UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROFMAT – Mestrado Profissional em Matemática em Rede Nacional

O Anel dos Inteiros de Gauss

AUTOR – Luciana Sequeira Cury e Lima

RIO DE JANEIRO / RJ

2016

Luciana Sequeira Cury e Lima

O Anel dos Inteiros de Gauss

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Orientador: Silas Fantin
Doutor em Matemática

Rio de Janeiro
2016

Cury e Lima, Luciana Sequeira

O Anel dos Inteiros de Gauss / Luciana Sequeira Cury e Lima – 2016

65.p

1.Matemática 2. Álgebra. I. Título

CDU 536.21

Luciana Sequeira Cury e Lima

O ANEL DOS INTEIROS DE GAUSS

Trabalho Final de Curso apresentado a Coordenação de Pós-Graduação *Stricto-sensu* da Universidade Federal do Estado do rio de Janeiro, como requisito parcial para a obtenção do título de Mestre em Matemática pelo Programa PROFMAT.

Aprovada em 20 de outubro de 2016.

BANCA EXAMINADORA

Dr. Silas Fantin – UNIRIO – Orientador

Dra. Cristiane de Mello – UNIRIO

Dr. Eduardo Dias Correa – UERJ

Dedicatória

Ao meu marido Marcelo Cury e Lima, meu grande amor, que me apoiou incondicionalmente sendo imprescindível para a conclusão deste curso.

Resumo

Neste trabalho de conclusão de curso do programa de Pós-Graduação em matemática PROFMAT da UNIRIO, iremos abordar a aritmética no conjunto dos inteiros de Gauss, similar a desenvolvida no estudo dos números inteiros.

Os conceitos básicos tais como: unidades, elementos primos e irredutíveis serão revistos no conjunto dos inteiros de Gauss $\mathbb{Z}[i] = \{ a + bi; a, b \in \mathbb{Z} \}$ onde seus elementos são denominados inteiros gaussianos, e de maneira similar a $\mathbb{Z}$, poderemos calcular o máximo divisor comum e mínimo múltiplo comum para estes elementos, em virtude de $\mathbb{Z}[i]$ ser um domínio de fatoração única.

Veremos também que é possível resolver alguns problemas dos números inteiros através da teoria dos inteiros gaussianos, como por exemplo, saber quais números inteiros podem ser escritos como soma de dois números inteiros quadrados.

Palavras–chaves: Inteiro Gaussiano, Números primos, Divisão Euclidiana, máximo divisor comum e soma de dois quadrados.

Abstract

The present ending study for the Mathematics Graduate Course of PROFMAT UNIRIO will consider arithmetic in all the Gaussian integers as similar developed on the study of integers.

The basic concepts such as units, cousins and irreducible elements are reviewed in the set of Gaussian integers Z [i] = {a + b; a, b ∈ Z} where elements are called integers Gaussian, and similarly the $\mathbb{Z}$, it can have calculated the greatest common divisor and least common multiple of these elements, by virtue of Z [i] be a unique factorization domain.

It will be also note some problems solutions of integers through the theory of Gaussian integers, for example, identify which integers can be written as a sum of two square integers.

Keywords: Full Gaussian, Prime numbers, Euclidean Division, Greatest common divisor and sum of two squares.

Agradecimentos

A Deus, pela força para enfrentar os obstáculos e por permitir a realização de mais um sonho;

À minha mãe Solange, sempre acreditando na minha capacidade;

Ao meu pai Adelino, pelo exemplo de trabalho árduo ao longo de sua vida;

Ao meu marido Marcelo, incansável na arte de amar e esperar;

Aos meus filhos Rapha e Cadu, por entender minha ausência e impaciência;

Aos meus enteados Laura e Vitor, abrindo mão do pouco tempo que temos;

Aos irmãos escolhidos Salvador e Simara Bruno por estarem sempre presentes;

Aos Professores do PROFMAT da UNIRIO, cujas aulas foram imprescindíveis;

À CAPES pelo suporte financeiro;

Ao meu orientador Dr. Silas Fantin, que não desistiu mesmo diante de tantas evidências contrárias, predispondo-se a me auxiliar nos momentos em que o acaso e a falta de tempo se impuseram como limitações;

E a todos que participaram de forma direta e indireta para a conclusão deste trabalho.

Sumário

INTRODUÇÃO

Gauss (1777-1855) ao estudar questões de teoria dos números relacionadas à reciprocidade cúbica e biquadrática percebeu que essa investigação se tornava mais simples trabalhando em um subconjunto dos números complexos $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ onde a parte real e parte imaginária eram dadas por números inteiros, e este subconjunto $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ é denominado anel dos inteiros de Gauss em sua homenagem.

Neste subconjunto $\mathbb{Z}[i]$, que estende a noção de número inteiro, pois $\mathbb{Z} \subseteq \mathbb{Z}[i]$, Gauss precisava mostrar que várias noções desenvolvidas na Teoria de Euclides tais como: caracterização de elementos primos e elementos irredutíveis, existência de fatoração única, cálculo do mdc, entre outras, poderiam ser transportadas para $\mathbb{Z}[i]$, trazendo conseqüências relevantes para o desenvolvimento de teoria dos números.

É salutar refletir que algumas noções básicas, tais como elementos primos, elementos irredutíveis e elementos inversíveis, muitas das vezes são passadas despercebidas pelo ciclo básico de ensino em sua literatura, pois dependendo onde o elemento esteja, sua caracterização é alterada. Por exemplo, $2 \in \mathbb{Z} \subseteq \mathbb{Z}[i] \subseteq \mathbb{C}$, mas 2 é um elemento primo e irredutível em $\mathbb{Z}$, 2 não é um elemento primo e nem um elemento irredutível em $\mathbb{Z}$[i], pois $2 = (1+i)(1-i)$ e portanto é um elemento composto e um elemento inversível em $\mathbb{C}$.

É fácil observar que os números inteiros primos $5, 13, 17$ são do tipo $4k+1$ e são soma de dois quadrados pois $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$ e $17 = 4^2 + 1^2$ e os números inteiros primos $3, 7, 11$ são do tipo $4k+3$ e não são soma de dois quadrados. É possível verificar que se p é um número primo ímpar menor do que 1000 então o primo p é soma de dois quadrados se ele é do tipo $4k+1$. Fermat (1601-1665) conjecturou e demonstrou que: "*um número primo p é soma de dois quadrados se e somente se $p = 2$ ou p é do tipo $4k+1$*". Veremos que o problema de caracterizar os inteiros primos $p = a^2 + b^2$ que são soma de dois quadrados é equivalente a um certo problema de fatoração no anel $\mathbb{Z}[i]$, onde $p = a^2 + b^2 = (a + ib)(a - ib)$ com $a, b \in \mathbb{Z}$. Iremos estudar o problema de fatoração única como consequência de que em $\mathbb{Z}$[i] existe uma noção de divisão com resto pequeno similar a divisão euclidiana em $\mathbb{Z}$.

Através das ideias de Gauss, nosso objetivo nesta pesquisa é estudar o conjunto numérico dos Inteiros Gaussianos. Para isso estudaremos suas propriedades, seus resultados e faremos um comparativo com os números inteiros.

Em Álgebra denotamos um domínio euclidiano como sendo um anel dotado de uma estrutura específica, a dizer, uma função euclidiana. Dessa forma, é possível a generalização do famoso Algoritmo de Euclides desenvolvido para regulamentar a divisão de dois elementos. Além disso, em um domínio euclidiano, é possível aplicar tal algoritmo para efetuar o cálculo do máximo divisor comum entre dois números.

A motivação para o estudo de uma estrutura assim caracterizada é representada pelo simples questionamento: o que acontece quando dois números inteiros a e b são tais que b divide a? A resposta para essa pergunta traz consigo outras concepções decorrentes, como a de domínio de fatoração única, por exemplo: a) É possível calcular o máximo divisor comum entre dois inteiros gaussianos? b) Seria mais simples resolver problemas de números inteiros utilizando os inteiros de Gauss? c) Todo número primo no conjunto dos inteiros também é primo nos inteiros gaussianos?

Iniciamos o trabalho abordando um pouco da biografia de Euclides e a sua importante contribuição para a Teoria dos Números. Faremos um resumo de teorias necessárias para o desenvolvimento de nosso trabalho. Apresentamos definições e teoremas importantes na Teoria dos Números.

A seguir apresentamos uma descrição sucinta de cada capítulo.

No primeiro capítulo desenvolvemos as noções e resultados preliminares de Anel, divisibilidade e Domínios Euclidianos e os dispositivos práticos para o cálculo do máximo divisor comum no Ensino Fundamental.

No segundo capítulo fazemos um estudo aprofundado sobre o domínio dos inteiros de Gauss, enfatizando, sobretudo, o fato de que este é um domínio euclidiano, e consequentemente de fatoração única. Apresentamos as definições de norma, divisibilidade, números primos, etc. Calculamos o máximo divisor comum nesse conjunto.

No terceiro Capítulo faremos aplicações da teoria dos inteiros gaussianos nos números inteiros, ou seja, resoluções de problemas dos inteiros que podem ser solucionados nos inteiros gaussianos.

No quarto capítulo apresentaremos propostas de atividades para a sala de aula do Ensino Médio. Finalmente no quinto capítulo, apresentaremos as respectivas soluções das atividades propostas.

CAPÍTULO 1 – Fundamentação Teórica.

"Um número é uma pluralidade composta de unidades"

Euclides

O presente capítulo pretende mostrar a importância de Euclides no estudo da Teoria dos Números posicionando o leitor na linha do tempo da história da matemática. Além disso, destina-se a apresentar os pré-requisitos que serão necessários para a compreensão deste trabalho.

No decorrer deste capítulo nos depararemos com conceitos como divisão euclidiana, teoremas como o do Eudoxius dentre outros pré-requisitos a fim de chegar aos métodos para o cálculo do máximo divisor comum (mdc) de dois números inteiros.

1.1. ARITMÉTICA: DE EUCLIDES A FERMAT

"A Aritmética é a base de toda a Matemática, pura ou aplicada. É a mais útil das ciências e provavelmente não existe nenhum outro ramo do conhecimento humano tão espalhado entre as massas. "

A Teoria dos Números é a ciência que tem por objetivo principal estudar as propriedades e relações entre os Números Inteiros. Essa teoria aparece como ferramenta em diversas áreas da Matemática, tais como: Probabilidade, Álgebra, Sistemas Dinâmicos, etc., servindo de alicerce para resultados significativos.

É na Grécia que inicialmente identificamos a Teoria dos Números tal como a entendemos hoje. Foram os pitagóricos que estudaram as relações entre números do ponto de vista do que hoje denominamos Teoria dos Números.

Euclides nasceu em 330 a.C, em Alexandria. Geômetra grego, professor de Matemática a convite do então imperador da parte egípcia da Grécia Antiga: Ptolomeu I. Como Pitágoras ele acreditava na busca da verdade matemática pura e não buscava aplicações para o seu trabalho. Uma história conta de um estudante que indagou ao mestre sobre a utilidade da Matemática que estava aprendendo. Depois de terminar a

aula, *Euclides* virou para um de seus assessores e disse: "*De uma moeda ao rapaz, já que ele deseja ter lucros com tudo o que apreende e depois o dispense do curso*".

Euclides dedicou boa parte de sua vida ao trabalho de escrever *os Elementos*, escrita em 13 volumes e abrangendo grande parte da matemática da época. Euclides explorava uma arma lógica em sua obra conhecida como ***redução ao absurdo***, ou ***prova por contradição***. Sua abordagem envolve a ideia de provar que um teorema é verdadeiro, presumindo primeiro que a tese seja falsa. Explorando as consequências lógicas do teorema ser falso, obtêm se uma contradição de algum fato que sabemos ser verdade, e, portanto, concluímos que o teorema original não pode ser falso, ou seja, o teorema deve ser verdadeiro.

O matemático inglês G.H.Hardy resumiu o espírito da redução ao absurdo em seu livro *Apologia do matemático* da seguinte maneira: "Redução ao absurdo, que Euclides tanto amava, é uma das melhores armas do matemático. É um desafio muito maior do que qualquer jogo de xadrez pode praticar. O jogador de xadrez pode oferecer o sacrifício de um peão ou de uma peça mais importante, mas o matemático oferece o jogo inteiro ".

O matemático que escreveu um livro equivalente, sobre teoria dos números, foi Diofante de Alexandria, o último herói da tradição matemática grega. Embora as realizações de Diofante na teoria dos números estejam bem documentadas, quase nada se conhece sobre este matemático formidável. Presume-se que Diofante deve ter vivido antes do ano 364 de nossa era, e uma data em torno de 250, é geralmente aceita como sendo a estimativa mais provável.

Um exemplo do tipo de problema que Diofante apreciava foi gravado na lápide de seu túmulo e dizia o seguinte: "*Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois por uns doze anos, ele cobriu seu rosto com a barba. A luz do casamento iluminou-o após a sétima parte de cinco anos depois do casamento. Ele concedeu-lhe um filho. Ah! Criança tardia e má, depois de viver metade da vida de seu pai o destino frio o levou. Após consultar sua mágoa em ciência dos números, por quatro anos, Diofante terminou sua vida.* " O desafio é calcular quanto tempo Diofante viveu. Diofante viveu em Alexandria, e reuniu em seu tratado, intitulado *Aritmética*, diversos problemas bem conhecidos e criou uma série de novos problemas. Dos treze volumes que formavam a *Aritmética de Diofante*, somente seis sobreviveram e inspiraram matemáticos da renascença, incluindo Pierre de Fermat. Os outros sete livros

foram perdidos numa série de acontecimentos trágicos que enviaram a Matemática de volta para a era babilônica.

Euclides foi professor, matemático e escritor. Sua principal obra (e contribuição) para a matemática foram "Os elementos", em que são estabelecidas as bases da geometria euclidiana. Em teoria de números, é possível enumerar diversos resultados notáveis (e usados até hoje) atribuídos a ele, como o algoritmo para a divisão, a demonstração da irracionalidade do número $\sqrt{2}$ (diagonal de um quadrado de lado 1) e a prova da infinitude dos números primos.

Embora a Matemática tenha sido intensamente estudada por outros autores gregos, e, posteriormente, por árabes, indianos e europeus, a Teoria dos Números caiu em esquecimento até o século XVII.

Bachet, em 1612, publicou o texto original em grego da Aritmética de Diofanto, incluindo uma tradução latina, que era a língua usada pelos eruditos europeus da época. Entre 1621 e 1636, o francês Pierre de Fermat nascido em 1601, magistrado da corte de Toulouse, adquiriu uma cópia desse livro. Fermat leu o texto de Diofanto, anotando na margem as ideias que lhe ocorriam. Isso marcou o início de seu interesse pela Teoria dos Números, que posteriormente, expressou uma torrente de resultados importantes.

1.2. **Conceitos preliminares**

Um conceito que abordaremos nesta seção, é o de máximo divisor comum entre dois números inteiros diferentes de zero. Se a e b são inteiros não nulos, definimos o máximo divisor comum de a e b como sendo o maior inteiro positivo que divide simutaneamente a e b, e o denotaremos por $mdc(a, b)$.

Estamos interessados em apresentar um método simples e eficiente de encontrar o máximo divisor comum entre dois números inteiros diferentes de zero. Um dos algoritmos mais antigos, conhecido desde que surgiu nos Livros VII e X da obra Elementos de Euclides por volta de 300 a.C. e conhecido na literatura clássica como o **algoritmo de Euclides**. O algoritmo não exige qualquer fatoração e é um dos algoritmos numéricos mais antigos ainda em uso corrente.

O algoritmo tem muitas aplicações teóricas e práticas. Ele pode ser usado para gerar importantes aplicações tradicionais usados em diferentes culturas em todo o mundo. Ele é um elemento-chave dos algarismos de RSA, um método de codificação de mensagem de chave pública usado no comércio eletrônico. Também é usado para resolver equações diofantinas, que são equações do tipo $ax + by = n$ com $a, b, n \in \mathbb{Z}$, onde procuramos soluções inteiras, e é uma ferramenta básica para obter o Teorema Fundamental da Aritmética, que diz que todo número inteiro positivo maior do que 1 pode ser escrito de maneira única a menos da ordem, como produto de números primos. Isto permitirá o cálculo do *mdc* de dois números inteiros observando sua fatoração, maneira esta, utilizada no ensino básico.

Estaremos interessados em estender o conceito de máximo divisor comum para um subconjunto dos números complexos $\mathbb{C}$, que são denominados por **anel dos inteiros de Gauss** e denotados por

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

Princípio da Boa Ordenação (PBO): Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente então S possui um menor elemento**.**

A seguir apresentaremos o algoritmo de Euclides que garante que dados dois inteiros positivo, a divisão de um deles pelo outro (não nulo) é sempre possível, mesmo que para isso tenhamos que deixar um resto. É muito comum este resultado ser apresentado sem prova, nos livros didáticos do 6º ano do ensino fundamental.

Proposição 1.1 (Divisão Euclidiana em ℕ): Dados dois inteiros positivos a e b com $b \neq 0$, e $0 < a < b$ então existe um único par de inteiros positivos q e r, com $0 \leq r < a$ tais que

$$b = qa + r$$

Prova: Como $b > a$, considere o seguinte conjunto

$$S = \{b, b - 1a, b - 2a, \ldots, b - na\} \subseteq \mathbb{N}$$

Pelo princípio da boa ordenação, S tem um menor elemento r onde

$$r = b - qa \quad \Rightarrow \quad b = qa + r,$$

Afirmação: $r < a$.

De fato, caso contrário

$r > a \Rightarrow \exists\, c \in \mathbb{N};\ r = a + c$

$\Rightarrow\ c = r - a = (b - qa) - a = b - (q+1)a \in S$

$\Rightarrow c < r \ \ com\ c \in S$

Isto gera um absurdo pois r é o menor elemento de S. ■

Teorema de Eudoxius (300 A.C) Dados $a, b \in \mathbb{Z}$ então

a) b é múltiplo de a ;

b) b se encontra entre dois múltiplos consecutivos de a,

Proposição 1.2 (Divisão Euclidiana em ℤ): Dados dois inteiros a e b com $a \neq 0$, e então existe um único par de inteiros $q\ e\ r$, com $0 \leq r < |a|$ tais que

$$b = qa + r.$$

Prova: Existem duas possibilidades a serem analisadas.

1. $a > 0$
2. $a < 0$

Caso 1: ($\boldsymbol{a} > 0$) Segue do Teorema do Eudoxius

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

Por um lado

$$qa \leq b \Rightarrow 0 \leq b - qa \qquad (I)$$

Por outro lado

$$b < (q+1)a \Rightarrow b < qa + ba \Rightarrow b - qa < a \qquad (II)$$

Defina $r = b - qa$. Portanto podemos concluir de (I) e (II) que

$$0 \leq r < a \qquad e \qquad b = qa + r$$

Caso 2: ($\boldsymbol{a} < 0$) Segue do Teorema do Eudoxius

$$qa \leq b < (q-1)a$$

Por um lado

$$qa \leq b \Rightarrow 0 < b - qa \qquad (III)$$

Por outro lado

$$b < (q-1)a \Rightarrow b < qa - a \Rightarrow b - qa < -a \qquad (IV)$$

Defina $r = b - qa$. Portanto podemos concluir de (III) e (IV) que

$$0 \leq r < -a \quad e \quad b = qa + r. \quad \blacksquare$$

Definição 1.3 (Divisibilidade): Sejam $a, b \in \mathbb{Z}$ com $a \in \mathbb{Z}$. Dizemos que *a divide b* se existir $k \in \mathbb{Z}$ tal que $b = k.a$. Usaremos a seguinte notação: $a \mid b$ (lê-se *a divide b*)

Exemplo: $3 \mid 12$, pois $12 = 4.3$

Propriedades da divisão: Sejam $a \; e \; b \in A$.

i. $a \mid a$, para todo $a \in A, a \neq 0$.
ii. $Se \; a \mid b \; e \; b \mid a, então \; a = b$.
iii. $Se \; a \mid b \; e \; b \mid c, então \; a \mid c$.
iv. $Se \; a \mid b \; e \; b \mid c \;\; então \; a \mid (b.x + c.y) \;\; para \; todo \; x, y \in A$.

Diremos que d é um divisor comum de $a \; e \; b \; se \; d \mid a \;\; e \;\; d \mid b$.

Definição 1.4 (Máximo Divisor Comum): Sendo $a \; e \; b \in A$ com $a \neq 0$ ou $b \neq 0$

$$mdc(a, b) = \{maior \; inteiro \; que \; divide \; a \; e \; b\}$$

No ensino básico, inicialmente se aborda o conceito de máximo divisor comum entre dois números inteiros de maneira intuitiva da seguinte forma.

Vejamos o seguinte exemplo, calcule o máximo divisor comum entre $82 \; e \; 30$.

Solução: Primeiramente determinamos os divisores de 82:

$$D(82) = \{1,2,41,82\}$$

Em seguida determinamos os divisores de 30:

$$D(30) = \{1,2,3,5,6,10,15,30\}$$

Dessa forma, por observação, o aluno determina que o máximo divisor comum de a e b será dado pelo elemento máximo do conjunto $D(a) \cap D(b)$. Neste caso:

$$mdc(82,30) = \max\{D(82) \cap D(30)\} = \max\{1,2\} = 2. \quad \blacksquare$$

Para valores maiores, esse método poderia ser demorado, além de levar a um possível "esquecimento" de algum divisor. A partir daí propõe-se o ***algoritmo de Euclides*** como alternativa para determinação do máximo divisor comum entre dois

números inteiros. Em resumo, o algoritmo é um método de divisões sucessivas entre o divisor e o resto anterior, até obtermos o ultimo resto não nulo, que será o $mdc(a,b)$.

	q_1	q_2	$\cdots$	q_n	q_{n+1}
a	b	r_1	$\cdots$	r_{n-1}	r_n
r_1	r_2	r_3	$\cdots$	$r_{n+1}=0$	

Para $a = 82$ e $b = 30$, vemos que, $mdc(82,30) = 2$

	$q_1 = 2$	$q_2 = 1$	$q_3 = 2$	$q_4 = 1$	$q_5 = 3$
a =82	b =30	$r_1 = 22$	$r_2 = 8$	$r_3 = 6$	$r_4 = 2$
$r_1 = 22$	$r_2 = 8$	$r_3 = 6$	$r_4 = 2$	$r_5 = 0$	

A seguir, abordaremos a justificativa algébrica do algoritmo Euclides para o cálculo do máximo divisor comum, que dependerá exclusivamente do algoritmo da divisão euclidiana e do Lema de Euclides que apresentaremos a seguir.

Lema 1.5 (Lema de Euclides):

Se $a, b, n \in \mathbb{Z}$ então $mdc\,(a,b) = mdc\,(a, b-na)$

Prova: Seja $c = mdc\,(a,b)$ $e\ d = mdc(a, b-na)$.

Como:

$d = mdc(a, b-na) \Rightarrow d \mid a\ e\ d \mid (b-na)$

$\Rightarrow d \mid b\ pois\ b = (b-na)+na$

$\Rightarrow d \mid a\ e\ d \mid b$

$\Rightarrow d \mid c$

Por outro lado, como:

$c = mdc\,(a,b) \Rightarrow c \mid a\ e\ c \mid b$

$\Rightarrow c \mid a\ e\ c \mid (b-na)$

$\Rightarrow c \mid d$

Como c e d são ambos positivos, segue que $c = d$. ■

Em virtude do algoritmo da divisão euclidiana e do Lema de Euclides, podemos obter o Algoritmo de Euclides para o cálculo do máximo divisor comum procedendo da seguinte maneira:

Dados $a, b \in \mathbb{Z}$, segue da divisão euclidiana que existem $q_1, r_1 \in \mathbb{Z}$ tal que $b = aq_1 + r_1$. Assim

$$mdc(a, b) = mdc(a, a.q_1 + r_1)$$

Segue agora do Lema de Euclides que

$$mdc\ (a, b) = mdc\ (a, a.q_1 + r_1) = mdc\ (a, r_1)$$

Da mesma forma, para os inteiros $a, r_1 \in \mathbb{Z}$ segue da divisão euclidiana que existem $q_2, r_2 \in \mathbb{Z}$ tal que a $= r_1 q_2 + r_2$. Assim

$$mdc\ (r_1, a) = mdc\ (r_1, r_1 q_2 + r_2)$$

Segue agora do Lema de Euclides que

$$mdc\ (r_1, a) = mdc\ (r_1, r_1 q_2 + r_2) = mdc\ (r_1, r_2)$$

Portanto, podemos concluir que

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

Procedendo desta forma, de maneira recursivamente, o $mdc\ (a, b)$ será o ultimo resto não nulo.

No exemplo para $a = 82$ e $b = 30$, temos que

$$mdc\ (82{,}30) = mdc(30{,}22) = mdc(22{,}8) = mdc(8{,}6) = mdc(6{,}2) = 2$$

A seguir, apresentaremos um resultado clássico, que afirma que se d é o máximo divisor comum entre dois inteiros a e b então, d pode ser escrito como soma de um múltiplo de a com um múltiplo de b. Isto permitirá concluir que todo divisor comum de a e b será um divisor de $d = mdc(a, b)$.

Teorema 1.6 (Teorema de Be'zout):

Se $d = mdc\ (a, b)$ então existem $s, t \in \mathbb{Z}$ tal que $d = s.a + t.b$

Prova: Seja $B = \{m.a + n.b; m, n \in \mathbb{Z}\}$. Pelo Princípio da Boa Ordem existe $c \in B$ menor inteiro positivo e $c = s.a + t.b$ com $s, t \in A$.

Suponha por absurdo que c não divide a. Então, existem $q, r \in \mathbb{Z}$ tal que $a = q.c + r$, com $0 < r < c$. Logo,

$$r = a - q.c = a - q.(s.a + t.b) = (1 - q.s).a + (-q.t).b$$

Então, $r \in B$ (ABSURDO), pois $0 < r < c$ e c é menor inteiro positivo de B. Como $d = mdc(a, b)$, temos que d é divisor comum de a e b. Então

$$a = k_1.d \text{ e } b = k_2.d \Rightarrow c = s.a + t.b = s.(k_1.d) + t.(k_2.d) \Rightarrow d \mid c.$$

Como d e c são positivos temos $d \leq c$. Mas como $d < c$ não é possível pois d é o maior divisor comum de a e b então $d = c$ e $d = s.a + t.b$. ■

O corolário abaixo pode ser usado como definição de máximo divisor comum, e mostra que todo divisor comum de a e b, necessariamente é um divisor do máximo divisor comum de a e b, denotado por $mdc\ (a, b)$.

Corolário 1.7: Se c divide a e b e $d = mdc(a, b)$ então c divide d.

Prova: Sendo $d = mdc(a, b)$. Pelo teorema, temos que $d = s.a + t.b$.
Como $c \mid a$ e $c \mid b$ temos que $d = s.(k_1.c) + t.(k_2.c)$. Logo $c \mid d$. ■

Diremos que a *e* b são ***relativamente primos*** *quando* $mdc(a, b) = 1$

Um conjunto A munido da operação de soma e produto, denotado por $(A, +, *)$, é chamado anel se, para quaisquer elementos $a, b, c \in A$, satisfazem as propriedades a seguir:

i. **Comutatividade**: $a + b = b + a \ e \ a * b = b * a$
ii. **Associatividade**: $(a + b) + c = a + (b + c) \ e \ (a * b) * c = a * (b * c)$
iii. **Existência de elementos neutros (0 e 1)**:
$a + 0 = 0 + a = a \ e \ a * 1 = 1 * a = a$
iv. **Existência de simétrico** $\forall \ a \in A, \ \exists -a \in A ; \ a + (-a) = 0$
v. **Distributividade**: $a * (b + c) = a * b + a * c$

É fácil ver que os elementos neutros da soma e produto em um anel são únicos. De fato, supondo que 0 e $0'$ são elementos neutro da soma, segue que $0 = 0 + 0' = 0'$. Analogamente, supondo que 1 e $1'$ são elementos neutros do produto, segue que $1 = 1 * 1' = 1'$

O conjunto $\mathbb{Z}$ dos inteiros munido da operação de soma e produto satisfaz as propriedades acima é chamado de anel dos inteiros.

Estamos interessados em trabalhar no seguinte subconjunto dos números complexos $\mathbb{C}$ definido por

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

É fácil observar que o conjunto $\mathbb{Z}[i]$ munido das operações de soma e produto:

$$(+)\ z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)\,i$$

$$(*)\ \ z_1 * z_2 = (a_1 + b_1 i) * (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)\,i$$

satisfazem as propriedades definidas acima e este conjunto é conhecido como anel dos inteiros de Gauss.

Dizemos que um anel $(A, +, *)$ é ***um domínio*** quando possui a seguinte propriedade adicional para todos os elementos $a, b \in A$

$$ab = 0 \ \Rightarrow\ \ a = 0 \quad ou \quad b = 0$$

Podemos notar que o anel dos inteiros $(\mathbb{Z}. +, *)$ é um domínio, assim como o conjunto dos números irracionais $(\mathbb{Q}, +, *)$, o conjunto dos números reais $(\mathbb{R}, +, *)$ e o conjunto dos números complexos $(\mathbb{C}, +, *)$, munidos com suas operações de soma e produto usuais, são exemplos de domínios.

Definição 1.8 (**Unidade/Elemento Inverso**): Seja A um anel. Diremos que $a \in A$ é uma unidade ou é inversível se existe $b \in A$, tal que $a\,.\,b = 1$, e neste caso, diremos que b é o inverso de a.

É fácil ver que o inverso de um elemento, caso exista, é único. De fato, se b e b' são inversos de a temos $b = b.1 = b.(a.b') = (b.a).b' = 1.b' = b'$

Definição 1.9 (Números Primos): Um número inteiro $p \geq 2$ é dito primo se os seus únicos divisores são um dos elementos do conjunto $\{1, -1, p, -p\}$

Por exemplo, $2,3,5,7,11, \ldots$, são números primos em $\mathbb{Z}$. Um dos primeiros a produzir tabelas de números primos, foi Eratóstenes no terceiro século a.C. Ele escrevia inicialmente uma lista com todos os números de 1 a 100. Em seguida escolhia o primeiro primo 2, e eliminava da lista todos os seus múltiplos. Passava ao número seguinte que não fora eliminado e procedia também eliminando todos os seus múltiplos. Desta forma Eratóstenes produziu tabelas de primos, mais tarde este procedimento passou a se chamar de crivo de Eratóstenes.

Assim obtemos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89. 91, 97, ... A partir desse procedimento podemos simplificar a descobertas de primos usando o seguinte Lema:

Se um número natural $n > 1$ não é divisível por nenhum primo p tal que $p^2 \leq n$, então ele é primo.

Este lema fornece um teste de primalidade, pois, para verificar se um dado número n é primo, basta verificar que não é divisível por nenhum p que não supere $\sqrt{n}$. Uma pergunta natural é se existem infinitos números primos. A resposta é afirmativa e foi dada por Euclides por volta de 300 a.C. Apresentaremos a seguir três provas elementares deste resultado, incluindo a prova dada por Euclides.

Teorema 1.10: A sequência dos números primos é infinita.

Prova 1: Euclides supôs que a sucessão $p_1 = 2, p_2 = 3, \ldots, p_r$ dos r números primos seja finita. Façamos $P = p_1 . p_2 \ldots p_r + 1$ e seja p um numero primo que divide P. Esse número não pode ser igual a qualquer um dos números $p_1, p_2, \ldots, p_r$ porque então ele dividiria a diferença $P - p_1 . p_2 \ldots p_r = 1$, o que é impossível. Assim p é um número primo que não pertence à sucessão e, por conseqüência, $p_1, p_2, \ldots, p_r$ não podem formar o conjunto de todos os números primos. ■

Prova 2: Em 1878, o matemático alemão Ernst Kummer (1810-1893) deu a seguinte variante da demonstração de Euclides:

Suponha por absurdo que exista somente um número finito n de números primos, isto é, digamos que:

$$(p_1 = 2) < p_2 < \cdots < p_n$$

e seja N o produto de todos os primos, isto é, $N = p_1.p_2 \ldots p_n > 2$.

Como o número $(N-1)$ é inteiro, ao olharmos para sua fatoração em números primos, temos que $(N-1)$ teria um fator primo p_i, .e p_i também é um fator primo do N. Assim este fator p_i dividiria $1 = N - (N-1)$, o que é absurdo. ■

Prova 3: A demonstração de Métrod de 1917 é igualmente muito simples.

Suponha por absurdo que exista somente um número finito n de números primos, isto é, digamos que:

$$(p_1 = 2) < p_2 < \cdots < p_n$$

e seja N o produto de todos os primos, isto é, $N = p_1.p_2 \ldots p_n > 2$.

Para cada $i = 1, \ldots, n$, defina $Q_i = \frac{N}{p_i}$ e $S = Q_1 + \cdots + Q_n$. Claramente temos que p_j divide todos os Q_i se $(j \neq i)$ e p_j não divide Q_j . Assim nenhum p_j pode dividir S, pois senão p_j dividiria $S - \left(Q_1 + \cdots + \widehat{Q_j} + \cdots Q_n\right) = Q_j$. Como o número S é inteiro, ao olharmos para sua fatoração em números, existiria um primo $q \neq p_j$ para todo $j = 1, \ldots, n,$. o que gera um absurdo pois assumimos que somente existem os primos $p_1, \ldots, p_n$. ■

Sendo A um domínio qualquer, apresentaremos a seguir a noção de elemento irredutível e elemento primo em A, e veremos que em alguns domínios esta noção coincide.

Definição 1.11 (*Elemento Irredutível*): Seja A um domínio com $a, b, p \in A$. Diremos que p é ***elemento irredutível*** em A se $p = a.b$ então a é unidade ou b é unidade.

Definição 1.12 (*Elemento primo*): Seja A um domínio com $a, b, p \in A$. Diremos que p é ***elemento primo*** em A se p divide $(a.b)$ então p divide a ou p divide b.

Proposição 1.13: *Seja A um domínio.*

Se p é primo em A então p é irredutível em A.

Prova: Vamos mostrar que $p = ab$ então a é unidade ou b é unidade. De fato, como

$$p = ab \Rightarrow p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b$$

Caso $p|a$: Segue que

$$a = k_1.p \Rightarrow p = a.b = (k_1.p).b \Rightarrow p - k_1.p.b = 0 \Rightarrow p.(1 - k_1.b) = 0.$$

Como A é domínio e $p \neq 0$. Segue que

$$(1 - k_1 b) = 0 \Rightarrow k_1 b = 1 \Rightarrow b \text{ é } unidade.$$

Caso $p|b$: Segue que

$$b = k_2.p \Rightarrow p = a.b = a.(k_2.p) \Rightarrow p - a.k_2.p = 0 \Rightarrow p.(1 - ak_2) = 0\,.$$

Como A é domínio e $p \neq 0$. Segue que

$$(1 - k_2 a) = 0 \Rightarrow k_2 a = 1 \Rightarrow a \text{ é } unidade. \quad \blacksquare$$

Convêm observar que a recíproca do resultado anterior é falsa, isto é, em um domínio A, temos que um elemento p irredutível em A não implica que p seja primo em A. De fato, basta considerar o seguinte domínio

$$A = \mathbb{Z}\left[i\sqrt{5}\right] = \{\, a + bi\sqrt{5} \;;\; a, b \in \mathbb{Z} \,\}$$

Neste domínio, podemos escrever o elemento 6 de 2 maneiras distintas em produto de elementos irredutíveis, ou seja,

$$6 = 2.3 = \left(1 + i\sqrt{5}\right)(1 - i\sqrt{5})$$

Temos que 2 é um elemento irredutível em $A = \mathbb{Z}\left[i\sqrt{5}\right]$ e além disso:

- 2 divide $\left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right) = 6$
- 2 não divide $\left(1 + i\sqrt{5}\right)$

Com efeito, se 2 divide $\left(1+i\sqrt{5}\ \right)$ então existe $\left(a+bi\sqrt{5}\right)$ tal que

$$\left(1+i\sqrt{5}\right)=2\left(a+bi\sqrt{5}\right).$$

Temos, então que $\left(1+i\sqrt{5}\right)=2a+2bi\sqrt{5}$. Logo,

$$\begin{cases} 2a=1 \Longrightarrow a=\dfrac{1}{2}\notin \mathbb{Z} \\ 2b=1 \Rightarrow b=\dfrac{1}{2}\notin \mathbb{Z} \end{cases}$$

E, analogamente, 2 não divide $\left(1-i\sqrt{5}\ \right)$. E pela definição concluímos que 2 não é um elemento primo em $A=\ \mathbb{Z}\left[i\ \sqrt{5}\ \right]$.

Definição 1.14 (Domínio de Fatoração Única): Um domínio A é chamado domínio de fatoração única (DFU) se todo elemento não nulo e não inversível de A pode ser escrito de maneira única a menos da ordem, como produto de elementos irredutíveis.

$A=\ \mathbb{Z}\left[\ i\sqrt{5}\right]$ NÃO é domínio de fatoração única, pois o elemento 6 tem duas fatorações distintas em elementos irredutíveis em A. Veremos que quando A é DFU temos que todo elemento irredutível p em A é um elemento primo e vice-versa.

Proposição 1.15: *Seja A um domínio de fatoração única (DFU).*

$$p \text{ é irredutível em } A \ \Leftrightarrow\ p \text{ primo em } A.$$

Prova:

(⇐) Foi feito na proposição anterior.

(⇒) Seja p irredutível em A. Supondo que p divide ab e que p não divide a, vamos mostrar que p divide b. De fato. Como p divide ab segue que $ab=pk$ e como p é irredutível e p não divide a, segue que p aparece na fatoração do b. Portanto, p divide b e , consequentemente, p é primo em A. ■

Em virtude do conjunto dos números inteiros $\mathbb{Z}$ ser um domínio Fatorial, a decomposição de um elemento em fatores irredutíveis, se torna uma decomposição em fatores primos.

Teorema 1.16 (Teorema Fundamental da Aritmética):

Todo inteiro $a \geq 2$ ou é primo ou se escreve de maneira única, a menos da ordem dos fatores, como um produto de números primos.

Prova (**por indução**): Se $n = 2$, o resultado é obviamente verificado. Suponhamos o resultado valido para todo número inteiro menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números inteiros positivos n_1 e n_2 tais que $n = n_1 n_2$ com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$, tais que $n_1 = p_1 \ldots p_r$ e $n_2 = q_1 \ldots q_s$. Portanto $n = n_1 . n_2 = p_1 \ldots p_r . q_1 \ldots q_s$.

Vamos agora provar a unicidade da escrita, Suponha que tenhamos $n = p_1 \ldots p_r = q_1 \ldots q_s$, onde os p_1 e os q_j são números primos. Como $p_1 \mid q_1 \ldots q_s$ temos que $p_1 = q_j$ para algum j, que após reordenamento de $q_1, \ldots, q_s$ podemos supor que seja q_1. Portanto

$$p_2 \ldots p_r = q_2 \ldots q_s.$$

Como $p_2 \ldots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. ■

O Teorema Fundamental da Aritmética mostra que todo número inteiro $a \geq 2$ decompõe-se em fatores primos. Isso já mostra a importância dos números primos na aritmética. Essa importância não se restringe apenas ao aspecto teórico, ela está presente no nosso cotidiano.

Quando efetuamos uma transação bancária, seja num terminal de atendimento ou pela internet, fornecemos informações sigilosas. Para que o sigilo dessas informações seja mantido elas são codificadas por processos baseados em números primos. Nesses processos são utilizados números extremamente grandes. Quanto maiores forem os números primos utilizados, mais eficiente se torna a codificação da informação. Daí o interesse e a importância de se descobrirem números primos cada vez maiores. Além de

transações bancárias, muitas outras informações sigilosas trocadas pela internet também são codificadas.

No ensino básico, aprendemos que o máximo divisor comum de dois inteiros positivos a e b é o número obtido ao se tomar o produto de todos os fatores primos comuns de a e b, cada um desses fatores sendo escolhido com o menor expoente que aparece nas fatorações de a e b. Apresentamos a seguir uma demonstração desse fato.

Apresentamos a seguir uma demonstração desse fato.

Proposição 1.17: *Sejam a e b inteiros não negativos e não simultaneamente nulos com decomposições em fatores primos dadas por:*

$$a = p_1^{m_1} \dots p_s^{m_s} \cdot q_1^{k_1} \dots q_t^{k_t},$$

$$b = p_1^{n_1} \dots p_s^{n_s} \cdot r_1^{l_1} \dots r_t^{l_u},$$

em que os primos p_i, q_j, r_k são todos distintos onde $i \in \{1, \dots, s\}$, $j \in \{1, \dots, t\}$ e $k \in \{1, \dots, u\}$ todos os expoentes são positivos. Então

$$mdc(a, b) = p_1^{x_1} \dots p_s^{x_s}$$

em que $x_i = min\{m_i, n_i\}$ para $i = 1, \dots, s$

Prova: Seja $d = p_1^{x_1} \dots p_s^{x_s}$. Vamos mostrar que:

(1) $d \mid a$ e $d \mid b$

(2) $se\ c \in \mathbb{Z}\ tal\ que\ c \mid a\ e\ c \mid b\ então\ c \mid d$

Como $d > 0, x_i \leq m_j\ e\ , x_i \leq n_j$, (para $i = 1, \dots, s$), temos que $a = a_1 . d$ em que

$$a_1 = p_1^{m_1 - x_1} \dots p_s^{m_s - x_s} \cdot q_1^{k_1} \dots q_t^{k_t}$$

e $b = b_1 . d$ em que

$$b_1 = p_1^{n - x_1} \dots p_s^{n_s - x_s} \cdot r_1^{l_1} \dots r_t^{l_t}$$

Logo, $d|a$ e $d|b$, o que mostra (1).

Para mostrar (2) seja $c \mid a\ e\ c \mid b$. Temos, pelo Teorema Fundamental da Aritmética, c pode ser escrito como

$$c = p_1^{e_1} \dots p_s^{e_s}, \text{ em que } 0 \leq e_i \leq min\{m_i, n_i\}, \text{ para } i = 1, \dots, s.$$

Como $e_i \leq x_i$ (para $i = 1, \dots, s$), temos que:

$$d = p_1^{x_1} \dots p_s^{x_s} = \left(p_1^{e_1} \dots p_s^{e_s}\right)\left(p_1^{x_1 - e_1} \dots p_s^{x_s - e_s}\right) = c.\left(p_1^{x_1 - e_1} \dots p_s^{x_s - e_s}\right),$$

ou seja, $c|d$. ■

Exemplo 1.18: Determine o $mdc\ (450, 375)$.

Solução: Pela decomposição em fatores primos temos: $450 = 2.3^2.5^2$ e $375 = 3.5^3$. Pela definição de máximo divisor comum devemos selecionar os fatores primos comuns e elevar ao menor expoente que apareceu na decomposição. Logo:

$$mdc(450{,}375) = 3.5^2 = 75$$

Outro conceito importante abordado no Ensino Básico é o mínimo múltiplo comum (mmc). Assim como vimos que se a e b forem inteiros simultaneamente não nulos, então existe o maior divisor comum de a e b e que é possível calculá-lo por meio do algoritmo de Euclides, analogamente, se a e b forem não nulos, podemos considerar os múltiplos positivos comuns deles. O menor inteiro positivo que seja múltiplo tanto de a quanto de b (o qual existe pelo princípio da boa ordenação) é chamado mínimo múltiplo comum de a e b.

O mínimo múltiplo comum entre dois números positivos a e b é o número obtido ao se multiplicar os fatores primos comuns de a e b, cada um deles sendo tomado com o maior de seus expoentes que aparece nas decomposições de a e b, pelos fatores primos não comuns, esses com seus respectivos expoentes.

Proposição 1.19 (Cálculo do mmc): *Sejam a e b inteiros positivos, com decomposição em fatores primos descritas por:*

$$a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} \quad e \quad b = p_1^{s_1} p_2^{s_2} \dots p_s^{s_k},$$

em que cada fator p_i é um número primo distinto, $r_i \geq 0$ e $s_i \geq 0\ para\ i = 1, \dots, k$. Então,

$$mmc(a, b) = p_1^{t_1} \dots p_k^{t_k}$$

em que $t_i = max\{r_i, s_i\}$

Prova: Seja $m = mmc(a, b)$. Como m é múltiplo de a, todos os fatores primos $p_1 \dots, p_k$ aparecem na fatoração de m, com expoentes maiores ou iguais a $r_1 \dots, r_k$, respectivamente. Analogamente, como m também é múltiplo de b, os expoentes de $p_1 \dots, p_k$ na fatoração de m são maiores ou iguais a $s_1 \dots, s_k$, respectivamente. Mas qualquer múltiplo comum de a e de b, genericamente, é da forma $c = q(p_1^{t_1} \dots p_k^{t_k})$, em

que q é um inteiro e $t_i \geq max\{r_i, s_i\}$. Além disso, todo inteiro dessa forma é múltiplo comum de a e b pois podemos escrevê-lo como:

$$c = a.q(p_1^{t_1-r_1} \dots p_k^{t_k-r_k}) \quad \text{e} \quad c = b.q(p_1^{t_1-s_1} \dots p_k^{t_k-s_k})$$

em que os expoentes $t_1 - r_1$ *e* $t_1 - r_1$ são não negativos para todo $i = 1, \dots, k$. Portanto, o menor múltiplo comum positivo de a e b é obtido quando temos $q = 1$ e $t_i = max\{r_i, s_i\}$, para $i = 1, \dots, k$.

Exemplo 1.20: Determine o $mmc\ (450, 375)$

Solução: Pela decomposição em fatores primos temos: $450 = 2.3^2.5^2$ e $375 = 3.5^3$. Pela definição acima temos: $mmc(450{,}375) = 2.3^2.5^3 = 2250$

Para calcularmos o mínimo múltiplo comum entre dois números, no Ensino Básico, usamos um dispositivo prático chamado de Método da decomposição simultânea:

450,	375	2
225,	375	3
75,	125	3
25,	125	5
5	25	5
1	5	5
1	1	

Logo, $mmc(450{,}375) = 2.3.3.5.5.5 = 2250$

Existe uma estreita relação entre o máximo divisor comum e o mínimo múltiplo comum de dois números inteiros positivos não nulos. Esta relação possibilita estabelecer propriedades de um deles a partir das propriedades do outro.

Proposição 1.21: *Se a e b forem inteiros positivos não nulos temos que*

$$mdc(a, b).\ mmc(a, b) = a.b$$

Prova: Se $d = mdc(a, b)$, certamente $\frac{ab}{d}$ é um inteiro. Como a e b são não nulos e d é positivo, temos que $\frac{ab}{d} > 0$. Além disso, como d é divisor de a e b, existem inteiros a_1 *e* b_1 tais que $a = a_1.d$ e $b = b_1.d$. Logo,

$$\frac{ab}{d} = \frac{a_1.d.b_1.d}{d} = a_1.d.b_1 = a_1.b_1.d = a.b_1 = a_1.b.$$

Isso mostra que

$$\frac{ab}{d} \text{ é múltiplo de } a \text{ e } b.$$

Mas se c for um múltiplo de a e b, temos que

$$\frac{ab}{d} \text{ divide } c$$

De fato, se $d = mdc(a,b)$ então, existem inteiros x e y tais que $xa + yb = d$. Multiplicando ambos os membros por c, temos: $xac + ybc = dc \ \ (I)$.

Como a/c e b/c sabemos que existem inteiros positivos a_1 e b_1, tais que:

$$c = aa_1 \quad e \quad c = bb_1 \ \ (II)$$

Substituindo convenientemente (II) em (I) temos:

$$xa(bb_1) + yb(aa_1) = dc$$

ou seja,

$$ab(xb_1 + ya_1) = dc.$$

Portanto $\frac{ab}{d}$ divide c. Pela definição de mínimo múltiplo comum temos que $\frac{ab}{d} = mmc(a,b)$. Assim, como $d = mdc(a,b)$ temos:

$$mdc(a,b).\ mmc(a,b) = a.b \quad \blacksquare$$

CAPÍTULO 2

"A Matemática é a rainha das Ciências, e a Teoria dos Números é a rainha da Matemática. "

C. F. Gauss

Entre os anos de 1808 e 1825, o matemático alemão Carl F. Gauss investigava questões relacionadas à reciprocidade cúbica e biquadrática envolvendo números primos p e q, quando percebeu que essa investigação se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$, o anel dos inteiros gaussianos.

Gauss estendeu a ideia de número inteiro quando definiu o conjunto $\mathbb{Z}[i]$, pois descobriu que muito da antiga teoria de Euclides sobre fatoração de inteiros poderia ser transportada para $\mathbb{Z}[i]$ com conseqüências importantes para teoria dos números. Ele desenvolveu uma teoria de fatorização em primos para esses números complexos e demonstrou que essa decomposição em números primos é única, como acontece com o conjunto dos números inteiros.

Nesse capítulo abordaremos a história de Gauss, situando o leitor na importância da continuidade e da ampliação dos estudos da teoria dos números em outro conjunto. Serão apresentadas todas as definições, teoremas, lemas e corolários necessários para essa ampliação.

A apresentação dos inteiros de Gauss no Ensino Médio não é feita explicitamente. O tópico abordado é o conjunto dos números complexos sem ser feita nenhuma comparação explícita com a teoria dos números já estudada no Conjunto dos números inteiros. Nenhum cálculo é feito em relação ao máximo divisor comum entre os inteiros de Gauss. Nenhum questionamento sobre as definições de números primos ou fatoração única para números inteiros são questionadas para os inteiros de Gauss.

2.1. **Teoria dos Números com Gauss**

Considerado como um dos maiores matemáticos, Carl Friedrich Gauss nasceu em Brunswich na Alemanha, em 1777, tendo demonstrado desde muito cedo os seus dotes para a Matemática. As suas contribuições para a Teoria dos Números, dos Números Complexos, da Geometria e da Álgebra são inúmeros. Por exemplo, a sua tese de doutoramento foi a primeira demonstração do teorema fundamental da Álgebra. Gauss teve também uma importante contribuição para a Astronomia, tendo-se interessado pelo estudo das órbitas planetárias e pela determinação da forma da Terra. Um exemplo dessa contribuição foi o desenvolvimento de um método para calcular, com grande precisão, os parâmetros de uma órbita planetária a partir de apenas três observações da posição do planeta. A partir de 1831, juntamente com Wilhelm Weber, desenvolveu o estudo teórico e experimental do eletromagnetismo. Por fim, outro importante contributo de Gauss para a ciência foi a determinação do campo magnético terrestre. Em reconhecimento desta contribuição, a unidade de campo magnético ficou com o seu nome.

O matemático alemão Carl F. Gauss (1777–1855) estendeu a ideia de número inteiro definindo o anel dos inteiros algébricos gaussianos, $\mathbb{Z}[i]$, e posteriormente na tentativa de se demonstrar o Último Teorema de Fermat. A Teoria dos Números Algébricos é uma das mais belas e profundas teorias em toda a Matemática.

A primeira motivação dessa investigação diz respeito à generalização do teorema da representação única dos números inteiros como um produto de números primos, a menos da ordem dos fatores, para inteiros algébricos. Gauss introduziu o anel dos inteiros algébricos, $Z[i]$, durante sua investigação sobre resíduos biquadráticos, e mostrou que nesse anel a fatoração em elementos primos existe, e é única a menos da ordem dos fatores.

2.2. **Inteiros de Gauss**

A seguir apresentamos uma definição em um domínio D onde é possível realizar a divisão euclidiana.

O conjunto dos inteiros de Gauss $\mathbb{Z}[i]$ são os números complexos escritos como:

$$\mathbb{Z}[i] = \{\, a + bi \,;\, a, b \in \mathbb{Z} \,\}, \text{ onde } (i^2 = -1).$$

Exemplo 2.1:

(i) $z_1 = 9 \in \mathbb{Z}[i]$

(ii) $z_2 = -2i \in \mathbb{Z}[i]$

(iii) $z_3 = -4 + 3i \in \mathbb{Z}[i]$

(iv) $z_4 = \sqrt{5} + 2i \notin \mathbb{Z}[i]$, pois $\sqrt{5} \notin \mathbb{Z}$

(v) $z_5 = \frac{4}{3} + \frac{i}{2} \notin \mathbb{Z}[i]$, pois $\frac{4}{3} + \frac{i}{2} \notin \mathbb{Z}$

Logo, $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$.

Vejamos algumas definições importantes para a aritmética nos inteiros de Gauss.

Definição 2.2: A função norma N: $\mathbb{Z}[i] \to \mathbb{N}$ é definida para todo $z = a + bi$ por

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

onde $\bar{z}$ é o conjugado complexo de z.

Observação: É fácil ver que a função norma é multiplicativa, isto é:

$$N(z_1.z_2) = N(z_1)\,.\, N(z_2).$$

De fato: Como $\overline{z_1.z_2} = \overline{z_1}\,.\,\overline{z_2}$, então

$$N(z_1).N(z_2) = z_1\overline{z_1}\; z_2\overline{z_2} = z_1z_2\overline{z_1}\,\overline{z_2} = z_1z_2\overline{z_1z_2} = N(z_1z_2)$$

Exemplo 2.3: Calcule a norma do inteiro gaussiano $z = -2 + 3i$

Solução: $N(-2 + 3i) = (-2)^2 + (3)^2 = 4 + 9 = 13.$

Afirmação 2.4: O conjunto das unidades em $\mathbb{Z}[i] = \{ 1, -1, i, -i \}$.

De fato: Assim como em $\mathbb{Z}$, as unidades em $\mathbb{Z}[i]$, são todos os elementos $z \epsilon \mathbb{Z}[i]$ que possuem inverso multiplicativo, isto é, existe $z' \in \mathbb{Z}[i]$ tal que $z.z' = 1$. Deste modo, se $z = a + bi$ é uma unidade, segue que:

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

Mas

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

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

Observe que $z \in \mathbb{Z}[i]$ é unidade se e somente se $N(z) = 1$.

Dados $a, b \in \mathbb{Z}[i]$, diremos que $a \; divide \; b.$ se $b = a \, . k.$ para algum $k \in \mathbb{Z}[i]$. Nesse caso, dizemos que a é divisor ou fator de b.

Observe que como $(14 - 3i) = (4 + 5i)(1 - 2i)$, segue que $(4 + 5i)$ divide $(14 - 3i)$

Proposição 2.5: *Para todo* $z = a + bi \in \mathbb{Z}[i]$, *temos que*

$N(z)$ é primo em $\mathbb{Z} \Rightarrow z$ é irredutível em $\mathbb{Z}[i]$.

Prova: Suponha por absurdo que $z \neq 0$ não é irredutível em $\mathbb{Z}[i]$. Assim, podemos escrever $z = z_1.z_2$ com z_1, z_2 ambos não nulos e não inversíveis. Assim

$$N(z) = \underbrace{N(z_1)}_{>1} . \underbrace{N(z_2)}_{>1} \Rightarrow N(z) \text{ não é primo em } \mathbb{Z}. \quad \blacksquare$$

Proposição 2.6: *Para todo* $a, b \in \mathbb{Z}[i]$, *temos que*

$$a \mid b \;\Rightarrow\; N(a) \mid N(b)\,.$$

Prova: Se $a \mid b$, temos: $b = a.k$. Aplicando a função norma em ambos os membros da igualdade temos:

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

Como $N(a)\ e\ N(b)\ e\ N(k)\ \in \mathbb{Z}$, temos que $N(a) \mid N(b)$ em $\mathbb{Z}$. ■

Exemplo 2.7 Como $(4 + 5i)\ divide\ (14 - 3i)$ em função da observação, segue que

- $N(4 + 5i) = 16 + 25 = 41$
- $N(14 - 3i) = 196 + 9 = 205$

Vemos claramente que

- $41 \mid 205$ pois $205 = 41\ x\ 5$

Exemplo 2.8: Determine os divisores de $3i$ em $\mathbb{Z}[i]$.

Solução: Queremos encontrar os inteiros gaussianos $z = a + bi$, tal que $z \mid 3i$.

Se z divide $3i$ então existirá um inteiro gaussiano k tal que $3i = z.k$. Aplicando a função norma nesta igualdade obtemos que:

$$N(3i) = 9 = N(z.k) = N(z).N(k).$$

Sabendo que a norma de um inteiro gaussiano é sempre positiva, a igualdade acima só é satisfeita se uma, e apenas uma das situações abaixo ocorrerem:

- ✓ $N(z) = a^2 + b^2 = 1 \Leftrightarrow z = \pm 1\ ou\ z = \pm i$
- ✓ $N(z) = 3 \Longrightarrow z \notin \mathbb{Z}[i]$
- ✓ $N(z) = 9 \Leftrightarrow z = \pm 3\ ou\ z = \pm 3i$

Logo os divisores de $3i$ em $\mathbb{Z}[i]$ são: $\{\pm 1, \pm i, \pm 3, \pm 3i\}$ ■

Podemos observar que dado um inteiro gaussiano não nulo z, tal que $N(z) \geq 2$, para encontrar todos os seus divisores em $\mathbb{Z}[i]$ devemos calcular a norma de z e construir o conjunto D, que será formado por todos os divisores inteiros de $N(z)$. Deste conjunto, aqueles divisores que forem escritos como soma de quadrados serão as normas dos divisores de z em $\mathbb{Z}[i]$.

Teorema 2.9 (Divisão Euclidiana em $\mathbb{Z}[i]$***):*** *Para todo* $a, b\, \mathbb{Z}[i]$, *com* $b \neq 0$ *existem* $q, r \in \mathbb{Z}[i]$ *tal que*

$$a = bq + r \;\; ; \quad 0 \leq \mathrm{N}(r) < N(b)$$

Prova: Sejam $a\ e\ b \in \mathbb{Z}[i]\ e\ x, y, z\ e\ w\ \in \mathbb{Z}$ com $a = (x + yi)\ e\ b = (z + wi)$

$$\frac{a}{b} = \frac{x+yi}{z+wi} = \frac{x+yi}{z+wi}.\frac{z-wi}{z-wi} = \frac{xz - xwi + yzi - ywi^2}{z^2 - w^2 i^2} = \frac{xz+yw}{z^2+w^2} + \frac{yz-xw}{z^2+w^2}\,i$$

Tomamos $m\ e\ n$ como os inteiros mais próximos de $\frac{xz+yw}{z^2+w^2}$ e $\frac{yz-xw}{z^2+w^2}$, respectivamente.

Notemos que

- $\left|m - \frac{xz+yw}{z^2+w^2}\right| \leq \frac{1}{2}$ e
- $\left|n - \frac{yz-xw}{z^2+w^2}\right| \leq \frac{1}{2}$.

Como $q = m + ni$, então

$$r = a - bq = b\left(\frac{a}{b} - q\right) = b\left[\frac{xz+yw}{z^2+w^2} + \frac{yz-xw}{z^2+w^2}\,i - m - ni\right]$$

$$= b\left[\frac{xz+yw}{z^2+w^2} - m + \left(\frac{yz-xw}{z^2+w^2} - n\right)i\right]$$

Aplicando a função norma em ambos os membros da igualdade temos:

$$N(r) = N\left(b\,.\left[\left(\frac{xz+yw}{z^2+w^2} - m\right) + \left(\frac{yz-xw}{z^2+w^2} - n\right)i\right]\right)$$

$$\leq N(b).\left[\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right] = N(b).\left(\frac{1}{2}\right)$$

Assim, $N(r) \leq N(b)$ ■

Se p é um primo de Gauss (ou seja, não pode ser escrito como o produto de dois inteiros de Gauss cuja as normas são maiores que 1), então sendo a e b inteiros de Gauss, se p divide ab então p divide a ou p divide b.

Proposição 2.10: *Sejam a e b em $\mathbb{Z}[i]$ e p é primo em $\mathbb{Z}[i]$. Se p divide $a.b$ então p divide a ou p divide b.*

Prova: Para demonstrar, vamos fazer divisões sucessivas onde

$$\begin{cases} a_0 = a \\ a_1 = p \end{cases}$$

Denotaremos por

- a_{k+2} o resto da divisão euclidiana de $a_k \; por \; a_{k+1}$.

Temos então as divisões:

- $a_0 = q_1.a_1 + a_2$
- $a_1 = q_2.a_2 + a_3$
- $a_2 = q_3.a_3 + a_4$
- ⋮
- $a_{n-2} = q_{n-1}.a_{n-1} + a_n$
- $a_{n-1} = q_n.a_n + a_{n+1}$

Observe que:

$$a_k \neq 0 \;\Rightarrow\; N(a_{k+1}) < N(a_k)$$

Como é uma sequência decrescente limitada por zero, podemos tomar n tal que

$$N(a_{n+1}) = 0 \;\Rightarrow\; a_{n+1} = 0 \;\Rightarrow\; a_n / a_{n-1}\,.$$

Observe que:

$$a_n/a_{k+1} \; e \;\; a_n/a_k \quad \Rightarrow \;\; a_n/a_{k-1}.$$

Como

$$a_n/a_n \quad e \quad a_n/a_{n-1} \;\Rightarrow\; a_n/a_k, \;\; \forall \;\; 0 \leq k \leq n$$

e, particularmente, $a_n/a_0 = a$ e $a_n/a_1 = p$. Tomando as $(j + i)$ primeiras equações e realizando substituições adequadas, temos que:

$$a_j = x_j.a_1 + y_j.a_0 = x_j.p + y_j.a\;;$$

Particularmente, para $j = n$:

$$a_n = x_n.p + y_n.a$$

Se p divide a nada temos a fazer.

Se p não divide a, como a_n divide p e a_n divide a Do fato que

$$a_n = x_n p + y_n a \quad \Rightarrow \quad a_n \in \{1, -1, i, -i\}$$

Temos que:

$$a_n = x_n.p + y_n.a \Leftrightarrow b = a_n a_n^{-1} b = a_n^{-1}\left(px_n b + \underbrace{ab}_{p\ divide}\ y_n\right) \Longrightarrow p \mid b \quad .\blacksquare$$

Vamos introduzir a noção de máximo divisor comum (mdc) em $Z[i]$ e estenderemos a ideia da divisão euclidiana. Mostraremos que é possível escrever o máximo divisor comum entre dois inteiros gaussianos como uma combinação linear entre ambos.

Definição 2.11: Sejam $a, b, d \in \mathbb{Z}[i]$ não nulos, dizemos que d é o máximo divisor comum de a e b quando:

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

(ii) Se existe $c \in \mathbb{Z}[i]$, tal que $c \mid a \;\; e \; c \mid b$ então $N(c) \leq N(d)$.

Em outras palavras, o máximo divisor de dois ou mais inteiros gaussianos será o divisor comum com a maior norma.

Lema 2.12: Sejam $a, b \; e \; c \in \mathbb{Z}[i]$. Então:

- $mdc(a, 0) = a$;
- $mdc(a, b) = mdc(b, a) = mdc(b, a - cb)$.

Prova: Sejam $a, b\ , c\ , d \in \mathbb{Z}[i]$. É imediato que:

- $mdc(a, 0) = a$ e
- $mdc(a, b) = mdc(b, a)$.

Considere agora que

$$d = mdc(a - cb, b).$$

Da definição, temos que $d \mid b \; e \; d \mid (a - cb)$. Como $d \mid cb$. Desta forma, $d \mid a$ pois

$$a = cb + (a - cb) \quad \blacksquare$$

Definição 2.13: Sejam a *e* b inteiros Gaussianos não nulos. Dizemos que a e b são *relativamente primos* quando seus fatores comuns são apenas as unidades $\{+1, -1, +i, -i\}$.

Processo prático (Algoritmo Euclidiano) para o cálculo do máximo divisor comum entre os inteiros gaussianos não nulos a e b.

Quociente	q_1	q_2	q_3	...	q_{n-2}	q_{n-1}	q_n
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = mdc(a,b)$
Resto	r_1	r_2	r_3	...	r_{n-1}	r_n	0

Exemplo 2.14: Determine o $mdc(64-28i, 26+3i)$, utilizando algoritmo de Euclides.

Quociente	$2-i$	$1+2i$	$1+i$	$3-i$
$64-28i$	$26+3i$	$9-8i$	$1-7i$	$1-2i$
Resto	$9-8i$	$1-7i$	$1-2i$	0

Assim vemos que Gauss desenvolveu uma teoria de fatoração em primos para esses números complexos $\mathbb{Z}[i]$. Gauss demonstrou que o conjunto dos inteiros gaussianos, munido das operações de adição e multiplicação, dá origem a uma estrutura denominada de Domínio Euclidiano. Além disso, os inteiros gaussianos admitem uma decomposição em primos, essa decomposição é única, assim como no conjunto dos inteiros. Entretanto, as questões de divisibilidade se tornam complexas nesse domínio. Observe que 5 é um número primo em $\mathbb{Z}$, mas deixa de ser primo em $\mathbb{Z}[i]$. De fato,

$$(1 + 2i).(1 - 2i) = 1 - 2i + 2i - 4i^2 = 1 - 4.(-1) = 5.$$

pois 5 não divide $(1+2i)$ e 5 não divide $(1-2i)$.

Definição 2.15 (**Domínio Euclidiano**): Um Domínio Euclidiano $(D, +, ., \varphi)$ é um domínio $(D, +, .)$ com uma função $\varphi: D\backslash\{0\} \to N = \{0,1,2,3, \dots\}$ satisfazendo as seguintes propriedades:

(1) $\forall\, a, b \in D, b \neq 0, existem\ t, r \in D\ tais\ que\ a = b.t + r\ com \begin{cases} \varphi(r) < \varphi(b) \\ ou \\ r = 0 \end{cases}$;

(2) $\forall\, a, b \in D\backslash\{0\}$, $\varphi(a) \leq \varphi(a.b)$.

Exemplo 2.16: O anel dos números inteiros $(\mathbb{Z}, +, ., |\ |)$ é um domínio euclidiano com a função valor absoluto dada por $|\ |: \mathbb{Z} \to \mathbb{N}$ onde $n \mapsto |n|$.

Solução: De fato, $(Z, +, .)$ é $um\ Domínio$ e $\forall\ a, b\ \in Z, com\ b \neq 0, \exists\ t, r\ \in Z$ tais que:

$$a = b.t + r\ com \begin{cases} |r| < |b| \\ ou \\ r = 0 \end{cases} \quad \text{e} \quad \forall\ a, b\ \in Z\backslash\{0\}\ , |a| \leq |a.b|$$

Exemplo 2.17: O anel dos números inteiros $(\mathbb{Z}, +, \ .\ , \mathrm{N})$ é um domínio euclidiano com a função norma dada por $\mathrm{N}: \mathbb{Z} \to \mathbb{N}$ onde $a \mapsto a^2$.

Solução: De fato, para todo $a, b\ \in \mathbb{Z} - \{0\}$ tem-se $N(a) \leq N(a.b)$. Logo

$$N(r) = r^2 < b^2 = N(b) \Leftrightarrow |r| < |b|$$

onde $\mathrm{N}: \mathbb{Z} \to \mathbb{N}$ é a restrição da função $N: (\mathbb{C} = \mathbb{R} + \mathbb{R}i) \to \mathbb{R}$ dada por

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

Veremos que o anel dos inteiros de Gauss $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ munido da função norma $N: \mathbb{Z}[i] \to \mathbb{N}$ dada por $N(a + bi) = a^2 + b^2$ é um domínio euclidiano.

Teorema 2.18: *O anel dos inteiros de Gauss* $\mathbb{Z}[i]$ *é um Domínio Euclidiano.*

Prova: Como $\mathbb{Z}[i]\ \subseteq\ \mathbb{C}$ e $\mathbb{C}$ é um corpo, temos que $\mathbb{Z}[i]$ é um domínio. Vamos mostrar que a norma induzida pela norma dos números complexos é uma norma euclidiana, ou seja, $N: \mathbb{Z}[i] \to \mathbb{N}$ definida por $N(a + bi)\ =\ a^2\ +\ b^2$ para todo $a, b\ \in \mathbb{Z}$ é uma norma euclidiana.

(1) Se $\alpha, \beta\ \in\ \mathbb{Z}[i]$ e β divide α então $\alpha = \beta\ \theta$ para algum $\theta\ \in\ \mathbb{Z}[i]$. Neste caso, $N(\beta) = N(\alpha).N(\theta)$ o que implica $N(\beta) \leq N(\alpha)$.

(2) Dados $\alpha, \beta\ \in\ \mathbb{Z}[i]$ com $\beta \neq 0$ temos que mostrar que existem então $t, r\ \in\ \mathbb{Z}[i]$ tais que para algum $\alpha = \beta\ t + r$. com $r\ =\ 0$ ou $N(r) < N(\beta)$, isto é, procuramos um elemento $t\ \in\ \mathbb{Z}[i]$ tal que

$$N(r) = N(\alpha - \beta.t) = N\left[\beta.\left(\frac{\alpha}{\beta} - t\right)\right] = N(\beta).N\left(\frac{\alpha}{\beta} - t\right) < N(\beta)$$

Isto é, procuramos $t \in Z[i]$ tal que $N\left(\frac{\alpha}{\beta} - t\right) < 1$. Como

$$\frac{\alpha}{\beta} \in \mathbb{C} = \mathbb{R} + \mathbb{R}i \Rightarrow \frac{\alpha}{\beta} = x + iy$$

Afirmamos que x e y podem ser efetivamente calculados e pertencem a $\mathbb{Q}$. De fato. Sendo $\alpha = a + bi$ e $\beta = c + di$, temos que

$$\frac{1}{\beta} = \frac{1}{c+di} = \frac{c-di}{c^2+d^2} = \frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}\, i \ .$$

Logo

$$\alpha.\frac{1}{\beta} = (a + bi).\left(\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i\right) = \underbrace{\frac{ac+bd}{c^2+d^2}}_{x} + \underbrace{\frac{bc-ad}{c^2+d^2}}_{y} i \ \in \mathbb{Q} + \mathbb{Q}i \ .$$

Agora, escolhemos $e, f \in \mathbb{Z}$ tal que

$$|x - e| \leq \frac{1}{2} \quad e \quad |y - f| \leq \frac{1}{2} \ .$$

E claro que, x e y sendo efetivamente calculáveis, tais elementos e e f podem ser efetivamente computados. Tomando $t = e + if$ temos que

$$N\left(\frac{\alpha}{\beta} - t\right) = N(\,(x + iy) - (e + if)\,) = N\big((x - e) + i(y - f)\big) =$$

$$= (x - e)^2 + (y - f)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1 \ .$$

Logo, o elemento $t = e + i\,f$ satisfaz a propriedade desejada. Além disso, o elemento t é efetivamente calculado. Naturalmente o elemento $r = \alpha - \beta t$ é efetivamente calculado também. ■

Um domínio fatorial D é um domínio se todo elemento não inversível de D se escreve de maneira única a menos da ordem como produto de elementos irredutíveis de D.

Desta forma, dados $a, b \in D$, podemos escrever

$$\begin{cases} a = p_1 \dots \dots \ p_n \text{ , com } p_i \text{ irredutível} \\ b = q_1 \dots \dots \ q_m \text{ , com } q_j \text{ irredutível} \end{cases}$$

Caso a e b tenham fatores irredutíveis comum, o $mdc(a, b)$ será o produto desses fatores comuns, caso contrário, o $mdc\ (a, b) = 1$.

Teorema 2.19: *Se (D, φ) um Domínio Euclidiano então D é um Domínio Fatorial*

Prova: Existência da fatoração

Seja $\delta = inf\{\varphi(d); d\ não\ invertível\}$. Afirmação:

$$\{a \in D;\ \varphi(a) = \delta\} \subseteq \{irredutíveis\ de\ D\}$$

De fato:

$$a \neq 0 \ \Rightarrow \ \varphi(a) = \varphi(a.1) \geq \varphi(1) \ \Rightarrow \ \varphi(1) \leq \varphi(a), \ \forall \ a \neq 0.$$

Seja $a \in \{a \in D; \varphi(a) = \delta\} \Rightarrow \varphi(a) = \delta > \varphi(1)$ pois

$$\varphi(d) > \varphi(1), \qquad \forall\, d \ \in D\ não\ invertível$$

$\Rightarrow a$ não é invertível em D. (Senão $\varphi(a) = \varphi(1)) \ \Rightarrow a$ é $irredutível\ em\ D$.

Com efeito,

$a = b.c\ com\ c\ não\ invertível \ \Rightarrow \varphi(b) < \varphi(b.c) = \varphi(a) = \delta$

$$\xRightarrow[minimalidade\ de\ \delta]{} b \text{ é } invertível\ em\ D.$$

$\varphi(a) = inf\{\varphi(d); d\ não\ invertível\ em\ D\} \Rightarrow a$ é $irredutível \ \Rightarrow a =$
$a\ como\ produto\ de\ irredutíveis$

$$\text{Se } \varphi(a) > inf\{\varphi(d); d\ não\ invertível\ em\ D\}$$

Suponha, por indução que:

$$\left[\begin{array}{c} \forall\, b \in D, b\ não\ invertível \\ \varphi(b) < \varphi(a) \end{array} \right] \Rightarrow \left[\begin{array}{c} b\ possui\ uma\ fatoração \\ em\ elementos\ irredutíveis. \end{array} \right]$$

Queremos mostrar que a possui também tal fatoração.

De fato: Se a é irredutível então possui tal fatoração.

Se a não é irredutível temos:

$$\exists\, b, c \in D, \text{não } invertíveis \text{ tais que } a = b.c \Rightarrow \begin{cases} \varphi(b) < \varphi(b.c) = \varphi(a) \\ (c \text{ não } invertível) \\ \varphi(c) < \varphi(b.c) = \varphi(a) \\ (b \text{ não } invertível) \end{cases}$$

$\overset{H.I}{\Rightarrow}$ tanto b quanto c possui uma fatoração em elementos irredutíveis

⇒ colocando juntas estas duas fatorações

⇒ obtemos uma fatoração para $b.c$

⇒ obtemos uma fatoração de $a = b.c$

Unicidade da Fatoração. Vamos mostrar que:

Se p é irredutível e p divide $(a.b)$ então p divide a ou p divide b.

Lembre-se que p é irredutível **não implica** p primo. Com efeito

$$6 = 2.3 = \left(1 + \sqrt{5}i\right)\left(1 - \sqrt{5}i\right) \; em \; \mathbb{Z}\left[i\sqrt{5}\right]$$

Temos que 2 é irredutível, 2 divide o produto $\left(1 + \sqrt{5}i\right)\left(1 - \sqrt{5}i\right)$ mas 2 não divide $\left(1 + \sqrt{5}i\right)$ e 2 não divide $\left(1 - \sqrt{5}i\right)$ e assim 2 não é primo em $\mathbb{Z}\left[i\sqrt{5}\right]$, como já demonstrado na página 24.

Afirmação: Se p não divide a então p divide b .

De fato, como p é irredutível os únicos elementos que p e a são elementos invertíveis de D. Então o $mdc(p, a) = 1$. Logo existem $e, f \in D$ tais que

$$1 = e.p + f.a \underset{\underbrace{\quad}_{x\ b}}{\Rightarrow} b = e.p.b + f.\underbrace{a.b}_{p\ divide} \Rightarrow p \mid b$$

(1) Sendo $a, b \in D \setminus \{0\}$ e $d = mdc(a, b)$ então

a) Existem $e, f \in D$ tais que $d = ea + fb$.
b) Tais e e f podem ser efetivamente calculados quando a divisão em D é efetiva.

De fato, sejam $a, b \in D\backslash\{0\}$. Vamos mostrar que se (D, φ) for um domínio euclidiano e se a divisão em D for efetiva, então e e f podem ser efetivamente calculados.

Pela propriedade Euclidiana ,existem $t_1, r_1 \in D$ tais que

$$a = b.t_1 + r_1 \quad \text{com} \quad \begin{cases} \varphi(r_1) < \varphi(b) \\ ou \\ r_1 = 0 \end{cases} \qquad (1)$$

Caso $r_1 = 0$ temos que o $mdc\ (a, b) = b$. Daí,

$$a = b.t_1 \Rightarrow \ b\ divide\ a \Rightarrow \ mdc(a, b) = b \ \Rightarrow \ b = 0.a + 1.b$$

Caso $r_1 \neq 0$ temos para $\theta \in D$, em virtude de (1),

$$\theta \mid a \ e \ \ \theta \mid b \ \Leftrightarrow \ \theta \mid b \ e \ \ \theta \mid r_1 .$$

Assim sendo,

$mdc(a, b) = d \Leftrightarrow mdc(b, r_1) = d.$

Agora consideremos $b\ e\ r_1$, existem $t_2, r_2 \in D$ tais que

$$b = r_1 t_2 + r_2 \quad \text{com} \quad \begin{cases} \varphi(r_2) < \varphi(r_1) \\ ou \\ r_2 = 0 \end{cases} \qquad (2)$$

Se $r_2 = 0$ temos $mdc(b, r_1) = r_1$ pois

$$b = r_1.t_2 \Rightarrow \frac{r_1}{b} \Rightarrow mdc(r_1, b) = r_1 \Rightarrow \ r_1 = 1.a + (-t_1).b \ .$$

Se $r_2 \neq 0$ então para $\beta \in D$, em virtude de (2)

$$\beta \mid b \ e \ \beta \mid r_1 \ \Leftrightarrow \ \beta \mid r_1 \ e \ \beta \mid r_2$$

Assim sendo, $mdc(b, r_1) = d \Leftrightarrow mdc(r_1, r_2) = d$.

Agora consideramos r_1 e r_2, existem $t_3, r_3 \in D$ tais que

$$r_1 = r_2.t_3 + r_3 \text{ com} \begin{cases} \varphi(r_3) < \varphi(r_2) \\ ou \\ r_3 = 0 \end{cases} \qquad (3)$$

Se $r_3 = 0$ temos $mdc\ (r_1, r_2)\ =\ r_2$ pois

$$r_1 = r_2.t_3 \Rightarrow r_2 \mid r_1 \Rightarrow mdc(r_2, r_1) = r_2$$

Em virtude de (1) $a = b.t_1 + r_1$ e de (2) $b = r_1.t_2 + r_2$ temos que

$r_2 = b - r_1.t_2 = b - (a - b.t_1).t_2$

$= b - a.t_2 + b.t_1.t_2$

$= (-t_2).a + (1 + t_1.t_2).b$

Se $r_3 \neq 0$, continuamos o processo.

Observe que nesse processo, quando $r_i \neq 0$, obtemos um r_{i+1} tal que

$$\begin{cases} \varphi(r_{i+1}) < \varphi(r_i) \\ ou \\ r_{i+1} = 0 \end{cases}$$

Já que a função $\varphi: D \to \mathbb{N}$ toma valores em $\mathbb{N}$, então não é possível ter uma sequência decrescente infinita. Logo, vai existir um inteiro n para o qual não será mais possível ter

$\varphi(r_{n+1}) < \varphi(r_n)$, isto é, para o qual $r_{n+1} = 0$.

Assim, obtemos um $n \in \mathbb{Z}$ tal que:

$$r_{n-1} = r_n.t_{n+1} + r_{n+1} = r_n.t_{n+1} \qquad (n+1)$$

Isto termina a prova, com $mdc\ (r_{n-1}, r_n)\ =\ r_n.$ e

$$mdc(a, b) = \ ... = \ mdc(r_{n-1}, r_n) = \ r_n$$

Em virtude das equações de (1) a (n) o elemento r_n se escreve como combinação linear de a e b com coeficientes em D, isto é,

$$d = r_n = mdc(a, b) = e.a + f.b \quad \blacksquare$$

Teorema 2.20: Se $\alpha \in \mathbb{Z}[i]$ é irredutível então existe um número primo $p \in \mathbb{Z}$ primo tal que α é um fator irredutível de p.

Prova: Seja $\boldsymbol{\alpha \epsilon Z}\,[i]$ irredutível

$\overline{\alpha}\,\boldsymbol{\epsilon Z}\,[i]$ é *irredutível* $\overset{def}{\Longrightarrow}$ α *não é invertível e* $\alpha \neq 0$

$$\Rightarrow N(\alpha) \neq N(1) = 1$$

$$\Rightarrow N(\alpha) > 1 \in N$$

$\Rightarrow$ Existe $p \in \mathbb{Z}$ primo tal que p divide $N(\alpha)$

$$\Rightarrow N(\alpha) = p.k \; com \; k \in \boldsymbol{Z}$$

$$\overset{N(\alpha)=\alpha.\overline{\alpha}}{\Longrightarrow} \alpha.\overline{\alpha} = p.k$$

Como $\boldsymbol{Z}\,[i]$ é um Domínio Fatorial, temos que os fatores irredutíveis de p em $\boldsymbol{Z}\,[i]$ são:

$$\begin{cases} (1)\ \alpha \ \ ou \\ (2)\ \overline{\alpha} \ ou. \\ (3)\ \alpha.\overline{\alpha} \end{cases}$$

Se ocorrer (1) ou (3) temos que

$$p = \alpha.k \; ou \; p = \alpha.\overline{\alpha}$$

Se ocorrer (2) temos que

$$p = \overline{\alpha}.\vartheta \;\Rightarrow\; \overline{p} = p = \overline{\overline{\alpha}.\vartheta} = \; \alpha.\overline{\vartheta}$$

Em qualquer dos casos, $\alpha \mid p$ ■

Observação: Fatoração única em anéis de Polinômios

Definição 2.21: Seja D um domínio fatorial. Dizemos que um polinômio $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ é *primitivo* se $mdc(a_n, \ldots, a_0) = 1$.

Dizemos que o polinômio não constante $f(X)$ é irredutível em $\mathbb{Z}[X]$ (ou irredutível sobre $\mathbb{Z}$) se é impossível expressar $f(X)$ como um produto $a(x)b(x)$ de dois polinômios $a(x)$ e $b(x)$ em $\mathbb{Z}[X]$ cujos graus são ambos maiores ou iguais a 1. Não faz sentido dizer que um dado polinômio $f(X)$ é irredutível, simplesmente. Para nos convencermos disso, basta olharmos um exemplo.

Exemplo 2.22: Seja $f(x) = x^2 + 1$. É fácil ver que $f(x)$ é irredutível sobre $\mathbb{Z}(X)$. De fato, se fosse possível escrever $x^2 + 1 = (ax + b)(cx + d)$, com $(ax + b)\, e\, (cx + d)$ de grau 1 e com coeficientes reais, então $x^2 + 1$ teria duas raízes reais, o que não é o caso. Por outro lado, sabemos que $x^2 + 1$ não é irredutível sobre $\mathbb{C}$, pois $x^2 + 1 = (x + i)(x - i)$.

Polinômios irredutíveis são importantes porque eles representam, entre os polinômios, o mesmo papel que os números primos representam em $\mathbb{Z}$.

Podemos estabelecer algumas condições suficientes para que um polinômio $f(X) \in \mathbb{Z}[X]$ seja irredutível.

Teorema 2.23 (**Critério de Eisenstein**):Sejam

- D um Domínio Fatorial
- $f(X) = a_nX^n + \cdots + a_1X + a_0 \in D[X]$ um polinômio de grau $n \geq 1$.

Se existe um elemento irredutível $p \in D$ tal que:

$$\begin{cases} p \nmid a_n \\ p \mid a_i \quad \forall\ i \leq n-1 \\ p^2 \nmid a_0 \end{cases}$$

então $f(X)$ não é o produto de dois polinômios de grau ≥ 1 em $D[X]$.

Prova: Suponha que a afirmação seja falsa, isto é:

$$f(X) = g(X).h(X)$$

onde

$$\begin{cases} g(X) = b_s X^s + \cdots + b_1 X + b_0 \\ h(X) = c_r X^r + \cdots + c_1 X + c_0 \\ 1 \leq s, r \leq n-1 \end{cases}$$

Temos $a_0 = \alpha_0.\beta_0$.

$$\left.\begin{array}{c} a_0 = b_0 c_0 \\ p \mid a_0 \\ p^2 \nmid a_0 \end{array}\right\} \quad \underbrace{\Rightarrow}_{D \text{ é } Fatorial} \quad \begin{cases} p \mid b_0 \ \ e \ \ p \nmid c_0 \\ ou \\ p \nmid b_0 \ \ e \ \ p \mid c_0 \end{cases}$$

Digamos que aconteça o caso $p \mid b_0 \ e \ \ p \nmid c_0$ (o outro caso seria tratado de maneira análoga). Analisando o coeficiente líder a_n de $f(X) = g(X)h(X)$ segue que

$$\left.\begin{array}{c} a_n = b_s c_r \\ e \\ p \nmid a_n \end{array}\right\} \quad \underbrace{\Rightarrow}_{D \text{ é } Fatorial} \quad \begin{cases} p \nmid b_s \\ e \\ p \nmid c_r \end{cases}$$

Seja b_u com $u \leq s \leq n-1$ o coeficiente do termo de mais baixo grau de $g(X)$ que p não divida, isto é:

$$p \mid b_0, p \mid b_1, \ldots, p \mid b_{u-1} \ mas \ p \nmid b_u$$

Considerando agora o coeficiente a_u em $f(X)$ temos que

$$a_u = \underbrace{b_0 c_u + b_1 c_{u-1} + \cdots + b_{u-1} c_1}_{p \ divide} + \underbrace{b_u c_0}_{p \text{ não } divide}$$

e portanto p não divide a_u. Isto contradiz a hipótese que o elemento p divide a_i para todo $i \leq n-1$. ■

Exemplo 2.24: Mostre que

$$f(X) = 2X^{12} + 5(2+3i)X^{10} + 39X^3 + 13$$

é irredutível em $\mathbb{Z}[i][X]$.

Solução: Observe que $p = (2+3i) \in \mathbb{Z}[i]$ é irredutível pois $N(p) = 2^2 + 3^2 = 13$ (primo) conforme Proposição 2.6 . Por outro lado, temos que

- $13 = (2+3i)(2-3i) = 2^2 - (3i)^2 = 4 - 9i^2 = 4 - 9(-1)$
- $39 = 3.13 = 3(2+3i)(2-3i)$

Agora é fácil ver que para $p = (2 + 3i) \in \mathbb{Z}[i]$ irredutível, temos que

$$\begin{cases} p \nmid a_{12} = 2 \\ p \mid 5(2 + 3i), 0, 39, 13 \\ p^2 \nmid a_0 = 13 \end{cases}$$

Pelo critério de Eisenstein:

$f(X)$ não é produto de dois polinômios de grau ≥ 1 em $\mathbb{Z}[i][X]$.

Por outro lado, como

$$mdc\ (2, 2 + 3i, 39,13) = 1$$

concluímos que o polinômio $f(X)$ é irredutível em $\mathbb{Z}[i][X]$. ■

CAPÍTULO 3 – Aplicações

Como aplicação do estudo de anel dos inteiros de Gauss $\boldsymbol{Z}[i]$, daremos uma caracterização simples dos inteiros que são soma de dois quadrados. Começaremos dando uma caracterização para os números primos. Mas antes, enunciamos um resultado clássico que será útil.

Proposição 3.1 (Pequeno Teorema de Fermat) Seja p um número primo e $a \in \mathbb{Z}$. Então

$$a^p \equiv a\ (mod\ p)\ ,\ \text{ou seja, } a^p - a = k.p\ ,\ \text{ para algum } k\ \in \mathbb{Z}.$$

Prova: Faremos indução sobre a.

Caso $a = 1$, temos $1^p - 1 = 0 = 0.p$.

Suponha que o resultado vale para $a\ =\ k$;

$$k^p - k = c.p \qquad (H.I)$$

Vamos mostrar que o resultado vale para $a\ =\ k + 1$:

$$(k+1)^p - (k+1) =\ d.p\ .$$

De fato, usando a formula binomial, segue que

$$(k+1)^p = k^p + \binom{p}{1} k^{p-1}.1 + \binom{p}{2} k^{p-2}.1 + \cdots + \binom{p}{p-1} k.1^{p-1} + 1^p$$

Como p divide $\binom{p}{i}$ para todo $i\ =\ 1, \ldots, (p-1)$, segue que

$$(k+1)^p = k^p +\ mp + 1$$

Subtraindo $(k+1)$ em ambos os termos

$$(k+1)^p - (k+1) = k^p +\ mp + 1 - (k+1) = (k^p - k) + mp \underbrace{=}_{H.I} cp + mp$$

Segue que

$$(k+1)^p - (k+1) = d.p \quad \blacksquare$$

Corolário 3.2:. Se p é primo e p não divide a, então

$$a^{p-1} \equiv 1\ (mod\ p), \text{ ou seja, } a^{p-1} - 1 = dp$$

Prova: Pelo Teorema 3.1, temos que

$$a^p - a = a.(a^{p-1} - 1) = k.p$$

Como $mdc(a,p) = 1$ pois p não divide a, então

p divide $(a^{p-1} - 1)$, isto é, $a^{p-1} \equiv 1\ (mod\ p)$. ■

Teorema 3.1 (Fermat): Se p é um número primo então as seguintes afirmações são equivalentes:

(i) $p = 2\ ou\ p = 4n + 1, com\ n \in \mathbb{Z}$

(ii) Existe $a \in Z$ tal que $a^2 = m.p - 1, com\ p \in \mathbb{Z}$

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

(iv) p é soma de dois quadrados.

Prova:

$(\boldsymbol{i}) \Rightarrow (\boldsymbol{ii})$: Se $p = 2$. Tome $a = 1$. Seja agora $p = 4n + 1$, com n ∈ ℕ. Pelo corolário 3.2, temos que $\overline{1}, \overline{2}, \ldots, \overline{(p-1)}$ são raízes do polinômio

$$\overline{1}\, X^{p-1} - \overline{1} \in (\mathbb{Z} / p\mathbb{Z})[X]$$

Logo,

$$X^{p-1} - \overline{1} = (X - \overline{1})(X - \overline{2}) \ldots (X - \overline{p-1}).$$

Como $p - 1 = 4n$, temos também

$$X^{p-1} - \overline{1} = X^{4n} - \overline{1} = (X^{2n} - \overline{1})(X^{2n} + \overline{1}).$$

e, portanto,

$$(X^{2n} - \overline{1})(X^{2n} + \overline{1}) = (X - \overline{1})(X - \overline{2}) \ldots (X - \overline{p-1}).$$

Como p é primo. $(\mathbb{Z}/p\mathbb{Z})$ é um corpo e portanto $(\mathbb{Z}/p\mathbb{Z})[X]$ é um domínio de fatoração única. Portanto, existe $x \in \{1,2,\dots,p-1\}$ é tal que $\bar{x}^{2n} + \bar{1} = \bar{0}$. Tomando $a = x^n$:

$$\bar{a}^2 = \bar{x}^{2n} = -\bar{1} \quad \Rightarrow \quad a^2 \equiv -1 \, mod \, p$$

$(\boldsymbol{ii}) \Rightarrow (\boldsymbol{iii})$ Por hipótese, existe $a \in Z$ tal que $a^2 = m.p - 1$ para algum $m \in \mathbb{Z}$. Logo $(a+i)(a-i) = m.p$, ou seja, $p/(a+i)(a-i)$. Porém, p não divide $a+i$ em $\mathbb{Z}[i]$ pois se ele dividisse teríamos $a + i = p.(e + f.i)$, com $e, f \in \mathbb{Z}$. Como o coeficiente de $i = 1$, obteríamos $1 = p.f$, o que é absurdo pois p não é invertível em $\mathbb{Z}$. Analogamente, p não divide $a - i$ em $\mathbb{Z}[i]$. Então, p não é elemento irredutível em $\mathbb{Z}[i]$.

$(\boldsymbol{iii}) \Rightarrow (\boldsymbol{iv})$ Por hipótese, existem $(a+bi), (c+di) \in \mathbb{Z}[i]$ tais que

$$p = (a+bi)(c+di)$$

com $N(a+bi) \neq 1$ e $N(c+di) \neq 1$. Temos então:

$$p^2 = N(p) = N(a+bi).N(c+di) = (a^2+b^2).(c^2+d^2),$$

onde $a^2 + b^2 \neq 1$ *e* $c^2 + d^2 \neq 1$. Sendo $\mathbb{Z}$ um domínio fatorial e p um elemento irredutível de $\mathbb{Z}$, devemos ter $p = a^2 + b^2$. Portanto, p primo é soma de dois quadrados.

$(\boldsymbol{iv}) \Rightarrow (\boldsymbol{i})$ Sendo p um número primo, temos somente três possibilidades

- $p = 2$
- p é do tipo $4n + 1$
- p é do tipo $4n + 3$

Basta então mostrar que nenhum inteiro do tipo $4n + 3$ é soma de dois quadrados.

Se a é um inteiro qualquer então $\bar{a} = \bar{0}, \bar{1}, \bar{2}$ ou $\bar{3}$ em $(\mathbb{Z}/4\mathbb{Z})$ e portanto $\bar{a}^2 = \bar{0}, \bar{1}, \bar{0}$ ou $\bar{1}$, isto é, $\bar{a}^2 = \bar{0}$ ou $\bar{1}$ em $(\mathbb{Z}/4\mathbb{Z})$. Então se a e b são dois inteiros quaisquer, as possibilidades para $\bar{a}^2 + \bar{b}^2$ são $\bar{0}, \bar{1}$ ou $\bar{2}$ em $(\mathbb{Z}/4\mathbb{Z})$ e $4n + 3 = \bar{3}$ em $(\mathbb{Z}/4\mathbb{Z})$ não é soma de dois quadrados. ■

Corolário 3.2: *Os elementos irredutíveis de* $\mathbb{Z}[i]$ *são exatamente os elementos dos seguintes tipos:*

- $\pm p, \pm ip$, *com p primo em Z tal que* $p = 4n + 3$ *com* $n \in Z$.
- $a + bi$ *com* $a^2 + b^2$ *igual a um primo de* $\mathbb{Z}$

Prova: Um elemento de $\mathbb{Z}[i]$ do tipo $\pm p, \pm ip$, com p primo em $\mathbb{Z}$ e $p = 4n + 3$ é irredutível pelo teorema anterior. Um elemento $a + bi \in \mathbb{Z}[i]$, com $a^2 + b^2$ igual a um primo em $\mathbb{Z}$, é irredutível em $\mathbb{Z}[i]$ pois senão teríamos

$$a + bi = \alpha.\beta \text{ com } \alpha, \beta \neq \pm 1, \pm i$$

Logo:

$$a^2 + b^2 = N(a + bi) = N(\alpha.\beta) = N(\alpha).N(\beta),$$

com $N(\alpha),\ N(\beta) \in \mathbb{Z}$, e $N(\alpha) \neq 1\ e\ N(\beta) \neq 1$, o que contradiz a hipótese de $a^2 + b^2$ ser primo em $\mathbb{Z}$.

Reciprocamente, seja $a + bi$ um elemento irredutível em $\mathbb{Z}[i]$. Usando a conjugação complexa é fácil mostrar que $(a - bi)$ é também irredutível em $\mathbb{Z}[i]$. Se $a^2 + b^2$ não é primo em $\mathbb{Z}$, então

$$a^2 + b^2 = n.m,$$

com $n, m \in Z$, com $n, m \neq \pm 1$. Logo,

$$(a + bi)(a - bi) = n.m$$

Pela unicidade da fatoração em $\mathbb{Z}[i]$ obtemos:

$$\begin{cases} a + bi = \varepsilon.n \\ a - bi = \varepsilon.m \end{cases},$$

com $\varepsilon \in \{\pm 1, \pm i\}$; logo $a = 0$ ou $b = 0$, ou seja,

$$\begin{cases} a + bi = \pm i.c \\ a + bi = \pm c \end{cases}$$

com $c \in \mathbb{N}$. Agora, sendo $a + bi$ irredutível em $\mathbb{Z}[i]$, vemos que c é irredutível em $\mathbb{Z}\,[i]$, e com muito mais razão, irredutível em $\mathbb{Z}$. Pelo Teorema anterior, este elemento é do tipo $c = 4k + 3$ ■

Observação 3.3:

a) quando um primo p é soma de dois quadrados, ele o é de maneira única.

De fato, suponha que $p = a^2 + b^2 = c^2 + d^2$. Temos, então,

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

Os elementos $(a + bi), (a - bi), (c + di), (c - di)$ são irredutíveis em $\mathbb{Z}[i]$, pois tem norma igual a p que é irredutível em $\mathbb{Z}$.

Sendo $\mathbb{Z}[i]$ Domínio Fatorial, obtemos que $(a + bi)$ é associado a $(c + di)$ ou a $(c - di)$; já que os elementos invertíveis de $\mathbb{Z}[i]$ são ± 1 e $\pm\, i$, daí:

$$\begin{cases} a = \pm c \\ b = \pm d \end{cases} \text{ ou } \begin{cases} a = \pm d \\ b = \pm c \end{cases}, \quad \text{logo} \quad \begin{cases} a^2 = c^2 \\ b^2 = d^2 \end{cases} \text{ ou } \begin{cases} a^2 = d^2 \\ b^2 = c^2 \end{cases}$$

b) Em geral, é possível para um inteiro positivo não-primo ser expresso como soma de dois quadrados de duas maneiras diferentes, por exemplo:

$$\begin{cases} 125 = 10^2 + 5^2 = 11^2 + 2^2 \\ 50 = 1^2 + 7^2 = 5^2 + 5^2 \end{cases}$$

Antes de generalizar o teorema anterior e caracterizar os inteiros que são soma de dois quadrados, observamos que o produto da soma de dois quadrados é uma soma de dois quadrados.

Lema 3.4: *Se f, g são dois inteiros que são soma de dois quadrados então o produto $f.g$ também é soma de dois quadrados*

Prova: Por hipótese, existem inteiros a, b, c, d tais que $f = a^2 + b^2$ e $g = c^2 + d^2$. Então,

$$fg = (a^2 + b^2)(c^2 + d^2) = N(a + bi)N(c + di)$$

$$= N[\,(a + bi).(c + di)] = N[\,(ac - bd) + (ad + bc)i\,]$$

$$= (ac - bd)^2 + (ad + bc)^2. \quad \blacksquare$$

Teorema 3.5 (Fermat): Seja n um número inteiro positivo e seja

$$n = 2^r p_1^{u_1} \dots p^{u_t} . q_v^{v_1} \dots q_s^{v_s}$$

sua decomposição irredutível em $\mathbb{Z}$, onde

- $p_1, \dots, p_t$ são primos do tipo $4k + 1$ e
- $q_1, \dots, q_s$ são primos do tipo $4k + 3$.

Então, n é soma de dois quadrados $se\ e\ somente\ se\ v_1, v_2, \dots, v_n$ são pares.

Prova: Se $v_1, v_2, \dots, v_s$ são pares, então $q_1^{v_1}, \dots, q_s^{v_s}$ são quadrados e, portanto, são soma de dois quadrados. O Teorema anterior nos diz que 2, $p_1, \dots, p_t$ são soma de dois quadrados e, portanto, aplicando sucessivamente o Lema anterior, temos que n é soma de dois quadrados.

Reciprocamente, suponhamos que $n = a^2 + b^2, com\ a, b \in Z$. Seja p um primo ímpar e suponhamos que a maior potência de p que divide n seja ímpar. Queremos mostrar que p é necessariamente do tipo $4k + 1$. Seja $d = mdc(a, b)$. Então, $a = da_1$ e $b = db_1$ com $a_1, b_1 \in \mathbb{Z}$ e $mdc\,(a_1, b_1) = 1$. Temos que:

$$n = a^2 + b^2 = d^2(a_1^2 + b_1^2)$$

e é claro que a maior potência de p que divide d^2 é par, consequentemente p divide $a_1^2 + b_1^2$, ou seja $\overline{a_1}^2 + \overline{b_1}^2 = \bar{0}$ em $(\mathbb{Z} / p\mathbb{Z})$. Note que $\bar{b}_1 \neq \bar{0}$ pois, caso contrário teríamos $\bar{a}_1^2 = -\bar{b}_1^2 = \bar{0}$, logo $\bar{a}_1 = 0$, isto é, teríamos que p divide a_1 e b_1, o que é impossível pois o $mdc(a_1, b_1) = 1$. Temos então:

$$\bar{0} = \overline{a_1}^2 + \overline{b_1}^2 = \overline{b_1}^2 . \left[\left(\frac{\overline{a_1}}{\overline{b_1}} \right)^2 + \bar{1} \right]$$

e portanto $\left(\bar{a}_1/\bar{b}_1\right)^2 + \bar{1} = \bar{0}$ pois $(\mathbb{Z}/p\mathbb{Z})$ é um domínio. Tomando $c \in \mathbb{Z}$ tal que

$$\bar{c} = \frac{\overline{a_1}}{\overline{b_1}} \Rightarrow \bar{c}^2 = -1 \Rightarrow c^2 \equiv -1 \ mod\, p$$

Pelo Teorema 3.1, concluímos que p é do tipo $4k + 1$. ■

Observação 3.6: Os números de Fermat são os números da forma:

$$F_n = 2^{2^n} + 1.$$

O quinto número primo de Fermat (os quatro primeiros são $5 = 2^{2^1} + 1$, $17 = 2^{2^2} + 1$, $257 = 2^{2^3} + 1$, $65537 = 2^{2^4} + 1$) $F_5 = 4294967297 = 2^{2^5} + 1$ é escrito como soma de dois quadrados: $F_5 = 4294967297 = 2^{2^5} + 1 = (2^{16})^2 + 1^2$.
Euler conseguiu escrever este mesmo número como soma de outros dois quadrados:

$$F_5 = (2^{16})^2 + 1^2 = (62264)^2 + (20449)^2$$

Isso realmente teve uma grande consequência. Fermat achava que seu quinto número era primo, mas o fato de ele ser escrito como soma de dois quadrados distintos provou que F_5 era composto.

Veja que $641 = 4^2 + 25^2 = 2^4 + 5^4 = 5.2^7 + 1$
Por outro lado,
$2^{32} = (2^{16})^2 = 2^4.2^{28} = (641 - 5^4).2^{28}$
$(641 - 5^4).2^{28} \equiv -5^4.2^{28} = -(5.2^7)^4 = -(641 - 1)^4 \equiv -1(mod 641).$
Logo 641 divide $2^{2^5} + 1$.

CAPÍTULO 4 – Atividades

4.1. Atividade 1

Essa atividade tem como objetivo principal verificar a compreensão do conceito de máximo divisor comum em problemas que envolvam valores inteiros. Não existe o comando claro de que deve ser calculado o mdc. A compreensão plena do conceito faz o entendimento possível. Somente após compreensão do que está sendo pedido o cálculo será feito a partir de um dos métodos existentes. Tais problemas são frequentemente exigidos nos exames de vestibulares em nosso país.

(PUC) "A Dengue é uma doença causada por um vírus, transmitida de uma pessoa doente para uma pessoa sadia por meio de um mosquito: o Aedes aegypti. Ela se manifesta de maneira súbita – com febre alta, dor atrás dos olhos e dores nas costas – e, como não existem vacinas específicas para o seu tratamento, a forma de prevenção é a única arma para combater a doença. "

Fonte (adaptado): prdu.unicamp.br/dengue/dengue.html

Assim sendo, suponha que 450 mulheres e 575 homens inscreveram-se como voluntários para percorrer alguns bairros do ABC paulista, a fim de orientar a população sobre os procedimentos a serem usados no combate à Dengue. Para tal, todas as 1.025 pessoas inscritas serão divididas em grupos, segundo o seguinte critério: todos os grupos deverão ter a mesma quantidade de pessoas e em cada grupo só haverá pessoas de um mesmo sexo. Nessas condições, se grupos distintos deverão visitar bairros distintos, o menor número de bairros a serem visitados é:

(A) 25
(B) 29
(C) 37
(D) 41
(E) 45

4.2. **Atividade 2**

O objetivo dessa atividade é verificar se o aluno é capaz de fazer o cálculo do máximo divisor comum de inteiros gaussianos redutíveis e irredutíveis.

Calcule o mdc em $\mathbb{Z}[i]$ dos seguintes elementos:

a) $\alpha = 8 + 9i \; e \; \beta = -1 + 7i$

b) $\alpha = 3 + 2i \; e \; \beta = 2 - i$

4.3. **Atividade 3**

O objetivo dessa atividade é fazer o aluno perceber que o número 2 não é primo nos inteiros gaussianos e determinar seus divisores.

O número 2 é primo em $\mathbb{Z}[i]$? Justifique.

4.4. **Atividade 4**

O seguinte questionamento motivou a aplicação dessa atividade: será que é possível escrever cubos como soma de dois quadrados?

Determine todos os pares $x, y \in \mathbb{Z} \; tal \; que \; y^3 = x^2 + 1$.

4.5. **Atividade 5**

O objetivo dessa atividade é verificar se o aluno compreende a diferença entre primo e composto no anel dos inteiros de Gauss.

$3 + 8i$ é um número primo ou composto em $\mathbb{Z}[i]$?

CAPITULO 5 – Respostas das Atividades

5.1. Solução da atividade 1

Quanto maior o número de pessoas em cada grupo, menor será o número total de grupos e, portanto, menor será o número de bairros visitados. Então, o número máximo de pessoas por grupo será o mdc entre o número de homens e o número de mulheres, ou seja, mdc$(450, 575) = 25$ pessoas por grupo. O número total de grupos será o número total de bairros visitados. Como temos $450:25 = 18$ grupos de mulheres e $575:25 = 23$ grupos de homens, teremos um total de $18 + 23 = 41$ grupos e, portanto, 41 bairros visitados. Letra D.

5.2. Solução da Atividade 2 (a):

$N(8 + 9i) = 64 + 81 = 145 = 29.5$

$N(-1 + 7i) = 1 + 49 = 50 = 2.5^2$

Por outro lado, $\gamma = a + bi$ tal que $N(\gamma) = 5 = a^2 + b^2$. Logo

$$\begin{cases} a^2 = 4 \\ e \\ b^2 = 1 \end{cases} \Rightarrow \begin{cases} a = \pm 2 \\ e \\ b = \pm 1 \end{cases} \quad \text{ou} \quad \begin{cases} a^2 = 1 \\ e \\ b^2 = 4 \end{cases} \Rightarrow \begin{cases} a = \pm 1 \\ e \\ b = \pm 2 \end{cases}$$

Em particular, $\gamma = 2 + i$ é irredutível, pois $N(\gamma) = 5$ é primo.

Da mesma forma, $\varphi = a + bi$ tal que $N(\varphi) = a^2 + b^2 = 29$. Logo

$$\begin{cases} a^2 = 25 \\ e \\ b^2 = 4 \end{cases} \Rightarrow \begin{cases} a = \pm 5 \\ e \\ b = \pm 2 \end{cases} \quad \text{ou} \quad \begin{cases} a^2 = 4 \\ e \\ b^2 = 25 \end{cases} \Rightarrow \begin{cases} a = \pm 2 \\ e \\ b = \pm 5 \end{cases}$$

Em particular, $\varphi = 5 + 2i$ é irredutível pois $N(\varphi) = 29$ é primo. Portanto

$$\alpha = 8 + 9i = (5 + 2i).(2 + i) = (10 - 2) + (5 + 4)i.$$

Por outro lado, analogamente,

$$\beta = -1 + 7i = (1 + 3i).(2 + i) = (1 + i)(2 + i)(2 + i) = (1 + i)(2 + i)^2$$

Logo

$$mdc(\alpha, \beta) = mdc[\,(5 + 2i)(2 + i), (1 + i)(2 + i)^2\,] = (2 + i)$$

5.3. **Solução da atividade 2.(b)**

Calculando a função norma nos elementos, temos que:

- $N(3 + 2i) = 9 + 4 = 13$ (primo)
- $N(2 - i) = 4 + 1 = 5$ (primo).

Pela **Proposição 2.5** segue que $\alpha = (3 + 2i)\ e\ \beta = (2 - i)$ são irredutíveis e consequentemente não tem fator comum, portanto

$$mdc(\alpha, \beta) = 1.$$

5.4. **Solução da atividade 3:**

Como $2 = (1 + i)(1 - i)$

O número 2 não é primo em $\mathbb{Z}[i]$ pois 2 não divide $(1 + i)$ nem $(1 - i)$.

Com efeito, se 2 divide $1 + i$ existe um inteiro gaussiano $\gamma = c + di$ tal que $1 + i = 2.(c + di)$. Resolvendo temos que $c = \frac{1}{2} \notin \mathbb{Z}$ e $d = \frac{1}{2} \notin \mathbb{Z}$.

Analogamente mostramos que 2 não divide $(1 - i)$.

5.5. **Solução da atividade 4:**

$y^3 = x^2 + 1 = (x + i)(x - i)$

Onde $i^2 = -1$.

$(x + i) = (\alpha_1)^{a_1}(\alpha_2)^{a_2}(\alpha_3)^{a_3}\dots(\alpha_{k_1})^{a_{k_1}}$
$(x - i) = (\beta_1)^{b_1}(\beta_2)^{b_2}(\beta_3)^{b_3}\dots(\beta_{k_2})^{b_{k_2}}$

onde α_n e β_n são primos de Gauss e a_n e b_n são os expoentes dos termos da fatoração.

Da fatoração acima, será necessário saber se existe algum α ou β iguais, ou seja, se algum dos primos da fatoração de $(x + i)$ é igual a algum dos primos da fatoração de $(x - i)$. O que se pode deduzir é que, **se** existe algum termo das fatorações de ambos que sejam iguais, então este primo também é um termo na fatoração de qualquer combinação aritmética (soma, subtração, divisão e multiplicação) entre eles.

Fazendo:

$$(x + i) - (x - i) = 2i$$

$$(x + i) + (x - i) = 2x$$

Portanto, caso exista algum α que seja igual a algum β, este é 2 (ou $2i$, ou -2, ou $-2\,i$), já que as unidades dos inteiros de Gauss são $1, -1, i \;e\; -i$.

Obs.: É importante perceber que o 2 não é, necessariamente, um termo da fatoração. O que se ressalta aqui é que se o 2 for termo da fatoração de um deles, então é dos dois e neste caso este seria o único termo em comum na fatoração de $(x + i)$ e $(x - i)$. Logo, qualquer α é diferente de qualquer β, exceto se um deles for 2. Assim, se 2 é fator da decomposição de $(x + i)$, então existe um $c = (a + bi)$ (inteiro de Gauss) tal que:

$$x + i = 2(a + bi) = 2a + 2bi$$

Ou seja:

$$2b = 1.$$

Mas como b é um inteiro, então $k = 0$.

Portanto, a equação inicial fica:

$$y^3 = [(\alpha_1)^{a_1}(\alpha_2)^{a_2}(\alpha_3)^{a_3}\dots(\alpha_{k_1})^{a_{k_1}}].[\,(\beta_1)^{b_1}(\beta_2)^{b_2}(\beta_3)^{b_3}\dots(\beta_{k_2})^{b_{k_2}}]$$

Porém, para que y seja inteiro, cada um dos expoentes $a_1, a_2, a_3, \dots, a_{k_1}$ e $b_1, b_2, b_3, \dots, b_{k_2}$ devem ser múltiplos de 3, já que todos os primos de Gauss α e β são diferentes. Desta forma podemos escrever a equação:

$$y^3 = [(\alpha_1)^{a'_1}(\alpha_2)^{a'_2}(\alpha_3)^{a'_3}\dots(\alpha_{k_1})^{a'_{k_1}}.\,(\beta_1)^{b'_1}(\beta_2)^{b'_2}(\beta_3)^{b'_3}\dots(\beta_{k_2})^{b'_{k_2}}]^3$$

Além disso:

$$(x + i) = [(\alpha_1)^{a'_1}(\alpha_2)^{a'_2}(\alpha_3)^{a'_3}\dots(\alpha_{k_1})^{a'_{k_1}}]^3$$

e

$$(x - i) = [(\beta_1)^{b'_1}(\beta_2)^{b'_2}(\beta_3)^{b'_3}\dots(\beta_{k_2})^{b'_{k_2}}]^3$$

Usando:

$$(\alpha_1)^{a'_1}(\alpha_2)^{a'_2}(\alpha_3)^{a'_3}\dots(\alpha_{k_1})^{a'_{k_1}} = u + vi$$

Onde $u + vi$ é um inteiro de Gauss, temos que:

$$\begin{aligned}(x + i) &= (u + vi)^3 = [u^3 + 3u^2vi + 3u(vi)^2 + (vi)^3] \\ &= u^3 + 3u^2vi - 3uv^2 - v^3i \\ &= (u^3 - 3uv^2) + i.(3u^2v - v^3)\end{aligned}$$

Então,

$$\begin{cases} (x + i) = (u^3 - 3uv^2) + i.(3u^2v - v^3) \\ (x - i) = (u^3 - 3uv^2) - i(3u^2v - v^3) \end{cases}$$

Logo,

$$3u^2v - v^3 = 1$$
$$3u^2 - v^2 = \frac{1}{v}$$

Porém, como u é um inteiro e v também é um inteiro, v só pode ser ± 1, caso contrário $\left|\frac{1}{v}\right| < 1$, o que não é uma solução possível para $3u^2 - v^2$ sendo u e v inteiros.

Assim, para $v = 1$ segue que $3u^2 - 1 = 1 \Rightarrow u^2 = \frac{3}{2}$, o que não é possível, pois *u* é inteiro.

Analogamente, para $v = -1$ segue que $3u^2 - 1 = -1 \Rightarrow u = 0$

Logo,

$$(x + i) = (u^3 - 3uv^2) + i.(3u^2v - v^3) = 0 + i,$$

ou seja, $x = 0$. Neste caso,

$$\begin{cases} y^3 = 0^2 + 1 \\ y = 1 \end{cases}$$

Portanto, este exercício só admite uma solução:

$$\begin{cases} x = 0 \\ y = 1 \end{cases}$$

5.6. **Solução da atividade 5**

Temos que

$$N(3+8i) = 9+64 = 73 \text{ é primo em } \mathbb{Z} \quad \text{e} \quad 73 = 3^2 + 8^2$$

Pelo corolário 3.2, como $73 = 18.4 + 1$, temos que

$$3+8i \text{ é primo em } \mathbb{Z}[i].$$

CONCLUSÃO

Durante a elaboração deste trabalho nossa preocupação foi evidenciar as ligações que há entre conteúdos distintos da Teoria Elementar dos Números. Verificamos propriedades de $\mathbb{Z}$ mantidas em $\mathbb{Z}[i]$: divisibilidade, o algoritmo de Euclides, a ideia de fatoração e de número primo e composto.

Explorando essas ligações percebemos o significado e funcionalidade nos conceitos trabalhados acarretando consequentemente a assimilação desses conteúdos.

No desenvolvimento dos conteúdos abordados como também na aplicação dos mesmos foi nossa intenção colocá-los dentro de um nível de compreensão e maturidade de um aluno do Ensino Fundamental e Médio.

Na troca de ideias com professores sobre o nosso assunto, as respostas obtidas foram muito importantes. O que fizemos em termos de pesquisa e consulta a amigos para a realização desse trabalho nos possibilitou aprender muito a respeito não só do tema em estudo, mas também do ensino da Matemática em geral.

Confesso que cresci pessoal e profissionalmente com esse trabalho tendo dessa forma ampliado meus horizontes para estudos na busca de melhoria do ensino da Matemática a partir dos anos finais do Ensino Fundamental.

Por fim, esperamos que esse trabalho possa contribuir como estímulo e ao mesmo tempo servir de fonte de consulta por parte de professores e alunos que estejam interessados neste tipo de assunto buscando ampliar seus conhecimentos com a finalidade de minimizar as dificuldades encontradas no trato dessa matéria.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] –HEFEZ, Abramo. Elementos de Aritmética. Segunda Edição. Rio de Janeiro: SBM. 2011.

[2] –HEFEZ, Abramo. Elementos da Aritmética. Textos Universitários. Sociedade Brasileira de Matemática. 2ª edição. Rio de Janeiro-RJ. 2011

[3] –MARTINEZ, Fabio B. MOREIRA, Carlos G. SALDANHA, Nicolau. TENGAN, Eduardo. Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro. Projeto Euclides. IMPA, Rio de Janeiro - 2011.

[4] –VIDIGAL Ângela, AVRITZER Dan, SOARES Eliana Farias e, BUENO Hamilton Prado, FERREIRA Maria Cristina Costa e FARIA Marília Costa de. Fundamentos de Álgebra. Editora UFMG. 1ª Edição atualizada.

[5] –GARCIA, Arnaldo, Elementos de Álgebra, IMPA, 2010.

[6] – GONÇALVES, Adilson, Introdução à álgebra, IMPA, 1999

SITES CONSULTADOS:

[1]- https://pt.wikipedia.org/wiki/Euclides

[2] - www.somatematica.com.br/biograf/euclides.php

[3] - https://pt.wikipedia.org/wiki/Carl_Friedrich_Gauss

[4] - www.somatematica.com.br/biograf/gauss.php

[5] - www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/DC_M2_FM_2013.pdf

[6] - www.obm.org.br/export/sites/default/revista_eureka/docs/artigos/gauss.doc

[7] - http://tede.ufam.edu.br/handle/tede/5074

[8] - http://www.profmat-sbm.org.br/dissertacoes? – FILHO, Fernando de Moraes Campos, Algumas Propriedades dos Inteiros de Gauss.

[9] - http://www.profmat-sbm.org.br/dissertacoes? - SOUSA, Márcio Monte Alegre. Divisibilidade em Domínios de Integridade

[10] - www.icmc.usp.br/~iresdias/material/sma306.pdf

[11] - www.mat.ufmg.br/~marques/Apostila-Aneis.pdf

[12] - https://ssa_mat.catalao.ufg.br/up/615/o/Notas_de_aula_-_Mar%C3%ADlia.pdf