

Teorema 2.3.1 (Euler)**.** *Seja p um número primo ímpar. Então a congruência $x^2 \equiv -1 \pmod{p}$ tem uma solução se, e somente se, $p \equiv 1 \pmod{4}$.*

Demonstração. Suponha que a congruência $x^2 \equiv -1 \pmod{p}$ tenha uma solução. Então p divide x^2+1; e segue que p não divide x, caso contrário p dividiria x^2 e também dividiria a diferença $(x^2+1)-x^2 = 1$. Assim, o Pequeno Teorema de Fermat (Proposição 2.2.7) garante que $x^{p-1} \equiv 1 \pmod{p}$. De $x^2 \equiv -1 \pmod{p}$, segue da Proposição 2.2.5 (iii) que $(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$, isto é, $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Como $x^{p-1} \equiv 1 \pmod{p}$, temos

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

e portanto p divide $(-1)^{\frac{p-1}{2}} - 1$. Observe que a expressão $(-1)^{\frac{p-1}{2}} - 1$ só pode valer 0 ou 2. Se ela for igual a 2, então p dividiria 2, o que contradiz a suposição de que p é um primo ímpar. Portanto, deve ser $(-1)^{\frac{p-1}{2}} - 1 = 0$, ou seja, o expoente $\dfrac{p-1}{2}$ é par. Assim $\dfrac{p-1}{2} = 2k$, para algum inteiro k, o que implica $p = 4k+1$, isto é $p \equiv 1 \pmod{4}$.

Para mostrar a recíproca, vamos exibir uma solução para a congruência $x^2 \equiv -1 \pmod{p}$. Como p é ímpar, $p-1$ é par. Podemos escrever

$$(p-1)! = \left(1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\right)\cdot\left(\frac{p-1}{2}+1\right)\cdot\left(\frac{p-1}{2}+2\right)\cdot\ldots\cdot\left(\frac{p+1}{2}+\frac{p-3}{2}\right)\cdot\left(\frac{p-1}{2}+\frac{p-1}{2}\right).$$

Observe que

$$\begin{aligned} \frac{p-1}{2}+1 &= p-\frac{p-1}{2}, \qquad \frac{p-1}{2}+2 = (p+1)-\frac{p-1}{2}, \cdots \\ \cdots, \frac{p+1}{2}+\frac{p-3}{2} &= p-2, \qquad \frac{p-1}{2}+\frac{p-1}{2} = p-1. \end{aligned}$$

$$\begin{aligned} \textit{Assim } (p-1)! &= \left(1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\right)\cdot (p-1)\cdot (p-2)\cdot \ldots \cdot \left(p+1-\frac{p-1}{2}\right)\cdot \left(p-\frac{p-1}{2}\right), \\ &= \left(1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\right)\cdot (p-1)\cdot (p-2)\cdot \ldots \cdot\ p-\left(\frac{p-1}{2}-1\right)\cdot \left(p-\frac{p-1}{2}\right). \end{aligned}$$

Como $p-k \equiv -k \pmod{p}$, podemos escrever

$$\begin{aligned} (p-1)! &\equiv \left[1\cdot 2\cdot \ldots \cdot \left(\frac{p-1}{2}-1\right)\cdot \frac{p-1}{2}\right]\cdot (-1)(-2)\cdot \ldots \cdot \left[-\left(\frac{p-1}{2}-1\right)\right]\cdot \left(-\frac{p-1}{2}\right) \pmod{p}, \\ &\equiv (-1)^{\frac{p-1}{2}}\left(1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\right)^2 \pmod{p}. \end{aligned}$$

Como $p \equiv 1 \pmod 4$, temos que $p-1=4k$ e assim $\dfrac{p-1}{2}=2k$, um inteiro par, logo a congruência anterior torna-se

$$(p-1)! \equiv \left(1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}\right)^2 \pmod{p}.$$

Pondo $x = 1\cdot 2\cdot \ldots \cdot \dfrac{p-1}{2}$, temos $x^2 \equiv (p-1)! \pmod{p}$. Pelo Teorema de Wilson (Proposição 2.2.8), temos $(p-1)! \equiv -1 \pmod{p}$. Assim $x^2 \equiv -1 \pmod{p}$. □

Uma consequência interessante desse teorema de Euler é existência de um infinidade de primos da forma $4k+1$.

Proposição 2.3.2. *Existem infinitos primos da forma* $4k+1$.

Demonstração. Sejam $p_1, \ldots, p_r$ os primeiros r primos da forma $4k+1$. Como 5 é dessa forma, nossa lista não é vazia. Mostraremos que existe um primo p da forma $4k+1$ que não está na lista. Seja

$$N = (p_1 p_2 \cdots p_r)^2 + 1.$$

Seja p um divisor primo de N. Então

$$N = (p_1 p_2 \cdots p_r)^2 + 1 \equiv 0 \pmod{p}.$$

Como a congruência $x^2 \equiv -1 \pmod{p}$ possui solução (tome $x = p_1 p_2 \ldots p_r$) segue do Teorema 2.3.1 que $p \equiv 1 \pmod 4$ isto é, $p = 4k+1$ para algum $n \in \mathbb{N}$. Mas nenhum dos p_i divide N, logo p é diferente de todos $p_1, p_2, \ldots, p_r$. □

Há também uma infinidade de primos da forma $4k+3$.

Proposição 2.3.3. *Existem infinitos primos da forma* $4k+3$.

Demonstração. De fato, suponha que $p_1, p_2, \ldots, p_r$ sejam todos os primos da forma $4k+3$ e pondo, $N_r = 4\cdot p_1 \cdot p_2 \ldots p_r - 1$, observe que $N_r - 3 = 4p_1 p_2 \ldots p_r - 4 \equiv 0 \pmod 4$, isto é, N_r é da forma $4k+3$.

Agora observe que pela Proposição 2.2.5 (iii), se $a \equiv 1 \pmod 4$ e $b \equiv 1 \pmod 4$, então $ab \equiv 1 \pmod 4$. Assim, se todos os fatores primos de N_r fossem da forma $4k+1$, então N_r também seria dessa forma. Portanto N_r deve ter um fator primo p da forma $4k+3$.

Observe que esse primo p é diferente de todos $p_1, p_2, ..., p_r$, caso contrário p dividiria $4p_1p_2 \ldots p_r$; e como já divide N_r, pela Proposição 1.1.8 dividiria a diferença $N_r - 4p_1p_2 \ldots p_r = -1$, o que não é possível. A proposição está demonstrada. □

3 INTEIROS GAUSSIANOS

Neste capítulo vamos estudar algumas propriedades do anel dos inteiros gaussianos $\mathbb{Z}[i]$, incluída aí a prova de que $\mathbb{Z}[i]$ é um anel euclidiano. Isso garantirá a validade da Proposição 1.1.30 nesse anel. Essa proposição, juntamente com o Teorema de Euler (Teorema 2.3.1), nos permitirá provar o Lema 3.4.1, um resultado chave para provar o Teorema 3.4.4, que é o objetivo principal desta monografia.

3.1 NÚMEROS COMPLEXOS

Um número complexo é um número da forma $z = a + bi$ onde $a, b \in \mathbb{R}$ e $i^2 = -1$. O conjunto dos números complexos é denotado por $\mathbb{C} = \{a + bi \mid x, y \in \mathbb{R}\}$.

Em $\mathbb{C}$ estão definidas as operações de adição e multiplicação da seguinte maneira:

$$(a+bi)+(c+di) = (a+c)+(b+d)i, \tag{3.1}$$

$$(a+bi)(c+di) = ac-bd+(ad+bc)i. \tag{3.2}$$

Pode-se mostrar que as operações (3.1) e (3.2) tornam $\mathbb{C}$ um anel comutativo e com unidade.

O módulo de um número complexo $z = a + bi$ é definido por $|z| = \sqrt{a^2+b^2}$. O conjugado de um número complexo $z = a + bi$ é definido por $\overline{z} = a - bi$. Observe que

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

Proposição 3.1.1. *Sejam $z = a + bi$ e $w = c + di \in \mathbb{C}$; são válidas as seguintes propriedades*

(a) $|z| = 0 \Leftrightarrow z = 0$;

(b) $\overline{zw} = \overline{z} \cdot \overline{w}$.

Demonstração.

(a) Como $|z| = \sqrt{a^2+b^2}$, temos $|z| = 0 \Leftrightarrow |z|^2 = 0 \Leftrightarrow a^2+b^2 = 0 \Leftrightarrow$ $a = 0$ *e* $b = 0$.

(b) De fato

$$\overline{zw} = \overline{(a+bi)(c+di)} = \overline{ac-bd+(ad+cb)i} = ac-bd-(ad+bc)i = ac-bd-adi-bci$$
$$= ac-adi-bci-bd = a(c-di)-bi(c-di) = (a-bi)(c-di) = \overline{a+bi}\cdot\overline{c+di} = \overline{z}\cdot\overline{w}. \quad \square$$

Mais ainda, para qualquer $z \in \mathbb{C}$ com $z \neq 0$, existe $w \in \mathbb{C}$ tal que

$$zw = 1.$$

De fato, como $z =\neq 0$, segue da Proposição 3.1.1 (a) que $|z^{-1}| \neq 0$. Pondo $w = \overline{z}|z|^{-2}$ segue que $zw = z(\overline{z}|z|^{-2}) = (z\overline{z})|z|^{-2} = |z|^2|z|^{-2} = 1$. Esse número complexo w é chamado de inverso multiplicativo de z e é denotado por z^{-1} ou $\dfrac{1}{z}$.

A divisão z/w de um número complexo z por um número complexo $w \neq 0$ é definida por

$$\frac{z}{w} = z\frac{1}{w}.$$

3.2 O ANEL DOS INTEIROS GAUSSIANOS

Um inteiro gaussiano é um número complexo da forma $\alpha = a + bi$ onde a e $b \in \mathbb{Z}$ e $i^2 = -1$. Como já comentamos no Exemplo 1.1.3, o conjunto dos inteiros gaussianos

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

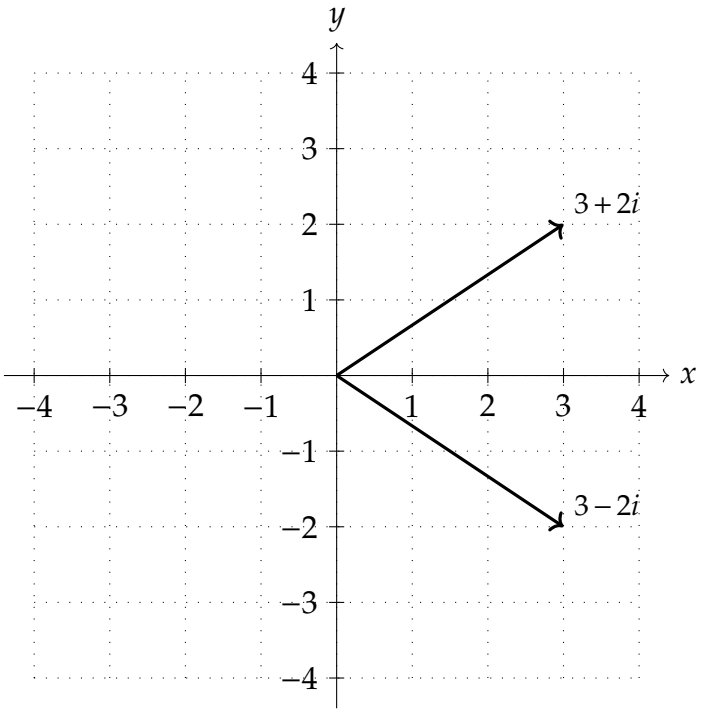
munido das operações

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

é um anel. Como já vimos na Seção 3.1, o conjugado de $\alpha = a + bi \in \mathbb{Z}[i]$ é definido por $\overline{\alpha} = a - bi$.

Por exemplo, o conjugado de $\alpha = 3 + 2i$ é $\overline{\alpha} = 3 - 2i$.

Figura 2 – O conjugado de $\alpha = 3 + 2i$.



Fonte: Elaborado pelo autor.

Agora, podemos definir a função norma sobre os inteiros gaussianos.

Definição 3.2.1. *A função norma $N : \mathbb{Z}[i] \to \mathbb{Z}$, para todo $\alpha = a + bi \in \mathbb{Z}[i]$, é definida como*

$$N(\alpha) = \alpha.\overline{\alpha} = a^2 + b^2.$$

Por exemplo dado $\alpha = 3 + 2i$, temos $N(\alpha) = 3^2 + 2^2 = 13$.

Observe que $N(0) = 0$ pois $N(0) = N(0 + 0i) = 0^2 + 0^2 = 0$. Observe também que se $N(\alpha) = 0$ então $\alpha = 0$. De fato, se $\alpha = a + bi$, então $N(\alpha) = 0 \Rightarrow a^2 + b^2 = 0 \Rightarrow a = b = 0$.

Proposição 3.2.2. *Se os inteiros a e b são soma de dois quadrados, então ab é uma soma de dois quadrados.*

Demonstração. Por hipótese existem inteiros r, s, t e u tais que $a = r^2 + s^2$ e $b = t^2 + u^2$. Pondo $\alpha = r + si$ e $\beta = t + ui$ temos $a = \alpha\overline{\alpha}$ e $b = \beta\overline{\beta}$. Assim

$$ab = \alpha\overline{\alpha}\beta\overline{\beta} = \alpha\beta\overline{\alpha}\overline{\beta}.$$

Pela Proposição 3.1.1 (b), temos que $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$. Assim $ab = \alpha\beta\overline{\alpha\beta}$, e essa igualdade implica que ab é uma soma de dois quadrados. □

Decorre da parte final da demonstração acima que para quaisquer inteiros r, s, t e u vale a igualdade

$$(r^2 + s^2)(t^2 + u^2) = (rt + su)^2 + (ru - st)^2.$$

De fato, basta substituir $a = r^2 + s^2$, $b = t^2 + u^2$, $\alpha = r + si$ e $\beta = t + ui$ em $ab = \alpha\beta\overline{\alpha\beta}$ realizar os cálculos.

A seguinte propriedade da função norma $N(\alpha) = \alpha\overline{\alpha}$ é fundamental.

Proposição 3.2.3. *Para quaisquer $\alpha, \beta \in \mathbb{Z}[i]$ temos que $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Demonstração. Por definição, $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta}$. Como e $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$ (Proposição 3.1.1 (b), temos que $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = (\alpha\beta)(\overline{\alpha}\overline{\beta}) = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$. □

Corolário 3.2.4. *O anel dos inteiros gaussianos $\mathbb{Z}[i]$ é de integridade.*

Demonstração. Seja $\alpha, \beta \in \mathbb{Z}[i]$ com $\alpha\beta = 0$. Como $N(0) = 0$, segue da Proposição 3.2.3 que $N(\alpha)N(\beta) = 0$. Como $\mathbb{Z}$ é um anel de integridade, temos $N(\alpha) = 0$ ou $N(\beta) = 0$. Logo $\alpha = 0$ ou $\beta = 0$. Portanto $\mathbb{Z}[i]$ é um anel de integridade. □

O teorema seguinte mostra que $\mathbb{Z}[i]$ é um anel euclidiano.

Proposição 3.2.5. *Dados dois inteiros gaussianos α e β, com $\beta \neq 0$, existem inteiros gaussianos γ e θ tais que $\alpha = \beta\gamma + \theta$ e $N(\theta) < N(\beta)$.*

Demonstração. Para quaisquer inteiros gaussianos α e β, com $\beta \neq 0$, podemos escrever

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{a+bi}{N(\beta)},$$

em que $a = Re(\alpha\overline{\beta})$ e $b = Im(\alpha\overline{\beta})$. Ao aplicarmos o Corolário 1.1.12, obtemos inteiros q_1, q_2, r_1 e r_2 tais que $a = N(\beta)q_1 + r_1$, $b = N(\beta)q_2 + r_2$, $|r_1| \leq (\frac{1}{2})N(\beta)$ e $|r_2| \leq (\frac{1}{2})N(\beta)$. Assim

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

Multiplicando ambos os lados da igualdade acima por β e tomando $\gamma = q_1 + q_2 i$, obtemos

$$\alpha = \beta\gamma + \frac{r_1 + r_2 i}{\overline{\beta}}.$$

Agora, defina $\theta = \alpha - \beta\gamma = \dfrac{r_1 + r_2 i}{\overline{\beta}}$ e note que $\theta \in \mathbb{Z}[i]$, pois $\mathbb{Z}[i]$ é um anel e α, β *e* $\gamma \in \mathbb{Z}[i]$. Como $|r_1| \leq \dfrac{1}{2}N(\beta)$ e $|r_2| \leq \dfrac{1}{2}N(\beta)$, segue que

$$N(\theta) = N\left(\frac{r_1 + r_2 i}{\overline{\beta}}\right) = N\left(\frac{(r_1 + r_2 i)\beta}{\overline{\beta}\beta}\right) = N\left(\frac{(r_1 + r_2 i)\beta}{N(\beta)}\right),$$

$$= \frac{(r_1^2 + r_2^2 i)N(\beta)}{N(\beta)^2} = \frac{(r_1^2 + r_2^2 i)}{N(\beta)} \leq \frac{\frac{1}{4}N(\beta)^2 + \frac{1}{4}N(\beta)^2}{N(\beta)} = \frac{1}{2}N(\beta).$$

Isso conclui a demonstração. □

3.3 PRIMOS GAUSSIANOS

Vamos começar com uma caracterização das unidades no anel dos inteiros gaussianos.

Proposição 3.3.1. *Um elemento $\alpha \in \mathbb{Z}[i]$ é uma unidade se, e somente se, $N(\alpha) = 1$.*

Demonstração. Se α é uma unidade de $\mathbb{Z}[i]$, então existe um inteiro gaussiano β tal que $\alpha\beta = 1$. Pela propriedade multiplicativa da norma (Proposição 3.2.3), temos $N(\alpha)N(\beta) = 1$, e consequentemente $N(\alpha) = 1$, uma vez que $N(\alpha)$ e $N(\beta)$ são inteiros não negativos.

Para mostrar a recíproca, note que se $\alpha = a + bi$, então $N(\alpha) = 1$ implica $(a + bi)(a - bi) = 1$, ou seja, α é uma unidade em $\mathbb{Z}[i]$. □

As unidades em $\mathbb{Z}[i]$ são ± 1 *e* $\pm i$. De fato, dado $\alpha = a + bi \in \mathbb{Z}[i]$, temos

$$N(\alpha) = 1 \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow a = \pm 1 \; e \; b = 0 \; ou \; a = 0 \; e \; b = \pm 1 \Leftrightarrow \alpha = \pm 1 \text{ ou } \alpha = \pm i.$$

Proposição 3.3.2. *Um primo p em $\mathbb{Z}$ é composto em $\mathbb{Z}[i]$ se, somente se, pode ser expresso como uma soma de dois quadrados*

Demonstração. Seja p um primo em $\mathbb{Z}$. Se p é composto em $\mathbb{Z}[i]$, então existem inteiros gaussianos α e β tais que $p = \alpha\beta$, com $N(\alpha) > 1$ e $N(\beta) > 1$. Aplicando a norma em ambos os lados da igualdade $p = \alpha\beta$ e usando a multiplicidade da norma, obtemos $p^2 = N(\alpha)N(\beta)$. Pelo Teorema Fundamental da Aritmética (Proposição 2.1.1) segue que $N(\alpha) = p$. Escrevendo $\alpha = a + bi$, com $a, b \in \mathbb{Z}$, temos que $p = N(\alpha) = a^2 + b^2$.

Reciprocamente, suponha que existam inteiros a e b tais que $p = a^2 + b^2$. Logo $p = (a + bi)(a - bi)$, e p é composto em $\mathbb{Z}[i]$. □

Corolário 3.3.3. *Seja p um primo em $\mathbb{Z}$. Então p é primo em $\mathbb{Z}[i]$ se, e somente se, $p = 4k + 3$ com $k \in \mathbb{Z}$.*

Demonstração. Pela Proposição 2.2.3 e o Teorema 3.4.2, um primo p em $\mathbb{Z}$ é uma soma de dois quadrados se, e somente se, $p = 2$ ou $p = 4k + 1$. Isso significa que um primo p em $\mathbb{Z}$ não é uma soma de dois quadrados se, e somente se, $p = 4k + 3$. Portanto, segue da Proposição 3.3.2 que um primo p em $\mathbb{Z}$ é primo em $\mathbb{Z}[i]$ se, e somente se, $p = 4k + 3$. □

3.4 INTEIROS QUE SÃO SOMA DE DOIS QUADRADOS

Nesta seção provaremos o resultado principal desta monografia, que é uma caracterização dos inteiros que são soma de dois quadrados.

Lema 3.4.1. *Seja p um primo em $\mathbb{Z}$ e suponha que para algum inteiro c, relativamente primo a p, podemos encontrar inteiros x e y tal que $x^2 + y^2 = cp$. Então existem inteiros a e b tais que $p = a^2 + b^2$.*

Demonstração. Suponhamos que o inteiro p também seja um elemento primo de $\mathbb{Z}[i]$. Como $x^2 + y^2 = cp$, temos

$$cp = (x + yi)(x - yi).$$

Pelo Proposição 1.1.30, sabemos que $p \mid (x + yi)$ *ou* $p \mid (x - yi)$. Mas se $p \mid (x + yi)$, então $x + yi = p(u + vi)$, com $u, v \in \mathbb{Z}$, o que significa que $x = pu$ e $y = pv$ de modo que, pela Proposição 1.1.8, p também dividiria $(x - yi)$. Pela Proposição 1.1.8 (ii) concluímos que $p^2 \mid (x + yi)(x - yi)$, isto é, $p^2 \mid cp$ e consequentemente $p \mid c$, contrário a nossa hipótese de que c é relativamente primo a p.

Analogamente, se $p \mid (x - yi)$, então $p \mid c$, novamente contrário a nossa hipótese. Assim p não é um elemento primo em $\mathbb{Z}[i]$. Consequentemente, $p = (a + bi)(g + di)$ onde $a + bi$ e $g + di$ não são unidades em $\mathbb{Z}[i]$. Agora, por um lado, segue da Proposição 3.3.1 que

$$a^2 + b^2 \neq 1 \; e \; g^2 + d^2 \neq 1.$$

Por outro lado, segue da propriedade multiplicativa de da norma (Proposição 3.2.3) que

$$p = (a+bi)(g+di) \Rightarrow N(p) = N(a+bi)N(g+di) \Rightarrow p^2 = (a^2+b^2)(g^2+d^2).$$

Pelo Teorema Fundamental da Aritmética (Proposição 2.1.1) , temos $a^2+b^2 = 1$, p ou p^2. Observe que $a^2+b^2 \neq 1$, pois $a+bi$ não é uma unidade em $\mathbb{Z}[i]$, se $a^2+b^2 = p^2$, teríamos $g^2+d^2 = 1$, contrário ao fato de $g+di$ não ser uma unidade em $\mathbb{Z}[i]$. Assim a única possibilidade é que $a^2+b^2 = p$ e o lema está demonstrado. □

Deste ponto em diante, estaremos trabalhando apenas no anel dos inteiros $\mathbb{Z}$.

Teorema 3.4.2. *Se p é um primo da forma $4k+1$, então existem inteiros a e b tais que $p = a^2+b^2$.*

Demonstração. Pelo Teorema 2.3.1 existe um inteiro x tal que $x^2 \equiv -1 \pmod{p}$ e x pode ser escolhido de modo que $0 \leq x \leq p-1$, pois basta usar o resto da divisão de x por p, a saber, de modo a satisfazer $|x| \leq \frac{p}{2}$. De fato, se $x > \frac{p}{2}$, então $y = p-x$ satisfaz $y^2 \equiv -1 \pmod{p}$ mas $|y| \leq \frac{p}{2}$. Assim podemos admitir que temos um inteiro x tal que $|x| \leq \frac{p}{2}$ e x^2+1 é um múltiplo p, digamos cp. Ora

$$cp = x^2+1 \leq \frac{p^2}{4}+1 < p^2.$$

Para verificar a última desigualdade, observe que

$$\frac{p^2}{4}+1 < p^2 \Leftrightarrow \frac{p^2}{4} < p^2-1 \Leftrightarrow p^2 < 4p^2-4 \Leftrightarrow 3p^2 > 4,$$

que é verdade, pois $p > 1$. Assim $cp < p^2$, que implica $c < p$.

Logo $cp = x^2+1$, com $mdc(p,c) = 1$. Pelo Lema 3.4.1 existem inteiros a e b tais que $p = a^2+b^2$, demonstrando o teorema. □

Lema 3.4.3. *Se n é uma soma de dois quadrados e m é um inteiro qualquer, então nm^2 é uma soma de dois quadrados.*

Demonstração. Seja $n = a^2+b^2$ com a e b inteiros. Como

$$nm^2 = (a^2+b^2)m^2 = a^2m^2+b^2m^2 = (am)^2+(bm)^2,$$

segue que nm^2 é uma soma de dois quadrados. □

Finalmente estamos prontos para demonstrar o resultado principal desta monografia.

Teorema 3.4.4 (Fermat)**.** *Um inteiro n pode ser representado como soma de dois quadrados se, e somente se, tiver fatoração da forma*

$$n = 2^{\alpha} {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r} {q_1}^{\beta_1} {q_2}^{\beta_2} \cdots {q_s}^{\beta_s} \tag{3.3}$$

onde cada p_i é um primo da forma $4k+1$, cada q_j é um primo da forma $4k+3$, α e cada α_i são inteiros não negativos e todos os β_j são inteiros pares.

Demonstração. Seja $n = 2^{\alpha}{p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_r}^{\alpha_r}{q_1}^{\beta_1}{q_2}^{\beta_2}\cdots{q_s}^{\beta_s}$ com as condições dadas em (3.3). De $p_i \equiv 1 \pmod 4$, segue do Teorema 3.4.2 que cada p_i é uma soma de dois quadrados. Também $2 = 1^2 + 1^2$. Como o produto de uma soma de dois quadrados é uma soma de dois quadrados (Proposição 3.2.2), segue que $2^{\alpha}{p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_r}^{\alpha_r}$ é uma soma de dois quadrados. Como os β_j são todos pares, temos $\beta_1 = 2b_1, \beta_2 = 2b_2, \cdots, \beta_s = 2b_s$, e assim $q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s} = (q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s})^2$ é um quadrado. Segue do Lema 3.4.3 que n é uma soma de dois quadrados.

Para mostrar a direção contrária, observe primeiramente que, pelo Algoritmo da Divisão (Proposição 1.1.11), todo número primo maior que 2 é da forma $4k+1$ ou $4k+3$, Assim, pelo Teorema Fundamental da Aritmética (Proposição 2.1.1), podemos escrever

$$n = 2^{\alpha}{p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_r}^{\alpha_r}{q_1}^{\beta_1}{q_2}^{\beta_2}\cdots{q_s}^{\beta_s} \tag{3.4}$$

onde cada p_i é da forma $4k+1$ e cada q_j é da forma $4k+3$. Agora mostremos que se n é uma soma de dois quadrados, digamos $n = a^2 + b^2$, então todos os β_j são pares.

Se um primo q_j da forma $4k+3$ não aparece na decomposição de n então $\beta_j = 0$. Caso contrário, se q_j aparece na decomposição de $n = a^2 + b^2$ então q_j divide $a^2 + b^2 = (a+bi)(a-bi)$. Como q_j é primo em $\mathbb{Z}[i]$ (Corolório 3.3.3), segue que q_j divide $a+bi$ ou q_j divide $a-bi$. Em qualquer dos casos existem inteiros c e d tais que $a = q_j c$ e $b = q_j d$. Assim

$$n = a^2 + b^2 = (q_j c)^2 + (q_j d)^2 = q_j^2(c^2 + d^2).$$

Se q_j não aparece na decomposição de $c^2 + d^2$ então $\beta_j = 2$. Caso contrário, se q_j aparece na decomposição de $c^2 + d^2$, repetimos o mesmo argumento para mostrar que q_j^2 aparece na decomposição de $c^2 + d^2$, e portanto q_j^4 aparece na decomposição de n. Continuando assim vemos que β_j é par. □

Observe que a Proposição 2.2.1 é uma consequência do Teorema 3.4.4. De fato, não podem existir inteiros x, y e z tais que $x^2 + y^2 = 3z^2$ porque na decomposição de $3z^2$ em fatores primos, 3 aparece um número ímpar de vezes e 3 é um primo da forma $4k+3$.

CONSIDERAÇÕES FINAIS

O curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Valparaíso, possui duas disciplinas destinadas à elaboração e defesa de um Trabalho de Conclusão de Curso (TCC). Essas disciplinas são TCC I e TCC II, e são ministradas nos dois semestres finais do curso.

Para ser aceito na disciplina de TCC I, é necessário ter a carta de aceite de um orientador e a aprovação de um pré-projeto pelo Núcleo Docente Estruturante do curso. Após obter um orientador, e em comum acordo com ele, submeti um projeto cujo tema abordava aplicações de algumas médias. Meu projeto foi aprovado e matriculei-me na disciplina de TCC I.

No começo do semestre letivo, ao começarmos uma pesquisa bibliográfica mais aprofundada, meu orientador e eu percebemos que as referências sobre o tema eram escassas e que não poderíamos basear a pesquisa apenas na dissertação de mestrado que tomamos como base para a elaboração do pré-projeto.

Nesse mesmo semestre, eu também era aluno do meu orientador na disciplina *Funções de Variáveis Complexas*. Após ele ministrar um terço do curso, no qual tratou das propriedades operatórias dos números complexos, ele me propôs um novo tema para o TCC, que era sobre uma caracterização dos primos que são soma de dois quadrados. Esse é um resultado clássico da teoria dos números, atribuído a Fermat. Os pré-requisitos para estudar esse problema envolviam alguns conhecimentos sobre números complexos, que eu tinha obtido na disciplina, e alguns conhecimentos da teoria clássica de números, que aprendi na disciplina Teoria dos Números quando a frequentei no quarto semestre.

Após realizar alguns levantamentos bibliográficos sobre o meu novo tema, concentrei meus estudos, com a ajuda do meu orientador, no Capítulo 3 do livro Tópicos de Álgebra (Herstein, 2005) e no artigo Inteiros Gaussianos (Charra; Moura; Strey, 2023).

O estudo de Charra, Moura e Strey (2023) foi importante para compreender como certas propriedades do anel dos inteiros $\mathbb{Z}$ se conectam com algumas propriedades do anel dos inteiros gaussianos $\mathbb{Z}[i]$.

O Capítulo 3 de Herstein (2005) forneceu uma estrutura para esta monografia. Por exemplo, foi desse capítulo que extraímos o Lema 3.4.1 e o Teorema 3.4.2.

Foi no livro de Santos (2002) que encontramos o enunciado do Teorema 3.4.4 (nosso teorema principal). Achamos esse enunciado interessante porque ele fornece, de maneira explícita, uma condição necessária e suficiente para que um inteiro positivo n seja soma de dois quadrados. Como a demonstração desse teorema em Santos (2002) não usava os mesmos pré-requisitos já estudados por mim, resolvemos adaptar um roteiro de demonstração que encontramos em Aigner Martin; Ziegler (2017).

Os resultados da Seção 2.3 foram todos retirados de Goldman (1998).

Para demonstrar que $\mathbb{Z}[i]$ é anel euclidiano (Proposição 3.2.5) utilizamos Charra, Moura e Strey (2023). Para demonstrar o Algoritmo da Divisão (Teorema 1.1.11) usamos Milies (2020).

Para elaborar o Capítulo 1 desta monografia, precisei realizar um estudo sobre anéis. Essa foi uma barreira a ser vencida, tendo em vista que durante o curso não tive nenhum contado com esse tema. Para escrever esse capítulo, usamos principalmente (Gonçalves, 2026) e (Herstein, 2005).

Outro desafio encontrado na elaboração desta monografia foi a leitura de textos em língua inglesa e a escrita usando latex. Para a tradução de alguns trechos de livros, usamos o ChatGPT[1], e para a escrita e compilação do texto em latex, usamos o Overleaf[2].

Julgamos ser importante fornecer alguns conextos históricos para alguns resultados apresentados na monografia. Para isso, as seguintes referências foram consultadas: (Boyer, 1974),(Eves, 2011), (Gray, 2018), (Cajori, 1909), (Gray, 2018).

Nesta monografia tratamos da caracaterização dos inteiros que podem ser escritos como uma soma de dois quadrados. Esse resultado já foi generalizado em várias direções por diversos autores.

Por exemplo, pode-se perguntar: um inteiro positivo qualquer pode ser representado como soma de no máximo quantos quadrados? Essa pergunta foi respondida por Lagrange em 1770: "Todo inteiro não negativo pode ser representado como soma de no máximo quatro quadrados."(Eves, 2011, p. 391). Uma demonstração moderna desse resultado, usando o chamado anel dos quatérnios inteiros de Hurwitz, encontra-se em (Andrade, 2014).

Segundo Cox (1989, p. 1), também são de Fermat os seguintes resultados sobre os números inteiros:

Se p é um primo ímpar, então $p = x^2 + 2y^2$, se e somente se $p \equiv 1,3 \pmod 8$.

Se p é um primo ímpar, então $p = x^2 + 3y^2$, se e somente se $p = 3$ ou $\equiv 1 \pmod 3$.

O livro de Cox (1989) trata da seguinte questão: dado um inteiro positivo n, quais primos p podem ser expressos da forma $p = x^2 + ny^2$, onde x e y são inteiros?

No livro (Aigner Martin; Ziegler, 2017) é apresentada uma segunda demonstração de que cada primo da forma 4k+1 é uma soma de dois quadrados. Essa prova foi descoberta por Roger Heath-Brown em 1971 e apareceu em 1984.

[1] CHATGPT. Modelo de inteligência artificial desenvolvido pela OpenAI para geração de textos e respostas automáticas em linguagem natural. Disponível em: <https://chat.openai.com/>. Acesso em: 7 jul. 2025.

[2] OVERLEAF. Editor online para projetos em LaTeX. Disponível em: <https://www.overleaf.com/>. Acesso em: 7 jul. 2025.

REFERÊNCIAS

AIGNER MARTIN; ZIEGLER, G. M. *Paul Erdös Paul Erdös As Mais Belas Demonstrações Matemáticas*. São Paulo: Blucher, 2017.

ANDRADE, J. F. S. *Tópicos especiais em álgebra*. [S.l.]: SBM, 2014.

BOYER, C. B. *História da matemática*. São Paulo: Editora USP, 1974.

CAJORI, F. *A History of Mathematics*. London: The Macmillan Company, 1909.

CHARRA, L. A.; MOURA, R. d. P.; STREY, E. Inteiros gaussianos. *Sociedade Brasileira de Matemática*, 2023.

COX, D. A. *Prime of the form* $x^2 + ny^2$. New Jersey: Wiley-Interscience, 1989.

EVES, H. *Introdução à história da matemática*. Campinas: Edutora da Unicamp, 2011.

GOLDMAN, J. R. *The Queen of Mathematics: a historically motivated guide to number theory*. New York: CRC Press, 1998.

GONÇALVES, A. *Introdução à álgebra*. Rio de Janeiro: IMPA, 2026.

GRAY, J. *A History of Abstract Algebra*. Boston: Springer Undergraduate Mathematics Series, 2018.

GUZMÁN, M. D. *Aventuras Matemáticas*. Lisboa: Gradiva, 1991.

HERSTEIN, I. N. *Tópicos de Álgebra*. Massachusetts: LTC, 2005.

LIMA, E. L. *Análise Real volume 1. Funções de Uma Variável*. Rio de Janeiro: IMPA, 2014.

MILIES, C. p. *Tópicos de álgebra clássica: um prelúdio á álgebra moderna*. São Paulo: Livradia da Física, 2020.

SANTOS, J. P. d. O. *Introdução a Teoria dos Números*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2002.

SHOKRANIAN, S. *Uma Breve História da Teoria dos Números no Século Vinte*. Rio de Janeiro: Moderna, 2010.

SMITH, D. E. *History of Modern Mathematics*. New York: John Wiley, 1906.