Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Algumas Propriedades dos Inteiros de Gauss

Luiz Fernando de Moraes Campos Filho
Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT
Setembro de 2014

Algumas Propriedades dos Inteiros de Gauss

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Luiz Fernando de Moraes Campos Filho e aprovada pela comissão julgadora.

Cuiabá, 26 de setembro de 2014.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo
Prof. Dr. José de Arimatéia Fernandes
Prof. Dr. Reinaldo de Marchi

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, desenvolvido pela Sociedade Brasileira de Matemática na Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título de **Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

F481a Filho, Luiz Fernando de Moraes Campos.
Algumas Propriedades dos Inteiros de Gauss / Luiz Fernando de Moraes Campos Filho. -- 2014
x, 88 f. : il. color. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2014.
Inclui bibliografia.

1. Divisão Euclidiana. 2. Números Complexos. 3. Soma de dois quadrados. 4. Inteiro Gaussiano. I. Título.

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

Dissertação de Mestrado defendida em 26 de setembro de 2014 e aprovada pela banca examinadora composta pelos Professores Doutores

_____

Prof. Dr. Martinho da Costa Araújo

_____

Prof. Dr. José de Arimatéia Fernandes

_____

Prof. Dr. Reinaldo de Marchi

Agradecimentos

A Deus pela graça da vida e pelas oportunidades que tive.

A minha família, em especial à minha mãe Regina Lúcia dos Santos Campos, irmã Marivane Campos e cunhado Ricardo Santos pelo incentivo nos estudos e pelo apoio finaceiro durante a graduação.

Aos meus colegas de graduação e Mestrado, pela companhia, estudos, angústias e alegrias em especial à Ricardo Sávio, Nivaldo Vitor, Gilliard Hortêncio, Jessé Garcia e Marco Antônio sem os quais provavelmente não terminaria esta Tese.

Aos meus Professores da graduação e Mestrado em especial ao meu orientador Prof. Dr. Martinho da Costa Araújo.

Aos meus colegas de profissão da Escola Estadual Professora Arlete Maria da Silva pela compreensão e auxílio nestes dois anos de estudo em especial à Elisângela, Regina e Adenilza.

Por fim agradeço à Capes pelo auxílio financeiro. Muito obrigado a todos.

Voltei-me e vi debaixo do sol que
não é dos ligeiros a carreira,
nem dos valentes a peleja,
nem tão pouco dos sábios o pão,
nem ainda dos prudentes a riqueza
nem dos entendidos o favor,
mas que o tempo e a sorte pertence a
todos.

(Eclesiastes 9:11).

Resumo

O presente trabalho consiste no estudo do conjunto $\mathbb{Z}[i]$, formado pelos pares (a, b), onde a e b são números inteiros e $i^2 = -1$. Neste conjunto definiremos uma função multiplicativa chamada Norma e desenvolveremos uma teoria similar à desenvolvida no estudo de Números Inteiros. O principal resultado consiste que em $\mathbb{Z}[i]$ a fatoração em primos é mantida, ou seja, todo inteiro gaussiano não nulo pode ser escrito como produto de primos. Por fim, mostramos que é possível resolver problemas de números inteiros através da teoria dos Inteiros de Gauss, tais como: um primo que é escrito como soma de dois quadrados, um quadrado que é escrito como soma de dois quadrados e um cubo que é escrito como soma de dois quadrados.

Palavras chave: Divisão Euclidiana, Soma de dois quadrados, Número Complexo, Número Primo, Inteiro Gaussiano.

Abstract

This present work consists in the study of $\mathbb{Z}[i]$, formed by the pair (a, b) where com a and b are integers and $i^2 = -1$. In this set we define a certain multiplicative function called Norma and develop a similar sequence developed in the study of numbers Integers theory. The main result is that in $\mathbb{Z}[i]$ the factorization into primes is maintained, ie, all nonzero Gaussian integer can be written as a product of primes. Finally, we show that it is possible to solve problems of integers through the theory of Gaussian integers, such as a prime that is written as a sum of squares, a square that is written as a sum of squares and a cube that is written as a sum square.

Keywords: Euclidian division, Sum square, complex number, prime number, Gaussian integers.

Sumário

Lista de Figuras

Introdução

"O pensamento é apenas um lampejo entre duas longas noites, mas esse lampejo é tudo."

(H. Poincaré)

Um pouco sobre a história de Gauss

Johann Carl Friedrich Gauss (1777-1855) foi um matemático e cientista alemão, que contribuiu significativamente para diversas áreas, incluindo a teoria dos números, estatística, análise, geometria diferencial, geodesia, geofísica, eletrostática, astronomia e ótica.

Ele teve uma influência notável em muitos campos da matemática e ciência e está classificado como um dos matemáticos mais influentes da história. Ele se refere a matemática como "a rainha das ciências". Gauss foi uma criança prodígio, pois começou sua história com a matemática logo cedo, ainda na infância. Mesmo sendo filho de camponeses pobres, teve apoio de sua mãe e de seu tio para estudar. Aos três anos de idade, Gauss já realizava algumas operações aritméticas, tendo, desenvolvido precocemente as suas façanhas matemáticas.

Conta-se que, segundo Boyer(1996, p. 343):

Um dia, para ocupar a classe, o Professor mandou que os alunos somassem todos os números de um a cem, com instrução para que cada um colocasse sua ardósia[1] *sobre a mesa logo que completasse a tarefa. Quase imediatamente, Gauss colocou sua ardósia sobre a mesa, dizendo: 'Ai está!' O professor olhou-o com desdém enquanto os outros*

[1] seria uma espécie de pequena lousa.

trabalhavam diligentemente. Quando o instrutor finalmente olhou o resultado, a ardósia de Gauss era a única com a resposta correta, 5050.

Gauss tinha 10 anos de idade.

Espantou o seu mestre, Buttner, quando iniciou os estudos de aritmética mostrando grande facilidade em resolver operações matemáticas consideradas complicadas. Buttner tinha, nessa época, um jovem assistente, de 17 anos, Johann Martin Bartels, apaixonado pela matemática, a quem entregou a tarefa de ensinar ao precoce Gauss. Entre os dois moços firmou-se sólida amizade, que durou até a morte de Bartels. Um dos frutos dessa amizade foi o caminho que Bartels abriu para Gauss, pois o fez conhecido do duque de Braunschweig, Carl Wilhelm Ferdinand, este se tornou protetor de Gauss e lhe proporcionou condições de estudo.

No ano de 1792, Gauss se matriculou no colégio Carolinum, permanecendo três anos. Estudou profundamente as obras de Leonhard Euler, Joseph-Louis Lagrange e Isaac Newton. Nesta época Gauss iniciou as suas investigações sobre Aritmética Superior, que o tornaria imortal e lhe daria o título de "Príncipe da Matemática". Gauss deixou o Collegium Carolinum em outubro de 1795, para entrar na Universidade de Göttingen. Em 1796 define suas preferências difinitivamente, decidindo dedicar-se à matemática. No dia 30 de março desse ano, Gauss começa a redigir um diário científico, anotando as suas descobertas. Esse diário só foi divulgado 43 anos após a morte de Gauss. O diário contém 146 anotações, breves exposições dos descobrimentos feitos pelo seu autor no período de 1796 a 1814. Os três anos passados em Göttingen foram dos mais prolíficos de sua vida. As ideias que vinha recolhendo desde os 17 anos, foram, nessa época, ordenadas e esmiuçadas, resultando, em 1798, nas Indagações Aritméticas, por muitos considerada a obra prima de Gauss.

O percurso vitorioso de Gauss viria a terminar a 23 de fevereiro de 1855, dia em que faleceu enquanto dormia. Apesar da sua morte, o seu trabalho e as suas poderosas contribuições para a Matemática estão, ainda hoje, mais vivas do que nunca. Em um olhar pela história da Matemática e da Astronomia será impossível não reconhecer o quanto o

trabalho realizado por Gauss permitiu que estas duas ciências progredissem e tivessem o grau de rigor e precisão que hoje as caracterizam.

Um pouco sobre a história dos números inteiros gaussianos

Entre os anos de 1808 e 1825, Gauss investigava questões relacionadas à reciprocidade cúbica: $x^3 \equiv q \ (mod\ p)$, onde x é inteiro e p, q primos e a reciprocidade biquadrática: $x^4 \equiv q \ (mod\ p)$, onde x é inteiro e p, q primos, que podem ser escritas da seguinte maneira, respectivamente: $\alpha.p = x^3 - q$ e $\alpha.p = x^4 - q$, quando percebeu que essa investigação se tornava mais simples trabalhando em um subconjunto dos números complexos $\mathbb{Z}[i]$, o conjunto 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 consequências importantes na Teoria dos Números. Ele desenvolveu uma teoria de fatoração em primos para esses números complexos e demonstrou que essa decomposição em primos é única, como acontece com o conjunto dos números inteiros.

Proposta do Trabalho

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.

Será que problemas complexos em $\mathbb{Z}$ são mais simples em $\mathbb{Z}[i]$? Será que é possível resolver problemas dos inteiros usando a teoria dos inteiros gaussianos? Dados dois números complexos $\alpha = a + bi$ e $\beta = c + di$, com a, b, c, d inteiros, será que é possível obter outros complexos $\gamma = m + ni$ e $r = w + zi$, com m, n, w, z inteiros, tal que $\alpha = \beta\gamma + r$? Será que existe uma expressão que descreva todos os pontos da Figura 1? Observe que os primos $5 = 1^2+2^2, 13 = 2^2+3^2, 17 = 1^2+4^2, 29 = 2^2+5^2, 37 = 1^2+6^2$ têm características semelhantes: são escritos como soma de quadrados e deixam resto 1 quando

dividido por 4. Será que números com estas características sempre serão escritos como soma de quadrados? Agora observe que os primos $3, 7, 11, 19$ também possuem características semelhantes: não são escritos como soma de quadrados e deixam resto 3 quando divididos por 4. Será que números com estas características não podem ser escritos como soma de quadrados? Observe que $125 = 5^3 = 121 + 4 = 11^2 + 2^2$, $8 = 2^3 = 4 + 4 = 2^2 + 2^2$. Será que sempre é possível escrever um cubo como soma de quadrados? Será que é possível falar em número primo em $\mathbb{Z}[i]$? Será que todos os números primos em $\mathbb{Z}$ são primos em $\mathbb{Z}[i]$?

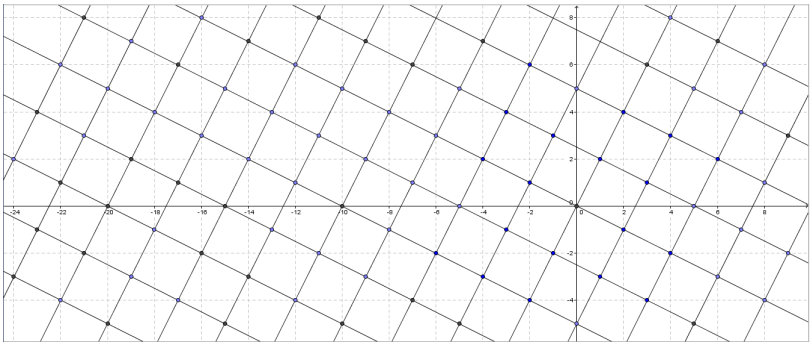


Figura 1: Existe uma expressão que descreva todos os pontos desta malha?

Na busca destas respostas e no desenvolvimento desta teoria, este estudo se constitui numa pesquisa qualitativa do tipo bibliográfica. Pretendemos transformar todo este estudo em um material didático com a teoria necessária para servir de apoio ao Professor e/ou estudante matemático e atividades numéricas, curiosas e de fácil acesso para o leitor interessado no assunto.

A ideia é construir um material com uma linguagem mais simplificada, não usando termos da Álgebra, mas seguindo o padrão do estudo dos naturais no ensino fundamental.

No primeiro Capítulo faremos um resumo de teorias necessárias para o desenvolvimento de nosso trabalho. No segundo Capítulo faremos um estudo aprofundado da teoria dos inteiros gaussianos, isto é, definição, função norma, divisibilidade, primos, etc. 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 faremos as considerações sobre a pesquisa, comentários sobre o trabalho e sobre possíveis caminhos que este trabalho pode seguir. No quinto Capítulo faremos um compêndio de atividades, juntamente com suas soluções.

Capítulo 1

Um pouco de Teoria

Neste capítulo faremos um compêndio de assuntos que nos serão necessários para o desenvolvimento deste trabalho. Veremos assuntos relacionados a Aritmética indo até o estudo de congruência, Teorema de Wilson e o Pequeno Teorema de Fermat. Por fim falaremos um pouco sobre números complexos.

1.1 Noções de Aritmética

Neste seção apresentaremos um breve apanhado dos conceitos de Aritmética dos Inteiros que serão necessários para o desenvolvimento do segundo e terceiro capítulos deste trabalho.

1.1.1 Um pouco de Aritmética dos Inteiros

Nesta seção faremos um breve apanhado de conceitos de Aritmética dos Inteiros que serão úteis para este trabalho. Imaginamos que o leitor já tenha alguma noção dos conceitos básicos pré-requisitados, caso não tenha, recomendamos a leitura de HEFEZ [2011].

Começaremos nossa abordagem pelo conjunto dos números inteiros positivos $\mathbb{N} = \{1, 2, 3, 4...\}$, ou seja, o conjunto dos números naturais, apresentando a seguinte ferramenta: O Princípio da Indução Finita.

1.1.2 Princípio da Indução

Embora esses próximos conceitos possam ser estendidos, com algumas hipóteses adicionais, a todo o conjunto dos números inteiros, será suficiente para este texto apresentarmos como segue.

Axioma 1.1.2.1. (Princípio da Indução) Seja A um conjunto não vazio de $\mathbb{N}$. Se

i) $1 \in A$;

ii) $n+1 \in A$ sempre que $n \in A$.

Então $A = \mathbb{N}$.

Usaremos este Axioma para demonstrar a seguinte afirmação

Teorema 1.1.2.2. (Princípio da Boa Ordenação) Todo subconjunto não vazio dos naturais possui um menor elemento.
DEMONSTRAÇÃO: Sejam $\mathcal{A}$ um subconjunto não vazio dos naturais, $I_n = \{p \in \mathbb{N};\ 1 \leq p \leq n\}$ e $\mathcal{X} \subset \mathbb{N}$, um conjunto formado pelos elementos $n \in \mathbb{N}$ tais que $I_n \subset \mathbb{N} - \mathcal{A}$.
Se $1 \in \mathcal{A}$, então claramente 1 é o menor elemento de $\mathcal{A}$.
Agora, se $1 \notin \mathcal{A}$, então $1 \in \mathcal{X}$, tendo em vista que $I_1 = \{1\} \subset \mathbb{N} - \mathcal{A}$. Porém $\mathcal{X} \neq \mathbb{N}$, pois $\mathcal{A} \neq \{\ \}$ e $\mathcal{X} \subset \mathbb{N}$.
Logo, o princípio da indução não pode ser aplicado a $\mathcal{X}$, o que implica que o item ii) do **Axioma 1.1.2.1.** não vale em $\mathcal{X}$, isto é: existe um $n_0 \in \mathcal{X}$ tal que $n_0 + 1 \notin \mathcal{X}$.
Como $I_n \subset \mathbb{N} - \mathcal{A}$, temos que todos os números inteiros de 1 a n_0 pertencem a $\mathcal{X}$ e como $n_0 + 1 \notin \mathcal{X}$, temos que $n_0 + 1 \in \mathcal{A}$ e $I_n = \mathcal{X}$.
Portanto, $a = n_0 + 1$ é o menor elemento de $\mathcal{A}$.

■

Teorema 1.1.2.3. (Princípio da Indução Forte) Seja $\mathcal{A}$, um subconjunto não-vazio de $\mathbb{N}$. Se:

i) $1 \in \mathcal{A}$;

ii) $n+1 \in \mathcal{A}$ sempre que $1, 2, 3, 4, ..., n \in \mathcal{A}$.

Então $\mathcal{A} = \mathbb{N}$.

1.1.3 Algoritmo da Divisão Euclidiana

A partir de agora abordaremos, de fato, conceitos referentes a propriedades de números inteiros iniciando o estudo da divisibilidade de números inteiros tendo como principal resultado o Algoritmo da Divisão.

Definição 1.1.3.1. Sejam a, b números inteiros. Dizemos que b é **divisor** de a quando existe um número inteiro c, tal que $a = bc$. Dizemos também que "b divide a", ou "a é múltiplo de b", ou ainda, "a é divisível por b". Denotamos por $b|a$. Quando b não é um divisor de a, denotamos $b \nmid a$.

Exemplo 1.1.3.2. O inteiro 7 é divisor de 21 em $\mathbb{Z}$. Basta notar que $7.3 = 21$ e 3 é um número inteiro.

Proposição 1.1.3.3. Sejam $a, b, c, d, n_1, n_2, ..., n_s$ números inteiros. As seguintes afirmações são verdadeiras:

i) $a|0$ e $a|a$;

ii) Se $a|b$ e $b|c$, então $a|c$;

iii) Se $a|b$ e $c|d$, então $ac|bd$. Em particular, se $a|b$, então $ca|cb$;

iv) Se $a|(b + c)$ e $a|b$, então $a|c$;

v) Se $a|n_1$, $a|n_2$, ..., $a|n_s$, então $a|(c_1n_1+c_2n_2+...+c_sn_s)$ para todos os inteiros $c_1, c_2, ..., c_s$.

vi) Se $a|b$ e $b|a$, então $a = \pm b$.

DEMONSTRAÇÃO: Consulte SAMPAIO [2013].

■

Para enunciar o principal resultado desta seção e para sua demonstração necessitamos definir a função **Valor Absoluto** e demonstrar uma proposição chamada **Propriedade Arquimediana de** $\mathbb{Z}$.

Definição 1.1.3.4. A função $|\cdot|$ definida por:

$$\begin{aligned} |\cdot| \quad : \quad & \mathbb{Z} \longrightarrow \mathbb{Z}_+ \cup \{0\} \\ & a \longmapsto |a| = \begin{cases} a, & a \geq 0 \\ -a, & a < 0 \end{cases} \end{aligned}$$

é chamada **Valor Absoluto** em $\mathbb{Z}$.

Proposição 1.1.3.5. Sejam a, b, r números inteiros. Então:

i) $|ab| = |a|.|b|$;

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

iii) $|a| \leq r \Leftrightarrow -r \leq a \leq r$;

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

v) $0 \leq |a| \ \forall \ a \in \mathbb{Z}$

vi) $|a| = b \geq 0 \Rightarrow a = \pm b$.

DEMONSTRAÇÃO: Veja HEFEZ [2011].

■

Proposição 1.1.3.6. (Propriedade Arquimediana de $\mathbb{Z}$) Dados dois números inteiros a e b, com $b \neq 0$, existe um inteiro n tal que $nb \geq a$.
DEMONSTRAÇÃO: Como $b \neq 0$, temos que $|ab| \geq |a| \geq a$. Daí, quando $b > 0$, basta tomar $n = |a|$; daí, $nb = |a|.b = |a|.|b| = |ab| \geq |a| \geq a$. Por outro lado, se $b < 0$, basta tomar $n = -|a|$, o que acarreta $nb = (-|a|).b = |a|(-b) = |a||b| = |ab| \geq |a| \geq a$.

■

Agora vamos para o teorema que estabelece um método de divisão para números inteiros.

Teorema 1.1.3.7. (Algoritmo de Euclides para $\mathbb{Z}$) Seja $|\cdot| : \mathbb{Z} \longrightarrow \mathbb{Z}_+$ a função valor absoluto. Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem $t, r \in \mathbb{Z}$ tais que $a = bt + r$, onde

$0 \leq r < |b|$. Além disso, t e r são univocamente determinados por essas duas condições. Os inteiros t e r acima são chamados (respectivamente) **quociente** e **resto** da divisão euclidiana de a por b.

DEMONSTRAÇÃO: Para a demonstração, sejam $a, b \in \mathbb{Z}$, com $n \neq 0$ e consideremos o conjunto

$$\mathcal{S} = \{x \in \mathbb{Z}_+;\ x = a - bn;\ n \in \mathbb{Z}\}$$

É claro que $\mathcal{S}$ é limitado inferiormente. Além disso, afirmamos que $\mathcal{S} \neq \{\ \}$. Com efeito, existe, em decorrência da Propriedade Arquimediana, um inteiro n_0 tal que $n_0(-b) \geq -a$. Desse modo, obtemos $x_0 = a - bn_0 \geq 0$, com $n_0 \in \mathbb{Z}$, o que significa $x_0 = a - bn_0 \in \mathcal{S}$.

Assim, $\mathcal{S}$ está nas hipóteses do Princípio da Boa Ordenação, implicando assim a existência de $r = min\ \mathcal{S}$. Como $r \in \mathcal{S}$, temos que $r = a - bt \geq 0$, para algum $t \in \mathbb{Z}$.

Resta provar que $r < |b|$. Suponhamos que ocorresse $r \geq |b|$, isto é, $r = |b| + s$, para algum $s \in \mathbb{Z}$, tal que $0 \leq s < r$. Teríamos, então, $a = bt + r = bt + |b| + s = b(t \pm 1) + s$, e, consequentemente, $s = a - b(t \pm 1) \in \mathcal{S}$, pois $(t \pm 1 \in \mathbb{Z})$, e $s \geq 0$. Assim, s seria um elemento de $\mathcal{S}$ menor do que $r = min\ \mathcal{S}$. Contradição.

Para demonstrar a unicidade de t e r, suponhamos que

$$a = bt_1 + r_1 = bt_2 + r_2, \qquad (IV)$$

onde $t_1, t_2, r_1, r_2 \in \mathbb{Z}$, com $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$.

Multiplicando a primeira desigualdade por (-1), obtemos $-|b| < -r_1 \leq 0$. Daí, somando membro a membro as desigualdades $0 \leq r_2 < |b|$ e $-|b| < -r_1 \leq 0$, encontramos $-|b| < r_2 - r_1 \leq |b|$. Dessa última igualdade e de (IV), obtemos:

$$b(t_1 - t_2) = r_1 - r_2 \Rightarrow |b||t_1 - t_2| = |r_1 - r_2| < |b| \Rightarrow |t_1 - t_2| < 1 \Rightarrow |t_1 - t_2| = 0 \Rightarrow t_1 - t_2 = 1.$$

Logo $t_1 = t_2$, o que implica em $r_2 - r_1 < 1 = b(t_1 - t_2) = b.0 = 0$, isto é, $r_1 = r_2$.

■

Observe que, a função valor absoluto é que garante a unicidade do resto e em consequência disso a unicidade do quociente, pois se exigíssemos apenas $0 \leq r < b$, obteríamos dois possíveis quocientes e dois restos (um se b for positivo e outro se b for negativo).

1.1.4 Máximo Divisor Comum

Definição 1.1.4.1. Dados dois inteiros a e b, chama-se máximo divisor comum de a e b o inteiro d, que satisfaz as condições:

(1) Se $a = b = 0$ então $d = 0$;

(2) Se $a \neq 0$ ou $b \neq 0$ então d é caracterizado pelas propriedades:

i) $d|a$ e $d|b$;

ii) Para cada inteiro x, se $x|a$ e $x|b$ então $x|d$. Neste caso, temos $x \leq d$.

Observação 1.1.4.2. Se d é o máximo divisor comum de a e b, denotamos por $d = mdc(a, b) = (a, b)$. De maneira mais geral podemos definir $mdc(a_1, a_2, ...a_n)$ para inteiros $a_1, a_2, ...a_n$.

Exemplo 1.1.4.3. Os divisores comuns de 24 e 32 são $\pm 1, \pm 2, \pm 4$ *e* ± 8. Portanto, $(24, 32) = 8$. Analogamente, olhando os conjuntos de divisores comuns, concluímos que $(35, 55) = 5, (0, 5) = 5, (3, 2) = 1, (-9, -15) = 3$.

Definição 1.1.4.4. Dois inteiros são ditos **primos entre si** quando $(a, b) = 1$.

A proposição seguinte garante a existência do (a, b) em $\mathbb{Z}$, para a e b não simultaneamente nulos. Além disso, fornece uma caracterização extremamente útil para esse (a, b).

Proposição 1.1.4.5. Sejam a e b números inteiros não simultaneamente nulos. Então existe $d = (a, b)$ em $\mathbb{Z}$. Além disso, $d = (a, b) = min\{ma + nb > 0; m, n \in Z\}$.
DEMONSTRAÇÃO: Consideremos o conjunto $\mathcal{L} = \{ma + nb > 0; m, n \in Z\} \subset Z$. Inicialmente, note que $\mathcal{L} \neq \{\ \}$. De fato, como $a \neq 0$ ou $b \neq 0$, concluímos o inteiro $|a| + |b| > 0$

pertence a $\mathcal{L}$. Além disso, é fácil ver que $\mathcal{L}$ é limitado inferiormente. Logo, pelo Princípio da Boa Ordem, existe $d = min\ \mathcal{L}$.
Resta mostrar que $d = (a, b)$.

Com efeito, por um lado, como $d \in \mathcal{L}$, podemos escrever $d = m_0a + n_0b > 0$, com $m_0, n_0 \in \mathbb{Z}$. Por outro lado, efetuando a divisão euclidiana de a por d, obtemos $t, r \in \mathbb{Z}$ tais que $a = dt + r$, com $0 \leq r < d$. Daí:

$$r = a - dt = a - (m_0a + n_0b)t = a - m_0at - n_0bt = (1 - m_0t)a + (n_0t)b$$

Isto nos permite concluir que $r = 0$. De fato, se fosse $r > 0$, teríamos $r \in \mathcal{L}$, o que não pode ocorrer, uma vez que implicaria em $r < d = min\ \mathcal{L}$. Em vista da equação acima e do fato que $r = 0$, podemos conluir que $a = dt$, e, portanto, $d|a$.

Um raciocínio análogo (efetuando a divisão euclidiana de b por d) nos permite conluir que $d|b$. Logo, $d|a$ e $d|b$, e a condição (i) da definição de mdc está demonstrada.
Para mostrarmos que a condição (ii) também ocorre, seja $x \in \mathbb{Z}$ tal que $x|a$ e $x|b$. Então, existem $u, v \in \mathbb{Z}$ tais que $a = ux$ e $b = vx$. Devemos provar que $x|d$.
Com efeito, uma vez que $d \in \mathcal{L}$, podemos escrever $d = m_0a + n_0b$, $m_0, n_0 \in \mathbb{Z}$. Daí:

$$d = m_0a + n_0b = m_0(ux) + n_0(vx) = (m_0u + n_0v)x$$

O que significa que $x|d$ como queríamos.

■

Corolário 1.1.4.6. Sejam $a, b \in \mathbb{Z}$ e $d = (a, b)$. Então existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Em particular, se $a, b \in \mathbb{Z}$ são primos entre si, então existem $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$
DEMONSTRAÇÃO: Segue imediatamente do teorema anterior.

■

Teorema 1.1.4.7. Se $a|bc$ e $(a, b) = 1$, então $a|c$.
DEMONSTRAÇÃO: Como $(a, b) = 1$ pelo resultado acima existem inteiros n e m tais que

$na + mb = 1$. Multiplicando-se os dois lados desta igualdade por c, temos $cna + cmb = c$. Como $a|ac$ e, por hipótese, $a|bc$ então $a|(n(ac) + m(bc))$ e, portanto $a|c$.

■

Proposição 1.1.4.8. Para todo inteiro positivo t, $(ta, tb) = t(a, b)$.
DEMONSTRAÇÃO: Pelo **Teorema 1.1.4.6.** (ta, tb) é o menor valor positivo de $mta+ntb$ (m e n inteiros), que é igual a t vezes o menor valor positivo de $mta + ntb = t(ma + nb) = t(a, b)$.

■

Proposição 1.1.4.9 Se $c > 0$ e a e b são divisíveis por c, então

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

DEMONSTRAÇÃO: Como a e b são divisíveis por c, temos que a/c e b/c são números inteiros. Basta, então substituir na **Proposição 1.1.4.8.** "a" por "a/c" e "b" por "b/c", tomando $t = c$.

■

Corolário 1.1.4.10. Se $(a, b) = d$, temos que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
DEMONSTRAÇÃO: No que acabamos de demonstrar c é um divisor comum de a e b. Se tomarmos c como sendo o máximo divisor comum d, teremos o resultado desejado.

■

1.1.5 Números Primos

Nesta seção abordaremos um dos conceitos mais importantes e enigmáticos de toda a Matemática, os números primos. Esses números atraíram, desde os tempos remotos, a atenção dos maiores matemáticos existentes. Grandes esforços já foram depositados no estudo desses números, pois eles estão envolvidos em muitos problemas famosos, inclusive uma grande parte destes ainda resistem sem solução há muitos anos. Nestas linhas voltamos nossa atenção, única e exclusivamente, ao papel fundamental que os números primos desempenham, ou seja, ao de decompor todos os números inteiros maiores que 1

em produto de fatores primos.

Definição 1.1.5.1. Um número inteiro não nulo é dito **primo** quando:

i) $p \notin \{-1, 1\}$;

ii) Os únicos divisores de p são ± 1 e $\pm p$.

Um número inteiro $n \notin \{-1, 0, 1\}$ que não é primo, é chamado de **composto**. Isto significa que n possui um divisor $x \neq 0$ com $x < |n|$.
Provaremos agora uma proposição que é consequência imediata da definição de número primo. Na verdade este resultado que provaremos é equivalente a tal definição, sendo em muitos textos utilizados como definição.

Proposição 1.1.5.2. Sejam a, b, p números inteiros com p primo. Se $p|ab$, então $p|a$ ou $p|b$.
DEMONSTRAÇÃO: Para demonstrar esta proposição vamos supor que $p \nmid a$ e concluir que $p|b$.

Seja p um inteiro primo e a, b inteiros onde $p|ab$ e $p \nmid a$.
Se $p \nmid a$, então $(a, p) = 1$. Isto significa que a e p são relativamente primos. Sendo assim, temos através do **Corolário 1.1.4.6.** que existem inteiros x e y tais que

$$xa + yp = 1.$$

Multiplicando ambos os membros da equação acima por b, obtemos

$$abx + pby = b$$

Como $p|ab$, $p|p$, temos que $p|(abx + bpy)$ e, portanto, $p|b$.

■

Corolário 1.1.5.3. Sejam $p, a_1, a_2, ..., a_n$ números inteiros com $n \geq 2$ e p primo. Se $p|(a_1 a_2 ... a_n)$ então $p|a_i$ para algum índice $i \in \{1, 2, 3, ..., n\}$.
DEMONSTRAÇÃO: A demonstração se faz por indução sobre n. O leitor interessado pode consultar SAMPAIO [2013].

■

Por fim enunciaremos e demonstraremos o principal teorema desta seção que permite decompor um número inteiro em um produto de fatores primos, como dito anteriormente.

Teorema 1.1.5.4. (Teorema Fundamental da Aritmética) Todo inteiro n não nulo pode ser escrito na forma

$$n = u.p_1.p_2...p_k \qquad (I)$$

onde $u \in \{-1, 1\}$ e $p_1 \leq p_2 \leq ... \leq p_k$ são primos positivos. Além disso a expressão é única.

DEMONSTRAÇÃO: É suficiente mostrar o caso $u = 1$, isto é, faremos a demonstração para inteiros positivos. Reduzimos assim a expressão (I) a $n = p_1.p_2...p_k$.

A demonstração se faz utilizando o segundo princípio de indução sobre n.

Supondo então que todo número inteiro m, com $1 \leq m < n$ pode ser escrito como produto de primos (hipótese de indução). Afirmamos que n também pode.

De fato, se n é primo, nada temos para fazer. Mas se n é composto, então existem inteiros m_1 e m_2, com $1 \leq m_1 < n$ e $1 \leq m_2 < n$, tais que $n = m_1 m_2$. Logo, pela hipótese de indução existem $q_1 \leq q_2 \leq ... \leq q_r$ e $t_1 \leq t_2 \leq ... \leq t_s$ primos positivos tais que:

$$m_1 = q_1 \leq q_2 \leq ... \leq q_r \quad e \quad m_2 = t_1 \leq t_2 \leq ... \leq t_s.$$

Portanto

$$n = m_1 m_2 = (q_1 \leq q_2 \leq ... \leq q_r)(t_1 \leq t_2 \leq ... \leq t_s) \qquad (II)$$

Reorganizando os números primos $q_1 \leq q_2 \leq ... \leq q_s$ e $t_1 \leq t_2 \leq ... \leq t_s$ em (II), obtemos

$$n = p_1.p_2...p_k.$$

com $p_1 \leq p_2 \leq ... \leq p_k$ primos positivos e $k = r + s$, como queríamos.

Provaremos agora a unicidade desta decomposição.

Suponha que

$$n = p_1.p_2...p_k = p'_1.p'_2...p'_t \qquad (III)$$

onde $p_1 \leq p_2 \leq ... \leq p_k$ e $p'_1 \leq p'_2 \leq ... \leq p'_t$ são primos positivos.

Novamente pelo segundo princípio de indução sobre k, temos que se $k = 1$ então $p_1 = p'_1.p'_2...p'_t$

Logo $p'_i | p_1$ para algum $i \in \{1, 2, ...t\}$ e como p'_i e p_1 são primos, temos que $p'_i = p_1$, implicando assim que $k = 1 = t$.

Supondo agora que a unicidade acontece sempre que tivermos um produto de r fatores primos, onde $1 \leq r < k$. Vamos provar, a partir disso, que a unicidade vale para um inteiro positivo formado por um produto de k fatores primos.

De fato, se $p_1.p_2...p_k = p'_1.p'_2...p'_t$, com $k \geq 2$ então p_1 divide algum p'_i e, como os dois são número primos, temos que $p'_i = p_1$. Sem perda de generalidade podemos supor que $p'_1 = p_1$. Assim na equação (III) podemos cancelar $p'_1 = p_1$, obtendo

$$p_2.p_3...p_k = p'_2.p'_3...p'_t.$$

Note que no primeiro membro da equação acima temos $k-1$ fatores primos e pela hipótese de indução o produto $p_2.p_3...p_k$ é único. Portanto $k - 1 = t - 1 \Leftrightarrow k = t$ e assim $p'_i = p_i$ $\forall\ i \in \{1, 2, ...t\}$, encerrando nossa demonstração.

■

Antes de iniciarmos o novo tópico, vamos revisar algumas definições.

Definição 1.1.5.5. Sejam A e B dois conjuntos não vazios. Chama-se produto cartesiano de A por B, denotada por $A \times B$ o conjunto formado por todos os pares ordenados (x, y) tais que o primeiro elemento x pertence ao conjunto A e o segundo elemento y pertence ao conjunto B.

Definição 1.1.5.6. Sejam A e B dois conjuntos não vazios. Chama-se de relação binária de A em B ou apenas de relação de A em B todo subconjunto R de $A \times B$, isto é:

$$R \text{ é relação de } A \text{ em } B \Longleftrightarrow R \subset A \times B.$$

Definição 1.1.5.7. Sejam A um conjunto e R uma relação sobre A. Dizemos que R é uma relação de equivalência se, para todos $x, y, z \in A$:

1) [Propriedade Reflexiva] xRx.

2) [Propriedade Simétrica] Se xRy então yRx.

3) [Propriedade Transitiva] Se xRy e yRz então xRz.

Exemplo 1.1.5.8. São exemplos de relação sobre $\mathbb{Z}$ as seguintes ações $<, >, \neq, =$. Destas, apenas a ação $=$ é uma relação de equivalência.

Definição 1.1.5.9. Sejam R uma relação sobre o conjunto A e o elemento $a \in A$. Chama-se classe de equivalência determinada por a, módulo R, o subconjunto de A, definido por:

$$\overline{a} = \{x \in A \mid xRa\} \text{ ou } \overline{a} = \{x \in A \mid aRx\}$$

1.1.6 Aritmética dos Restos

Seja m um número natural diferente de zero. Diremos que dois números naturais a e b são *congruentes* módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \; mod \; m$$

Por exemplo, $21 \equiv 13 \; mod \; 2$, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Quando a relação $a \equiv b \; mod \; m$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso, $a \not\equiv b \; mod \; m$.

Como o resto da divisão de um número natural qualquer por 1 é sempre nulo, temos $a \equiv b \; mod \; 1$, quaisquer que sejam $a, \; b \in \mathbb{N}$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $m > 1$.

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente

aplicar o seguinte resultado:

Proposição 1.1.6.1. Suponha que $a,\ b \in \mathbb{N}$ são tais que $b \geq a$. Então $a \equiv b\ mod\ m$ *se, e somente se,* $m|b - a$.

DEMONSTRAÇÃO: Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = \begin{cases} m(q' - q) + (r' - r), & se\ r' \geq r \\ m(q' - q) - (r' - r), & se\ r \geq r' \end{cases}$$

onde $r' - r < m$, *ou* $r - r' < m$. Portanto, $a \equiv b\ mod\ m$ se, e somente se, $r = r'$, o que é equivalente a dizer que $m|b - a$.

■

Decorre, imediatamente, da definição que a congruência módulo um inteiro fixado m, é uma relação de equivalência. Vamos enunciar isto explicitamente abaixo.

Proposição 1.1.6.2. Seja $m \in \mathbb{N}$, com $m > 1$. Para todos $a, b, c \in \mathbb{N}$, tem-se que

(i) [Propriedade Reflexiva] $a \equiv a\ mod\ m$,

(ii) [Propriedade Simétrica] Se $a \equiv b\ mod\ m$, então $b \equiv a\ mod\ m$,

(iii) [Propriedade Transitiva] Se $a \equiv b\ mod\ m$ e $b \equiv c\ mod\ m$, então $a \equiv c\ mod\ m$.

DEMONSTRAÇÃO:
i) Note que $a - a = 0 = 0m$, logo $m|a - a$ o que é euivalente a dizer que $a \equiv a\ mod\ m$;
ii) Se $a \equiv b\ mod\ m$, então os restos da divisão de a e b por m são idênticos, isto é, existem q e q' tais que $a = qm + r$ e $b = q'm + r$. Agora note que $b - a = (q' - q)m$, o que é equivalente a $b \equiv a\ mod\ m$;
iii) Se $a \equiv b\ mod\ m$ e $b \equiv c\ mod\ m$ então os restos da divisão de a, b e c por m são idênticos, isto é, existem q, q' e q'' tais que $a = qm + r$, $b = q'm + r$ e $c = q''m + r$. Agora note que $a - c = (q - q'')m$, o que é equivalente a $a \equiv c\ mod\ m$.

■

Note que todo número natural é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $0, 1, ..., m-1$. Além disso, dois desses números distintos não são congruentes módulo m.

Portanto, para achar o resto da divisão de um número a por m, basta achar o número natural r dentre os números $0, 1, ..., m-1$ que seja congruente a a módulo m. Chamaremos de *sistema completo de resíduos* módulo m a todo conjunto de números naturais cujos resto pela divisão por m são os números $0, 1, ..., m-1$, sem repetições e em uma ordem qualquer.

Portanto, um sistema completo de resíduos módulo m possui m elementos. É claro que, se $a_1, ..., a_m$ são m números naturais, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que são os números $0, 1, ..., m-1$ em alguma ordem.

O que torna útil e poderosa a noção de congruência é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 1.1.6.3. Seja $a, b, c, d, m \in \mathbb{N}$, com $m > 1$.

(i) Se $a \equiv b \, mod \, m \;\; e \;\; c \equiv d \, mod \, m$, então $a + c \equiv b + d \, mod \, m$.

(ii) Se $a \equiv b \, mod \, m \;\; e \;\; c \equiv d \, mod \, m$, então $ac \equiv bd \, mod \, m$.

DEMONSTRAÇÃO: Suponhamos que $a \equiv b \, mod \, m \;\; e \;\; c \equiv d \, mod \, m$. Podemos, sem perca de generalidade, supor que $b \geq a \;\; e \;\; d \geq c$. Logo, temos que $m|b-a \;\; e \;\; m|d-c$.

(i) Basta observar que $m|(b-a)+(d-c)$ e, portanto, $m|(b+d)-(a+c)$, o que prova essa parte do resultado.

(ii) Basta notar que $bd - ac = d(b-a) + a(d-c)$ e concluir que $m|bd - ac$.

■

Corolário 1.1.6.4. *Para todo* $n \in \mathbb{N}$, $a, b \in \mathbb{N}$, *se* $a \equiv b \, mod \, m$, *então* $a^n \equiv b^n \, mod \, m$.
DEMONSTRAÇÃO: Note inicialmente que se $a \equiv b \ mod \ m$, então $m|a-b$. Repare também que

$$a^n - b^n = (a-b)a^{n-1} + a^{n-2}b + a^{n-3}b^2 + ... + ab^{n-2} + b^{n-1}.$$

Da igualdade acima, obtemos que $m|(a^n - b^n)$ e, portanto $a^n \equiv b^n \ mod \ m$.

■

Teorema 1.1.6.5 Se a,b,c e m são inteiros e $ac \equiv bc \ (mod \ m)$, então $a \equiv b \ (mod \ m/d)$, onde $d = (c, m)$.
DEMONSTRAÇÃO: Se $ac \equiv bc \ (mod \ m)$, então $m|(ac - bc) = c(a-b)$. Logo existe um inteiro k, tal que

$$c(a-b) = km.$$

Se dividirmos os dois membros da equação acima por d, obtemos $(c/d)(a-b) = k(m/d)$. Logo $(m/d)|(c/d)(a-b)$ e, como $(m/d, c/d) = 1$, pelo **Teorema 1.1.4.7.**, $(m/d)|(a-b)$, o que implica que $a \equiv b \ (mod \ m/d)$.

Definição 1.1.6.6. Se h e k são dois inteiros com $h \equiv k \ (mod \ m)$, dizemos que k é um resíduo de h módulo m.

Definição 1.1.6.7. O conjunto dos inteiros $\{r_1, r_2, ..., r_s\}$ é um sistema completo de resíduos módulo m se

i) $r_i \not\equiv r_j \ (mod \ m)$ para $i \neq j$.

ii) Para todo inteiro n existe um r_i tal que $n \equiv r_i \ (mod \ m)$.

Teorema 1.1.6.8. O conjunto $\{r_1, r_2, ..., r_k\}$ formam um sistema completo de resíduos módulo m então $k = m$.
DEMONSTRAÇÃO: Primeiramente demonstraremos que os inteiros $t_0, t_1, ..., t_{m-1}$, com $t_i = i$ formam, de fato, um sistema completo de resíduos módulo m. Pelo **Teorema 1.1.3.7** sabemos que, para cada n, existe uma único par de inteiros q e s, tal que $n =$

$mq + s$, $0 \leq s < m$. Logo $n \equiv\ s\ (mod\ m)$, sendo s um dos t_i. Como $|t_i - t_j| \leq m - 1$, temos que $t_i \not\equiv t_j\ (mod\ m)$ para $i \neq j$. Portanto, o conjunto $\{t_0, t_1, ..., t_{m-1}\}$ é um sistema completo de resíduos módulo m. Disto concluímos que cada r_i é congruente a exatamente um dos r_i, o que nos garante $k \leq m$. Como o conjunto $\{r_1, r_2, ..., r_s\}$ forma, por hipótese, um sistema completo de resíduos módulo m, cada t_i é congruente a exatamente um dos r_i e portanto $m \leq k$. Desta forma $k = m$.

■

Teorema 1.1.6.9. Se $\{r_1, r_2, ..., r_m\}$ é um sistema completo de resíduos módulo m, a e b são inteiros com $(a, m) = 1$, então

$$\{ar_1 + b, ar_2 + b, ..., ar_m + b\}$$

também é um sistema completo de resíduos módulo m.
DEMONSTRAÇÃO: Considerando-se o resultado do teorema anterior, será suficiente mostrar que quaisquer dois inteiros do conjunto $ar_1+b, ar_2+b, ..., ar_m+b$, são incongruentes módulo m. Para isto, vamos supor que $ar_i + b \equiv\ ar_j b\ (mod\ m)$. Logo, pela **Proposição 1.1.6.3.** temos $ar_i \equiv\ ar_j\ (mod\ m)$. Mas, como $(a, m) = 1$, o **Teorema 1.1.6.5** nos diz que $r_i \equiv\ r_j\ (mod\ m)$. O fato de $r_i \equiv\ r_j\ (mod\ m)$ implica $i = j$, uma vez que $r_1, r_2, ..., r_m$ formam um sistema completo de resíduos módulo m, o que completa a demonstração.

■

Congruência Linear 1.1.6.10. Chamamos de congruência linear em uma variável a uma congruência da forma $ax \equiv b\ (mod\ m)$ onde x é uma incógnita.

Definição 1.1.6.11. Uma equação da forma $ax + by = c$, onde a, b e c são inteiros é chamada de equação diofantina linear[1].

Teorema 1.1.6.12. Sejam a e b inteiros e $d = (a, b)$. Se $d \not| c$ então a equação $ax+by = c$ não possui nenhuma solução inteira. Se $d|c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por

$$x = x_0 + (b/d)k$$

[1]O nome vem do matemático grego Diofanto.

$$y = y_0 - (a/d)k$$

onde k é inteiro.

DEMONSTRAÇÃO: Se $d \not| c$, então a equação $ax+by = c$, não possui solução, pois, como $d|a$ e $d|b$, d deveria dividir c, o qual é uma combinação linear de a e b. Suponhamos, pois, que $d|c$. Pela **Proposição 1.1.4.6** existem inteiros n_0 e m_0, tais que

$$an_0 + bm_0 = d.$$

Como $d|c$, existe um inteiro k tal que $c = kd$. Se multiplicarmos, ambos os membros da equação acima por k, teremos $kan_0 + kbm_0 = kd = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. É fácil a verificação de que os pares da forma

$$x = x_0 + (b/d)k$$

$$y = y_0 - (a/d)k$$

são soluções, uma vez que

$$ax + by = a(x_0 + (b/d)k) + b(y_0 - (a/d)k)$$

$$ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k = ax_0 + by_0 = c$$

Mostramos assim que conhecida uma solução particular (x_0, y_0), podemos, a partir dela, gerar infinitas soluções. Precisamos, agora, mostrar que toda solução da equação $ax+by = c$ é da forma $x = x_0 + (b/d)k$, $y = y_0 - (a/d)k$. Vamos supor que (x, y) seja uma solução, isto é, $ax + by = c$. Mas, como $ax_0 + by_0 = c$, obtemos, subtraindo membro a membro, que

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0,$$

o que implica $a(x - x_0) = -b(y - y_0) = b(y_0 - y)$. Como $d = (a, b)$ temos, pelo corolário da **Proposição 1.1.4.10**,

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

Portanto, dividindo-se os dois membros da última igualdade por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

Logo, pelo **Proposição 1.1.4.7**, $(b/d)|(x-x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k(b/d)$, ou seja $x = x_0 + (b/d)k$. Substituindo-se estes valor de x na equação acima, obtemos $y = y_0 - (a/d)k$, o que conclui a demonstração.

■

Teorema 1.1.6.13. Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \not| b$ a congruência $ax \equiv b \ (mod\ m)$ não possui nenhuma solução e quando $d|b$, possui exatamente d soluções incongruentes módulo m.

DEMONSTRAÇÃO: Sabemos que um inteiro x é solução de $ax \equiv b \ (mod\ m)$ se, e somente se, existe outro inteiro y tal que $ax = b + my$, ou, o que é equivalente, $ax + my = b$. Do teorema anterior sabemos que esta equação não possui nenhuma solução caso $d \not| b$, e que se $d|b$ ela possui infinitas soluções dadas $x = x_0 + (b/d)k$ e $y = y_0 - (a/d)k$ onde (x_0, y_0) é uma solução particular de $ax - my = b$. Logo a congruência $ax \equiv b \ (mod\ m)$ possui infinitas soluções dadas por $x = x_0 - \frac{m}{d}k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob que condições $x_1 = x_0 - (m/d)k_1$ e $x_2 = x_0 - (m/d)k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes então $x_0 - (m/d)k_1 \equiv x_0 - (m/d)k_2 \ (mod\ m)$. Isto implica $(m/d)k_1 \equiv (m/d)k_2 \ (mod\ m)$, e como $(m/d)|m$, temos $(m/d, m) = m/d$, o que nos permite o cancelamento de m/d resultando, pelo **Teorema 1.1.6.5**, que $k_1 \equiv k_2 \ (mod\ m)$. Observe que m foi substituído por $d = m/(m/d)$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração.

■

Teorema 1.1.6.14. (Teorema de Wilson) Se p é primo, então $(p-1)! \equiv -1 \ (mod\ p)$.

DEMONSTRAÇÃO: Como $(2-1)! \equiv 1 \equiv -1 \ (mod\ 2)$ o resultado é válido para $p = 2$. Pelo **Teorema 1.1.6.12**, a congruência $ax \equiv 1 \ (mod\ m)$ tem uma única solução para todo a no conjunto $\{1, 2, 3, ..., p-1\}$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, 4, ..., p-2$ em $(p-3)/2$

pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos, pelo **Teorema 1.1.6.3** que:

$$2 \times 3 \times 4 \times ... \times (p-2) \equiv 1 \ (mod\ p).$$

Multiplicando-se ambos os lados desta congruência por $p-1$ teremos

$$2 \times 3 \times 4 \times ... \times (p-2)(p-1) \equiv (p-1) \equiv -1 \ (mod\ p).$$

■

Teorema 1.1.6.15. Se n é um inteiro tal que $(n-1)! \equiv -1 \ (mod\ n)$, então n é primo.
DEMONSTRAÇÃO: A prova é por contradição. Vamos supor que $(n-1)! \equiv -1 \ (mod\ n)$, isto é, $n|((n-1)!+1)$ e que n não seja primo, ou seja, $n = rs$, $1 < r < n$ e $1 < s < n$. Nestas condições $r|(n-1)!$ e, sendo r um divisor de n, $r|(n-1)!+1$ e, portanto, r deve dividir a diferença $(n-1)!+1-(n-1)! = 1$, o que é absurdo, uma vez que $r > 1$. Logo, um n satisfazendo $(n-1)! \equiv -1 \ (mod\ p)$ deve ser primo.

■

Teorema 1.1.6.16. (Pequeno Teorema de Fermat) Seja p primo. Se $p \not| a$ então $a^{p-1} \equiv 1 \ (mod\ p)$.
DEMONSTRAÇÃO: Sabemos que o conjunto formados pelos p números $0, 1, 2, 3, ..., p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, 3, ..., p-1\}$. Vamos, agora, considerar os números $a, 2a, 3a, ..., (p-1)a$. Como $(a, p) = 1$, nenhum destes números ia, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p.
Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak \ (mod\ p)$ implica $j \equiv k \ (mod\ p)$ e isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, ..., p-1$. Se multiplicarmos estas incongruências, membro a membro, teremos:

$$(a)(2a)(3a)...(p-1)a \equiv 1.2.3...(p-1) \ (mod\ p)$$

ou seja, $a^{p-1}(p-1)! \equiv (p-1)!\ (mod\ p)$. Mas, como $((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

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

o que conclui a demonstração.

■

Teorema 1.1.6.17. Para p primo, a congruência $x^2 \equiv\ -1\ (mod\ p)$ tem solução se, e somente se, $p = 2$ ou $p \equiv\ 1\ (mod\ 4)$.

DEMONSTRAÇÃO: É claro que $x = 1$ nos fornece uma solução $p = 2$. Vamos construir uma solução para o caso $p \equiv\ 1\ (mod\ 4)$.

Para p um primo ímpar podemos escrever o Teorema de Wilson da seguinte forma

$$\left(1.2.3...j...\frac{p-1}{2}\right)\left(\frac{p+1}{2}(p-j)...(p-2)(p-1)\right) \equiv -1\ (mod\ p)$$

Observamos que o produto $(p-1)!$ está dividido em duas partes, cada uma com o mesmo número de fatores. Podemos reescrever este produto formando pares, uma vez que para cada fator j na primeira parte temos o fator $(p-j)$ na segunda. Logo, o Teorema de Wilson pode ser escrito como:

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1\ (mod\ p).$$

Como $j(p-j) \equiv -j^2\ (mod\ p)$, temos:

$$-1 \equiv \prod_{j=1}^{(p-1)/2} (-j^2) \equiv (-1)^{(p-1)/2}\left(\prod_{j=1}^{(p-1)/2} j\right)^2\ (mod\ p)$$

Mas sendo $p \equiv\ 1\ (mod\ 4)$, segue que $(p-1)/2$ é par e, portanto

$$x = \prod_{j=1}^{(p-1)/2} j = \left(\frac{(p-1)}{2}\right)!$$

é uma solução de $x^2 \equiv\ -1\ (mod\ p)$.

Suponhamos, agora, que a congruência $x^2 \equiv\ -1\ (mod\ p)$ tenha solução e que $p > 2$.

Elevando ambos os membros à potência $(p-1)/2$, obtemos

$$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \ (mod\ p).$$

Como $(x^2)^{(p-1)/2} \equiv x^{(p-1)} \ (mod\ p)$, pelo **Teorema 1.1.6.16** (observe que $p \not| x$ pois $x^2 \equiv -1 \ (mod\ p)$), temos que

$$(-1)^{(p-1)/2} \equiv 1 \ (mod\ p).$$

Logo $(p-1)/2$ é par, ou seja, $p \equiv 1 \ (mod\ 4)$.

■

1.2 Um pouco de Números Complexos

Definição 1.2.1 Um número complexo é um número da forma $x + yi$, com x, y números reais e $i = \sqrt{-1}$.

Fixando um sistema de coordenadas no plano, o complexo $z = x + yi$ é representado pelo ponto $P(x, y)$. O ponto P é chamado de imagem do complexo z. Como a correspondência entre os complexos e suas imagens é um-a-um, frequentemente identificaremos os complexos e suas imagens escrevendo $(x, y) = x + yi$. O plano na qual representamos os complexos é chamado de plano de Argand-Gauss[2].

Os números representados no eixo x são da forma $(x, 0) = x + 0i = x$, isto é, são números reais. Por esse motivo, o eixo dos x é chamado eixo real. Os números representados no eixo y são da forma $(0, y) = 0 + yi = yi$. Esses complexos são chamados de números imaginários puros.

As coordenadas x, y do complexo $z = x + yi$ são chamadas respectivamente de parte real e parte imaginária de z. Escreve-se $Re(z) = x$ e $Im(z) = y$.

[2]Argand J. R. (1768-1822) matemático francês.

Por definição, os complexos $z = x + yi$ e $z' = x' + y'i$ são iguais se, e somente se, $x = x'$ e $y = y'$. Em particular, tem-se $x + yi = 0$ se, e somente se, $x = y = 0$. O conjugado do complexo $z = x + yi$ é o complexo $\bar{z} = x - yi$. É fácil ver que complexos conjugados têm imagens simétricas em relação aos eixo real. Note que o produto

$$z.\bar{z} = (x + yi)(x - yi) = x^2 - y^2 i^2 = x^2 + y^2$$

é um número real.

Definição 1.2.2. Para dividir números complexos, multiplicamos dividendo e divisor pelo conjugado do divisor, o que transforma o problema em uma divisão por um número real.

Exemplo 1.2.3. Realize a divisão em $\mathbb{C}$ de $2 + 3i$ por $4 - i$.
Conforme as instruções da **Definição 1.2.2.**, temos

$$\frac{2+3i}{4-i} = \frac{(2+3i)}{(4-i)}\frac{(4+i)}{(4+i)} = \frac{8+2i+12i+3i^2}{(16-i^2)} = \frac{5+14i}{17} = \frac{5}{17} + \frac{14}{17}i$$

As potências de i apresentam um comportamento interessante. Observe abaixo o cálculo das sete primeiras potências:

$$i^0 = 1, \quad i^1 = i; \quad i^2 = -1, \quad i^3 = i^2.i = -i, \quad i^4 = i^2.i^2 = (-1)(-1) = 1$$

$$i^5 = i^4.i = 1.i = i; \quad i^6 = i^4.i^2 = 1.(-1) = -1; \quad i^7 = i^4.i^3 = 1.(-i) = -i$$

Estas potências se repetem em ciclos de 4. Com efeito, $i^{n+4} = i^n.i^4 = i^n.1 = i^n$. Isso nos permite estabelecer uma regra para o cálculo de potências de i. Para calcular i^n, divida n por 4; se r é o resto dessa divisão, temos $i^n = i^r$. Com efeito, se q é o quociente da divisão, $i^n = i^{4q+r} = i^{4q}.i^r = (i^4)^q.i^r = (1)^q.i^r = i^r$.

Teorema 1.2.4. Se z e w são complexos, então:

i) $\overline{z + w} = \overline{z} + \overline{w}$.

ii) $\overline{z - w} = \overline{z} - \overline{w}$.

iii) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

iv) Se $w \neq 0$, $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.

v) Se z é real, então $z = \overline{z}$.

vi) $\overline{\overline{z}} = z$.

vii) Se n é um inteiro positivo, então $\overline{z}^n = \overline{z^n}$.

DEMONSTRAÇÃO: Consulte LIMA [2006].

Definição 1.2.5. (A Forma Trigonométrica) Suponhamos fixado um sistema de coordenadas no plano.

Vamos agora representar cada complexo $z = x + yi$ não mais pelo ponto $P(x, y)$, mas sim pelo vetor $\vec{OP} = (x, y)$.

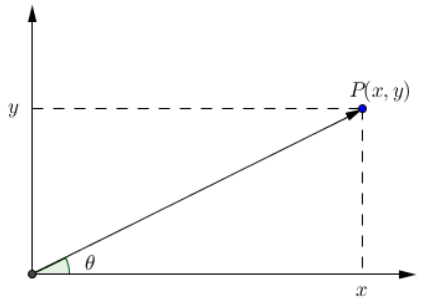


Figura 1.1: Outra maneira de representar um número complexo z.

O módulo de um complexo $z = x + yi$ é definido como sendo o módulo do vetor que o representa, ou seja, é o valor r da distância de sua imagem P à origem. Portanto,

$$|z| = r = \sqrt{x^2 + y^2}.$$

Um *argumento* de um número complexo $z \neq 0$, $z = x + yi$, é, por definição, qualquer dos ângulos $\theta = arg\ z$ que o vetor $\vec{OP}$ forma com o semi-eixo positivo dos x.

É claro que todo complexo não-nulo tem uma infinidade de argumentos, dois quaisquer deles diferindo entre si por um múltiplo de 2π. O argumento que pertence ao intervalo $(-\pi, \pi]$ é chamado de argumento principal e é representado por $Arg\ z$.

Se θ é um argumento de $z = x+yi$ então $x = rcos(\theta)$ e $y = rsen(\theta)$, o que permite escrever $z = x + yi = rcos(\theta) + irsen(\theta) = r(cos(\theta) + isen(\theta))$, ou que é a chamada *forma trigonométrica* ou *polar* do complexo z. (Os números r e θ são as *coordenadas polares* do ponto $P(x, y)$ do plano.)

Exemplo 1.2.6. Para o complexo $z = 2 + 2i$, temos

$$|z| = r = \sqrt{2^2 + 2^2} = \sqrt{8} = 2\sqrt{2}.$$

Além disso,

$$cos(\theta) = \frac{x}{r} = \frac{2}{2\sqrt{2}} = \frac{\sqrt{2}}{2} \quad \text{e} \quad sen(\theta) = \frac{y}{r} = \frac{2}{2\sqrt{2}} = \frac{\sqrt{2}}{2}.$$

Logo, um dos valores possíveis para θ é $\frac{\pi}{4}$ e a forma trigonométrica de z é

$$z = 2\sqrt{2}\left(cos\frac{\pi}{4} + isen\frac{\pi}{4}\right).$$

Agora, nosso objetivo é provar o seguinte resultado:

Proposição 1.2.7. Dado um complexo $z = x + yi$, com $z \neq 0$, cujo $Arg\ z = \theta$, então:

i) $Arg\ (zi) = \theta + \frac{\pi}{2}$;

ii) $Arg\ (-z) = \theta + \pi$;

iii) $Arg\ (-zi) = \theta + \frac{3\pi}{2}$.

DEMONSTRAÇÃO:

i) Note que $zi = (x + yi)i = xi + yi^2 = -y + xi$. Se chamarmos $Arg\ (zi) = \alpha$, temos que

$$cos(\alpha) = \frac{-y}{\sqrt{y^2 + x^2}} = -\frac{y}{\sqrt{y^2 + x^2}} = -sen(\theta).$$

Agora, note que

$$cos\left(\theta+\frac{\pi}{2}\right)=cos(\theta)cos\left(\frac{\pi}{2}\right)-sen(\theta)sen\left(\frac{\pi}{2}\right)=-sen(\theta)$$

Concluímos assim que $cos\left(\theta+\frac{\pi}{2}\right)=cos(\alpha)$, ou seja, um dos valores possíveis para α é $\theta+\frac{\pi}{2}$.

ii) Note que $-z=-x-yi$. Se chamarmos $Arg\ (-z)=\delta$, temos que

$$cos(\delta)=\frac{-x}{\sqrt{x^2+y^2}}=-\frac{x}{\sqrt{x^2+y^2}}=-cos(\theta).$$

Agora, note que

$$cos(\theta+\pi)=cos(\theta)cos(\pi)-sen(\theta)sen(\pi)=-cos(\theta)$$

Concluímos assim que $cos(\theta+\pi)=cos(\delta)$, ou seja, um dos valores possíveis para δ é $\theta+\pi$.

iii) Note que $-zi=-(x+yi)i=-xi-yi^2=y-xi$. Se chamarmos $Arg\ (-zi)=\gamma$, temos que

$$cos(\gamma)=\frac{y}{\sqrt{y^2+x^2}}=sen(\theta).$$

Agora, note que

$$cos\left(\theta+\frac{3\pi}{2}\right)=cos(\theta)cos\left(\frac{3\pi}{2}\right)-sen(\theta)sen\left(\frac{3\pi}{2}\right)=sen(\theta)$$

Concluímos assim que $cos\left(\theta+\frac{3\pi}{2}\right)=cos(\gamma)$, ou seja, um dos valores possíveis para γ é $\theta+\frac{3\pi}{2}$.

■

Com este resultado encerramos este capítulo e agora estamos em condições de abordar o assunto principal deste trabalho.

Capítulo 2

Inteiros Gaussianos

2.1 Definição

Chama-se **Inteiro Gaussiano** a todo número $\alpha = a + bi$, onde a e b são números inteiros e $i^2 = -1$. Denotamos por $\mathbb{Z}[i]$ ao conjunto numérico formado por todos os Inteiros Gaussianos.
Em $\mathbb{Z}[i]$ podemos definir as seguintes operações:

$$\begin{aligned} + \quad : \quad & \mathbb{Z}[i] \times \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i] \\ & (a+bi, c+di) \longmapsto (a+bi)+(c+di) := (a+c)+(b+d)i \end{aligned}$$

$$\begin{aligned} \cdot \quad : \quad & \mathbb{Z}[i] \times \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i] \\ & (a+bi, c+di) \longmapsto (a+bi)(c+di) := (ac-bd)+(ad+bc)i \end{aligned}$$

Observação 2.1.1. Dado o inteiro gaussiano $\alpha = a + bi$, chamaremos **a** de parte real e **b** de parte imaginária de α.

Exemplo 2.1.2. Considere os seguintes números complexos $\alpha_1 = 4$, $\alpha_2 = -3i$, $\alpha_3 = 1 + 5i$, $\alpha_4 = \sqrt{3} + i$, $\alpha_5 = \dfrac{3}{2} + \dfrac{9}{4}i$ e $\alpha_6 = 7 + \pi i$. É claro que $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}[i]$ e $\alpha_4, \alpha_5, \alpha_6 \notin \mathbb{Z}[i]$, pois os números $\sqrt{3}, \dfrac{3}{2}, \dfrac{9}{4}, \pi$ não são inteiros.
Com este exemplo observamos que $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$.

2.2 A Função Norma

Definição 2.2.1. A função $\mathcal{N}$ definida por

$$\begin{aligned} \mathcal{N} \ : \ \mathbb{Z}[i] \ &\longrightarrow \ \mathbb{Z}_+ \\ a+bi &\longmapsto a^2+b^2 \end{aligned}$$

é chamada de **Função Norma** em $\mathbb{Z}[i]$. A proposição seguinte encerra propriedades importantes da Função Norma, que utilizaremos no transcorrer deste texto.

Proposição 2.2.2. Seja $\mathcal{N}$ a Função Norma em $\mathbb{Z}[i]$. Então:
(i) $\mathcal{N}(\alpha) \geq 0, \ \forall \ \alpha \in \mathbb{Z}[i]$;
(ii) $\mathcal{N}(\alpha) = 0$, se, e somente se, $\alpha = 0$;
(iii) $\mathcal{N}(\alpha) = \alpha\bar{\alpha}$, para todo $\alpha \in \mathbb{Z}[i]$, onde $\bar{\alpha}$ denota o **conjugado** de α;
(iv) $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta), \ \forall \ \alpha, \beta \in \mathbb{Z}[i]$; isto é, a Função Norma preserva a multiplicação.
DEMONSTRAÇÃO:
(i) Seja $\alpha = a + bi \in \mathbb{Z}[i]$; isto é, $a, b \in \mathbb{Z}$. Basta notar que:

$$\mathcal{N}(\alpha) = \mathcal{N}(a + bi) = a^2 + b^2 \geq 0, \quad \forall \ a, b \in \mathbb{Z}.$$

(ii) ($\Rightarrow$) Seja $\alpha = a + bi \in \mathbb{Z}[i]$, e suponhamos que $\mathcal{N}(\alpha) = 0$. Então:

$$\mathcal{N}(\alpha) = \mathcal{N}(a + bi) = a^2 + b^2 = 0.$$

Como $a^2 \geq 0$ e $b^2 \geq 0$, segue de $a^2 + b^2 = 0$ que $a = b = 0$; e, portanto, $\alpha = 0 + 0i = 0$.
($\Leftarrow$) Se $\alpha = 0$, então $\mathcal{N}(\alpha) = \mathcal{N}(0 + 0i) = 0^2 + 0^2 = 0$.
(iii) Basta notar que:

$$\mathcal{N}(\alpha) = \mathcal{N}(a + bi) = a^2 + b^2 = (a + bi)(a - bi) = \alpha\bar{\alpha}, \ \forall \ \alpha \in \mathbb{Z}[i].$$

(iv) Dados $\alpha, \ \beta \in \mathbb{Z}[i]$, temos, em vista do item anterior, e utilizando propriedades dos conjugados de complexos, que:

$$\mathcal{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \mathcal{N}(\alpha)\mathcal{N}(\beta).$$

■

Exemplo 2.2.3. Calcule a norma dos inteiros gaussianos $\alpha = 3 + 4i$ e $\beta = 11 + i$.
$\mathcal{N}(\alpha) = 3^2 + 4^2 = 9 + 16 = 25$ e $\mathcal{N}(\beta) = 11^2 + 1^2 = 121 + 1 = 122$.

Observamos com este exemplo que através da função Norma, podemos comparar dois inteiros gaussianos.

Antes de entramos no assunto de divisibilidade no conjunto dos inteiros gaussianos, vamos encontrar os elementos inversíveis deste conjunto. Para isto, observe a proposição abaixo.

Proposição 2.2.4. Seja $\alpha \in \mathbb{Z}[i]$. As seguintes afirmações são equivalentes:
(i) α é inversível em $\mathbb{Z}[i]$;
(ii) $\mathcal{N}(\alpha) = 1$;
(iii) $\alpha \in \{-1,\ 1,\ -i,\ i\}$.
DEMONSTRAÇÃO:
(i)⇒(ii) Seja α um elemento inversível de $\mathbb{Z}[i]$. Então, existe um único $\beta \in \mathbb{Z}[i]$ tal que $\alpha\beta = 1$. Segue, do item (iv) da Proposição 3.2 que:

$$\mathcal{N}(\alpha)\mathcal{N}(\beta) = \mathcal{N}(\alpha\beta) = \mathcal{N}(1) = 1.$$

Mas $\mathcal{N}(\alpha) \in \mathbb{Z}_+$, pela definição de $\mathcal{N}$. Assim, pela igualdade acima, $\mathcal{N}(\alpha)$ é um divisor inteiro positivo de 1. Logo, $\mathcal{N}(\alpha) = 1$.
(ii)⇒(iii) Seja $\alpha = x + yi \in \mathbb{Z}[i]$, e suponhamos que $\mathcal{N}(\alpha) = \mathcal{N}(x + yi) = x^2 + y^2 = 1$. Como $x, y \in \mathbb{Z}$, a equação $x^2 + y^2 = 1$ admite exatamente quatro soluções; a saber, $(\pm 1, 0)$ e $(0, \pm 1)$. Portanto, se α é inversível em $\mathbb{Z}[i]$, então $\alpha \in \{-1,\ 1,\ -i,\ i\}$.
(iii)⇒(i) Trivial.

Observação 2.2.5. Quando falarmos neste texto do conjunto das unidades (ou inversíveis) em $\mathbb{Z}[i]$, estaremos nos referindo ao conjunto $\{1,\ -1,\ i,\ -i\}$.

Definição 2.2.6. Dados α e β inteiros gaussianos. Diremos que α e β são associa-

dos ou múltiplos unitários um do outro se $\alpha = u.\beta$, com $u \in \{-1,\ 1,\ -i,\ i\}$.

Exemplo 2.2.7. Note que $\alpha = 3 + i$ e $\beta = -1 + 3i$ são associados, pois $\alpha = i.\beta$.

2.3 Divisibilidade

Nesta seção, temos por objetivo estabelecer quando um inteiro de Gauss é divisível por outro. Além disso, descreveremos uma maneira, através de exemplos, de como se obter os divisores de um inteiro de Gauss.

Definição 2.3.1. Dizemos que para $\alpha,\ \beta \in \mathbb{Z}[i]$, α divide β e denotamos por $\alpha|\beta$ se existir $\gamma \in \mathbb{Z}[i]$ tal que $\beta = \alpha.\gamma$.

Exemplo 2.3.2. $(1 + 2i)|5$, pois $5 = (1 - 2i)(1 + 2i)$.

Exemplo 2.3.3. $(4 + 5i)|(14 - 3i)$, pois $14 - 3i = (4 + 5i)(1 - 2i)$

Proposição 2.3.4. Sejam α e β inteiros gaussianos tais que $\alpha|\beta$, então $\mathcal{N}(\alpha)|\mathcal{N}(\beta)$ em $\mathbb{Z}$.

DEMONSTRAÇÃO: Se $\alpha|\beta$, então existe um inteiro gaussiano γ tal que $\beta = \gamma.\alpha$. Aplicando a função norma em ambas as parcelas da igualdade, obtemos que: $\mathcal{N}(\beta) = \mathcal{N}(\gamma.\alpha)$ e como a função norma é multiplicativa, segue que $\mathcal{N}(\beta) = \mathcal{N}(\gamma).\mathcal{N}(\alpha)$ e, portanto $\mathcal{N}(\alpha)|\mathcal{N}(\beta)$.

■

Exemplo 2.3.5. Encontre todos os divisores de 11 em $\mathbb{Z}[i]$.

Queremos encontrar os inteiros gaussianos $\alpha = a + bi$, tal que $\alpha|11$. Se $\alpha|11$ então existirá um inteiro gaussiano γ tal que $11 = \alpha\gamma$. Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(11) = \mathcal{N}(\alpha\gamma) \Leftrightarrow 121 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar o comportamento apenas de α e sabendo que a Norma de um inteiro gaussiano é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = a^2 + b^2 = 1 \Leftrightarrow \alpha = \pm 1\ ou\ \alpha = \pm i$

- $\mathcal{N}(\alpha) = 11 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 121 \Leftrightarrow \alpha = \pm 11 \; ou \; \alpha = \pm 11i$.

Logo os divisores de 11 em $\mathbb{Z}[i]$ são:

$$\{1, 11\}$$

e suas multiplicações pelas unidades.

Exemplo 2.3.6. Encontre todos os divisores de $6i$ em $\mathbb{Z}[i]$.
Queremos encontrar os inteiros gaussianos $\alpha = a + bi$, tal que $\alpha | 6i$. Se $\alpha | 6i$ então existirá um inteiro gaussiano γ tal que $6i = \alpha\gamma$. Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(6i) = \mathcal{N}(\alpha\gamma) \Leftrightarrow 36 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar o comportamento apenas de α e sabendo que a Norma de um inteiro gaussiano é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma, das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = a^2 + b^2 = 1 \Leftrightarrow \alpha = \pm 1 \; ou \; \alpha = \pm i$
- $\mathcal{N}(\alpha) = 2 \Leftrightarrow \alpha = \pm 1 \pm i$;
- $\mathcal{N}(\alpha) = 3 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 4 \Leftrightarrow \alpha = \pm 2 \; ou \; \alpha = \pm 2i$;
- $\mathcal{N}(\alpha) = 6 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 9 \Leftrightarrow \alpha = \pm 3 \; ou \; \alpha = \pm 3i$;
- $\mathcal{N}(\alpha) = 12 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 18 \Rightarrow \alpha = \pm 3 \pm 3i$;
- $\mathcal{N}(\alpha) = 36 \Leftrightarrow \alpha = \pm 6 \; ou \; \alpha = \pm 6i$.

Logo os divisores de $6i$ em $\mathbb{Z}[i]$ são:

$$\{1, 1 + i, 2, 3, 3 + 3i, 6\}$$

e suas multiplicações pelas unidades.

Exemplo 2.3.7. Encontre todos os divisores de $3+i$ em $\mathbb{Z}[i]$.
Queremos encontrar os inteiros gaussianos $\alpha = a+bi$, tal que $\alpha|3+i$. Se $\alpha|3+i$ então existirá um inteiro gaussiano γ tal que $3+i = \alpha\gamma$. Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(3+i) = \mathcal{N}(\alpha\gamma) \Leftrightarrow 10 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar o comportamento apenas de α e sabendo que a Norma de um inteiro gaussiano é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma, das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = a^2 + b^2 = 1 \Leftrightarrow \alpha = \pm 1 \;\; ou \;\; \alpha = \pm i$
- $\mathcal{N}(\alpha) = 2 \Leftrightarrow \alpha = \pm 1 \pm i$
- $\mathcal{N}(\alpha) = 5 \Leftrightarrow \alpha = \pm 1 \pm 2i \;\; ou \;\; \alpha = \pm 2 \pm i$
- $\mathcal{N}(\alpha) = 10 \Leftrightarrow \alpha = \pm 3 \pm i \;\; ou \;\; \alpha = \pm 1 \pm 3i.$

Logo os divisores de $3+i$ em $\mathbb{Z}[i]$ são:

$$\{1, 1+i, 1+2i, 1-2i, 3+i, 3-i\}$$

e suas multiplicações pelas unidades.

Observação 2.3.8. Com esta seção e estes exemplos, observamos que dado um inteiro gaussiano não nulo α, tal que $\mathcal{N}(\alpha) > 1$, para encontrar todos os seus divisores em $\mathbb{Z}[i]$ devemos calcular a Norma de α e construir o conjunto D, que será formado por todos os divisores inteiros de $\mathcal{N}(\alpha)$. Deste conjunto, aqueles divisores que forem escritos como soma de quadrados serão as normas dos divisores de α em $\mathbb{Z}[i]$.

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

Nesta seção estabeleceremos um método de divisão entre dois inteiros de Gauss.

Teorema 2.4.1. Dados $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$, existem $q, r \in \mathbb{Z}[i]$ tais que $\alpha = \beta.q + r$ com $r = 0$ ou $\mathcal{N}(r) < \mathcal{N}(\beta)$.
DEMONSTRAÇÃO: Inicialmente vamos calcular a divisão conforme aprendemos nos números complexos, obtendo

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

com x,y racionais.

Se x e y são inteiros, então $q = x + yi$ e $r = 0$. Caso x e y não sejam números inteiros, então devemos procurar m,n inteiros mais próximos de x e y, ou seja, m e n tais que $|x - m| \leq \frac{1}{2}$ e $|y - n| \leq \frac{1}{2}$. Tomando $q = m + ni$ e $r = \alpha - \beta q$, obtemos

$$\mathcal{N}\left(\frac{\alpha}{\beta} - q\right) = \mathcal{N}(x + yi - (m - ni)) = \mathcal{N}((x - m) + (y - n)i) = (x - m)^2 + (y - n)^2 \leq$$
$$\frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

Se $\mathcal{N}\left(\frac{\alpha}{\beta} - q\right) < 1$, então $\mathcal{N}\left(\frac{\alpha}{\beta} - q\right)\mathcal{N}(\beta) < 1\mathcal{N}(\beta) \Leftrightarrow \mathcal{N}\left((\frac{\alpha}{\beta} - q)\beta\right) < \mathcal{N}(\beta) \Leftrightarrow \mathcal{N}(\underbrace{\alpha - q\beta}_{r}) < \mathcal{N}(\beta)$, temos portanto

$$\mathcal{N}(r) < \mathcal{N}(\beta).$$

■

Exemplo 2.4.2. Encontre o quociente e o resto da divisão de $\alpha = 15 + 5i$ por $\beta = 1 + 2i$ em $\mathbb{Z}[i]$.

O quociente e o resto são encontrados seguindo a mesma sequência de ideias usadas na demonstração do Teorema 2.4.1.

O primeiro passo é calcular a divisão conforme é calculada nos números complexos.

$$\frac{\alpha}{\beta} = \frac{15 + 5i}{1 + 2i} = \frac{15 + 5i}{1 + 2i} \cdot \frac{(1 - 2i)}{(1 - 2i)} = \frac{15 - 30i + 5i - 10i^2}{1 - 4i^2} = \frac{15 - 25i + 10}{1 + 4} = \frac{25 - 25i}{5} = \frac{25}{5} - \frac{25}{5}i.$$

Como $\frac{25}{5} = 5$ e $-\frac{25}{5} = -5$ são inteiros, temos $q = 5 - 5i$ e $r = 0$.

Exemplo 2.4.3. Encontre o quociente e o resto da divisão de $\alpha = 26 + 72i$ por $\beta = 3 + 4i$ em $\mathbb{Z}[i]$.

O quociente e o resto são encontrados seguinte a mesma sequência de ideias usadas na demonstração do Teorema 2.4.1.

O primeiro passo é calcular a divisão conforme é calculada nos números complexos.

$$\frac{\alpha}{\beta} = \frac{26 + 72i}{3 + 4i} = \frac{26 + 72i}{3 + 4i} \cdot \frac{(3 - 4i)}{(3 - 4i)} =$$

$$= \frac{78 - 104i + 216i - 288i^2}{9 - 16i^2} = \frac{78 + 112i + 288}{9 + 16} = \frac{366 + 112i}{25} = \frac{366}{25} + \frac{112}{25}i.$$

Observe que $\frac{366}{25}$ e $\frac{112}{25}$ não são números inteiros, logo precisamos encontrar **m** e **n** tais que $\left|\frac{366}{25} - m\right| \leq \frac{1}{2}$ e $\left|\frac{112}{25} - n\right| \leq \frac{1}{2}$. Veja:

$$\left|\frac{366}{25} - m\right| \leq \frac{1}{2} \Leftrightarrow -\frac{1}{2} \leq \frac{366}{25} - m \leq \frac{1}{2} \Leftrightarrow \frac{1}{2} - \frac{366}{25} \leq -m \leq \frac{1}{2} - \frac{366}{25} \Leftrightarrow$$

$$\Leftrightarrow -\frac{757}{50} \leq -m \leq -\frac{707}{50} \Leftrightarrow \frac{707}{50} \leq m \leq \frac{757}{50} \Leftrightarrow 14,14 \leq m \leq 15,14.$$

$$e$$

$$\left|\frac{112}{25} - n\right| \leq \frac{1}{2} \Leftrightarrow -\frac{1}{2} \leq \frac{112}{25} - n \leq \frac{1}{2} \Leftrightarrow \frac{1}{2} - \frac{112}{25} \leq -n \leq \frac{1}{2} - \frac{112}{25} \Leftrightarrow$$

$$\Leftrightarrow -\frac{249}{50} \leq -n \leq -\frac{199}{50} \Leftrightarrow \frac{199}{50} \leq n \leq \frac{249}{50} \Leftrightarrow 3,98 \leq n \leq 4,98.$$

Portanto $m = 15$ e $n = 4$.

Desta forma já determinamos q, pois $q = m + ni$, ou seja $q = 15 + 4i$. Para determinar r, basta lembrarmos que $r = \alpha - \beta.q$, ou seja $r = (26 + 72i) - (3 + 4i)(15 + 4i) = 26 + 72i - (45 + 12i + 60i + 16i^2) = 26 + 72i - (29 + 72i) = 26 - 29 = -3$

Concluímos assim que $q = 15 + 4i$ e $r = -3$.

Exemplo 2.4.4. Encontre o quociente e o resto da divisão de $\alpha = 4 + 5i$ por $\beta = 1 + i$ em $\mathbb{Z}[i]$.

O quociente e o resto são encontrados seguindo a mesma sequência de ideias usada na demonstração do Teorema 2.4.1. Inicialmente, calculamos $\frac{\alpha}{\beta}$:

$$\frac{\alpha}{\beta} = \frac{4 + 5i}{1 + i} = \frac{4 + 5i}{1 + i} \cdot \frac{(1 - i)}{(1 - i)} = \frac{(4 + 5i)(1 - i)}{2} = \frac{9 + i}{2} = \frac{9}{2} + \frac{1}{2}i;$$

isto é, aqui, $x = \frac{9}{2}$ e $y = \frac{1}{2}$.

O próximo passo consiste em encontrarmos $e, f \in \mathbb{Z}$, tais que:

$$\left|\frac{9}{2} - e\right| \leq \frac{1}{2} \;\; e \;\; \left|\frac{1}{2} - f\right| \leq \frac{1}{2}.$$

Para isto, observe que, se $e, f \in \mathbb{Z}$, então:

$$\left|\frac{9}{2} - e\right| \leq \frac{1}{2} \Leftrightarrow 4 \leq e \leq 5 \Leftrightarrow \ e \in \{4, 5\}; \quad \text{e}$$

$$\left|\frac{1}{2} - f\right| \leq \frac{1}{2} \Leftrightarrow \ 0 \leq e \leq 1 \Leftrightarrow \ f \in \{0, 1\}.$$

Assim, existem quatro possíveis quocientes $t = e + fi \in \mathbb{Z}[i]$ para essa divisão, a saber, $t_1 = 4$, $t_2 = 5$, $t_3 = 4+i$ e $t_4 = 5+i$. E é claro que a cada quociente t_i, $i = \{1, 2, 3, 4\}$ está associado o seu respectivo resto $r_i \in \mathbb{Z}[i]$, obtido através de $r = \alpha - \beta t$; a saber, $r_1 = i$, $r_2 = -1$, $r_3 = 1$ e $r_4 = -i$.

Logo, dados $\alpha = 4 + 5i$ e $\beta = 1 + i$ em $\mathbb{Z}[i]$, existem quatro possíveis pares ordenados $(t_i, r_i) \in \mathbb{Z}[i]$ tais que $\alpha = \beta t_i + r_i$, com $\mathcal{N}(r_i) < \mathcal{N}(\beta)$:

$$(t_1, r_1) = (4, i), \quad (t_2, r_2) = (4, -1), \quad (t_3, r_3) = (4 + i, 1) \quad \text{e} \quad (t_4, r_4) = (5 + i, -i).$$

Exemplo 2.4.5. Encontre o quociente e o resto da divisão de $\alpha = 31 + 7i$ por $\beta = 2 + 5i$ em $\mathbb{Z}[i]$.

Neste exemplo, usaremos uma maneira mais prática de se encontrar o quociente q e o resto r. Inicialmente faremos a divisão usual dos números complexos.

$$\frac{\alpha}{\beta} = \frac{31 + 7i}{2 + 5i} = \frac{31 + 7i}{2 + 5i} \cdot \frac{(2 - 5i)}{(2 - 5i)} = \frac{62 - 155i + 14i - 35i^2}{4 - 25i^2} = \frac{62 + 35 - 141}{4 + 25} = \frac{97 - 141i}{29} = \frac{97}{29} - \frac{141}{29}i$$

Observe que $\dfrac{97}{29}$ e $-\dfrac{141}{29}$ não são inteiros, logo precisamos encontrar os inteiros m e n mais próximos destas racionais.

Para isto, ao invés de usarmos o módulo conforme os exemplos acima, realizaremos a divisão dos racionais e tomaremos o inteiro mais próximo, isto é:

$$\frac{97}{29} \approx 3,34 \ \ e \ \ -\frac{141}{29} \approx -4,86,$$

portanto $m = 3$, $n = -5$ e $q = m + ni = 3 - 5i$.

Como queremos $\alpha = \beta.q + r$, logo $r = \alpha - \beta.q$ e, portanto $r = (31+7i) - (2+5i)(3-5i) = 2i$

Concluímos assim que $(31 + 7i) = (2 + 5i)(3 - 5i) + 2i$, ou seja, $q = 3 - 5i$ e $q = -2i$.

Observação 2.4.6. No exemplo anterior, a aproximação é justificada, pois realizar o cálculo $\left|\frac{97}{29} - m\right| \leq \frac{1}{2}$ e $\left|-\frac{141}{29} - n\right| \leq \frac{1}{2}$, nada mais é que encontrar o inteiro m mais próximo do racional $\frac{97}{29}$ e o inteiro n mais próximo do racional $-\frac{141}{29}$.

2.5 O Algoritmo da Divisão Euclidiana em $\mathbb{Z}[i]$

Nesta seção introduziremos a definição de máximo divisor comum em $\mathbb{Z}[i]$ e estenderemos a idéia da divisão euclidiana. Com estas ferramentas, mostraremos que dados os inteiros de Gauss α, β e γ, tais que $\text{mdc}(\alpha, \beta) = \gamma$, é possível escrever γ como combinação linear de α e β.

Definição 2.5.1. Sejam α, β e γ inteiros gaussianos não nulos. Diremos que γ será o máximo divisor comum de α e β quando:

i) $\gamma|\alpha$ e $\gamma|\beta$;

ii) Se existe $c \in Z[i]$ tal que $c|\alpha$ e $c|\beta$ então $\mathcal{N}(c) \leq \mathcal{N}(\gamma)$.

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

Lema 2.5.2. Sejam α, β e γ inteiros gaussianos. Então $\text{mdc}(\alpha, 0) = \alpha$, e $\text{mdc}(\alpha, \beta)$=$\text{mdc}(\beta, \alpha)$=$\text{mdc}($ $\gamma\beta, \beta)$.

DEMONSTRAÇÃO: Sejam d, α, β, γ inteiros gaussianos. Os fatos que $\text{mdc}(\alpha, 0) = \alpha$ e $\text{mdc}(\alpha, \beta)$=$\text{mdc}(\beta, \alpha)$ são triviais.

Considere agora que d =$\text{mdc}(\beta, \alpha - \gamma\beta)$. Logo $d|\beta$ (implicando que $d|\gamma\beta$) e $d|\alpha - \gamma\beta$. Desta forma, $d|\alpha$, pois $\alpha = \gamma\beta + (\alpha - \gamma\beta)$.

■

Definição 2.5.3. Sejam α e β inteiros gaussianos não nulos. Se estes possuem como fatores comum as unidades $\{+1, -1, +i, -i\}$, então dizemos que α e β são relativamente primos.

Teorema 2.5.4. (Algoritmo Euclidiano). Sejam α e β inteiros gaussianos não nulos. Se aplicarmos o Teorema 2.4.1, iniciando pela divisão de α por β, obtemos um quociente γ_1 e um resto r_1, com $\mathcal{N}(r_1) < \mathcal{N}(\gamma_1)$. Com este β e o r_1 repetimos o processo, obtendo um novo quociente γ_2 e um resto r_2 com $\mathcal{N}(r_2) < \mathcal{N}(\gamma_2)$, gerando a sequência abaixo:

$$\begin{aligned}
\alpha &= \beta\gamma_1 + r_1,\ \mathcal{N}(r_1) < \mathcal{N}(\gamma_1) \\
\beta &= r_1\gamma_2 + r_2,\ \mathcal{N}(r_2) < \mathcal{N}(\gamma_2) \\
\mathrm{r}_1 &= r_2\gamma_3 + r_3,\ \mathcal{N}(r_3) < \mathcal{N}(\gamma_3) \\
&\vdots
\end{aligned}$$

O último resto não nulo é divisível por todos todos os divisores comuns de α e β, e é em si um divisor comum, por isso é o Maior Divisor Comum de α e β.

DEMONSTRAÇÃO: A demonstração é idêntica à usada nos inteiros. Entretanto, vamos reescrevê-la.

Pela divisão euclidiana, temos que:

$$\alpha = \beta.\gamma_1 + r_1,\ \text{com}\ \mathcal{N}(r_1) < \mathcal{N}(\gamma_1)$$

Da igualdade acima e pelo Lema 2.5.2, temos que:

$$mdc(\alpha, \beta) = mdc(\alpha - \beta.\gamma_1, \beta) = mdc(r_1, \beta) = mdc(\beta, r_1)$$

Desta forma, podemos ter duas situações:

- $\mathcal{N}(r_1) = 0$: neste caso, temos que mdc(α, β)=mdc$(\beta, r_1) = \beta$;
- $\mathcal{N}(r_1) \neq 0$: neste caso, efetuamos a divisão euclidiana de β por r_1, obtendo:

$$\beta = r_1\gamma_2 + r_2,\ com\ \mathcal{N}(r_2) < \mathcal{N}(r_1)$$

Segue que:

$$mdc(\alpha, \beta) = mdc(\beta, r_1) = mdc(r_1, r_2)$$

Novamente, duas situações podem ocorrer:

- $\mathcal{N}(r_2) = 0$: neste caso, temos que mdc(α, β)=mdc$(r_1, 0) = r_1$;
- $\mathcal{N}(r_2) \neq 0$: neste caso, efetuamos a divisão euclidiana de r_1 por r_2, obtendo:

$$r_1 = r_2\gamma_3 + r_3, \ com \ \mathcal{N}(r_3) < \mathcal{N}(r_2)$$

Segue que:

$$mdc(\alpha, \beta) = mdc(\beta, r_1) = mdc(r_1, r_2) = mdc(r_2, r_3)$$

e assim sucessivamente.

Definindo $r_0 = \beta$, existe um valor n natural que $r_{n+1} = 0$ e $r_n \neq 0$. De fato, se tivéssemos para todo $n \neq 0$, teríamos uma sequência infinita

$$r_0 > r_1 > r_2 > r_3 > ... > 0$$

Segue que:

$$mdc(\alpha, \beta) = mdc(\beta, r_1) = mdc(r_1, r_2) = ... = mdc(r_n, r_{n+1}) = mdc(r_n, 0) = r_n$$

Portanto, o último resto não nulo r_n deste processo, fornece o valor de mdc(α, β).

■

Calculamos o mdc(α, β), com α e β inteiros gaussianos através do dispositivo prático que decorre do processo acima.

Quociente	γ_1	γ_2	γ_3	...	γ_{n-2}	γ_{n-1}	γ_n
α	β	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = mdc(\alpha, \beta)$
Resto	r_1	r_2	r_3	...	r_{n-1}	r_n	0

Exemplo 2.5.5. Utilizando o Algoritmo de Euclides, encontre o mdc$(32 + 9i, 4 + 11i)$.

Note que:

$$32 + 9i = (4 + 11i)(2 - 2i) + 2 - 5i$$
$$4 + 11i = (2 - 5i)(-2 + i) + 3 - i$$
$$2 - 5i = (3 - i)(1 - i) - i$$
$$3 - i = (-i)(1 + 3i) + 0.$$

Ou seguindo o esquema acima:

Quociente	$2 - 2i$	$-2 + i$	$1 - i$	$1 + 3i$
$32 + 9i$	$4 + 11i$	$2 - 5i$	$3 - i$	$-i$
Resto	$2 - 5i$	$3 - i$	$-i$	0

Concluímos assim que mdc$(32+9i, 4+11i) = -i$, ou seja $32+9i$ e $4+11i$ são relativamente primos.

Exemplo 2.5.6. Neste exemplo mostraremos que o máximo divisor comum em $\mathbb{Z}[i]$ não é único. Sejam $\alpha = 11 + 3i$ e $\beta = 1 + 8i$. Temos:

$$11 + 3i = (1 + 8i)(1 - i) + 2 - 4i$$
$$1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i$$
$$2 - 4i = (-1 + 2i)(-2) + 0.$$

Ou seja, o máximo divisor comum de α e β é $-1 + 2i$.
Entretanto, podemos fazer da seguinte maneira:

$$11 + 3i = (1 + 8i)(1 - i) + 2 - 4i$$
$$1 + 8i = (2 - 4i)(-2 + i) + 1 - 2i$$
$$2 - 4i = (1 - 2i)(2) + 0.$$

Ou seja, máximo divisor comum de α e β é $1 - 2i$. Essas duas respostas não são inconsistentes, pois $-1 + 2i = (-1)(1 - 2i)$, ou seja, são múltiplos unitários um do outro.

Teorema 2.5.7.(Bachét- Bezout) Seja δ qualquer máximo divisor comum de dois inteiros gaussianos α e β não nulos. Então existem x e y $\in \mathbb{Z}[i]$ tais que

$$\alpha.x + \beta.y = \delta.$$

DEMONSTRAÇÃO: O caso de $\alpha = 0 = \beta$ é trivial, pois $(x = 0 = y = 0)$. Nos outros casos, considere o conjunto de todas as combinações $\mathbb{Z}[i]$-Lineares de α e β:

$$I(\alpha, \beta) \stackrel{def}{=} \{\alpha.x + \beta.y : x, y \ \in \ \mathbb{Z}[i]\}.$$

Seja $\delta = \alpha.x_0 + \beta.y_0$ o elemento com menor norma de $I(\alpha, \beta)$. Afirmamos que δ divide todos os elementos $I(\alpha, \beta)$. De fato, dado $m = \alpha.x + \beta.y \in I(\alpha, \beta)$, sejam q e r inteiros gaussianos o quociente e o resto da divisão euclidiana de m por δ, de modo que $m = \delta.q+r$ e $0 \leq \mathcal{N}(r) < \mathcal{N}(\delta)$.Temos

$$r = m-\delta.q = (\alpha.x+\beta.y)-(\alpha.x_0+\beta.y_0).q = \alpha.x-\alpha.x_0q+\beta.y-\beta.y_0q = \alpha(x-x_0q)+\beta(y-y_0q).$$

Logo $r \in I(\alpha, \beta)$. Como $\mathcal{N}(r) < \mathcal{N}(\delta)$ e $\mathcal{N}(\delta)$ é a menor norma de $I(\alpha, \beta)$, segue que $r = 0 + 0i = 0$ (pois $\mathcal{N}(\delta)$ é um número natural) e, portanto $\delta | m$, pois $m = \delta.q + r = \delta.q + 0 = \delta.q$.

■

Corolário 2.5.8. Sejam α e β dois elementos em $\mathbb{Z}[i]$ primos entre si, isto é, cujos únicos divisores comuns são unidades. Então existem x,y $\in \mathbb{Z}[i]$ tais que

$$\alpha.x + \beta.y = 1.$$

DEMONSTRAÇÃO: Sejam α e β dois elementos em $\mathbb{Z}[i]$ primos entre si, isto é, mdc$(\alpha, \beta) = m$, onde $m \in \{1, -1, i, -i\}$. Decorre imediatamente do teorema acima que existem inteiros gaussiano x e y, tal que:

$$\alpha.x + \beta.y = m.$$

Estudaremos os casos.

- Se $m = 1$ demonstrado!;
- Se $m = -1$, então $\alpha.x + \beta.y = -1 \Leftrightarrow \alpha.(-x) + \beta.(-y) = 1$;
- Se $m = i$, então $\alpha.x + \beta.y = i \Leftrightarrow \alpha.(-x.i) + \beta.(-y.i) = 1$;
- Se $m = -i$, então $\alpha.x + \beta.y = -i \Leftrightarrow \alpha.(x.i) + \beta.(y.i) = 1$.

■

Exemplo 2.5.9. Já vimos que $\alpha = 32 + 9i$ e $\beta = 4 + 11i$ são relativamente primos, pois mdc$(32 + 9i, 4 + 11i) = -i$. Agora escreveremos $-i$ como combinação de α e β. Veja: Já vimos através do **Exemplo 2.5.5** que

Quociente	$2 - 2i$	$-2 + i$	$1 - i$	$1 + 3i$
$32 + 9i$	$4 + 11i$	$2 - 5i$	$3 - i$	$-i$
Resto	$2 - 5i$	$3 - i$	$-i$	0

Agora vamos escrever $-i$ como combinação linear de $32 + 9i$ e $4 + 11i$.
Através do esquema acima, podemos escrever as seguintes equações

$$\begin{cases} 32 + 9i = (4 + 11i)(2 - 2i) + (2 - 5i) \quad (I) \\ 4 + 11i = (2 - 5i)(-2 + i) + (3 - i) \quad (II) \\ 2 - 5i = (3 - i)(1 - i) + (-i) \quad (III) \end{cases}$$

Isolando $-i$ na equação (III) e aplicando as equações (II) e (I) na equação (III) obtemos

$$2-5i-(3-i)(1-i)=-i$$

$$2-5i-((4+11i)-(2-5i)(-2+i))(1-i)=-i$$

$$2-5i-(4+11i)(1-i)+(2-5i)(-2+i)(1-i)=-i$$

$$(2-5i)-(4+11i)(1-i)+(2-5i)(-1+3i)=-i$$

$$(2-5i)(1-1+3i)-(4+11i)(1-i)=-i$$

$$(2-5i)(3i)-(4+11i)(1-i)=-i$$

$$((32+9i)-(4+11i)(2-2i))(3i)-(4+11i)(1-i)=-i$$

$$(32+9i)(3i)-(4+11i)(2-2i)(3i)-(4+11i)(1-i)=-i$$

$$(32+9i)(3i)-(4+11i)(6+6i)-(4+11i)(1-i)=-i$$

$$(32+9i)(3i)-(4+11i)(7+5i)=-i$$

$$(32+9i)(3i)+(4+11i)(-7-5i)=-i$$

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

2.6 Fatoração Única

Nesta seção definiremos Inteiros Gaussianos primos e compostos. Também provaremos aqui o Teorema da Fatoração Única em $\mathbb{Z}[i]$.

Lema 2.6.1. Seja α um inteiro gaussiano não nulo:

i) qualquer divisor β de α que possui norma igual a 1 é uma unidade;

ii) qualquer divisor β de α, tal que $\mathcal{N}(\beta)=\mathcal{N}(\alpha)$ será um múltiplo unitário de α;

DEMONSTRAÇÃO:
i) Sejam α e β inteiros gaussianos tal que $\beta|\alpha$ e $\mathcal{N}(\beta)=1$, então é imediato verificar que $\beta=\pm1$ ou $\beta=\pm i$.

ii) Se $\beta|\alpha$ e $\mathcal{N}(\beta) = \mathcal{N}(\alpha)$, então podemos considerar que exista um inteiro gaussiano γ tal que $\alpha = \beta\gamma$. Aplicando a função norma em ambos os lados da igualdade, obtemos que $\mathcal{N}(\alpha) = \mathcal{N}(\beta\gamma) = \mathcal{N}(\beta)\mathcal{N}(\gamma) \Longleftrightarrow 1 = \mathcal{N}(\gamma)$, pois $\mathcal{N}(\beta) = \mathcal{N}(\alpha)$. Mas, se $1 = \mathcal{N}(\gamma)$, concluímos que $\gamma = \pm 1$ ou $\gamma = \pm i$. Portanto β deve ser igual $u.\alpha$, com $u \in \{1, -1, i, -i\}$, ou seja, β é um múltiplo unitário de α.

■

O que o Lema 2.6.1 quer dizer é que os únicos inteiros Gaussianos que dividem α e tem norma igual a $\mathcal{N}(\alpha)$ são $\pm\alpha$ ou $\pm i\alpha$.

Ele não diz que os únicos inteiros gaussianos que possuem norma $\mathcal{N}(\alpha)$ são $\pm\alpha$ ou $\pm i\alpha$. Veja por exemplo que $1 + 8i$ e $4 + 7i$ possuem norma 65 e nem são unidades multiplicativas um do outro.

Quando $\mathcal{N}(\alpha) > 1$, obtemos imeditamente oito divisores de α, a saber: $\pm 1, \pm i, \pm\alpha, \pm i\alpha$. Estes são os chamados divisores triviais de α. Qualquer outro divisor será chamado de não trivial. Pelo Lema, concluímos que os divisores não triviais de um inteiro gaussiano α são aqueles cuja norma está estritamente entre 1 e $\mathcal{N}(\alpha)$.

Definição 2.6.2. Seja α um inteiro gaussiano na qual $\mathcal{N}(\alpha) > 1$. O inteiro gaussiano α será chamado de composto se possuir algum divisor não trivial. Se α possuir apenas divisores triviais, então ele será chamado de primo.

Teorema 2.6.3. Se a norma de um inteiro Gaussiano α é um número primo em $\mathbb{Z}$, então α será um número primo em $\mathbb{Z}[i]$.
DEMONSTRAÇÃO: Seja $\alpha = a + bi$ um inteiro gaussiano e p um natural primo tal que $\mathcal{N}(\alpha) = p$. Suponha que $\alpha = \beta\gamma$, com β e γ inteiro gaussianos. Aplicando a função Norma em ambos os lados da igualdade, obtemos: $\mathcal{N}(\alpha) = \mathcal{N}(\beta\gamma)$ e como a função Norma é multiplcativa, obtemos: $\mathcal{N}(\alpha) = \mathcal{N}(\beta)\mathcal{N}(\gamma)$. Desta forma, temos que $\mathcal{N}(\beta)\mathcal{N}(\gamma) = p$. Como p é natural primo, segue que:

$$\mathcal{N}(\beta) = 1 \text{ e } \mathcal{N}(\gamma) = p$$

ou

$$\mathcal{N}(\beta) = p \text{ e } \mathcal{N}(\gamma) = 1$$

Com isso, observamos que β é uma unidade e γ é múltiplo unitário de α ou γ é uma unidade e β é um múltiplo unitário de α e, portanto, α possui apenas divisores triviais, ou seja, α é primo.

■

Lema 2.6.4. Seja π um inteiro gaussiano primo. Se $\pi|\alpha\beta$, então $\pi|\alpha$ ou $\pi|\beta$ para α, $\beta \in \mathbb{Z}[i]$.

DEMONSTRAÇÃO: Para demonstrar este lema vamos supor que $\pi \nmid \alpha$ e concluir que $\pi|\beta$.

Seja π um inteiro gaussiano primo e α e β inteiros gaussianos onde $\pi|\alpha\beta$ e $\pi \nmid \alpha$.

Se $\pi \nmid \alpha$, então $\text{mdc}(\alpha, \pi) = u$, onde $u \in \{1, -1, i, -i\}$. Isto significa que α e β são relativamente primos. Sendo assim, temos através do **Corolário 2.5.8** que existem inteiros gaussianos x e y tais que

$$x\alpha + y\pi = 1.$$

Multiplicando ambos os membros da equação acima por β, obtemos

$$\beta\alpha x + \beta\pi y = \beta$$

Como $\pi|\alpha\beta$, $\pi|\pi$, temos que $\pi|(\beta\alpha x + \beta\pi y)$ e, portanto, $\pi|\beta$.

■

Teorema 2.6.5. (Fatoração única) Qualquer elemento $\alpha \neq 0$ de $\mathbb{Z}[i]$ admite uma fatoração

$$\alpha = \pi_1\pi_2\pi_3...\pi_n$$

em elementos irredutíveis (primos) π_i. Tal fatoração é única a menos de ordem dos fatores e da multiplicação por unidades (isto é, a menos de associados).

DEMONSTRAÇÃO: A prova da unicidade da fatoração é idêntica à dos inteiros, utilizando o lema anterior. A prova da existência da fatoração é também similar, mas agora utilizamos indução em $\mathcal{N}(\alpha)$. Antes, vamos mostrar que para as quatro primeiras normas possíveis, obtemos sempre um inteiro gaussiano que é escrito como produto de primos em $\mathbb{Z}[i]$. Se $\mathcal{N}(\alpha) = 2$ então α é irredutível, pois $\alpha = \pm 1 \pm i$ é irredutível (ou primo). Se $\mathcal{N}(\alpha) = 4$ então α é escrito como produto de primos, pois $\alpha = \pm 2 = \pm(1 + i)(1 - i)$ ou

$\pm 2i = \pm(1+i)(1-i)i$. Se $\mathcal{N}(\alpha) = 5$ então α é primo, pois $\alpha = \pm 1 \pm 2i$ ou $\alpha = \pm 2 \pm i$ são primos em $\mathbb{Z}[i]$. Se $\mathcal{N}(\alpha) = 8$ então α é escrito como produto de primos, pois $\alpha = \pm 2 \pm 2i = \pm 2(1+i) = \pm(1+i)(1-i)(1+i)$. Suponha válido agora para um certo inteiro gaussiano ϕ, isto é, Se β é inteiro gaussiano, onde $\mathcal{N}(\beta) < \mathcal{N}(\phi)$, então β será fatorado em primos em $\mathbb{Z}[i]$.

Se ϕ é irredutível, não há nada a fazer; caso contrário, temos que ϕ será composto, ou seja, existe uma fatoração $\phi = \delta\pi$, onde nem δ e nem π são unidades, isto é, $\mathcal{N}(\delta) \neq 1$ e $\mathcal{N}(\pi) \neq 1$. Como $\mathcal{N}(\phi) = \mathcal{N}(\delta)\mathcal{N}(\pi)$, temos que δ e π possuem norma estritamente menor do que $\mathcal{N}(\phi)$. Por hipótese de indução, δ e ϕ podem ser fatorados em irredutíveis, e combinando as duas fatorações temos uma fatoração de ϕ.

■

2.7 Aritmética Modular

Assim como nos números inteiros, congruências são definidas usando a ideia de divisibilidade.

Seja α um inteiro gaussiano diferente de zero. Diremos que dois inteiros gaussianos β e γ são *congruentes* módulo α se os restos de sua divisão euclidiana por α são iguais. Quando os inteiros gaussianos β e γ são congruentes módulo m, escreve-se

$$\beta \equiv \gamma \; mod \; \alpha$$

Quando a relação $\beta \equiv \gamma \; mod \; \alpha$ for falsa, diremos que β e γ não são congruentes, ou que são incongruentes, módulo α. Escreveremos, neste caso, $\beta \not\equiv \gamma \; mod \; \alpha$.

Decorre, imediatamente, da definição que a congruência, módulo um inteiro gaussiano fixado α, é uma relação de equivalência. Vamos enunciar isto explicitamente abaixo.

Proposição 2.7.1. Seja $\alpha \in \mathbb{Z}[i]$, com $\mathcal{N}(\alpha) > 1$. Para todos θ, β e $\gamma \in \mathbb{Z}[i]$, temos:

i) [Propriedade Reflexiva] $\theta \equiv \theta \; mod \; \alpha$,

ii) [Propriedade Simétrica] Se $\theta \equiv \beta \; mod \; \alpha$, então $\beta \equiv \theta \; mod \; \alpha$,

iii) [Propriedade Transitiva] Se $\theta \equiv \beta \; mod \; \alpha$ e $\beta \equiv \gamma \; mod \; \alpha$, então $\theta \equiv \gamma \; mod \; \alpha$.

DEMONSTRAÇÃO: A demonstração é idêntica à que é feita em $\mathbb{Z}$.

Para verificar se dois inteiros são congruentes módulo α, não é necessário efetuar a divisão euclidiana de ambos por α para depois comparar os seus restos. É suficiente aplicar a seguinte definição:

Definição 2.7.2. Sejam que α, β e $\gamma \in \mathbb{Z}[i]$. Escrevemos $\alpha \equiv \beta \; mod \; \gamma$ quando $\gamma|(\alpha-\beta)$.

Exemplo 2.7.3. Prove que $(1+12i) \equiv (2-i) \; mod \; (3+i)$.
De fato. Note inicialmente que $(1+12i)-(2-i) = -1+13i$. Agora, é evidente que $(3+i)|(-1+13i)$, pois $\dfrac{-1+13i}{3+i} = \dfrac{10+40i}{10} = 1+4i$.

Exemplo 2.7.4. Vamos calcular o resto da divisão de $(3+2i)^2$ por $4+i$.
Note inicialmente que $(3+2i)^2 = 9+12i+4i^2 = 9-4+12i = 5+12i$. Observe também que $5+12i = (4+i)(2+3i)-2i$. Portanto $(3+2i)^2 \equiv (-2i) \; mod \; (4+i)$.

Exemplo 2.7.5. Vamos encontrar todos os múltiplos de $1+2i$ em $\mathbb{Z}[i]$, isto é:

$$(1+2i)(m+ni) = m+ni+2im+2ni^2 = m+ni+2im-2n = m(1+2i)+n(-2+i),$$

com m e n inteiros. Vamos plotar em um plano cartesiano os inteiros gaussianos $1+2i$ e $-2+i$.

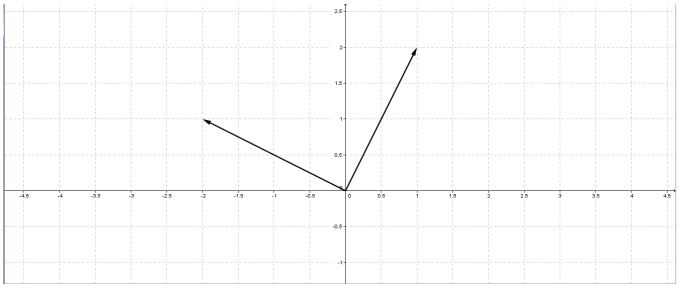


Figura 2.1: Representação Gráfica de $1+2i$ e $-2+i$

Agora, vamos observar uma curiosidade gráfica da representação de um múltiplo de um inteiro gaussiano. Se $m = 1$ e $n = 1$, então o inteiro gaussiano gerado é $1(1+2i)+1(-2+i) = -1+3i$. Interpretaremos este resultado como o ponto do plano

(x, y), onde $x = m - 2n$ é a parte real e $y = 2m + n$ a parte imaginária. Fazendo todas as combinações para $m = 0, \pm 1, \pm 2$ e $n = 0, \pm 1, \pm 2$, obtemos os seguintes pontos do plano.

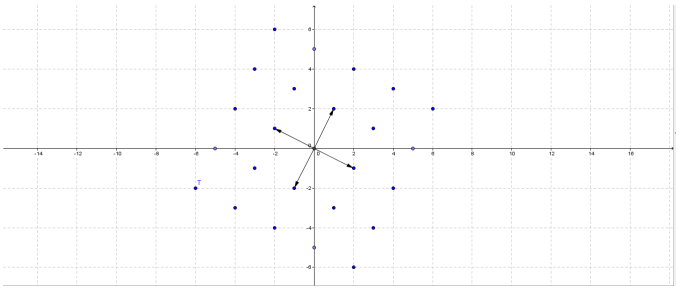


Figura 2.2: $(x = m - 2n, y = 2m + n)$, com $m = 0, \pm 1, \pm 2$ e $n = 0, \pm 1, \pm 2$.

Fazendo todas as combinações para $(x = m - 2n, y = 2m + n)$, com m e n inteiros e encaixando os vetores geradores deste pontos, obtemos um reticulado[1] no plano cartesiano, conforme a imagem abaixo:

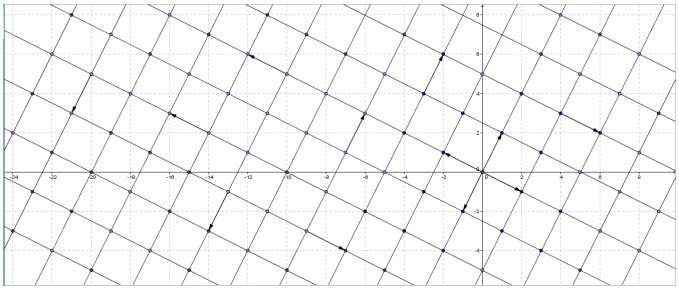


Figura 2.3: Todos os pontos gerados por $(x = m - 2n, y = 2m + n)$.

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

Lema 2.8.1. Um número natural p primo é composto em $\mathbb{Z}[i]$, se, e somente se ele for escrito como soma de dois quadrados.

DEMONSTRAÇÃO:

$\Rightarrow$) Seja p um natural primo em $\mathbb{Z}$ e composto em $\mathbb{Z}[i]$. Logo p pode ser escrito através de uma fatoração não trivial, isto é, $p = \alpha.\beta$ (I) com α e β inteiros gaussianos e $\mathcal{N}(\beta) < \mathcal{N}(p)$.

[1]Para maiores informações sobre o assunto consulte a página 140 de [6].

Aplicando a função Norma na equação (I) e usando o fato que esta função é multiplicativa, obtemos que:

$$\mathcal{N}(p) = \mathcal{N}(\alpha\beta) \Leftrightarrow p^2 = \mathcal{N}(\alpha)\mathcal{N}(\beta) \ (II)$$

Da expressão (II), obtemos que $\mathcal{N}(\alpha) = \mathcal{N}(\beta) = p$, com p primo. Adotando $\alpha = a + bi$, segue que $\mathcal{N}(\alpha) = a^2 + b^2 = p$, ou seja, p é escrito como soma de dois quadrados.

$\Leftarrow$) Suponha que p seja um número natural primo em $\mathbb{Z}$ que é escrito como soma de dois quadrados, isto é, existem inteiros a e b tais que $p = a^2 + b^2$. Mas, observe que também podemos escrever p da seguinte maneira $p = (a+bi)(a-bi)$ que é uma fatoração não trivial em $\mathbb{Z}[i]$. Logo, p é composto em $\mathbb{Z}[i]$.

■

Exemplo 2.8.2. Observe os 68 primeiros naturais primos que são escritos como soma de dois quadrados.

$2 = 1^2 + 1^2$	$173 = 2^2 + 13^2$	$377 = 4^2 + 19^2$	$593 = 8^2 + 23^2$
$5 = 1^2 + 2^2$	$181 = 9^2 + 10^2$	$389 = 10^2 + 17^2$	$601 = 5^2 + 24^2$
$13 = 2^2 + 3^2$	$193 = 7^2 + 12^2$	$397 = 6^2 + 19^2$	$613 = 17^2 + 18^2$
$17 = 1^2 + 4^2$	$197 = 1^2 + 14^2$	$401 = 1^2 + 20^2$	$617 = 16^2 + 19^2$
$29 = 2^2 + 5^2$	$229 = 2^2 + 15^2$	$409 = 3^2 + 20^2$	$641 = 4^2 + 25^2$
$37 = 1^2 + 6^2$	$233 = 8^2 + 13^2$	$421 = 14^2 + 15^2$	$653 = 13^2 + 22^2$
$41 = 4^2 + 5^2$	$241 = 4^2 + 15^2$	$433 = 12^2 + 17^2$	$661 = 6^2 + 25^2$
$53 = 2^2 + 7^2$	$257 = 1^2 + 16^2$	$449 = 7^2 + 20^2$	$673 = 12^2 + 23^2$
$61 = 5^2 + 6^2$	$269 = 10^2 + 13^2$	$457 = 4^2 + 21^2$	$677 = 1^2 + 26^2$
$73 = 3^2 + 8^2$	$277 = 9^2 + 14^2$	$461 = 10^2 + 19^2$	$701 = 5^2 + 26^2$
$89 = 5^2 + 8^2$	$293 = 2^2 + 17^2$	$477 = 5^2 + 21^2$	$709 = 15^2 + 22^2$
$97 = 4^2 + 9^2$	$313 = 12^2 + 13^2$	$509 = 5^2 + 22^2$	$733 = 2^2 + 27^2$
$109 = 9^2 + 10^2$	$317 = 11^2 + 14^2$	$521 = 11^2 + 20^2$	$757 = 9^2 + 26^2$
$113 = 7^2 + 8^2$	$337 = 9^2 + 16^2$	$541 = 10^2 + 21^2$	$769 = 12^2 + 25^2$
$137 = 4^2 + 11^2$	$349 = 5^2 + 18^2$	$557 = 14^2 + 19^2$	$773 = 17^2 + 22^2$
$149 = 2^2 + 12^2$	$353 = 8^2 + 17^2$	$569 = 13^2 + 20^2$	$797 = 11^2 + 26^2$
$157 = 6^2 + 11^2$	$373 = 7^2 + 18^2$	$577 = 1^2 + 24^2$	$809 = 5^2 + 28^2$

Tabela 2.1: Os 68 primeiros naturais primos que são escritos como soma de dois quadrados

Observe que todos os primos desta tabela satisfazem a congruência $p \equiv 1 \ mod(4)$.

Na confecção desta tabela, construímos via EXCEL duas ferramentas eletrônicas que podem ser úteis no ensino de aritmética.

Primeiro construímos uma planilha iterativa que testa se um certo natural k é primo ou composto, com $k \leq 10000$. A segunda planilha iterativa consiste na escrita de um certo natural m como soma de dois quadrados, com $m \leq 1225$.

Elas estão disponíveis em:
http://www-mat-ams.blogspot.com.br/2014/05/ola-galera-uma-das-ideias-mais.html e
http://www-mat-ams.blogspot.com.br/2014/05/um-metodo-iterativo-para-escrever.html.

Lema 2.8.3. Sejam a e b dois números inteiros. Então $a^2 + b^2 \equiv 0, 1$ *ou* 2 $(mod\ 4)$.
DEMONSTRAÇÃO: Se a é um número inteiro, então a assume uma das seguintes formas:

$$a = 4k; a = 4k + 1; a = 4k + \ 2; a = 4k + 3$$

Desta maneira a^2 assume uma das seguintes formas

$$16k^2 = 4(4k^2); 16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1;$$

$$16k^2 + 16k + 4 = 4(4k^2 + 4k + 1); 16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1$$

Logo

$$a^2 \equiv 0\ (mod\ 4)\ ou\ \equiv 1\ (mod\ 4)$$

Isto nos diz que um quadrado ao ser dividido por 4, deixa resto 0 ou resto 1. Desta forma, observamos que a soma de dois quadrados será

$a^2+b^2 \equiv (0+0)\ (mod\, 4);\ a^2+b^2 \equiv (1+0)\ (mod\, 4); a^2+b^2 \equiv (0+1)\ (mod\, 4); a^2+b^2 \equiv (1+1)\ (mod\, 4).$

Logo, fica evidente que se um número natural k satisfaz $k \equiv 3\ (mod\ 4)$, então k não pode ser escrito como soma de dois quadrados.

■

Exemplo 2.8.4. Observe os 30 primeiros primos:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79,$$

$$83, 89, 97, 101, 103, 107, 109, 113$$

Todos eles, exceto o 2, satisfazem uma das conguências abaixo:

$$p \equiv\ 1\ mod(4)\ (I)\ ou\ p \equiv\ 3\ mod(4)\ (II).$$

Os que satisfazem a congruência (I) podem ser escritos como soma de dois quadrados, conforme conjecturamos na **Tabela 2.1** e provaremos a seguir no **Teorema 2.8.6**. Já os que satisfazem a congruência (II) não podem ser escritos como soma de dois quadrados, conforme **Lema 2.8.3**.

Corolário 2.8.5. Seja p um natural primo em $\mathbb{Z}$ que satisfaz $p \equiv\ 3\ mod(4)$, então p não pode ser escrito como soma de dois quadrados e, além disso, p é primo em $\mathbb{Z}[i]$.
DEMONSTRAÇÃO: Se p é um natural primo em $\mathbb{Z}$ que satisfaz $p \equiv\ 3\ mod(4)$, então pelo **Lema 2.8.3**, p não pode ser escrito como soma de dois quadrados.
Se p não pode ser escrito como soma de dois quadrados, então pelo **Lema 2.8.1**, temos que p é não composto em $\mathbb{Z}[i]$, ou seja, p é primo em $\mathbb{Z}[i]$.

■

Teorema 2.8.6. Sendo p um natural primo, a equação $x^2 + y^2 = p$ possui soluções inteiras $(x, y) \in \mathbb{N} \times \mathbb{N}$ se, e somente se, $p = 2$ ou $p \equiv 1\ mod(4)$.
DEMONSTRAÇÃO: Observamos, incialmente, que $2 = 1^2 + 1^2$. Sabemos que para todo primo ímpar p temos $p \equiv 1\ mod(4)$ ou $p \equiv 3\ mod(4)$.
Como, para todo inteiro a, $a^2 \equiv (0\ ou\ 1)\ mod(4)$ **(Lema 2.8.3)** vemos que se $x^2 + y^2 = p$ então $p \equiv 1\ mod(4)$.
Nos resta mostrar que para todo p satisfazendo $p \equiv 1\ mod(4)$ pode ser escrito como soma de dois quadrados.
Tomamos, pois, um primo $p \equiv 1\ mod(4)$. **Pelo Teorema 1.1.6.16** existe x tal que $x^2 \equiv -1 mod(p)$. Com este x definimos a função $f(u, v) = u + xv$ e tomamos $m = \lfloor\sqrt{p}\rfloor^2$. Como $\sqrt{p}$ não é um inteiro temos $m < \sqrt{p} < m + 1$. Consideramos os pares (u, v) de inteiros onde $0 \leq u \leq m$ e $0 \leq v \leq m$. Desta forma, vemos que u pode assumir m+1 valores e v, também, pode assumir m+1 valores. Portanto, o número total de pares é

[2] A função "maior inteiro"é a que associa a cada real x o maior inteiro menor ou igual a x. Denotamos este valor por $\lfloor x \rfloor$.

$(m+1)^2$. Como $m+1 > \sqrt{p}$, temos que $(m+1)^2 > p$, isto é, o total de pares é superior a p. Como um sistema completo de resíduos módulo p possui exatamente p elementos, concluímos que se considerarmos $f(u,v)$ módulo p teremos mais números do que classes de resíduos para colocá-los. Logo, pelo Princípio das Casas dos Pombos, existem pelo menos dois pares distintos (u_1, v_1) e (u_2, v_2) com coordenadas satisfazendo $0 \leq u_i \leq m$ e $0 \leq v_i \leq m$ (i=1,2), para os quais

$$f(u_1, v_1) \equiv f(u_2, v_2)(mod(p)).$$

Isto equivale a $(u_1 + xv_1) \equiv (u_2 + xv_2)(mod(p))$, isto é, $(u_1 - u_2) \equiv -x(v_1 - v_2)(mod(p))$. Elevando-se ao quadrado ambos os membros desta última congruência, temos:

$$(u_1 - u_2)^2 \equiv -x^2(v_1 - v_2)^2 \equiv -(v_1 - v_2)^2(mod(p))$$

uma vez que $x^2 \equiv -1 mod(p)$.
Definindo $a = u_1 - u_2$ e $b = v_1 - v_2$, obtemos:

$$a^2 + b^2 \equiv 0(mod(p))$$

ou seja, $p|(a^2 + b^2)$. Como os pares (u_1, v_1) e (u_2, v_2) são distintos, a e b não são ambos nulos, isto é, $a^2 + b^2 > 0$.
Sendo u_1 e u_2 inteiros no intervalo $[0, m]$, temos que $a = u_1 - u_2$ satisfaz $-m \leq a \leq m$. Também para $b = v_1 - v_2$, temos $-m \leq b \leq m$ pela mesma razão. Como $m < \sqrt{p}$, concluímos que $|a| < \sqrt{p}$ e $|b| < \sqrt{p}$. Isto nos diz que $a^2 + b^2 < 2p$.
Logo, $a^2 + b^2$ é um inteiro divisível por p e satisfazendo $0 < a^2 + b^2 < 2p$. Como o único inteiro múltiplo de p neste intervalo é p, concluímos que $a^2 + b^2 = p$.

■

Existem números naturais compostos que também podem ser escritos como soma de quadrados, por exemplo $8 = 2^2 + 2^2$ e $20 = 2^2 + 4^2$. Vamos estudar os 20 primeiros naturais compostos que são escritos como soma de quadrados e verificar se existe algum padrão para estes números.

$$4 = 2^2 + 0^2 = 2^2;\ 8 = 2^2 + 2^2 = 2^3;\ 9 = 3^2 + 0^2 = 3^2;\ 10 = 3^2 + 1^2 = 2 \times 5$$

$$16 = 4^2 + 0^2 = 2^4;\ 18 = 3^2 + 3^2 = 2 \times 3^2;\ 20 = 4^2 + 2^2 = 2^2 \times 5;\ 25 = 3^2 + 4^2 = 5^2$$

$$26 = 1^2 + 5^2 = 2 \times 13;\ 32 = 4^2 + 4^2 = 2^5;\ 34 = 3^2 + 5^2 = 2 \times 17;\ 36 = 6^2 + 0^2 = 2^2 \times 3^2$$

$$40 = 2^2 + 6^2 = 2^3 \times 5;\ 45 = 3^2 + 6^2 = 3^2 \times 5;\ 49 = 7^2 + 0^2 = 7^2;\ 50 = 1^2 + 7^2 = 2 \times 5^2$$

$$52 = 4^2 + 6^2 = 2^2 \times 13;\ 58 = 3^2 + 7^2 = 2 \times 29;\ 64 = 8^2 + 0^2 = 2^6;\ 65 = 8^2 + 1^2 = 5 \times 13$$

Com estes exemplos, observamos e conjecturamos o seguinte padrão para um número ser escrito como soma de quadrados.

Dado um número natural p que é escrito como soma de quadrados. Sua fatoração em primos assume uma das opções abaixo:

- Será uma potência de 2;
- Será $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, com $p_i \equiv\ 1(mod\ 4)$ e $i = 1, 2, ..., r$ [Tabela 2.1];
- Será $q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$, com $q_j \equiv\ 3(mod\ 4)$, $j = 1, 2, ..., s$ e todos os expoentes β_j são pares;
- Será uma combinação das opções acima.

Para enunciar de uma forma mais clara e provar esta conjectura destacamos o teorema abaixo.

Teorema 2.8.7. Um inteiro n pode ser representado como soma de dois quadrados se, e somente se, tiver fatoração da forma

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

onde $p_i \equiv\ 1(mod\ 4)$ e $q_j \equiv\ 3(mod\ 4)$, $i = 1, 2, ..., r$, $j = 1, 2, ..., s$ e todos os expoentes β_j são pares.

DEMONSTRAÇÃO: Sabemos que $2 = 1^2 + 1^2$ e que pelo **Teorema 2.8.6** todos os p_i's podem ser representados pela soma de dois quadrados. Logo, se todos os β_j's forem pares, cada um pode ser escrito como $\beta_i = 2\beta_i'$ o que nos diz que $q_j^{\beta_j} = (q_j^2)^{\beta_j}$. Mas $q_j^2 = q_j^2 + 0^2$, ou seja, q_j^2 é soma de dois quadrados.

Disto concluímos, que se todos os β_j's forem pares, n terá representação como soma de dois quadrados.

Suponhamos, agora, que n possa ser representado como soma de dois quadrados e que algum β_j seja ímpar. Sem perda de generalidade, podemos considerar β_1 ímpar. Seja $d = mdc(a, b)$ onde a e b são inteiros tais que $a^2 + b^2 = n$. Como $d|a$ e $d|b$, temos que $a = k_1 d$ e $b = k_2 d$. Sabemos, pelo **Corolário 1.1.4.10** que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, isto é, $(k_1, k_2) = 1$. Como $d^2|n$, temos $n = kd^2$. Portanto,

$$k = \frac{n}{d^2} = \frac{a^2 + b^2}{d^2} = \frac{a^2}{d^2} + \frac{b^2}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = k_1^2 + k_2^2.$$

Como estamos supondo β_1 ímpar o expoente de q_1 em k será ímpar, pois $k = n/d^2$. Logo, $q_1|k$ e como $(k_1, k_2) = 1$ podemos concluir que

$$(q_1, k_1) = (q_1, k_2) = 1.$$

Logo, pelo **Teorema 1.1.6.12**, existe x tal que $k_1 x \equiv k_2 (mod\ q_1)$ e, portanto

$$0 \equiv k = k_1^2 + k_2^2 \equiv k_1^2 + k_1^2 x^2 \equiv k_1^2(1 + x^2)(mod\ q_1).$$

Como $q_1 \not| k_1\ 2$, temos que $x^2 + 1 \equiv 0(mod\ q_1)$ ou seja, $x^2 \equiv -1(mod\ q_1)$. Sendo $q_1 \equiv 3(mod\ 4)$ sabemos que esta última congruência não é possível (**Lema 2.8.3**). Disto concluímos que todos os β_j's devem ser pares caso n possua representação como soma de quadrados.

■

Teorema 2.8.8. Seja p um natural primo em $\mathbb{Z}$. Se $p \equiv 1\ mod(4)$, então p é composto em $\mathbb{Z}[i]$.

DEMONSTRAÇÃO: Pelo **Teorema 2.8.6**, temos que se p é um natural primo e $p \equiv 1\ mod(4)$, então p pode ser escrito como soma de dois quadrados. Se p pode ser escrito como soma de dois quadrados, então pelo **Lema 2.8.1** temos que p é composto em $\mathbb{Z}[i]$.

■

Teorema 2.8.9. Todo primo em $\mathbb{Z}[i]$ é um dos seguintes números:

1. $u.(1 + i)$;

2. $u.\pi$ ou $u.\overline{\pi}$, onde $\mathcal{N}(\pi) = p$ com p primo em $\mathbb{Z}$ e $p \equiv 1\ mod(4)$;

3. $u.p$, com p primo em $\mathbb{Z}$ e $p \equiv 3\ mod(4)$, com $u \in \{1, -1, i, -i\}$.

DEMONSTRAÇÃO:

1. Observe que a $\mathcal{N}(u(1+i)) = 2$ e 2 é primo em $\mathbb{Z}$. Logo, pelo **Teorema 2.6.3** $1+i$ é primo em $\mathbb{Z}[i]$.

2. Consequência do **Teorema 2.6.3**, pois se π é inteiro gaussiano e sua Norma é um inteiro primo, concluímos por este teorema que π será primo. Sendo $\pi = a + bi$ um inteiro gaussiano que tem como Norma um inteiro primo k, observamos que $\mathcal{N}(u.\pi) = \mathcal{N}(u)\mathcal{N}(a+bi) = \mathcal{N}(u)\mathcal{N}(a-bi) = \mathcal{N}(u.\overline{\pi}) = a^2 + b^2 = k$, de forma análoga concluímos que $\overline{\pi}$ é um inteiro gaussiano primo também.

3. Consequência do **Corolário 2.8.5.**, pois se p é primo em $\mathbb{Z}$ e $p \equiv 3\ mod(4)$, então por este teorema ele não pode ser escrito como soma de dois quadrados. Se ele não pode ser escrito como soma de dois quadrados então ele é não composto em $\mathbb{Z}[i]$, o que é equivalente a dizer que p é primo em $\mathbb{Z}[i]$.

■

Exemplo 2.8.10. Escreva 35 como produto de primos em $\mathbb{Z}[i]$.
A fatoração de 35 nos inteiros é $35 = 5.7$
Como $5 \equiv 1\ (mod(4))$, temos que 5 pode ser escrito como soma de quadrados, logo

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

e é evidente que $(1+2i)$ e $(1-2i)$ são primos em $\mathbb{Z}[i]$.
Observe também que 7 é primo em $\mathbb{Z}[i]$, pois $7 \equiv 3\ (mod(4))$, logo

$$35 = 5.7 = (1+2i)(1-2i)7.$$

Exemplo 2.8.11. Escreva $2+i$ como produto de primos em $\mathbb{Z}[i]$.
Observe que $\mathcal{N}(2+i) = 5$ e 5 é primo em $\mathbb{Z}$. Logo $2+i$ é primo em $\mathbb{Z}[i]$ e sua fatoração

é $u.(2+i)$, com $u \in \{1, -1, i, -i\}$.

Exemplo 2.8.12. Escreva $\alpha = 3 + i$ como produto de primos em $\mathbb{Z}[i]$.
Inicialmente note que $\mathcal{N}(\alpha) = 9 + 1 = 10$. Logo, α é composto em $\mathbb{Z}[i]$.
Já vimos através do **Exemplo 2.3.7** que os divisores de α são:

$$\{1, 1+i, 1+2i, 1-2i, 3+i, 3-i\}$$

e suas multiplicações pelas unidades.
Note que destes divisores, são primos

$$\{1+i, 1+2i, 1-2i\}$$

e suas multiplicações pelas unidades.
Escolhemos um deles e realizamos a divisão de α por este primo. Para este exemplo, escolheremos $1 + i$. Logo

$$\frac{3+i}{1+i} = \frac{(3+i)}{(1+i)}\frac{(1-i)}{(1-i)} = \frac{4-2i}{2} = 2 - i.$$

Como $2 - i$ é primo em $\mathbb{Z}[i]$, obtemos que a fatoração de α em primos em $\mathbb{Z}[i]$ é

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

Exemplo 2.8.13. Mostraremos neste exemplo uma outra forma de encontrar a fatoração de um inteiro gaussiano em termos primos em $\mathbb{Z}[i]$ utilizando agora a Função Norma e sua propriedade de ser multiplicativa.
Para exemplificar considere o inteiro gaussiano $\beta = 17+33i$. É evidente que $\mathcal{N}(\beta) = 1378$. A fatoração desta norma em $\mathbb{Z}$ é $1378 = 2.13.53$. Agora, note que os três primos gerados são escritos como soma de quadrados e automaticamente escritos como produtos de primos em $\mathbb{Z}[i]$, pois $2 = 1^2 + 1^2 = (1 + i)(1 - i), 13 = 2^2 + 3^2 = (2 + 3i)(2 - 3i), 53 = 2^2 + 7^2 = (2 + 7i)(2 - 7i)$. Utilizando a multiplicidade da função Norma, podemos escrever

$$\mathcal{N}(\beta) = 1378 = 2.13.53 = \mathcal{N}(\gamma_1)\mathcal{N}(\gamma_2)\mathcal{N}(\gamma_3),$$

onde $\gamma_1 = 1 + i$ ou $\gamma_1 = 1 - i$, $\gamma_2 = 2 + 3i$ ou $\gamma_2 = 2 - 3i$ e $\gamma_3 = 2 + 7i$ ou $\gamma_3 = 2 - 7i$, ou seja, β será uma das oito possibilidades geradas acima. Concluímos assim que a fatoração de β em $\mathbb{Z}[i]$ em termos primos é

$$17 + 33i = (1 + i)(2 - 3i)(2 + 7i).$$

Observação 2.8.14. Este resultado é válido, pois provamos no **Teorema 2.6.5** que para todo inteiro gaussiano não nulo existe uma fatoração única em primos. Sendo assim, se α é um inteiro gaussiano não nulo, então existem inteiros gaussianos primos $\pi_1, \pi_2, ...\pi_n$, tal que

$$\alpha = u\pi_1\pi_2...\pi_n,$$

com u sendo unidade de $\mathbb{Z}[i]$. Aplicando a função norma em ambos os lados da equação acima, obtemos

$$\mathcal{N}(\alpha) = \mathcal{N}(u\pi_1\pi_2...\pi_n) = \mathcal{N}(u)\mathcal{N}(\pi_1)\mathcal{N}(\pi_2)...\mathcal{N}(\pi_n) = \mathcal{N}(\pi_1)\mathcal{N}(\pi_2)...\mathcal{N}(\pi_n).$$

Exemplo 2.8.15. Fatore o inteiro gaussiano $\beta = 2319 + 1694i$.
Note que $\mathcal{N}(\beta) = 8247397$. A fatoração desta norma em $\mathbb{Z}$ é $8247397 = 17.29.16729$. Agora, note que os três primos gerados são escritos como soma de quadrados e automaticamente escritos como produtos de primos em $\mathbb{Z}[i]$, pois $17 = 1^2+4^2 = (1+2i)(1-2i), 29 = 2^2 + 5^2 = (2 + 5i)(2 - 5i), 16729$[3]$= 40^2 + 123^2 = (40 + 123i)(40 - 123i)$. Utilizando a multiplicidade da função Norma, podemos escrever

$$\mathcal{N}(\beta) = 8247397 = 17.29.16729 = \mathcal{N}(\gamma_1)\mathcal{N}(\gamma_2)\mathcal{N}(\gamma_3),$$

onde $\gamma_1 = 1 + 4i$ ou $\gamma_1 = 1 - 4i$, $\gamma_2 = 2 + 5i$ ou $\gamma_2 = 2 - 5i$ e $\gamma_3 = 40 + 123i$ ou $\gamma_3 = 40 - 123i$, ou seja, β será uma das oito possibilidades geradas acima. Concluímos

[3] A verificação de que este número é primo foi feita via o teste de primalidade presente em [1] na página 89.

assim que a fatoração de β em $\mathbb{Z}[i]$ em termos primos é

$$2319 + 1694i = -(1 + 4i)(2 + 5i)(40 + 123i).$$

Com estes exemplos, podemos escrever dois métodos de fatoração em primos em $\mathbb{Z}[i]$.

2.8.1 Métodos de decomposição de fatores primos em $\mathbb{Z}[i]$

Método 1: Seja γ um inteiro gaussiano. Para fatorar γ em fatores primos em $\mathbb{Z}[i]$ devemos seguir os passos abaixo:

i) Se γ for primo, então não há nada a fazer;

ii) Se γ for composto, então encontre um divisor primo π de γ, tal que $\gamma = \pi\gamma_1$;

iii) Se γ_1 for primo, então não há mais nada a fazer e $\gamma = \pi\gamma_1$;

iv) Se γ_1 for composto, volte no passo ii).

Justificativa deste método: Seja $\alpha = a+bi$ um inteiro gaussiano não nulo e $\mathcal{N}(\alpha) > 1$. Se α for primo, então não há nada o que fazer. Se α for composto, então calculamos sua norma, obtendo $\mathcal{N}(\alpha) = a^2 + b^2$. Como esta norma é um número natural, sabemos que este pode ser fatorado em números primos. Desta forma, obtemos o conjunto de divisores $d_1, d_2, ..., d_k$ de $\mathcal{N}(\alpha)$. Deste conjunto de divisores, escolhemos os d_i, com $i = 1, 2, ..., k$ que são escritos como soma de quadrados. Logo, encontramos os divisores de α, digamos $\alpha_1, \alpha_2, ...\alpha_r$ (já vimos neste trabalho que é possível encontrar todos os divisores de um inteiro gaussiano através de sua Norma). De todos os divisores de α selecionamos aqueles que são primos (basta usar o **Teorema 2.8.8**). Escolhemos um desses divisores e realizamos a divisão euclidiana de α por este divisor primo, gerando um quociente q_1. Se este quociente for primo, então não há nada a fazer. Caso q_1 for composto, repetimos o processo até obter um quociente primo!

Método 2: Seja γ um inteiro gaussiano. Para fatorar γ em fatores primos em $\mathbb{Z}[i]$ devemos seguir os passos abaixo:

i) Calcule a norma de γ;

ii) Fatore a norma de γ em $\mathbb{Z}$, obtendo os primos $p_1, p_2, ..., p_n$;

iii) Se o primo obtido deixar resto 3 quando dividido por 4, então ele será primo em $Z[i]$. Os primos que deixam resto 1 quando dividido por 4 deverão ser escritos como soma de quadrados;

iv) Fatore estes primos (que deixam resto 1 quando dividido por 4) em um produto de primos conjugados em $\mathbb{Z}[i]$;

v) Para cada primo gerado na fatoração da norma, aparecem um inteiro gaussiano primo ou dois inteiros gaussianos primos como candidato a fator. Logo existem no máximo 2^n produtos de inteiros gaussianos primos candidatos a fatoração de γ;

vi) Fazendo os testes das opções, determinamos a fatoração exata de γ.

Justificativa deste método: Seja $\alpha = a+bi$ um inteiro gaussiano não nulo e $\mathcal{N}(\alpha) > 1$. Sabemos pelo Teorema 2.6.5. que α pode ser fatorado em primos, isto é,

$$\alpha = u\pi_1\pi_2...\pi_n,$$

com u sendo unidade de $\mathbb{Z}[i]$ e $\pi_1, \pi_2, ..., \pi_n$ primos em $\mathbb{Z}[i]$. Aplicando a função norma em ambos os lados da equação acima, obtemos

$$\mathcal{N}(\alpha) = \mathcal{N}(u\pi_1\pi_2...\pi_n) = \mathcal{N}(u)\mathcal{N}(\pi_1)\mathcal{N}(\pi_2)...\mathcal{N}(\pi_n) = \mathcal{N}(\pi_1)\mathcal{N}(\pi_2)...\mathcal{N}(\pi_n).$$

Como $\pi_1, \pi_2, ..., \pi_n$ são primos em $\mathbb{Z}[i]$, temos então que cada π_i, com $i \in \{1, 2, 3, ...n\}$ assumirá umas das formas apresentadas no **Teorema 2.8.8**, isto é:

- $\pi_i = 1 + i$;
- $\pi_i = \phi$ ou $\pi_i = \overline{\phi}$, onde $\mathcal{N}(\pi_i) = p$, com p primo e $p \equiv 1$ $(mod\ 4)$;
- $\pi_i = p$, com p primo e $p \equiv 3$ $(mod\ 4)$.

. Desta forma $\mathcal{N}(\pi_1), \mathcal{N}(\pi_2), ..., \mathcal{N}(\pi_n)$ serão escritos como:

- $\mathcal{N}(\pi_i) = 2 = (1 - i)(1 + i)$;

- $\mathcal{N}(\pi_i) = p$, com p primo positivo e que deixa resto 1 quando divididos por 4. Logo, $\mathcal{N}(\pi_i) = a_i^2 + b_i^2$, então $\mathcal{N}(\pi_i) = a_i^2 + b_i^2 = (a_i - b_i i)(a_i + b_i i)$. Isto nos diz que para cada fator primo da multiplicação $\pi_1 \cdot \pi_2 \cdot ... \cdot \pi_n$ que satisfazer este item, teremos duas possibilidades, totalizando um total de 2^t combinações possíveis, com t sendo a quantidade de inteiros de Gauss com norma prima.

- $\mathcal{N}(\pi_i) = \pi_i \pi_i$

Desta forma, teremos no máximo 2^n possibilidades de produtos para resultar em α e fazendo os testes encontraremos uma combinação que satisfaça a equação $\alpha = u\pi_1\pi_2...\pi_n$.

Capítulo 3

Resolvendo Problemas dos Inteiros em $\mathbb{Z}[i]$

Estamos prontos para fazer aplicações da aritmética de $\mathbb{Z}[i]$ nas propriedades de $\mathbb{Z}$. Todas estas aplicações estão relacionadas com somas de dois quadrados, mais precisamente pela seguinte equação:

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

Nossas aplicações irão abordar as seguintes questões:

- Um número primo que é escrito de forma única como soma de dois quadrados;
- Classificação de ternas pitagóricas primitivas;
- Classificação de soluções primitivas para a equação $a^2 + b^2 = c^3$;
- A única solução inteira para a equação diofantina $y^2 = x^3 - 1$ é $(x, y) = (1, 0)$.

3.1 É possível um número primo ser escrito como soma de dois quadrados?

Conforme comentamos na introdução deste trabalho, será que é possível escrever um número primo como soma de quadrados? Se sim, sob quais critérios? Já respondemos à estas questões no **Teorema 2.8.6**. Nesta seção apenas apresentaremos uma maneira

diferente de provar que quando um primo é escrito como soma de quadrados, esta soma é única.

Teorema 3.1.1. Se um número inteiro primo p é uma soma de dois quadrados, então ele é escrito de forma única da seguinte maneira: $p = a^2 + b^2$, onde os inteiros a e b são únicos a menos da ordem e do sinal.
DEMONSTRAÇÃO: seja p inteiro primo tal que $p = a^2 + b^2$ com a, b inteiros. Usando os inteiros gaussianos, podemos escrever p de outra maneira, isto é

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

Aplicando a função norma em ambos os lados da equação acima, obtemos

$$\mathcal{N}(p) = \mathcal{N}((a + bi)(a - bi)) = \mathcal{N}(a + bi)\mathcal{N}(a - bi) = p^2$$

A única opção possível para que a equação acima seja satisafeita é

$$\mathcal{N}(a + bi) = \mathcal{N}(a - bi) = p.$$

Logo, pelo **Teorema 2.6.3** concluímos que $a + bi$ e $a - bi$ são primos em $\mathbb{Z}[i]$.
Agora suponha que existam c, d inteiros tais que

$$p = c^2 + d^2 = (c + di)(c - di),$$

logo, pela mesma justificativa apresentada acima, teremos que $c+di$ e $c-di$ serão primos $\mathbb{Z}[i]$.
Mas, pelo **Teorema 2.6.5**, temos que a fatoração em $\mathbb{Z}[i]$ é única (à menos de associados). Isto significa que

$$a + bi = u(c + di) \text{ } ou \text{ } a + bi = u(c - di),$$

onde u é unidade de $\mathbb{Z}[i]$.
Vamos estudar o caso em que $a + bi = u(c + di)$, pois os outros casos são análogos.

- Se $u = 1$ então $a + bi = c + di$, ou seja $a = c$ e $b = d$;
- Se $u = -1$ então $a + bi = -c - di$, ou seja $a = -c$ e $b = -d$;

- Se $u = i$ então $a + bi = ic + di^2 = -d + ci$, ou seja $a = -d$ e $b = c$;
- Se $u = -i$ então $a + bi = -ic - di^2 = d - ci$, ou seja $a = d$ e $b = -c$.

Desta forma, concluímos que se p é primo e é escrito como $p = a^2 + b^2$, então a e b são únicos.

■

Observação 3.1.2. Somente os números primos que possuem esta propriedade. Observe os números 50 e 65

$$50 = 5^2 + 5^2 = 1^2 + 7^2; 65 = 1^2 + 8^2 = 4^2 + 7^2,$$

são escritos como soma de dois quadrados distintos.

Exemplo 3.1.3. 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 $5 = 2^{2^1} + 1$, $17 = 2^{2^2} + 1$, $256 = 2^{2^3} + 1$, $65537 = 2^{2^4} + 1$) $F_5 = 2^{2^5} + 1 = 4294967297$ é escrito como soma de dois quadrados: $2^{2^5} + 1 = 4294967297 = (2^{16})^2 + 1^2$. Euler conseguiu escrever este mesmo número como soma de outros dois quadrados:

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

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. Euler ainda encontrou qual era o fator não trivial de F_5 ($2^{2^5} + 1 = 4294967297 = 641.6700417$).

3.2 Obtendo Ternos Pitagóricos Primitivos através de $\mathbb{Z}[i]$

O objetivo desta seção é encontrar as soluções inteiras da equação $a^2 + b^2 = c^2$, onde $(a, b, c) = 1$. Será que é possível? Se sim, será que existe uma fórmula que descreva estas soluções? Nesta seção mostraremos que a resposta para ambas as questões é SIM!

Teorema 3.2.1. Todo terno Pitagórico Primitivo (a, b, c) tem a seguinte forma

$$a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2$$

com $m > n > 0$, $(m, n) = 1$ e $m \not\equiv\ n\ mod(2)$.
Antes de demonstrarmos este resultado, vamos nos lembrar do que é um terno Pitagórico (TP) e do que é um Terno Pitagórico Primitivo (TPP).

Definição 3.2.2. Um *terno pitagórico* (TP) é uma tripla de inteiros positivos (a,b,c) tal que

$$a^2 + b^2 = c^2$$

Também chamamos o TP(a,b,c) de *triângulo pitagórico* cujos catetos são a,b e hipotenusa c.
Em outros termos, terno pitagórico é toda solução inteira e positiva da equação diofantina:

$$x^2 + y^2 = z^2$$

Assim, por exemplo, são ternos pitagóricos:

(3,4,5), (6,8,10), (5,12,13) e (12,35,37),

pois:

$3^2 + 4^2 = 5^2$, $6^2 + 8^2 = 10^2$, $5^2 + 12^2 = 13^2$ e $12^2 + 35^2 = 37^2$.

Definição 3.2.3. Um terno pitagórico primitivo (TPP) é um TP(a,b,c) com $\text{mdc}(a, b, c) = 1$. Também chamamos o TPP(a,b,c) de triângulo pitagórico primitivo cujos catetos são a,b e hipotenusa c.

Assim, (3,4,5) e (5,12,13) são exemplos de ternos pitagóricos primitivos, pois $3^2+4^2=5^2$, $5^2+12^2=13^2$ e mdc$(3,4,5)$=mdc$(5,12,13)=1$.

Chamamos de ternos pitagóricos compostos ou não-primitivo, todo TP(a,b,c) com mdc$(a,b,c)\neq 1$. Assim, (6,8,10) e (15,36,39) são ternos compostos ou não-primitivos, pois $6^2+8^2=10^2$, $15^2+36^2=39^2$, mdc$(6,8,10)=2$ e mdc$(15,36,39)=3$.

Antes de demonstramos o teorema, vamos relembrar alguns resultados dos inteiros que são preservados nos inteiros gaussianos.

Propriedade 3.2.4. Sejam a,b,d inteiros gaussianos tais que d=mdc(a,b), então $d|(a\pm b)$.

DEMONSTRAÇÃO: Sejam a,b,d inteiros gaussianos. Se d=mdc(a,b), então existem inteiros gaussianos w e y tais que $a=d.w$ e $b=d.y$. desta forma a expressão $a\pm b=dw\pm dy=d(w\pm y)$, ou seja, $d|(a\pm b)$.

■

DEMONSTRAÇÃO DO TEOREMA 3.2.1: Nosso objetivo aqui é encontrar todas as soluções da equação $a^2+b^2=c^2$, sendo a,b e c números inteiros e mdc$(a,b,c)=1$.

Se $mdc(a,b)=1$, então a e b não são pares simultaneamente. Logo ou a e b são ímpares ou são de paridade distintas.

Suponha que a e b sejam ímpares. Logo $a^2+b^2\equiv 2\ (mod\ 4)$, implicando que $c^2=a^2+b^2\equiv 2\ (mod\ 4)$. Mas, um quadrado ao ser dividido por 4 deixa resto 0 ou resto 1 **(Lema 2.8.3.)**. Concluímos assim que a e b possuem paridade distinta, ou seja, $a\not\equiv\ b\ mod(2)$.

Vamos mostrar agora que $mdc(a+bi,a-bi)=1$.

Suponha que $mdc(a+bi,a-bi)=\delta$, então **Propriedade 3.2.4** $\delta|2a$ e $\delta|2b$, implicando então que $\delta|2$, pois mdc$(a,b)=1$.

Neste momento temos duas possibilidades: $\delta=2$ ou $\delta=1$

Se $\delta=2$, então $2|(a^2+b^2)$. Logo a e b tem a mesma paridade o que é um absurdo, pois já mostramos acima que a e b possuem paridade distintas. Concluímos assim que $\delta=1$, ou seja, $a+bi$ e $a-bi$ são relativamentes primos. Como $c^2=a^2+b^2=(a+bi)(a-bi)$, temos que $a+bi$ e $a-bi$ serão necessariamente quadrados perfeitos, ou seja, existem $x,y,z,w\in\mathbb{Z}$, tal que:

$$\begin{cases} a+bi=(x+y)^2=x^2+2xyi+y^2i^2=(x^2-y^2)+2xyi \\ a-bi=(z+w)^2=z^2-2zwi+w^2i^2=(z^2-w^2)-2zwi \end{cases}$$

Da igualdade de inteiros gaussianos obtemos:

$$\begin{cases} a = x^2 - y^2; \quad b = 2xy \\ a = z^2 - w^2; \quad b = 2zw \end{cases} \iff \begin{cases} x = z \\ y = w \end{cases}$$

Como $\text{mdc}(a, b) = 1$, concluímos que $\text{mdc}(x, y) = \text{mdc}(w, z) = 1$. Logo obtemos

$$\begin{cases} a = x^2 - y^2; \\ b = 2xy \end{cases}$$

e, portanto $c^2 = a^2 + b^2 = (x^4 - 2x^2y^2 + y^4) + 4x^2y^2 = x^4 + 2x^2y^2 + y^4 = (x^2 + y^2)^2$.

■

Este resultado tem grande relevância no ensino de matemática e consiste em um excelente apoio pedagógico ao professor de matemática do Ensino Médio, pois ao trabalhar com problemas em triângulos retângulos com lados inteiros, basta o professor escolher dois números naturais (digamos m e n) de paridade distinta e primos entre si que ele terá infinitos triângulos retângulos, pois além do triângulo $(a = m^2 - n^2, b = 2mn, c = m^2 + n^2)$ ele terá infinitos outros, pois (ka, kb, kc), com k natural também será triângulo retângulo com lados inteiros. Desta forma, o professor não fica preso aos ternos $(3, 4, 5)$, $(5, 12, 13)$. Para exemplicar tome $m = 6$ e $n = 1$, obtemos $a = 36 - 1 = 35$, $b = 2.6.1 = 12$ e $c = 36 + 1 = 37$ que é um TPP.
No exercício 14 do capítulo 5 construímos uma tabela com os 29 primeiros ternos pitagóricos primitivos.

3.3 É possível escrever cubos como somas de dois quadrados?

Conforme comentamos na introdução deste trabalho, será que é possível escrever cubos como soma de dois quadrados? Se sim, sob quais condições? Nesta seção, temos por objetivo responder à estas questões.

Lema 3.3.1. Todo número natural que é um cubo perfeito nunca deixa resto 2 quando dividido por 8.

DEMONSTRAÇÃO: Seja k um número natural. Se dividirmos k por 8, podemos obter um dos seguintes restos

$$0, 1, 2, 3, 4, 5, 6 \ ou \ 7.$$

Isto é equivalente a dizer que uma das oito congruências será satisfeita

$$k \equiv \ m \ (mod \ 8),$$

onde $m \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. Elevando ambos os membros da congruência acima ao cubo, obtemos

$$k^3 \equiv \ m^3 \ (mod \ 8),$$

onde $m^3 \in \{0, 1, 8, 27, 64, 125, 216, 343\}$.

Como $0 \equiv 0 \ (mod \ 8)$, $1 \equiv 1 \ (mod \ 8)$, $8 \equiv 0 \ (mod \ 8)$, $27 \equiv 3 \ (mod \ 8)$, $64 \equiv 0 \ (mod \ 8)$, $125 \equiv 5 \ (mod \ 8)$, $216 \equiv 0 \ (mod \ 8)$ e $343 \equiv 7 \ (mod \ 8)$, concluímos que quando um cubo perfeito é dividido por 8 ele pode deixar apenas os seguintes restos

$$0, 1, 3, 5 \ ou \ 7$$

ou seja, um cubo perfeito nunca deixa resto 2 quando dividido por 8.

■

Teorema 3.3.2. As soluções inteiras da equação $a^2 + b^2 = c^3$, com $(a, b) = 1$ são descritas pelas seguintes equações

$$a = x^3 - 3xy^2, \ b = 3x^2y - y^3, \ c = x^2 + y^2,$$

com $(x, y) = 1$ e $x \not\equiv \ y \ mod(2)$.

DEMONSTRAÇÃO: Nosso objetivo aqui é encontrar todas as soluções da equação $a^2 + b^2 = c^3$, sendo a,b e c números inteiros.

Se $mdc(a, b) = 1$, então a e b não são pares simultaneamente. Logo ou a e b são ímpares ou são de paridade distintas.

Suponha que a e b sejam ímpares. Logo $a^2 \equiv b^2 \equiv 1 \ (mod \, 8)$, implicando que $c^3 = a^2 + b^2 \equiv$

2 (mod 8). Mas um cubo ao ser dividido por 8 nunca deixa resto igual a 2 **(Lema 3.3.1.)**.
Concluímos assim que a e b possuem paridade distinta, ou seja, $a \not\equiv b\ mod(2)$.
Vamos mostrar agora que $mdc(a+bi, a-bi) = 1$.
Suponha que $mdc(a+bi, a-bi) = \delta$, então **Propriedade 3.2.4.** $\delta|2a$ e $\delta|2b$, implicando então que $\delta|2$, pois mdc$(a,b) = 1$.
Neste momento temos duas possibilidades: $\delta = 2$ ou $\delta = 1$
Se $\delta = 2$, então $2|(a^2+b^2)$. Logo a e b tem a mesma paridade o que é um absurdo, pois já mostramos acima que a e b possuem paridade distintas. Concluímos assim que $\delta = 1$, ou seja, $a+bi$ e $a-bi$ são relativamentes primos. Como $c^3 = a^2+b^2 = (a+bi)(a-bi)$, temos que $a+bi$ e $a-bi$ serão necessariamente cubos perfeitos, ou seja, existem $x, y, z, w \in \mathbb{Z}$, tal que:

$$\begin{cases} a+bi = (x+yi)^3 = x^3+3x^2yi+3xy^2i^2+(yi)^3 = (x^3-3xy^2)+(3x^2y-y^3)i \\ a-bi = (z+wi)^3 = z^3+3z^2wi+3zw^2i^2+(wi)^3 = (z^3-3zw^2)+(3z^2w-w^3)i \end{cases}$$

Da igualdade de inteiros gaussianos obtemos:

$$\begin{cases} a = x^3-3xy^2; \quad b = 3x^2y-y^3 \\ a = z^3-3zw^2; \quad b = 3z^2w-w^3 \end{cases} \iff \begin{cases} x = z \\ y = w \end{cases}$$

Como mdc$(a,b) = 1$, concluímos que mdc(x,y) =mdc$(w,z) = 1$.
Além disso, $x \not\equiv y\ (mod\ 2)$, pois se x e y fossem de mesma paridade, teríamos que $a \equiv 0\ (mod\ 2)$ e $b \equiv 0\ (mod\ 2)$, o que é um absurdo, pois mdc$(a,b) = 1$. Logo se mdc$(x,y) = 1$ e $x \not\equiv y\ (mod\ 2)$, temos que $a = x^3-3xy^2$, $b = 3x^2y-y^3$ e $c = x^2+y^2$.

■

Exemplo 3.3.3. Resolva a equação diofantina $y^3 = x^2+4$
Podemos usar o **Teorema 3.3.2.** para confeccionar uma tabela para candidatos a solução deste problema. Antes, como neste exemplo $b = 2$, vamos analisar quais valores inteiros m, n satisfazem a equação $2 = 3m^2n-n^3 = n(3m^2-n^2) \Leftrightarrow \dfrac{2}{n} = 3m^2-n^2$. Esta equação só tem sentido se $n = \pm 1$ ou $n = \pm 2$. Fazendo os teste (tabela abaixo), obtemos as soluções.
Portanto as soluções desta equação diofantina são: $(11,5), (-11,5), (2,2), (-2,2)$.

Tabela 3.1: Candidatos a solução da equação diofantina $y^3 = x^2 + 4$

m	-1	1	1	-1
n	1	1	-2	-2
$a = m^3 - 3mn^2$	2	-2	-11	11
$b = 3m^2n - n^3$	2	2	2	2
$c = m^2 + n^2$	2	2	5	5
$a^2 + b^2$	8	8	125	125
c^3	8	8	125	125

Teorema 3.3.4. A única solução inteira da equação $y^2 = x^3 - 1$ é $(x, y) = (1, 0)$.

DEMONSTRAÇÃO: Observe que podemos escrever a equação acima da seguinte maneira $x^3 = y^2 + 1$. Utilizando o **Teorema 3.3.2** obtemos que $b = 1 = 3m^2n - n^3 = n(3m^2 - n^2) \Leftrightarrow \frac{1}{n} = 3m^2 - n^2$. Como m,n são inteiros, temos que a equação terá sentido se $n = \pm 1$.

Se $n = 1$ então $1 = 3m^2 - 1 \Leftrightarrow 3m^2 = 2$, ou seja m não será inteiro. Se $n = -1$ então $-1 = 3m^2 - 1 \Leftrightarrow 3m^2 = 0$, ou seja $m = 0$. Desta forma, concluímos que $n = -1$, $m = 0$, $b = 1$, $a = x = 0$ e $c = y = 1$.

Capítulo 4

Considerações sobre a Pesquisa

Iniciamos este Capítulo ressaltando as propriedades de $\mathbb{Z}$ que são mantidas em $\mathbb{Z}[i]$ e fazendo um breve comparativo.

- A ideia de divisibilidade é mantida;
- A ideia de divisão euclidiana é mantida, trocando apenas a maneira de comparar os números, a função Norma no lugar da função Módulo;
- O Algoritmo de Euclides é mantido;
- O número de unidades em $\mathbb{Z}$ é 2, já em $\mathbb{Z}[i]$ é 4;
- O Teorema de Bezout é mantido;
- A ideia de fatorar um número não nulo e diferente das unidades em fatores primos é mantida;
- As ideias de aritmética modular são preservadas;
- A ideia de número primo e composto é mantida;
- Os números primos em $\mathbb{Z}$ que satisfazem $p \equiv 1 \ (mod \ 4)$ são compostos em $\mathbb{Z}[i]$;
- A ideia de múltiplo de um número é expandida, pois em $\mathbb{Z}$ ela consiste em um subconjunto de uma reta numérica e em $\mathbb{Z}[i]$ ela consiste em um subconjunto do plano, pois gera um reticulado.

Ressaltamos também os resultados obtidos no capítulo 3. Neste capítulo mostramos um resultado que pode ser muito útil ao professor de Matemática do Ensino Médio. Na elaboração de exercícios que envolvam o Teorema de Pitágoras, o professor normalmente fica preso aos seguintes ternos $(3, 4, 5)$, $(5, 12, 13)$, $(3k, 4k, 5k)$ e $(5k, 12k, 13k)$, com k natural (podendo ser real, mas não tratamos neste texto sobre isso). Com o critério abordado aqui "entregamos"ao professor uma gama de novos problemas, por exemplo, através do TPP $(99, 20, 101)$ ele tem imediatamente infinitas opções de criar um novo problema: $k(99, 20, 101)$, com k natural.

Destacamos também o critério fornecido para resolver a equação $c^3 = a^2 + b^2$, com $\text{mdc}(a, b) = 1$. Observamos que será possível escrever um cubo como soma de quadrados se

$$a = x^3 - 3xy^2,\ b = 3x^2y - y^3,\ c = x^2 + y^2,$$

com $(x, y) = 1$ e $x \not\equiv\ y\ mod(2)$. Observamos imediatamente deste resultado que uma condição necessária para este problema é que

$$\frac{a}{x} = x^2 - 3y^2,\ \frac{b}{y} = 3x^2 - y^2,$$

ou seja, x deve ser um divisor de a e y um divisor de b.

Um trabalho futuro para este texto seria estudar de forma aprofundada a aritmética modular em $\mathbb{Z}[i]$ e verificar se é possível fazer uso da função ϕ de Euler para resolver potências grandes de Inteiros de Gauss.

Outro trabalho futuro para este texto é verificar se é possível escrever uma fórmula que quantifique o número de divisores que um inteiro gaussiano não nulo possui.

Consideramos este material como um excelente texto introdutório à este assunto, pois além de apresentarmos vários exemplos e exercícios, apresentamos a fundamentação teórica de cada tópico aqui estudado.

Capítulo 5

Atividades e soluções

5.1 Exercícios Propostos

Exercício 1) $1 + i$ divide 2?

Exercício 2) Encontre todos os divisores de $9 + 3i$ em $\mathbb{Z}[i]$.

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

Exercício 4) $4 + 3i$ é primo ou composto em $\mathbb{Z}[i]$?

Exercício 5) Encontre todos os divisores de $11 + 2i$ em $\mathbb{Z}[i]$ e depois selecione apenas os divisores primos.

Exercício 6) Determine o quociente e o resto para a divisão entre $26 + 72i$ e $3 + 41i$.

Exercício 7) Encontre o $mdc(18 - i, 11 + 7i)$.

Exercício 8) Escreva 50 como produto de primos em $\mathbb{Z}[i]$.

Exercício 9) Resolva a equação diofantina $y^3 = x^2 + 4$.

Exercício 10) Resolva a equação diofantina $y^3 = x^2 + 9$.

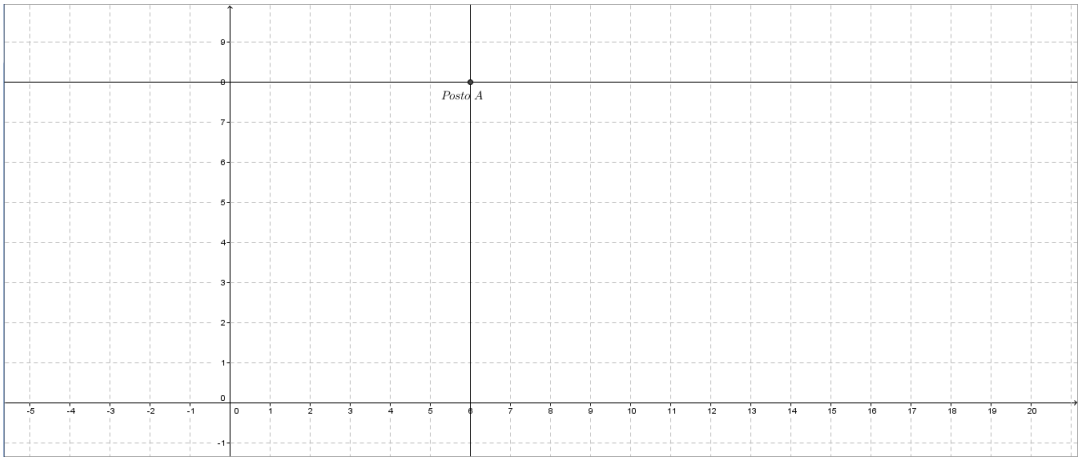
Exercício 11) Encontre a fatoração em primos de $7 + 4i$ em $\mathbb{Z}[i]$ pelo método 1.

Exercício 12) Encontre as fatoração em primos de $11 + 2i$ em $\mathbb{Z}[i]$ pelo método 2.

Exercício 13) Utilize o algoritmo de Euclides para calcular o mdc de $5 + 12i$ e $7 - 10i$ em $\mathbb{Z}[i]$. Em seguida, expresse este mdc como combinação linear destes dois números.

Exercício 14) Encontre os 29 primeiros Ternos Pitagóricos Primitivos através da teoria dos inteiros gaussianos.

Exercício 15) Em uma gincana recebes uma tarefa em que o objetivo é chegar ao posto A, partindo do ponto inicial (0,0), mas para isto deves passar por postos intermediários onde receberás senhas. Os pontos intermediários são determinados pelos divisores primos do correspondente inteiro de Gauss associado ao posto A. Marque no mapa abaixo os postos onde deves passar.



Exercício 16) Mostre que se z é primo em $\mathbb{Z}[i]$, então o seu conjugado também é primo em $\mathbb{Z}[i]$.

Exercício 17) Prove que todo número primo $p = 4n + 3$ é primo em $\mathbb{Z}[i]$.

Exercício 18) Sejam z e w $\in \mathbb{Z}[i]$. Mostre que se $z|w$ então $\mathcal{N}(z)|\mathcal{N}(w)$.

Exercício 19) Se f e g são inteiros que são soma de dois quadrados, então o produto $f.g$ também é soma de dois quadrados.

5.2 Solução das atividades

Exercício 1)

Solução 1: Se $(1+i)|2$, então existe um inteiro gaussiano $\gamma = c + di$, tal que a expressão $2 = (1+i)(c+di) = c + di + ic - d = (c-d) + (d+c)i$ tenha soluções inteiras. Isto equivale a resolver o sistema:

$$\begin{cases} 2 = c - d \\ 0 = d + c \end{cases}$$

A solução deste sistema é $c = 1$ e $d = -1$. Como a solução é inteira, então $(1+i)|2$.

Solução 2: Queremos encontrar os inteiros gaussianos α, tal que $\alpha|2$. Se $\alpha|2$ então existirá um inteiro gaussiano γ tal que $2 = \alpha\gamma$. Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(2) = \mathcal{N}(\alpha\gamma) \Leftrightarrow 4 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar o comportamento apenas de α e sabendo que a Norma de um inteiro gaussiano é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = 1 \Leftrightarrow \alpha = \pm 1 \; ou \; \alpha = \pm i$
- $\mathcal{N}(\alpha) = 2 \Leftrightarrow \alpha = \pm 1 \pm i$
- $\mathcal{N}(\alpha) = 4 \Leftrightarrow \alpha = \pm 2 \; ou \; \pm 2i$.

Logo os divisores de 2 em $\mathbb{Z}[i]$ são:

$$\{1, -1, i, -i, \mathbf{1+i}, 1-i, -1+i, -1-i, 2, -2, 2i, -2i\}$$

e, portanto $(1+i)|2$.

Exercício 2) Queremos encontrar os inteiros gaussianos α, tal que $\alpha|(9+3i)$. Se $\alpha|(9+3i)$ então existirá um inteiro gaussiano γ tal que $(9+3i) = \alpha\gamma$. Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(9+3i) = \mathcal{N}(\alpha\gamma) \Leftrightarrow 90 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar o comportamento apenas de α e sabendo que a Norma de um inteiro gaussiano

é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = 1 \Leftrightarrow \alpha = \pm 1 \; ou \; \alpha = \pm i$;
- $\mathcal{N}(\alpha) = 2 \Leftrightarrow \alpha = \pm 1 \pm i$;
- $\mathcal{N}(\alpha) = 3 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 5 \Leftrightarrow \alpha = \pm 2 \pm i \; ou \; \pm 1 \pm 2i$;
- $\mathcal{N}(\alpha) = 6 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 9 \Leftrightarrow \alpha = \pm 3 \; ou \; \pm 3i$;
- $\mathcal{N}(\alpha) = 10 \Leftrightarrow \alpha = \pm 3 \pm i \; ou \; \pm 1 \pm 3i$;
- $\mathcal{N}(\alpha) = 15 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 18 \Leftrightarrow \alpha = \pm 3 \pm 3i$;
- $\mathcal{N}(\alpha) = 30 \Rightarrow \alpha \notin \mathbb{Z}[i]$;
- $\mathcal{N}(\alpha) = 45 \Leftrightarrow \alpha = \pm 6 \pm 3i \; ou \; \pm 3 \pm 6i$;
- $\mathcal{N}(\alpha) = 90 \Leftrightarrow \alpha = \pm 3 \pm 9i \; ou \; \alpha = \pm 9 \pm 3i$

Logo os divisores de $9 + 3i$ em $\mathbb{Z}[i]$ são:

$$\{i, 1+i, 1+2i, 2+i, 3, 3+i, 3-i, 3+3i, 6+3i, 6-3i, 9+3i, 9-3i\}$$

e suas multiplicações pelas unidades.

Exercício 3) Note que $\mathcal{N}(3 + 8i) = 9 + 64 = 73$. 73 é primo e $73 \equiv 1(mod(4))$. Desta forma, pelo **Teorema 2.8.8** $3 + 8i$ é primo.

Exercício 4) Note que $\mathcal{N}(4 + 3i) = 16 + 9 = 25$. Note que $25 \equiv 1(mod(4))$, mas 25 não é primo. Logo, por este caminho nada podemos afirmar. A ideia aqui é encontrar todos os divisores de $4 + 3i$ e verificar se são divisores triviais.
Então, queremos encontrar os inteiros gaussianos α, tal que $\alpha|(4 + 3i)$ e verificar se estes divisores são triviais. Se $\alpha|(4+3i)$ então existirá um inteiro gaussiano γ tal que $4+3i = \alpha\gamma$.

Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(4+3i) = \mathcal{N}(\alpha\gamma) \Leftrightarrow 25 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar apenas o comportamento de α e sabendo que a Norma de um inteiro gaussiano é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = 1 \Leftrightarrow \alpha = \pm 1 \; ou \; \alpha = \pm i$
- $\mathcal{N}(\alpha) = 5 \Leftrightarrow \alpha = \pm 1 \pm 2i \; ou \; \alpha = \pm 2 \pm i$
- $\mathcal{N}(\alpha) = 25 \Leftrightarrow \alpha = \pm 5 \; , \alpha = \pm 5i, \; , \; \alpha = \pm 3 \pm 4i, \; \alpha = \pm 4 \pm 3i.$

Logo os divisores de $4+3i$ em $\mathbb{Z}[i]$ são:

$$\{1, 1+2i, 1-2i, 5, 4+3i, 4-3i\}$$

e suas multiplicações pelas unidades.
Como existem divisores não triviais de $4+3i$, concluímos que este número é composto em $\mathbb{Z}[i]$.

Exercício 5) Queremos encontrar os inteiros gaussianos $\alpha = a + bi$, tal que $\alpha|(11+2i)$ e selecionar destes apenas os primos. Se $\alpha|(11+2i)$ então existirá um inteiro gaussiano γ tal que $11+2i = \alpha\gamma$. Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(11+2i) = \mathcal{N}(\alpha)\mathcal{N}(\gamma) \Leftrightarrow 125 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar apenas o comportamento de α e sabendo que a Norma de um inteiro gaussiano é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = a^2 + b^2 = 1 \Leftrightarrow \alpha = \pm 1 \; ou \; \alpha = \pm i$
- $\mathcal{N}(\alpha) = 5 \Leftrightarrow \alpha = \pm 1 \pm 2i \; ou \; \alpha = \pm 2 \pm i$
- $\mathcal{N}(\alpha) = 25 \Leftrightarrow \alpha = \pm 5 \; ou \; \pm 5i \; ou \; \pm 3 \pm 4i \; ou \; \pm 4 \pm 3i;$
- $\mathcal{N}(\alpha) = 125 \Leftrightarrow \alpha = \pm 11 \pm 2i \; ou \; \alpha = \pm 2 \pm 11i$

Logo os divisores de $11+2i$ em $\mathbb{Z}[i]$ são:

$$\{1, 1+2i, 5, 3+4i, 11+2i\}$$

e suas multiplicações pelas unidades.

Deste conjunto de divisores, observamos que os únicos primos são $1+2i$ e suas multiplicações pelas unidades, pois $\mathcal{N}(\pm 1 \pm 2i) = \mathcal{N}(\pm 2 \pm i) = 5$.

Exercício 6) Inicialmente faremos a divisão usual dos números complexos.

$$\frac{\alpha}{\beta} = \frac{26+72i}{3+41i} = \frac{26+72i}{3+41i}\frac{(3-41i)}{(3-41i)} = \frac{78-1066i+216i-2952i^2}{9-1681i^2} =$$

$$= \frac{78+2952-850i}{9+1681} = \frac{3030-850i}{1690} = \frac{3030}{1690} - \frac{850}{1690}i.$$

Observe que $\dfrac{3030}{1690}$ e $-\dfrac{850}{1690}$ não são inteiros, logo precisamos encontrar os inteiros m e n mais próximos destas racionais.

Para isto, realizaremos a divisão dos racionais e tomaremos o inteiro mais próximo, isto é:

$$\frac{3030}{1690} \approx 1,792 \quad e \quad -\frac{850}{1690} \approx -0,502,$$

portanto $m = 2$, $n = -1$ e $q = m + ni = 2 - i$.

Como queremos $\alpha = \beta.q + r$, logo $r = \alpha - \beta.q$ e, portanto $r = (26+72i) - (3+41i)(2-i) = -21 - 7i$

Concluímos assim que $(26+72i) = (3+41i)(2-i) + (-21-7i)$, ou seja, $q = 2-i$ e $r = -21-7i$.

Exercício 7) Para resolver este exercício, vamos utilizar o algoritmo de Euclides.

Inicialmente vamos dividir $18-i$ por $11+7i$.

Fazendo a divisão de $18-i$ por $11+7i$, obtemos $q = 1-i$ e $r = 3i$. Fazendo a divisão de $11+7i$ por $3i$, obtemos $q = 2-4i$ e $r = -1+i$.

Fazendo a divisão de $3i$ por $-1+i$, obtemos:

- $q = 1-i$, $r = i$ e, portanto $\text{mdc}(18-i, 11+7i) = i$;
- $q = 1-2i$, $r = -1$ e, portanto $\text{mdc}(18-i, 11+7i) = -1$;
- $q = 2-i$, $r = 1$ e, portanto $\text{mdc}(18-i, 11+7i) = 1$
- $q = 2-2i$, $r = -i$ e, portanto $\text{mdc}(18-i, 11+7i) = -i$.

Concluímos assim que $18 - i$ e $11 + 7i$ são primos entre si.

Exercício 8) Note que $50 = 2.5.5 = 2.5^2$. Como $2 = (1+i)(1-i)$, $5 = (2+i)(2-i)$ e que $1 \pm i$, $2 \pm i$ são primos em $\mathbb{Z}[i]$, temos que a fatoração de 50 em primos nos inteiros gaussianos é

$$50 = 2.5.5 = 2.5^2 = (1+i)(1-i)((2+i)(2-i))^2 = (1+i)(1-i)(2+i)^2(2-i)^2.$$

Exercício 9) Exemplo 3.3.3.

Exercício 10) Utilizando o **Teorema 3.3.2.** obtemos que $b = 3 = 3m^2n - n^3 = n(3m^2 - n^2) \Leftrightarrow \dfrac{3}{n} = 3m^2 - n^2$. Como m, n são inteiros, temos que a equação terá sentido se $n = \pm 1$ ou $n = \pm 3$.
Logo

- Se $n = 1$ então $3 = 3m^2 - 1 \Leftrightarrow 3m^2 = 4$, ou seja m não será inteiro;
- Se $n = -1$ então $-3 = 3m^2 - 1 \Leftrightarrow 3m^2 = -2$, ou seja m não será inteiro;
- Se $n = 3$ então $1 = 3m^2 - 9 \Leftrightarrow 3m^2 = 10$, ou seja, m não será inteiro;
- Se $n = -3$ então $-1 = 3m^2 - 9 \Leftrightarrow 3m^2 = 8$, ou seja m não será inteiro.

Concluímos assim que a equação $y^3 = x^2 + 9$ não possui soluções inteiras!

Exercício 11) Inicialmente note que $\mathcal{N}(\alpha) = 49 + 16 = 65$. Logo, α é composto em $\mathbb{Z}[i]$.
Se fizermos o mesmo procedimento dos Exemplos 2.3.5,2.3.6 e 2.3.7 veremos que os divisores de α são:

$$\{1, 1+2i, 1-2i, 2+3i, 2-3i, 7+4i, 7-4i\}$$

e suas multiplicações pelas unidades.
Note que deste divisores, são primos

$$\{1 \pm 2i, 2 \pm 3i\}$$

e suas multiplicações pelas unidades.

Escolhemos um deles e realizamos a divisão de α por este primo. Para este exercício, escolheremos $1+2i$. Logo

$$\frac{7+4i}{1+2i} = \frac{(7+4i)}{(1+2i)}\frac{(1-2i)}{(1-2i)} = \frac{15-10i}{5} = 3-2i.$$

Como $3-2i$ é primo em $\mathbb{Z}[i]$, obtemos que a fatoração de α em primos em $\mathbb{Z}[i]$ é

$$7+4i = (1+2i)(3-2i).$$

Exercício 12) É evidente que $\mathcal{N}(\beta) = 125$. A fatoração desta norma em $\mathbb{Z}$ é $125 = 5.5.5 = 5^3$. Agora, note que o primo gerado é escrito como soma de quadrados e automaticamente escrito como produtos de primos em $\mathbb{Z}[i]$, pois $5 = 1^2 + 2^2 = (1+2i)(1-2i)$. Utilizando a multiplicidade da função Norma, podemos escrever

$$\mathcal{N}(\beta) = 5.5.5 = \mathcal{N}(\gamma_1)\mathcal{N}(\gamma_2)\mathcal{N}(\gamma_3),$$

onde $\gamma_1 = 1 \pm 2i$, $\gamma_2 = 1 \pm 2i$ e $\gamma_3 = 1 \pm 2i$, ou seja β será uma das quatro possibilidades geradas acima. Fazendo os testes, obtemos

$$(1+2i)^3 = -11-2i;\ (1-2i)^3 = -11+2i;\ (1+2i)(1+2i)(1-2i) = 5+10i;$$

$$(1+2i)(1-2i)(1-2i) = 5-10i.$$

Concluímos assim que a fatoração de β em $\mathbb{Z}[i]$ em termos primos é

$$11+4i = -(1+2i)(1+2i)(1+2i) = -(1+2i)^3.$$

Exercício 13) Utilizando o algoritmo de Euclides, obtemos

Quociente	$-1+i$	$2+i$	$1+2i$	$-2+2i$
$5+12i$	$7-10i$	$2-5i$	$-2-2i$	i
Resto	$2-5i$	$-2-2i$	i	0

Concluímos assim que $\text{mdc}(5+12i, 7-10i) = i$, ou seja $5+12i$ e $7-10i$ são relativamente primos.

Agora vamos escrever i como combinação linear de $5+12i$ e $7-10i$.

Através do esquema acima, podemos escrever as seguintes equações

$$\begin{cases} 5+12i = (7-10i)(-1+i) + (2-5i) \quad (I) \\ 7-10i = (2-5i)(2+i) + (-2-2i) \quad (II) \\ 2-5i = (-2-2i)(1+2i) + i \quad (III) \end{cases}$$

Isolando i na equação (III) e aplicando as equações (II) e (I) na equação (III) obtemos

$$2-5i-(-2-2i)(1+2i) = i$$

$$2-5i-(7-10i-(2-5i)(2+i))(1+2i) = i$$

$$2-5i-(7-10i)(1+2i)+(2-5i)(2+i)(1+2i) = i$$

$$2-5i-(7-10i)(1+2i)+(2-5i)(5i) = i$$

$$(2-5i)(1+5i)-(7-10i)(1+2i) = i$$

$$(5+12i-(7-10i)(-1+i))(1+5i)-(7-10i)(1+2i) = i$$

$$(5+12i)(1+5i)-(7-10i)(-1+i)(1+5i)-(7-10i)(1+2i) = i$$

$$(5+12i)(1+5i)-(7-10i)(-6-4i)-(7-10i)(1+2i) = i$$

$$(5+12i)(1+5i)+(7-10i)(6+4i-1-2i) = i$$

$$(5+12i)(1+5i)+(7-10i)(5+2i) = i$$

Exercício 14) Utilizando o **Teorema 3.2.1.** faremos a varredura da seguinte maneira: $m > n > 0$, onde $\text{mdc}(m,n) = 1$, e m e n com paridades distintas. Iniciamos com $m = 2$, depois $m = 3$, $m = 4$,...,$m = 12$ até elencarmos 29 ternos pitagóricos. Além disso, calcularemos a área e o perímetro de cada triângulo retângulo.

m	n	$a = m^2 - n^2$	$b = 2mn$	$c = m^2 + n^2$	Área	Perímetro
2	1	3	4	5	6	12
3	2	5	12	13	30	30
4	1	15	8	17	60	40
4	3	7	24	25	84	56
5	2	21	20	29	210	70
5	4	9	40	41	180	90
6	1	35	12	37	210	84
6	5	11	60	61	330	132
7	2	45	28	53	630	126
7	4	33	56	65	924	154
7	6	13	84	85	546	182
8	1	63	16	65	504	144
8	3	55	48	73	1320	176
8	5	39	80	89	1560	208
8	7	15	112	113	840	240
9	2	77	36	85	1386	198
9	4	65	72	97	2340	234
9	8	17	144	145	1224	306
10	1	99	20	101	990	220
10	3	91	60	109	2730	260
10	7	51	140	149	3570	340
10	9	19	180	181	1710	380
11	2	117	44	125	2574	286
11	4	105	88	137	4620	330
11	6	85	132	157	5610	374
11	8	57	176	185	5016	418
11	10	21	220	221	2310	462
12	1	143	24	145	1716	312
12	5	119	120	169	7140	408

Exercício 15) Observando a figura do exercício 15, concluímos que o inteiro gaussiano em análise é $\alpha = 6 + 8i$. Queremos agora encontrar os inteiros gaussianos $\alpha = a + bi$, tal

que $\alpha|(6+8i)$ e selecionar destes apenas os primos. Se $\alpha|(6+8i)$ então existirá um inteiro gaussiano γ tal que $6+8i = \alpha\gamma$. Aplicando a função Norma nesta igualdade, obtemos que $\mathcal{N}(6+8i) = \mathcal{N}(\alpha)\mathcal{N}(\gamma) \Leftrightarrow 100 = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$. Como nos interessa estudar apenas o comportamento de α e sabendo que a Norma de um inteiro gaussiano é sempre positiva, a igualdade só é satisfeita se uma, e apenas uma das situações abaixo ocorrer:

- $\mathcal{N}(\alpha) = a^2 + b^2 = 1 \Leftrightarrow \alpha = \pm 1 \; ou \; \alpha = \pm i$;
- $\mathcal{N}(\alpha) = 2 \Leftrightarrow \alpha = \pm 1 \pm i$;
- $\mathcal{N}(\alpha) = 4 \Leftrightarrow \alpha = \pm 2 \; ou \; \alpha = \pm 2i$;
- $\mathcal{N}(\alpha) = 5 \Leftrightarrow \alpha = \pm 1 \pm 2i \; ou \; \alpha = \pm 2 \pm i$;
- $\mathcal{N}(\alpha) = 10 \Leftrightarrow \alpha = \pm 3 \pm i \; ou \; \alpha = \pm 1 \pm 3i$;
- $\mathcal{N}(\alpha) = 20 \Leftrightarrow \alpha = \pm 2 \pm 4i \; ou \; \alpha = \pm 4 \pm 2i$;
- $\mathcal{N}(\alpha) = 25 \Leftrightarrow \alpha = \pm 5 \; ou \; \pm 5i \; ou \; \pm 3 \pm 4i \; ou \; \pm 4 \pm 3i$;
- $\mathcal{N}(\alpha) = 50 \Leftrightarrow \alpha = \pm 5, \; \alpha = \pm 5i, \; \alpha = \pm 3 \pm 4i \; ou \; \alpha = \pm 4 \pm 3i$;
- $\mathcal{N}(\alpha) = 100 \Leftrightarrow \alpha = \pm 10 \; ou \; \pm 10i \; ou \; \pm 6 \pm 8i \; ou \; \pm 8 \pm 6i$;

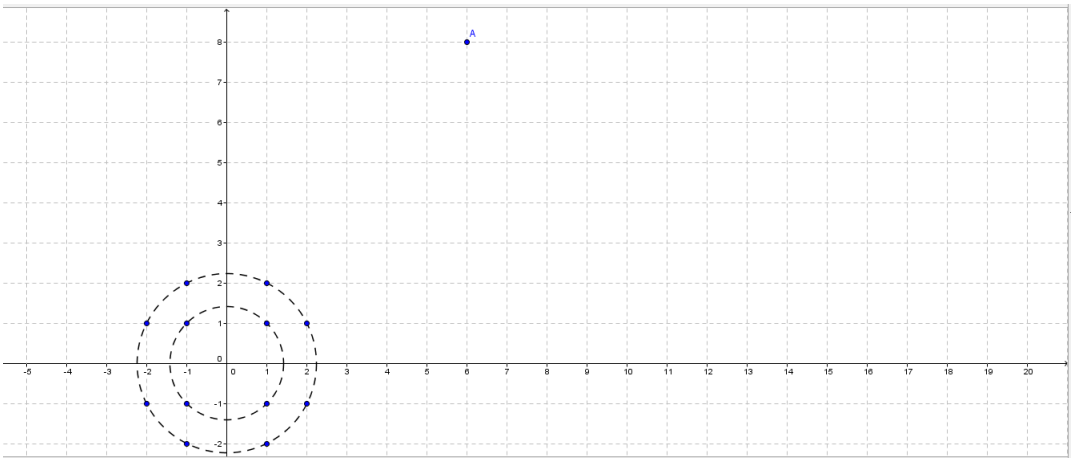
Logo os divisores de $6+8i$ em $\mathbb{Z}[i]$ são:

$$1, 2, 5, 10, 1+i, 1+2i, 1-2i, 3+i, 3-i, 2+4i, 2-4i, 3+4i,$$

$$3-4i, 5+5i, 7+i, 7-i, 6+8i, 6-8i$$

e suas multiplicações pelas unidades.
Deste conjunto de divisores, observamos que os únicos primos são $1+i, 1+2i, 1-2i$ e suas multiplicações pelas unidades, pois $\mathcal{N}(\pm 1 \pm 2i) = \mathcal{N}(\pm 2 \pm i) = 5$ e $\mathcal{N}(\pm 1 \pm i) = 2$. Observe como fica esta solução graficamente, onde os pontos em azul consistem na representação gráfica dos divisores primos de α em $\mathbb{Z}[i]$.

Exercício 16) Seja α um inteiro gaussiano primo. Logo:



$\alpha = p + 0i$, com p primo e $p \equiv 3\ (mod\ 4)$;

$\alpha = 0 + pi$ com p primo e $p \equiv 3\ (mod\ 4)$;

$\alpha = a + bi$, com $\mathcal{N}(\alpha)$ primo em $\mathbb{Z}$.

Se ocorrer a opção i) então o conjugado é $\bar{\alpha} = p$ que também é primo em $\mathbb{Z}[i]$. Se ocorrer ii) então o conjugado é $\bar{\alpha} = -pi$ que também é primo em $\mathbb{Z}[i]$. Se ocorrer iii) então o conjugado é $\bar{\alpha} = a - bi$ e $\mathcal{N}(\alpha) = \mathcal{N}(\bar{\alpha})$ e, portanto $\bar{\alpha}$ também é primo em $\mathbb{Z}[i]$.

Exercício 17) Seja p um número primo, tal que $p = 4n + 3$. Podemos escrever p da seguinte maneira $p \equiv 3\ (mod\ 4)$. Desta forma, sendo p primo e $p \equiv 3\ (mod\ 4)$, então a demonstração consiste no **Corolário 2.8.5.**

Exercício 18) A solução é a demonstração da **Proposição 2.3.4.**

Exercício 19) Se f e g são escritos como soma de quadrados, então existem a,b,c,d inteiros tais que $f = a^2 + b^2$ e $g = c^2 + d^2$. Note também que $a^2 + b^2 = \mathcal{N}(a + bi)$ e $c^2 + d^2 = \mathcal{N}(c + di)$. Logo o produto de f por g é

$$f.g = (a^2 + b^2)(c^2 + b^2) = \mathcal{N}(a + bi)\mathcal{N}(c + di)$$

Usando o fato de que a função norma é multiplicativa, obtemos

$$f.g = \mathcal{N}((a+bi)(c+di)) = \mathcal{N}(ac+adi+cbi+dbi^2) = \mathcal{N}((ac-db)+(ad+cb)i) = (ac-db)^2+(ad+cb)^2$$

Portanto

$$f.g = (ac - db)^2 + (ad + cb)^2.$$

Referências Bibliográficas

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

[2] ARAUJO, Martinho C., e Nascimento, Thais S. *Propriedades dos Ternos Pitagóricos*. V Bienal de Matemática. SBM. 2010

[3] BOYER, Carl B.. *História da Matemática*. Segunda Edição. Editora Edgard Blücher. São Paulo-SP. 2001.

[4] GONÇALVES, Adilson. *Introdução a Álgebra*. Projeto Euclides. 5ª edição. Instituto de Matemática Pura e Aplicada. Rio de Janeiro-RJ. 2012.

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

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

[7] SAMPAIO, João C. V.. *Notas do Curso de Estruturas Algébricas*. Disponível no Site: http://www.dm.ufscar.br/ sampaio/algebra.html. UFSCar. 2013.

[8] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. Coleção Matemática Universitária. Instituto de Matemática Pura e Aplicada. 1998.

[9] GARCIA, Arnaldo & Lequian, Yves. *Elementos de Álgebra*. Sexta edição. Rio de Janeiro: IMPA. 2011.

[11] FARIAS, Jessé Garcia. *Caracterização de inteiros que são Soma de dois quadrados*. Monografia de Graduação. Licenciatura Plena em Matemática. Universidade do Estado de Mato Grosso. Cáceres. 2006.

[11] FARIAS, Jessé Garcia. *Algumas propriedades de ternos quase pitagóricos*. Tese de Mestrado. Mestrado Profissional em Matemática. Universidade Federal de Mato Grosso. Cuiabá. 2014.

[12] LIMA, Elon Lages; CARVALHO, Paulo César Pinto; WAGNER, Eduardo; MORGADO, Augusto César. *A Matemática do Ensino Médio*. Volume 3. Sexta Edição. Rio de Janeiro: IMPA. 2006.

[13] PISSINI, M. M. & MAIOCHI, M. A. *Monografia 2: Inteiros de Gauss*. Trabalho de disciplina MA 148. Graduação em Matemática. Universidade Estadual de Campinas. Campinas. 2013.

[14] CONRAD, Kate (2013). *The Gaussian Integers*. Disponível em $< http : //www.math.uconn.edu/\ kconrad/blurbs/ugradnumthy/Zinotes.pdf >$. Acesso em 10 de novembro de 2013.

[15] KILLHIAN, K. *O algoritmo de Euclides para determinação do MDC*. Disponível em $< http : //obaricentrodamente.blogspot.com.br/2012/08/o - algoritmo - de - euclides - para.html >$. Acesso em 12 de novembro de 2013. 2012.

[16] Autor desconhecido. *Os inteiros de Gauss*. Disponível em $< http : //www.mtm.ufsc.br/jane/acap2/cap2.htm >$. Acesso em 10 de agosto de 2013.

[17] FUJIWARA, G (2011). *Os Inteiros de Gauss e inteiros de Eisenstein*. Disponível em $< www.obm.org.br/export/sites/default/revistaeureka/docs/... /gauss.doc >$. Acesso em 12 de novembro de 2013.

[18] COUTINHO, Severino Collier (2011). *Números Inteiros e Criptografia RSA*. Primeira edição. Rio de Janeiro: IMPA.