UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro - SP

Gabrielle Eduarda Perissotto

O Algoritmo RSA e o Algoritmo RSA nos Inteiros Gaussianos

Rio Claro - SP

2020

UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro - SP

O Algoritmo RSA e o Algoritmo RSA nos Inteiros Gaussianos

Gabrielle Eduarda Perissotto

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Rio Claro - SP.

Orientadora
Profa. Dra. Carina Alves Severo

Rio Claro - SP
2020

P446a

Perissotto, Gabrielle Eduarda
O Algoritmo RSA e o Algoritmo RSA nos Inteiros Gaussianos / Gabrielle Eduarda Perissotto. -- Rio Claro, 2020
82 p. : il., tabs.

Dissertação (mestrado profissional) - Universidade Estadual Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio Claro
Orientadora: Carina Alves Severo

1. Álgebra. 2. Criptografia. 3. Teoria dos números. 4. Números primos. 5. Numeros complexos. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

Gabrielle Eduarda Perissotto

O ALGORITMO RSA E O ALGORITMO RSA NOS INTEIROS GAUSSIANOS

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves Severo
Orientadora

Prof. Dr. Wladimir Seixas
Departamento de Matemática - UFSCar (São Carlos)

Profa. Dra. Cintya Wink de Oliveira Benedito
Engenharia de Telecomunicações - UNESP (São João da Boa Vista)

Rio Claro - SP, 27 de novembro de 2020

Aos meus pais:
Gislene e José.

Agradecimentos

A Deus, por me permitir chegar até aqui, com sabedoria e perseverança, guiando sempre meus passos.

A minha família, meu pai José, minha mãe Gislene e meu irmão Eduardo, por todo suporte e apoio necessário. Obrigada por todo incentivo aos estudos e por darem condições para que isso fosse possível.

Aos meus professores, que compartilharam seus conhecimentos da melhor maneira e me inspiraram. Em especial, a minha orientadora, Prof. Dr. Carina Alves Severo, pela competência e seriedade na orientação deste estudo. Obrigada pelo seu empenho, por cada ensinamento e ajuda.

Aos membros da banca examinadora, tanto de qualificação como de defesa deste trabalho, minha gratidão pela dedicação na leitura deste e pelas sugestões, as quais contribuíram para a melhoria do mesmo.

Aos meus amigos, por tornarem essa caminhada mais leve. Em particular, Fernando, por sempre estar ao meu lado e não me deixar desistir e Carla, por todo companheirismo e palavras de apoio. Obrigada!

Não é o conhecimento, mas o ato de aprender,
não a posse mas o ato de chegar lá,
que concede a maior satisfação.
Carl Friedrich Gauss.

Resumo

O objetivo deste trabalho é apresentar uma extensão do algoritmo RSA, originalmente desenvolvido para os números inteiros, para o conjunto dos inteiros gaussianos. Para atingir este propósito, o estudo da teoria por trás dos inteiros gaussianos torna-se necessária, a fim de garantir que todas as propriedades sejam preservadas e para que a construção do algoritmo seja possível.

Palavras-chave: Criptografia, Inteiros Gaussianos, Teoria dos Números, Números Primos.

Abstract

The aim of this work is to present an extension of the RSA algorithm, originally developed for integers, for Gaussian integers. To achieve this purpose, the study of the theory behind of Gaussian integers sets becomes necessary, in order to ensure that all properties are preserved and that the construction of the algorithm is possible.

Keywords: Cryptography, Gaussian Integers, Number Theory, Prime Numbers.

Lista de Figuras

Sumário

Introdução

A criptografia é a ciência de escrever mensagens em *cifras*, estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos", que todos já praticamos quando criança. O mais simples deste método consiste em substituir uma letra pela seguinte; isto é, transladar o alfabeto uma casa para diante. Naturalmente todo código vem acompanhado de duas receitas: uma para codificar uma mensagem; outra para decodificar uma mensagem codificada. Decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Já decifrar significa ler uma mensagem codificada sem ser um usuário legítimo. Portanto, para decifrar é preciso "quebrar" o código. Porém, os primeiros códigos criados padeciam de um grande mal: eram muito fáceis de decifrar.

Hoje em dia, a comunicação entre computadores pela *Internet* vem criando novos desafios para a criptografia. Como é relativamente fácil interceptar mensagens enviadas por linha telefônica, torna-se necessário codificá-las, sempre que contenham informações sensíveis. Isto inclui transações bancárias ou comerciais, ou até mesmo uma compra feita com cartão de crédito. Assim, tornou-se necessário inventar novos códigos, que fossem difíceis de decifrar; mesmo com a ajuda de um computador. Estes códigos foram criados para o uso em aplicações comerciais e são todos de *chave pública*. Em um código como esse, saber codificar não implica saber decodificar. Neste trabalho veremos que "desfazer" o processo de codificação pode não ser tão simples quanto parece.

O mais conhecido dos métodos de criptografia de chave pública é o RSA. Há vários outros códigos de chave pública, mas esse é, atualmente, o mais usado em aplicações comerciais (COUTINHO, 2011). A descrição completa do método RSA só será possível depois do estudo de toda teoria matemática que o envolve. Desse modo, no Capítulo 1 abordaremos os principais resultados sobre os números inteiros, necessários para o desenvolvimento passo a passo do algoritmo RSA, o qual será apresentado no Capítulo 3.

Com o objetivo de tornar o algoritmo RSA mais eficiente, neste trabalho apresentaremos uma extensão do método de criptografia RSA, inicialmente feito com os números inteiros, para os inteiros de Gauss. Gauss fez a extensão das propriedades de $\mathbb{Z}$ para $\mathbb{Z}[i]$, o anel

formado pelos números complexos da forma $a + bi$, onde a e b pertence a $\mathbb{Z}$ e $i^2 = -1$, e percebeu que grande parte da Teoria de Euclides poderia ser transportada para $\mathbb{Z}[i]$, o que consequentemente trouxe diversas contribuições para a Teoria dos Números. Assim, no Capítulo 2 faremos um estudo das principais definições, teoremas e propriedades sobre $\mathbb{Z}[i]$, para finalmente, no Capítulo 4, desenvolver todos as etapas do algoritmo RSA nos Inteiros Gaussianos. Todas as figuras deste trabalho foram confeccionadas utilizando o software livre *Geogebra*.

1 Os Números Inteiros

No conjunto dos números naturais, $\mathbb{N} := \{0, 1, 2, 3, \cdots\}$, a operação de subtração entre a e b só está definida se $a \geq b$. Porém existem questões envolvendo essa operação em que $b > a$, por exemplo, relacionadas a gastar mais do que se tem. Com apenas R$\$10,00$, adquirindo um produto no valor de R$\$15,00$, como podemos expressar essa dívida? Ou seja, a subtração entre 10 e 15? Para enfrentar essas questões, foi preciso ampliar o conjunto dos números naturais, com adjunção de novos números, os números inteiros negativos, introduzidos a princípio para possibilitar uma resposta a uma subtração qualquer de dois elementos de $\mathbb{N}$. Esse passo gerou naturalmente a necessidade de estender as operações e a relação de ordem de $\mathbb{N}$ a um novo conjunto, formado pelos números naturais e os números negativos, a saber: o conjunto dos números inteiros, denotado por $\mathbb{Z} := \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$.

Neste capítulo apresentamos algumas definições, propriedades e teoremas que estão relacionados com a aritmética dos inteiros, que serão ferramentas necessárias para o desenvolvimento do Capítulo 3. As principais referências utilizadas neste capítulo foram [1, 2, 3, 4, 5].

1.1 Operações em $\mathbb{Z}$

No conjunto $\mathbb{Z}$ estão definidas as operações de soma e produto

$$\begin{array}{rccc} +: & \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ & (x, y) & \mapsto & x + y \end{array} \qquad \text{e} \qquad \begin{array}{rccc} \cdot: & \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ & (x, y) & \mapsto & x.y \end{array}$$

as quais satisfazem os seguintes axiomas. Para todo x, y, z pertencentes a $\mathbb{Z}$:

A1) $(x + y) + z = x + (y + z)$ (associatividade da soma);

A2) Existe $0 \in \mathbb{Z}$ tal que $x + 0 = 0 + x = x$ (existência do elemento neutro);

A3) Existe $-x \in \mathbb{Z}$ tal que $x + (-x) = (-x) + x = 0$ (existência de inverso aditivo (ou oposto) de cada $x \in \mathbb{Z}$);

A4) $x + y = y + x$ (comutatividade da soma);

M1) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associatividade do produto);

M2) Existe $1 \in \mathbb{Z}$ tal que $x \cdot 1 = 1 \cdot x = x$ (existência da unidade em $\mathbb{Z}$);

M3) $x \cdot y = y \cdot x$ (comutatividade do produto);

D) $x \cdot (y + z) = x \cdot y + x \cdot z$ (distributividade do produto em relação à soma).

Observação 1.1. Dado $x \in \mathbb{Z}$, o axioma A3) garante a existência de um oposto para x com respeito à adição, denotado por $-x$.

Definição 1.2 (Subtração em $\mathbb{Z}$)**.** *Chama-se diferença de dois inteiros x e y à soma $x+(-y)$. A subtração em $\mathbb{Z}$ é a operação $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, que associa cada par ordenado (x, y) à diferença $x - y$.*

Teorema 1.3. *Para cada x, y, z em $\mathbb{Z}$, valem as propriedades:*

1. $x + y = x \Rightarrow y = 0$ *(ou seja, 0 é o único elemento neutro da adição em $\mathbb{Z}$);*
2. $x + y = 0 \Rightarrow y = -x$ *(ou seja, o oposto de um elemento x é único);*
3. $x + y = x + z \Rightarrow y = z$ *(lei do cancelamento da adição);*
4. $-(-x) = x$*;*
5. $-(x + y) = (-x) + (-y) = -x - y$*;*
6. $x \cdot 0 = 0$*;*
7. $(-x)y = -(xy)$*;*
8. $(-x)(-y) = xy$*;*
9. $(x - y)z = xz - yz$.

Observação 1.4. Os axiomas listados (A1, A2, A3, A4, M1, ...) ainda não são suficientes para caracterizar o conjunto $\mathbb{Z}$ de maneira única. Isto significa que existem outras estruturas algébricas familiares que também satisfazem às propriedades acima. Para caracterizar o conjunto dos números inteiros é introduzida uma relação de ordem $\leq$. Para maiores detalhes a referência [6] pode ser consultada.

1.2 Divisibilidade em $\mathbb{Z}$

O conjunto dos números inteiros é munido de diversas propriedades e definições, porém, apresentaremos apenas algumas, as quais são essenciais para o desenvolvimento deste trabalho.

Esta seção contém os principais algoritmos utilizados para estudar o sistema de criptografia RSA.

Definição 1.5. *Dados $a, b \in \mathbb{Z}$, com $a \neq 0$, dizemos que a divide b, e escrevemos $a \mid b$, se existir $k \in \mathbb{Z}$ tal que $b = ak$. Caso a não divida b, escrevemos $a \nmid b$.*

Seja a um inteiro não nulo. Se a dividir b, dizemos que a é um divisor de b, que b é divisível por a ou ainda que b é um múltiplo de a. Se $a \mid b$ e $a > 0$, então a é um divisor positivo de b. Notemos que todo inteiro não nulo é um divisor de si mesmo e de 0.

Exemplo 1.6. $4 \mid 28$ pois existe um inteiro $k = 7$ tal que $28 = 4 \cdot 7$.

Exemplo 1.7. $7 \nmid 12$ pois não existe um inteiro k tal que $12 = 7 \cdot k$.

Proposição 1.8. *Se a, b e c são inteiros, tais que $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Sejam a, b e c inteiros. Como $a \mid b$ e $b \mid c$, existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = bk_2$. Logo, $c = (ak_1)k_2 = a(k_1k_2)$ e portanto, $a \mid c$. □

Exemplo 1.9. Como $2 \mid 8$ e $8 \mid 16$, então $2 \mid 16$.

Proposição 1.10. *Se a, b e c são inteiros, tais que $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, para quaisquer $m, n \in \mathbb{Z}$.*

Demonstração. Sejam a, b e c inteiros. Como $a|b$ e $a|c$, existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = ak_2$. Multiplicando ambas as equações respectivamente por m e n obtemos $mb = mak_1$ e $nc = nak_2$. Logo, $mb + nc = mak_1 + nak_2 = a(mk_1 + nk_2)$. Portanto, $a \mid (mb + nc)$. □

Exemplo 1.11. Como $4 \mid 8$ e $4 \mid 16$, então $4 \mid (5 \cdot 8 + (-1) \cdot 16)$. Logo $4 \mid 24$.

Teorema 1.12. *(Algoritmo da Divisão em $\mathbb{Z}$) Dados $a, b \in \mathbb{Z}, b > 0$, existe um único par de inteiros q e r que satisfazem*

$$a = q \cdot b + r, \text{ com } 0 \leq r < b.$$

Demonstração. Seja b um número inteiro positivo não nulo. Se a pertence a $\mathbb{Z}$, então a é múltiplo de b ou está situado entre dois múltiplos consecutivos de b, isto é, $qb \leq a < (q+1)b$. Somando $-qb$ em todos os termos dessa desigualdade obtemos:

$$qb - qb \leq a - qb < qb + b - qb \Rightarrow$$
$$0 \leq a - qb < b.$$

Desta forma, tomando $r = a - qb$, segue que $a = qb + r$, em que $0 \leq r < b$.

Suponhamos agora, que existam inteiros q_1, q_2, r_1, r_2 , onde $q_1 \neq q_2$ e $r_1 \neq r_2$ e que satisfaçam às igualdades: $a = q_1 b + r_1$, com $0 \leq r_1 < b$ e $a = q_2 b + r_2$, com $0 \leq r_2 < b$. Se $b > r_1$ e $b > r_2$, então $b > r_2 - r_1$ e $a = bq_1 + r_1 = bq_2 + r_2$. Dessa forma, $b(q_2 - q_1) = r_1 - r_2$. Tomando $k = (q_2 - q_1)$, segue que $r_1 - r_2 = kb$, com k pertencente em $\mathbb{Z}$ e então $b \mid (r_1 - r_2)$. Portanto $b \leq (r_1 - r_2)$, o que é um absurdo, pois contradiz a hipótese. Logo, $r_1 = r_2$. Concluímos que $(q_2 - q_1)b = 0$. Sendo $b \neq 0$, temos que $(q_2 - q_1) = 0$ e portanto $q_2 = q_1$. □

Na equação $a = q \cdot b + r$, com $0 \leq r < b$, os inteiros, q e r são chamados respectivamente de *quociente* e *resto* da divisão de a por b. Vale lembrar que b somente é divisor de a se $r = 0$. Neste caso, temos que $a = bq$ e o quociente q na divisão exata de a por b pode ser indicado também por $\frac{a}{b}$ ou a/b.

Exemplo 1.13. Sabe-se que na divisão de 326 por $b > 0$, o quociente é 14 e o resto é r. Vejamos como determinar os possíveis valores de b e r.

Sabemos que $a = qb + r, 0 \leq r < b$. Assim, substituindo os valores dados, obtemos:

$$326 = 14b + r, 0 \leq r < b \Rightarrow r = 326 - 14b.$$

Logo,

$$0 \leq r < b \Rightarrow 0 \leq 326 - 14b < b.$$

Resolvendo essa desigualdade temos:

$$\begin{cases} 0 \leq 326 - 14b \Rightarrow b \leq \frac{326}{14}; \\ 326 - 14b < b \Rightarrow b > \frac{326}{15}. \end{cases}$$

Dessa forma, os possíveis valores para b e r são:

$$\begin{cases} b = 22 \quad e \quad r = 18 \\ \text{ou} \\ b = 23 \quad e \quad r = 4. \end{cases}$$

Exemplo 1.14. Sejam $n > m$ inteiros positivos. Se o resto da divisão de n por m é r, então o resto da divisão de $2^n - 1$ por $2^m - 1$ é $2^r - 1$. De fato, podemos escrever n como

$$n = mq + r,$$

sendo q um número inteiro positivo. Vamos mostrar que existe um inteiro q' tal que $0 \leq 2^r - 1 < 2^m - 1$ e $2^n - 1 = (2^m - 1)q' + 2^r - 1$. Note que

$$0 \leq r < m \Rightarrow 2^0 \leq 2^r < 2^m \Rightarrow 0 \leq 2^r - 1 < 2^m - 1.$$

Mostremos, agora, que q' é um número inteiro. Como

$$2^n - 1 = (2^m - 1)q' + 2^r - 1 \iff q' = \frac{(2^n - 1) - (2^r - 1)}{2^m - 1} \iff q' = \frac{2^n - 2^r}{2^m - 1},$$

segue que $2^n - 2^r = 2^r(2^{n-r} - 1) = 2^r(2^{mq} - 1)$. Mas, $2^{mq} - 1 = (2^m - 1)(2^{mq-1} + \cdots + 1)$ e assim,

$$q' = \frac{2^r(2^m - 1)(2^{mq-1} + \cdots + 1)}{2^m - 1} = 2^r(2^{mq-1} + \cdots + 1).$$

Portanto, q' é um número inteiro, concluindo a nossa afirmação.[1]

1.3 Máximo Divisor Comum

Quando falamos em máximo divisor comum de dois números inteiros, estamos interessados em encontrar o maior inteiro que divide esses dois números. Por exemplo, sabemos que o número inteiro 8 divide 24 e também divide 32 e, além disso, como podemos verificar, 8 é o maior número inteiro positivo com essa propriedade. Sendo assim, dizemos, que 8 é o máximo divisor comum de 24 e 32, podendo ser denotado por $(24, 32) = 8$ ou $mdc(24, 32) = 8$, isto nos leva a seguinte definição.

Definição 1.15. *O máximo divisor comum* (mdc) *de dois inteiros* a *e* b *(*a *e* b *diferentes de zero), denotado por* $mdc(a, b)$ *ou* (a, b)*, é o maior inteiro que divide* a *e* b*. Sendo assim, o* $mdc(a, b)$ *é o inteiro positivo* d *que satisfaz às condições:*

1. $d \mid a$ *e* $d \mid b$*;*
2. *se* $c \mid a$ *e* $c \mid b$*, então* $c \mid d$*.*

Pela condição 1 da Definição 1.15, d é um divisor comum de a e b, e pela condição 2, d é o maior dentre todos os divisores comuns de a e b.

Exemplo 1.16. Sejam $a = 12$ e $b = 54$. Vamos determinar $mdc(12, 54)$.

O conjunto dos divisores de $a = 12$ e de $b = 54$, os quais denotamos por D_{12} e D_{54}, são: $D_{12} = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ e $D_{54} = \{\pm1, \pm2, \pm3, \pm6, \pm9, \pm18, \pm27, \pm54\}$. Como $mdc(12, 54)$ é o maior inteiro que divide 12 e 54, para encontrar o máximo divisor comum entre estes números, basta determinar a intersecção $D_{12} \cap D_{54}$ e tomar o maior número em módulo desse conjunto. Logo, $D_{12,54} = D_{12} \cap D_{54} = \{\pm1, \pm2, \pm3, \pm6\}$, que tem máximo igual a 6, que é o $mdc(12, 54)$.

[1] Para a realização desse exemplo, foi utilizado a operação de potenciação e suas propriedades, para todo a, n e m em $\mathbb{Z}$:
i) $a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ vezes}}$, ii) $a^0 = 1$, iii) $a^n \cdot a^m = a^{n+m}$.

Definição 1.17. *Sejam a e b dois inteiros não nulos. Dizemos que a e b são primos entre si ou coprimos se, e somente se, $mdc(a, b) = 1$.*

Exemplo 1.18. Os inteiros 3 e 7, 9 e 11 são *primos entre si*, pois, temos:

$$mdc(3, 7) = 1 \text{ e } \ mdc(9, 11) = 1.$$

Proposição 1.19. *(Identidade de Bézout) Se $d = mdc(a, b)$, então existem n_0, $m_0 \in \mathbb{Z}$ tais que $d = n_0a + m_0b$, ou seja, d é uma combinação linear de a e b.*

Demonstração. Seja o conjunto $B = \{na + mb \mid n, m \in \mathbb{Z}\}$. Veja que $B \neq \emptyset$. Sejam n_0 e m_0 em $\mathbb{Z}$ tais que $c = n_0a + m_0b$ é o menor inteiro positivo pertencente a B, vamos provar que $c \mid a$ e $c \mid b$. Para tanto, suponhamos que $c \nmid a$.

Pelo algoritmo da divisão (Teorema 1.12), existem q e r inteiros, tais que $a = qc + r$, $0 \leq r < c$. Tomando $r = a - qc = a - q(n_0a + m_0b) = a(1 - n_0q) + b(-m_0q)$, ou seja, r é um número inteiro positivo e $r \in B$ uma vez que, $(1 - n_0q)$ e $(-m_0q) \in \mathbb{Z}$. Daí, temos que, $r \geq c$. Mas, $r < c$, o que é um absurdo. Logo, $c \mid a$. Analogamente, mostramos que $c \mid b$. Assim, c é um divisor comum, e como $d = mdc(a, b)$, temos que $c \leq d$.

Resta ainda, mostrar que $d = n_0a + m_0b$. Vejamos que, se $d = mdc(a, b)$ então $d \mid a$ e $d \mid b$, o que implica que $a = k_1d$ e $b = k_2d$ com k_1 e k_2 em $\mathbb{Z}$. Ainda, tomando $c = n_0a + m_0b = n_0(k_1d) + m_0(k_2d) = d(n_0k_1 + m_0k_2)$, resulta em $d \mid c$. Além disso, $c \neq 0$ implica $\mid d \mid \leq \mid c \mid$ e como não é possível termos $d < c$, uma vez que $d = mdc(a, b)$, então $d = c$, ou seja, $d = n_0a + m_0b$. □

Proposição 1.20. *Sejam a e b números inteiros positivos. Se existem inteiros q e r tais que $a = bq + r, 0 \leq r < b$, então $mdc(a, b) = mdc(b, r)$.*

Demonstração. Sejam

$$d_1 = mdc(a, b) \text{ e } d_2 = mdc(b, r).$$

Afirmamos que $d_1 \leq d_2$. De fato, existem inteiros positivos k_1 e k_2 tais que:

$$a = d_1k_1 \text{ e } b = d_1k_2.$$

Substituindo a e b na equação $a = bq + r$ obtemos:

$$r = d_1k_1 - d_1k_2q = d_1(k_1 - k_2q),$$

ou seja, d_1 é um divisor comum de b e r. Mas d_2 é o maior divisor de b e r e portanto, pela Proposição 1.19, $d_1 \leq d_2$ como queríamos. Seguindo um argumento semelhante, podemos provar o inverso, ou seja, $d_2 \leq d_1$, concluindo que $d_1 = d_2$. □

Teorema 1.21. *Se a e b são inteiros não nulos, então eles serão primos entre si se, e somente se, existirem inteiros x e y tais que $ax + by = 1$.*

Demonstração. ($\Rightarrow$) Se a e b são primos entre si, então $mdc(a,b) = 1$, consequentemente existem x e y tais que $ax + by = 1$.
($\Leftarrow$) Se existem inteiros x e y, tais que $ax + by = 1$ e se $mdc(a,b) = d$, então $d \mid a$ e $d \mid b$. Logo, $d \mid (ax + by)$ e como $d \mid 1$, resulta em $d = 1$, ou seja, $mdc(a,b) = 1$. □

Corolário 1.22. *Se* $mdc(a,b) = d$*, então* $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração. Vejamos que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros, pois d é um divisor comum de a e b. Sendo assim, se $mdc(a,b) = d$, então $d \mid a$, $d \mid b$ e existem inteiros x e y tais que $ax + by = d$. Logo, $\frac{a}{d}x + \frac{b}{d}y = 1$, o que nos leva a conclusão, pelo Teorema 1.21, que os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si e, portanto, $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Exemplo 1.23. Observe que $mdc(16,40) = 8$ e $mdc\left(\frac{16}{8}, \frac{40}{8}\right) = mdc(2,5) = 1$.

Corolário 1.24. *Se* $a \mid bc$ *e* $mdc(a,b) = 1$*, então* $a \mid c$.

Demonstração. Como $a \mid bc$, segue que $bc = ak$ com k inteiro e como a e b são primos entre si, $ax + by = 1$ para certos inteiros x e y. Multiplicando ambos os lados da igualdade por c temos

$$cax + cby = c.$$

Agora, $c = cax + aky = a(cx + ky)$ e, portanto, $a \mid c$. □

Um número natural d será dito mdc de dados números naturais $a_1, a_2, \ldots, a_n$ se possuir as seguintes propriedades:

i) d é um divisor comum de $a_1, a_2, \ldots, a_n$.

ii) Se c é um divisor comum de $a_1, a_2, \ldots, a_n$, então $c \mid d$.

O mdc, quando existe, é certamente único e será representado por $mdc(a_1, a_2, \ldots, a_n)$.

Proposição 1.25. *Dados números naturais* $a_1, a_2, \ldots, a_n$*, existe o seu* mdc *e*

$$mdc(a_1, a_2, \ldots, a_n) = mdc(a_1, a_2, \ldots, a_{n-2}, mdc(a_{n-1}, a_n)).$$

Demonstração. Vamos provar a proposição por indução sobre n ($n \geq 2$). Para $n = 2$, sabemos que o resultado é válido. Suponhamos que o resultado vale para n. Para provar que o resultado é válido $n + 1$, basta mostrar que

$$mdc(a_1, a_2, \ldots, a_n, a_{n+1}) = mdc(a_1, a_2, \ldots, mdc(a_n, a_{n+1})),$$

pois isso provará também a existência.

Seja $d = mdc(a_1, a_2, \ldots, mdc(a_n, a_{n+1}))$. Logo, $d \mid a_1, \ldots, d \mid mdc(a_n, a_{n+1})$. Portanto, $d \mid a_1, \ldots, d \mid a_{n-1}, d \mid a_n$ e $d \mid a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, \ldots, a_n, a_{n+1}$, teremos que c é divisor comum de $a_1, \ldots, a_{n-1}$ e $mdc(a_n, a_{n+1})$ e portanto, $c \mid d$. □

Para calcular o $mdc(a_1, \ldots, a_n)$, pode-se usar recursivamente o algoritmo de Euclides, que apresentamos na próxima seção.

1.3.1 Algoritmo de Euclides

Muito importante nas etapas de encriptação e decriptação de mensagens do sistema RSA, apresentamos a seguir o *Algoritmo de Euclides* e na seção seguinte, o *Algoritmo de Euclides estendido*.

Teorema 1.26 (Algoritmo de Euclides). *Sejam $r_0 = a$ e $r_1 = b$ inteiros não-negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_i = q_{i+1} r_{i+1} + r_{i+2}, \text{ com } 0 \leq r_{i+2} < r_{i+1},$$

para $i = 0, 1, 2, ..., n-1$ e $r_{n+1} = 0$, então $mdc(a, b) = r_n$, que é o último resto não-nulo.

Demonstração. Primeiramente, vamos dividir a por b. Assim, podemos escrever $a = bq_1 + r_2$, com q_1 e r_2 inteiros. Logo, $r_0 = qr_1 + r_2$. Em seguida, vamos dividir r_1 por r_2, e obtemos $r_1 = q_2 r_2 + r_3$. Fazemos isso sucessivamente até $r_{n+1} = 0$. Com isto, obtemos a seguinte sequência de equações

$$\begin{aligned}
a &= q_1 b + r_2, & 0 < r_2 < r_1,\\
r_1 &= q_2 r_2 + r_3, & 0 < r_3 < r_2,\\
r_2 &= q_3 r_3 + r_4, & 0 < r_4 < r_3,\\
&\vdots & \vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= q_n r_n + 0.
\end{aligned}$$

Pela Proposição 1.19, segue que o máximo divisor comum de r_n e r_{n-1} é r_n. Aplicando a Proposição 1.19 várias vezes, segue que:

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = \ldots = mdc(r_1, r_2) = mdc(r_0, r_1) = mdc(a, b).$$

Portanto, $mdc(a, b) = r_n$, que é o último resto não-nulo da sequência escrita. □

Exemplo 1.27. Utilizando o algoritmo de Euclides, vamos determinar o $mdc(894, 326)$. Sejam $r_0 = 894$ e $r_1 = 326$. Aplicando o algoritmo da divisão sucessivas vezes, obtem-se

$$
\begin{aligned}
894 &= 326 \cdot 2 + 242,\\
326 &= 242 \cdot 1 + 84,\\
242 &= 84 \cdot 2 + 74,\\
84 &= 74 \cdot 1 + 10,\\
74 &= 10 \cdot 7 + 4,\\
10 &= 4 \cdot 2 + 2,\\
4 &= 2 \cdot 2 + 0.
\end{aligned}
$$

Pelo algoritmo de Euclides, segue que $mdc(894, 326)$ é o último resto não nulo, ou seja, $mdc(894, 326) = 2$.

1.3.2 Algoritmo de Euclides estendido

O algoritmo de Euclides estendido consiste em encontrar α e β inteiros, tal que

$$\alpha a + \beta b = mdc(a, b), \text{ com } a \text{ e } b \text{ em } \mathbb{Z}.$$

Vamos supor que após o cálculo do $mdc(a, b)$, obtemos a seguinte sequência de divisões:

$$
\begin{array}{ccc}
a = bq_1 + r_1 & \text{e} & r_1 = ax_1 + by_1,\\
b = r_1q_2 + r_2 & \text{e} & r_2 = ax_2 + by_2,\\
r_1 = r_2q_3 + r_3 & \text{e} & r_3 = ax_3 + by_3,\\
r_2 = r_3q_4 + r_4 & \text{e} & r_4 = ax_4 + by_4,\\
r_3 = r_4q_5 + r_5 & \text{e} & r_5 = ax_5 + by_5,\\
\vdots & \text{e} & \vdots,\\
r_{n-3} = r_{n-2}qn - 1 + r_{n-1} & \text{e} & r_{n-1} = ax_{n-1} + by_{n-1},\\
r_{n-2} = r_{n-1}q_n & \text{e} & r_n = 0.
\end{array}
$$

Os números $x_1, \ldots, x_{n-1}$ e $y_1, \ldots, y_{n-1}$ são inteiros a determinar. Seja a seguinte tabela com essas informações:

Resto	Quociente	x	y
b	$*$	x_{-1}	y_{-1}
a	$*$	x_0	y_0
r_1	q_1	x_1	y_1
r_2	q_2	x_2	y_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-2}	q_{n-2}	x_{n-2}	y_{n-2}
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}

Consideremos a j-ésima linha e vamos dividir r_{j-2} por r_{j-1}, para encontrarmos r_j e q_j de forma que

$$r_{j-2} = r_{j-1}q_j + r_j \qquad \text{e} \qquad 0 \leq r_j < r_j - 1.$$

Assim,

$$r_j = r_{j-2} - r_{j-1}q_j.$$

Observando os valores de $x_{j-2},\ x_{j-1},\ y_{j-2}$ e y_{j-1} nas linhas $j-1$ e $j-2$, podemos escrever

$$r_{j-2} = ax_{j-2} + by_{j-2} \qquad \text{e} \qquad r_{j-1} = ax_{j-1} + by_{j-1}.$$

Desta forma,

$$\begin{aligned} r_j &= (ax_{j-2} + by_{j-2}) - (ax_{j-1} + by_{j-1})q_j \\ &= a(x_{j-2} - q_jx_{j-1}) + b(y_{j-2} - q_jy_{j-1}). \end{aligned}$$

Portanto,

$$x_j = x_{j-2} - q_jx_{j-1} \text{ e } y_j = y_{j-2} - q_jy_{j-1}.$$

Para calcularmos os valores de x_j e y_j da tabela, basta sabermos os valores das duas linhas imediatamente acima, através de um processo recursivo. Para determinarmos x e y iniciais, de modo análogo ao feito acima, devemos ter

$$a = ax_{-1} + by_{-1} \text{ e } a = ax_0 + by_0.$$

Com isto, podemos afirmar que $x_{-1} = 1, y_{-1} = 0$ e $x_0 = 1, y_0 = 0$. Assim, damos início a recursão. Como esse algoritmo nos fornece o máximo divisor comum correspondente ao resto $n-1$, segue que

$$mdc(a,b) = r_{n-1} = ax_{n-1} + by_{n-1},$$

ou seja,

$$\alpha = x_{n-1} \text{ e } \beta = y_{n-1}.$$

Exemplo 1.28. Vamos determinar $mdc(973, 101)$ e, em seguida, determinar α e β inteiros que satisfazem:

$$973\alpha + 101\beta = mdc(973, 101).$$

Para isso, utilizamos o *algoritmo de Euclides estendido*. Primeiramente, escrevemos a tabela, completando-a.

Resto	Quociente	α	β
973	$*$	1	0
101	$*$	0	1
64	9	$(1-0\cdot 9)=1$	$(0-1\cdot 9)=-9$
37	1	$(0-1\cdot 1)=-1$	$(1-(-9)\cdot 1)=10$
27	1	$(1-(-1)\cdot 1)=2$	$(-9-10\cdot 1)=-19$
10	1	$(-1-2\cdot 1)=-3$	$(10-(-19)\cdot 1)=29$
7	2	$(2-(-3)\cdot 2)=8$	$(-19-29\cdot 2)=-77$
3	1	$(-3-8\cdot 1)=-11$	$(29-(-77)\cdot 1)=106$
1	2	$(8-(-11)\cdot 2)=30$	$(-77-106\cdot 2)=-289$
0	1	$*$	$*$

Portanto, $mdc(973, 101) = 1$, $\alpha = 30$, $\beta = -289$ e

$$973 \cdot 30 + 101 \cdot (-289) = 1.$$

1.4 Números Primos

No processo de geração de chaves do método de criptografia RSA, utilizaremos o conceito de números primos. Para isso, nessa seção apresentamos os principais resultados relacionados aos números primos em $\mathbb{Z}$.

Definição 1.29. *O número $p > 1$ é um número **primo** se seus únicos divisores são ± 1 e $\pm p$.*

Qualquer número $n > 1$ tem pelo menos um divisor primo. Se n é primo, então esse divisor primo é o próprio n. De fato, se n não é primo, seja $a > 1$ seu menor divisor, $n = ab$, onde $1 < a \leqslant b$. Se a não fosse primo, então $a = a_1a_2$ com $1 < a_1 \leq a_2 < a$ e $a_1|n$, contradizendo a minimalidade de a.

Exemplo 1.30. Os menores números primos são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29,$\cdots$.

Indicamos por

$$\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ é primo}\},$$

o conjunto de todos os números primos.

Proposição 1.31. *Seja $p \in \mathbb{P}$. Então*

$$\forall a, b \in \mathbb{N}; p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b,$$

ou seja, um primo divide um produto, somente se ele divide um dos fatores.

Demonstração. Suponhamos que $p \mid ab$ e $p \nmid a$. Logo, $p \nmid a \Rightarrow mdc(p, a) = 1$, portanto, pelo Corolário 1.24, $p \mid b$. □

Um número $n > 1$ que não é primo é chamado **composto**. Se n é um número composto, então ele tem um divisor primo menor que $\sqrt{n}$. De fato, como acima, $n = ab$, onde $1 < a \leq b$ e a é o menor divisor de n. Logo $n \geqslant a^2$, e portanto $a \leqslant \sqrt{n}$. Essa ideia pertence ao matemático da Grécia Antiga Eratóstenes (250 a.C.).

Exemplo 1.32. Os menores números compostos são: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18,$\cdots$.

Teorema 1.33. *Todo inteiro composto possui um divisor primo.*

Demonstração. Seja n um inteiro composto. Consideremos $A \neq 0$ o conjunto de todos os divisores positivos de n, exceto os divisores 1 e n, isto é:

$$A = \{t : t \mid n; 1 < t < n; t \in \mathbb{N}\}.$$

Pelo Princípio da Boa Ordem [2] , existe um elemento $p \in A$ minimal, que vamos mostrar ser primo. Suponhamos que p seja composto, ou seja, admite pelo menos um divisor d tal que $1 < d < p$, então $d \mid p$ e $p \mid n$, o que implica $d \mid n$, isto é, p não seria o elemento mínimo de A, se fosse composto. Logo, p é primo. □

Exemplo 1.34. Veja que se $7 \mid ab$ então necessariamente um dos fatores a ou b (ou ambos) é múltiplo de 7, pois 7 é um número primo.

Proposição 1.35. *O conjunto dos números primos é infinito.*

Demonstração. É suficiente provarmos que o conjunto de números primos positivos é infinito. Suponhamos, por absurdo, que existem um número finito, $p_1, \cdots, p_n$ de primos positivos.

Se $m = p_1 \cdots p_n + 1$, existe pelo Teorema 1.12, um primo p tal que p divide m. Se $p = p_i$ para algum i, então p divide 1, o que é uma contradição. □

1.5 O Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética sustenta que todo inteiro positivo maior que 1 pode ser escrito como produto de números primos, sendo esta decomposição única a menos de permutações dos fatores.

[2] **Princípio da Boa Orderm (PBO):**
Todo conjunto não vazio de inteiros positivos contém um elemento mínimo.

Os números primos são os elementos mínimos da estrutura multiplicativa dos inteiros. Vejamos um exemplo:

$$165 = 3 \cdot 5 \cdot 11$$

donde 3, 5 e 11 são "mínimos", pois não podem ser fatorados.

Teorema 1.36. *(Teorema Fundamental da Aritmética) Todo inteiro n, $n \geq 2$, pode ser escrito na forma $n = p_1 \cdot \ldots \cdot p_s$, para determinados primos positivos $p_1, \ldots, p_s$, com $s \geq 1$ e $p_1 \leq p_2 \leq \ldots \leq p_s$. Além disso, os fatores primos $p_1, \ldots, p_s$, satisfazendo as condições apresentadas, são únicos, isto é, se $q_1, \ldots, q_r$, são também primos positivos com $q_1 \leq q_2 \leq \ldots \leq q_r$ e $n = q_1 \cdot \ldots \cdot q_r$, então $r = s$ e, além disso, $p_i = q_j$, para todo $i, j \in \{1, \ldots, r\}$.*

Demonstração. Mostramos a existência da fatoração de n em primos. Se $n = p$ é um número primo, a afirmação fica clara ($r = 1$). Agora, se n é composto, então, pelo Teorema 1.33, n possui um divisor primo p_1 e temos:

$$n = p_1 \cdot n_1,\ 1 < n_1 < n.$$

Vejamos que, se na afirmação acima n_1 é primo, então esta igualdade representa n como produto de fatores primos, e se, ao invés disso, n_1 é composto, então pelo Teorema 1.33, n_1 possui divisores p_2, isto é, $n_1 = p_2 \cdot n_2$, e temos:

$$n = p_1 \cdot p_2 \cdot n_2,\ 1 < n_2 < n.$$

Assim sendo, temos a sequência decrescente:

$$n > n_1 > n_2 > \ldots > 1.$$

Como existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente um n_k ($k \geq 1$) que é um primo p_s ($n_k = p_s$) e por consequência teremos:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s.$$

Por fim, mostramos a unicidade da fatoração de n, $n \geq 2$.

Suponhamos que $p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_r$ com $p_1, p_2, \ldots, p_s, q_1, q_2, \ldots, q_r \in \mathbb{P}$ e $p_1 \leq p_2 \leq \ldots \leq p_s$ assim como, $q_1 \leq q_2 \leq \ldots \leq q_r$. Temos que $p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_r$ donde concluímos, aplicando diversas vezes a Proposição 1.25, que p_1 tem que dividir pelo menos um dos fatores $q_1, q_2, \ldots, q_r$. Então existe k ($1 \leq k \leq r$) com $p_1 \mid q_k$. Como p_1 e q_k são primos, temos que $p_1 = q_k \geq q_1$. De modo análogo, $q_1 \mid p_l$ para algum l ($1 \leq l \leq s$) donde

segue $q_1 = p_l \geq p_1$. Desta forma, $p_1 = q_1$. Agora, de $p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_r$ segue

$$p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_r.$$

Por indução, concluímos que $s - 1 = r - 1$ (isto é, $s = r$) e $p_2 = q_2, p_3 = q_3, \ldots, p_s = q_r$. Como $p_1 = q_1$, vale a unicidade da fatoração. □

Outra forma de escrever a fatoração é

$$n = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s} = \prod_{k=1}^{s} p_k^{e_k}.$$

Podemos ainda representar um número inteiro como

$$n = 2^{e_2} 3^{e_3} \ldots p^{e_p} \ldots$$

onde o produto é tomado sobre todos os primos, que sabemos ser infinito, pela Proposição 1.35. Ao longo deste trabalho escolheremos qualquer destas representações acima e as mesmas serão referidas como a *fatoração canônica* de n em números primos.

Exemplo 1.37. A fatoração canônica do inteiro positivo $n = 4.200$ é dada pela igualdade:

$$4.200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Lema 1.38. *Sejam m e n em $\mathbb{N}$ e $mdc(m, n) = 1$. Se $mn = c^2$, então existem M e N com $m = M^2$ e $n = N^2$.*

Demonstração. Sejam $m = \prod_{k=1}^{r} p_k^{a_k}$ e $n = \prod_{k=1}^{s} q_k^{b_k}$ as fatorações canônicas de m e n. Então os q_k são diferentes dos p_l pois $mdc(m, n) = 1$. Segue que $mn = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r} \cdot q_1^{b_1} \cdot \ldots \cdot q_s^{b_s}$ é a decomposição primária de mn. Como $mn = c^2$ é quadrado perfeito, segue que todos os $a_1, \ldots, a_r, b_1, \ldots, b_s$ são pares. Logo, $m = M^2$ e $n = N^2$ para $M = \prod_{k=1}^{r} p_k^{a_k/2}$ e $N = \prod_{k=1}^{s} q_k^{b_k/2}$. □

1.6 Congruência Módulo m

A congruência módulo m é uma relação de equivalência, isto é, é reflexiva; simétrica e transitiva, no conjunto dos números inteiros, de tal forma que dados dois inteiros a e b, ao dividirmos por um número m (chamado módulo de congruência) deixam o mesmo resto. Através das propriedades de congruência, podemos encontrar o resto das divisões sem

muitos esforços e de forma breve. É o que abordaremos nesta seção, que será de extrema importância para encriptar e decriptar mensagens codificadas.

Definição 1.39. *Dados a, b e m em $\mathbb{Z}$, dizemos que a é congruente a b módulo m e denotamos:*

$$a \equiv b \,(mod\, m),$$

se $m \mid (a-b)$, ou seja, a e b têm o mesmo resto na divisão por m. Se a não for congruente (ou incongruente) a b, módulo m, escrevemos $a \not\equiv b \,(mod\, m)$.

Alternativamente temos que, dados três inteiros a, b e m,

$a \equiv b \,(mod\, m) \Leftrightarrow m \mid (a-b) \Leftrightarrow a - b = km \Leftrightarrow a = b + km$, para algum $k \in \mathbb{Z}$.

Exemplo 1.40. Temos que $3 \equiv 24 \,(mod\ 7)$, pois $7 \mid (3-24)$. Por outro lado, $25 \not\equiv 12 \,(mod\ 7)$, pois $7 \nmid (25-12)$.

Proposição 1.41. *Para quaisquer a, b, c, d e m pertencentes a $\mathbb{Z}$ temos:*

1. *Reflexiva: $a \equiv a \,(mod\, m)$;*
2. *Simétrica: Se $a \equiv b \,(mod\, m)$, então $b \equiv a \,(mod\, m)$;*
3. *Transitiva: Se $a \equiv b \,(mod\, m)$ e $b \equiv c \,(mod\, m)$, então $a \equiv c \,(mod\, m)$;*
4. *Compatibilidade com a soma e diferença:*

$$\begin{cases} a \equiv b \,(mod\, m) \\ c \equiv d (mod\, n) \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \,(mod\, m) \\ a - c \equiv b - d \,(mod\, m) \end{cases}$$

   Em particular, se $a \equiv b \,(mod\, m)$, então $ka \equiv kb \,(mod\, m)$ para todo $k \in \mathbb{Z}$.

5. *Compatibilidade com o produto: Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b \,(mod\, m) \\ c \equiv d \,(mod\, m) \end{cases} \Rightarrow \quad ac \equiv bd \,(mod\, m)$$

   Em particular, se $a \equiv b \,(mod\, m)$, então $a^k \equiv b^k \,(mod\, m)$ para todo $k \in \mathbb{Z}$.

6. *Cancelamento: Se $ac \equiv bc \,(mod\, m)$ e $mdc(c, m) = d$, então $a \equiv b \,\left(mod\, \frac{m}{d}\right)$.*

Demonstração. Para a, b, c, d e m inteiros, temos:

1. $m \mid 0 \Rightarrow m \mid (a-a) \Rightarrow a \equiv a \,(mod\, m)$.
2. $a \equiv b \,(mod\, m) \Rightarrow m \mid (a-b) \Longleftrightarrow m \mid -(a-b) \Rightarrow m \mid (b-a) \Rightarrow b \equiv a \,(mod\, m)$.

3. $a \equiv b\,(mod\,m)$ e $b \equiv c\,(mod\,m) \Rightarrow m \mid (a-b)$ e $m \mid (b-c) \Rightarrow m \mid [(a-b)+(b-c)] \Rightarrow m \mid (a-c) \Rightarrow a \equiv c\,(mod\,m)$.

4. $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m) \Rightarrow m \mid (a-b)$ e $m \mid (c-b) \Rightarrow m \mid [(a-b)+(c-d)] \Rightarrow m \mid [(a+c)-(b+d)] \Rightarrow a+c \equiv b+d\,(mod\,m)$. A compatibilidade com a diferença segue de modo análogo.

5. Como $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m)$, podemos concluir que existem inteiros s, t tais que $a = b+sm$ e $c = d+tm$, então $ac = (b+sm).(d+tm) = bd+btm+dsm+smtm = bd+(bt+ds+stm)m$, que por definição de congruência, $ac \equiv bd\,(mod\,m)$.

6. Se $ac \equiv bc\,(mod\,m)$, então $ac-bc = (a-b)c = km$, com $k \in \mathbb{Z}$. Ainda, se $mdc(c,m) = d$, existem inteiros r e s tais que $c = dr$ e $m = ds$, onde r e s são primos entre si. Portanto:

   $$(a-b)dr = kds \text{ ou } (a-b)r = ks,$$

   o que implica que, $s \mid (a-b)r$, com $mdc(r,s) = 1$. Logo, pelo Corolário 1.24, $s \mid (a-b)$ e daí $a \equiv b\,(mod\,s)$. Como $s = \dfrac{m}{d}$ segue que $a \equiv b\,\left(mod\,\dfrac{m}{d}\right)$.

□

Exemplo 1.42. Como $12 \equiv 22\,(mod\,5)$ e $8 \equiv 13\,(mod\,5)$ segue que

$$12+8 \equiv 22+13\,(mod\,5), \text{ ou seja, } 20 \equiv 35\,(mod\,5)$$

e

$$12 \cdot 8 \equiv 22 \cdot 13\,(mod\,5), \text{ ou seja, } 96 \equiv 286\,(mod\,5).$$

Exemplo 1.43. Vejamos que $31 \mid 20^{15}-1$.

Para verificar a expressão acima é suficiente mostrar que $20^{15} \equiv 1\,(mod\,31)$. Para tal, observemos que

$$20 \equiv -11\,(mod\,31) \tag{1.1}$$

e com isso, $20^2 \equiv (-11)^2\,(mod\,31) \Leftrightarrow 20^2 \equiv 121\,(mod\,31)$. Como $121 \equiv -3\,(mod\,31)$ temos

$$20^2 \equiv -3\,(mod\,31). \tag{1.2}$$

Multiplicando (1.1) e (1.2) membro a membro, obtemos $20^3 \equiv 33\,(mod\,31)$ e, como $33 \equiv 2\,(mod\,31)$,

$$20^3 \equiv 2\,(mod\,31). \tag{1.3}$$

Por fim, elevando (1.3) à potência 5, temos que $(20^3)^5 \equiv 2^5\,(mod\,31) \Rightarrow 20^{15} \equiv 32\,(mod\,31)$ e como $32 \equiv 1\,(mod\,31)$, obtemos $20^{15} \equiv 1\,(mod\,31)$.

1.7 Pequeno Teorema de Fermat

Os números primos possuem muitas propriedades. Uma delas foi encontrada por Pierre de Fermat, chamada de Pequeno Teorema de Fermat.

Antes de enunciarmos e demonstrarmos este teorema, apresentamos primeiramente um lema, necessário para a sua demonstração.

Lema 1.44. *Sejam p um número primo e a e b inteiros. Então,*

$$(a+b)^p \equiv a^p + b^p \,(mod\, p).$$

Demonstração. O lema é demonstrado utilizando a notação do binômio de Newton, no caso

$$(a+b)^p \equiv a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i.$$

Para provar a veracidade do lema, basta mostrar que

$$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i \equiv 0 \,(mod\, p).$$

Ao expandirmos o número binomial, temos

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{i!}.$$

Como não sabemos se a e b são múltiplos de p, nos resta tentar concluir que $\binom{p}{i}$ o seja. Como $\binom{p}{i}$ é um inteiro positivo, pois é o coeficiente a_i do polinômio $a_1X + \cdots + a_{p-1}X^{p-1}$, segue que todos os fatores de $i!$ são cancelados com fatores do numerador da fração. Como $1 \leq i \leq p-1$ e p é primo, concluímos que nenhum dos fatores do denominador da fração cancela o fator p. Portanto, $\binom{p}{i}$ é múltiplo de p.

□

Demonstrado o lema, podemos demonstrar o teorema por indução em n para os casos em que n é natural e depois estendermos para todos os inteiros.

Teorema 1.45 (Pequeno Teorema de Fermat)**.** *Seja p um número primo e a um número inteiro, então*

$$a^p \equiv a \,(mod\, p).$$

Demonstração. Inicialmente suponha que $n^p \equiv n \,(mod\, p)$. Para $n = 1$, temos $1^p \equiv 1 \,(mod\, p)$, que é obviamente verdadeira.

Assumimos então que $n^p \equiv n\,(mod\,p)$ é verdadeira, e utilizando o lema que acabamos de demonstrar, temos

$$(n+1)^p \equiv n^p + 1^p \equiv n + 1\,(mod\,p).$$

Caso tomemos n negativo, temos $-n$ positivo, logo vale

$$(-n)^p \equiv -n\,(mod\,p).$$

Aqui devemos considerar os dois casos possíveis de paridade de p. Ou p é par, especificamente o número 2, pois é o único primo par, ou p é ímpar.

Quando tivermos $p = 2$, teremos $(-n)^2 \equiv -n\,(mod\,2)$, ou seja,

$$n^2 \equiv -n\,(mod\,2).$$

Se estivermos tomando um n par, teremos $n^2 \equiv 0\,(mod\,2)$ e $-n \equiv 0\,(mod\,2)$, logo $n^2 \equiv -n\,(mod\,2)$. E caso tenhamos escolhido n ímpar, teremos $n^2 \equiv 1(mod\,2)$ e $-n \equiv 1\,(mod\,2)$, satisfazendo também $n^2 \equiv -n\,(mod\,2)$.

Já no caso em que p é ímpar, teremos

$$(-n)^p \equiv -n^p \equiv -n\,(mod\,p).$$

Mas como estamos trabalhando com congruências, podemos multiplicar ambos os lados da nossa congruência por (-1), obtendo $n^p \equiv n\,(mod\,p)$. □

O Pequeno Teorema de Fermat tem uma forma alternativa de ser enunciado, como podemos ver a seguir.

Teorema 1.46. *Seja p primo e a um inteiro não divisível por p. Então $a^{p-1} \equiv 1\,(mod\,p)$.*

Muitos algoritmos e testes de primalidade se basearam neste teorema para aumentar sua eficiência.

1.8 Função de Euler

Também muito importante no processo de encriptação de mensagens da criptografia RSA, apresentamos a *Função de Euler*.

Definição 1.47. *Chamamos de **função de Euler** a função $\phi : \mathbb{Z}_+ \to \mathbb{Z}_+$, que associa a cada número n ao número positivo s tal que:*

(i) $s \leqslant n$;

(ii) $mdc(s, n) = 1$.

É razoável, pela Definição 1.47, dizer que

$$1 \leqslant \phi(n) \leqslant n.$$

Teorema 1.48. *Se p é primo e a um inteiro positivo, então*

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

Demonstração. Pela definição de ϕ, segue que $\phi(p^a)$ é o número de inteiros positivos não-superiores a p^a e coprimo com p^a. Mas, os únicos inteiros não coprimo com p^a e menores ou iguais a p^a são os divisíveis por p. Como os múltiplos de p não superiores a p^a são p^{a-1}, segue que $\phi(p^a) = p^a - p^{a-1}$. □

Proposição 1.49. *Se $mdc(p, q) = 1$, então $\phi(pq) = \phi(p)\phi(q)$.*

Proposição 1.50. *Um inteiro positivo p é primo se, e somente se,*

$$\phi(p) = p - 1.$$

Demonstração. ($\Rightarrow$) Se p é primo, segue imediato pelo Teorema 1.48 que $\phi(p) = p - 1$. ($\Leftarrow$) Suponha que p não é primo. Então existe um elemento $q \in \mathbb{Z}$, diferente de 1 e p tal que $q \mid p$. Pela definição da função de Euler temos que $0 < \phi(p) \leqslant p - 1$, mas nesse caso o valor de q deve ser excluído, pois não é coprimo com p. Logo, $\phi(p) \neq p - 1$, o que é uma contradição. Portanto, p é primo. □

1.9 Equações Diofantinas

Estudaremos na Seção 3.5 do Capítulo 3, como encontrar um novo valor positivo para nosso componente da chave privada do sistema, caso o valor encontrado seja negativo. Para isso, utilizaremos o conceito e resultado apresentados a seguir.

Definição 1.51. *Uma equação nas variáveis inteiras x e y do tipo*

$$ax + by = c, \text{ com } a, b, c \in \mathbb{Z}$$

diz-se ***equação diofantina****.*

Teorema 1.52. *Sejam a e b inteiros positivos, $c \in \mathbb{Z}$ e $mdc(a, b) = d$. A equação*

$$ax + by = c, \text{ com } x, y \in \mathbb{Z}$$

tem solução se, e somente se, d divide c. Além disso, se x_0, y_0 são tais que $ax_0 + by_0 = c$, então a solução geral da equação $ax + by = c$ é dada por

$$x = x_0 + \left(\frac{b}{d}\right) k,$$
$$y = y_0 - \left(\frac{a}{d}\right) k,$$

onde $k \in \mathbb{Z}$.

Demonstração. Se $a = 0$ ou $b = 0$, então o resultado é imediato. Vejamos o caso em que $a \neq 0$ e $b \neq 0$. Nesse caso, a demonstração do teorema será dividida em duas partes, a primeira com relação a equação possuir solução se d divide c, e a segunda com relação a solução geral.

Primeira parte do teorema: Supondo que a equação $ax + by = c$ tenha solução em $\mathbb{Z}$, e $mdc(a, b) = d$, então $d|ax$ e $d|by$ e, portanto, $d|ax + by$ o que implica $d|c$. Reciprocamente, supondo que $d|c$, então existe $t \in \mathbb{Z}$ tal que $c = dt$. Pelo Teorema 1.19 existem $\alpha, \beta \in \mathbb{Z}$ tal que $a\alpha + b\beta = d$. Multiplicando essa última igualdade por t tem-se que $a(t\alpha) + b(t\beta) = dt = c$ e, portanto $x = \alpha t$ e $y = \beta t$ são soluções da equação $ax + by = c$.

Segunda parte do teorema: Sejam x_0 e y_0 tal que $ax_0 + by_0 = c$. Assim, se $k \in \mathbb{Z}$, então

$$a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k = ax_0 + by_0 = c,$$

o que mostra que $x = x_0 + \left(\frac{b}{d}\right) k$, $y = y_0 - \left(\frac{a}{d}\right) k$ é uma solução da equação $ax + by = c$. Vamos mostrar agora, que se $x, y \in \mathbb{Z}$ são tais que $ax + by = c$, então x, y são da forma dada acima. Para isso, vamos supor que o par (x', y') seja outra solução da equação. Assim,

$$ax' + by' = c = ax_0 + by_0,$$

mas isto é equivalente a

$$a(x' - x_0) = b(y_0 - y').$$

Como $mdc(a, b) = d$, segue que $d|a$ e $d|b$. Assim existem m e n inteiros tal que $a = md$ e $b = nd$, com $mdc(m, n) = 1$. Desta forma,

$$m(x' - x_0) = n(y_0 - y'),$$

e assim $m|n(y_0 - y')$. Como $mdc(m, n) = 1$, segue que m deve dividir $y_0 - y'$, isto é, $y_0 - y' = mk$, para algum $k \in \mathbb{Z}$. Portanto,

$$y' = y_0 - mk = y_0 - \frac{a}{d}k.$$

Assim, $m(x' - x_0) = n(y_0 - y') = nmk$, e portanto, $x' - x_0 = nk$, ou equivalentemente,

$$x' = x_0 + nk = x_0 + \frac{b}{d}k,$$

o que prova o resultado. □

Exemplo 1.53. Resolvemos a equação $5x + 12y = 81$, com soluções pertencentes ao conjunto dos números inteiros.

Iniciaremos fazendo uso do algoritmo de Euclides, para encontrar $mdc(12, 5)$. Sendo assim,

$$12 = 5 \cdot (2) + 2 \tag{1.4}$$

$$5 = 2 \cdot (2) + 1 \tag{1.5}$$

$$2 = 1 \cdot (2) + 0.$$

Logo, $mdc(12, 5) = 1$ e pelo Teorema (1.52), como $mdc(12, 5) = 1$ então a equação tem solução. Agora, isolamos os restos de (1.4) e (1.5), desconsiderando a última expressão, já que tem resto 0 e, portanto, não será substituída em nenhuma outra expressão. Logo,

$$2 = 12 + 5 \cdot (-2) \tag{1.6}$$

$$1 = 5 \cdot (1) + 2 \cdot (-2). \tag{1.7}$$

Substituindo (1.6) em (1.7), temos a expressão procurada:

$$= 5 \cdot (1) + (5 \cdot (-2) + 12) \cdot (-2) = 5 \cdot (5) + 12 \cdot (-2). \tag{1.8}$$

Multiplicando a Equação (1.8) por 81, segue que

$$81 = 5 \cdot (405) + 12 \cdot (-162).$$

Portanto, uma solução da equação $5x + 12y = 81$ é $x_0 = 405$ e $y_0 = -162$. Deste modo, temos que a solução geral no conjunto dos inteiros, será dada por:

$$S = \{(405 + 12k, -162 - 5k), \text{com } k \in \mathbb{Z}\}.$$

2 Os Inteiros Gaussianos

Neste capítulo estendemos para os inteiros gaussianos as clássicas propriedades de $\mathbb{Z}$, que serão suporte para a nossa extensão do algoritmo RSA aos inteiros gaussianos, o qual será abordado no Capítulo 4. Muitas das propriedades apresentadas na Seção 2.1 são válidas para os inteiros gaussianos, pois neste caso nos restringimos aos números complexos com coeficientes em $\mathbb{Z}$. Primeiramente discutimos propriedades resultantes da definição do conjunto dos números complexos $\mathbb{C}$. As principais referências utilizadas neste capítulo foram [7, 8, 9, 10, 11, 12, 13].

2.1 Números Complexos

O conceito de número complexo se desenvolveu gradativamente, como ocorreu com os demais tipos de números. Algumas equações de grau 2, como $x^2 + 1 = 0$, não haviam solução até o século XVI, pois para os matemáticos da época a raiz negativa não existia. Porém, não foi este o motivo pelo qual os números complexos surgiram. Ao passar dos anos, alguns matemáticos viram o mesmo problema para equações do 3º grau, onde perceberam que os números reais não eram suficientes para resolver este tipo de equação.

Para solucionar este problema alguns matemáticos europeus, principalmente italianos, desenvolveram pesquisas. Houve algumas disputas também.

Os números complexos começaram a ser desenvolvidos por Scipione dal Ferro. Ferro desenvolveu uma teoria para a solução das equações do tipo $x^3+px+q = 0$, mas acabou não a publicando. Antônio Maria Fior conheceu a teoria de Ferro e ampliou-a para as equações do tipo $x^3+px^2+q = 0$. Fior acabou desafiando Niccolò Fontana, conhecido como Tartaglia. Tartaglia venceu todas as disputas com Fior.

Neste momento, chega aos ouvidos de Girolamo Cardano que Tartaglia sabia resolver tais tipos de equações. Cardano implorou a "fórmula" para resolver essas equações. Com sua insistência e juramento de que não divulgaria o resultado, Tartaglia revelou a solução. Porém, Cardano não cumpriu com sua palavra, e em 1545 fez a publicação no livro *Ars Magna*. Ele somente fez uma menção de Tartaglia na sua obra e até hoje a fórmula é conhecida como

"Fórmula de Cardano"[3].

Após esta "luta" surge um problema inquietante que Cardano trouxe, conhecido na época como números "sofisticados", ou seja, as raízes quadradas de números negativos. Neste momento da história, se introduz a ideia de aceitar o imaginário, e não somente o real. Foi René Descartes que escreveu no seu livro *Géométrie* a seguinte frase: *"Nem sempre as raízes verdadeiras (positivas) ou falsas (negativas) de uma equação são reais. Às vezes elas são imaginárias"*. Com esta citação ficou definido que o número raiz quadrada de -1 seria chamado de número imaginário e que poderia ser manipulado de acordo com as regras da álgebra (GARBI, 1997, p. 75).

Em seguida, Leonhard Euler em 1777 simbolizou à raiz quadrada de -1 por i. Segundo ele, os números complexos também possuem uma parte real. Logo, os caracterizou como sendo do tipo: $z = a + bi$, onde a e b são números reais e $i^2 = -1$, mas esta ideia só foi mais aceita quando Carl Friedrich Gauss a introduziu, em 1832. Gauss além de introduzir a expressão do número complexo, realizou estudos relacionados a representação geométrica dos mesmos, que já tinha sido publicada e estudada também anteriormente por Jean Argand, em 1806.

Para maiores detalhes sobre a origem dos números complexos a referência BOYER, Carl B. História da Matemática. Trad. Elza F. Gomide. SP: Editora Edgard Blücher Ltda, 1996, pode ser consultada.

Definição 2.1. *Os números z da forma $a + bi$ são chamados de números complexos, onde $a, b \in \mathbb{R}$ e $i = \sqrt{-1}$, esta última denominada unidade imaginária.*

Denotaremos por $\mathbb{C}$ o conjunto dos números complexos. Dados os números complexos $z_1 = a_1 + b_1 i$ e $z_2 = a_2 + b_2 i$ definimos sua soma por

$$z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i \tag{2.1}$$

e seu produto por

$$z_1.z_2 = (a_1 + b_1 i).(a_2 + b_2 i) = (a_1.a_2 - b_1.b_2) + (a_1.b_2 + a_2.b_1)i \tag{2.2}$$

Exemplo 2.2. Consideremos os números complexos: $z_1 = 2 + 4i, z_2 = 5 - i, z_3 = 10$ e $z_4 = -\frac{1}{2}i$.

Pela definição de adição (2.1) e multiplicação (2.2) temos:

[3] **Fórmula de Cardano**
Uma solução para equação $x^3 + px + q$, com p e q reais é:

$$x = \sqrt[3]{\frac{-q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

- $z_1 + z_2 = (2 + 4i) + (5 - i) = (2 + 5) + (4 + (-1))i = 7 + 3i$;
- $z_3 + z_4 = (10) + \left(-\frac{1}{2}i\right) = (10 + 0i) + \left(0 - \frac{1}{2}i\right) = (10 + 0) + \left(0 + \left(-\frac{1}{2}i\right)\right) = 10 - \frac{1}{2}i$;
- $z_1.z_2 = (2 + 4i).(5 - i) = (2.5 - 4.(-1)) + (2.(-1) + 4.5)i = 14 + 18i$,
- $z_2.z_4 = (5 - i).\left(-\frac{1}{2}i\right) = (5 - i).\left(0 - \frac{1}{2}i\right) = \left((5.0) - (-1).\left(-\frac{1}{2}\right)\right) + + \left(5.\left(-\frac{1}{2}\right) + (-1).0\right)i = -\frac{1}{2} - \frac{5}{2}i$.

As operações (2.1) e (2.2) satisfazem as seguintes propriedades:

(C. 1) Comutatividade: Se z_1 e $z_2 \in \mathbb{C}$ então $z_1 + z_2 = z_2 + z_1$ e $z_1.z_2 = z_2.z_1$;

(C. 2) Associatividade: Se z_1, z_2 e $z_3 \in \mathbb{C}$ então $(z_1 + z_2)+z_3 = z_1+(z_2 + z_3)$ e $(z_1.z_2).z_3 = z_1.(z_2.z_3)$;

(C. 3) Distributividade: Se z_1, z_2 e $z_3 \in \mathbb{C}$ então $z_1.(z_2 + z_3) = z_1.z_2 + z_1.z_3$;

(C. 4) Existência do zero: Existe um elemento $0 = 0 + 0i \in \mathbb{C}$ tal que $0 + z = z$ para todo $z \in \mathbb{C}$;

(C. 5) Existência da unidade: Existe um elemento $1 = 1 + 0i \in \mathbb{C}$ tal que $1.z = z$ para todo $z \in \mathbb{C}$;

(C. 6) Existência do inverso aditivo: Dado $z = a + bi \in \mathbb{C}$ existe um único $w = (-a) + (-b)\,i \in \mathbb{C}$ tal que $z + w = 0$. Notação: $w = -z$,

(C. 7) Existência do inverso multiplicativo: Dado $z = a + bi \in \mathbb{C}$, tal que $a \neq 0$ ou $b \neq 0$, existe $w = a\,(a^2 + b^2)^{-1} - b\,(a^2 + b^2)^{-1}\,i$ tal que $z.w = 1$. Notação: $w = z^{-1} = \frac{1}{z}$.

Dizemos então que $\mathbb{C}$ é um corpo com as operações (2.1) e (2.2). Um fato que devemos ter em mente é que o corpo dos reais está naturalmente mergulhado em $\mathbb{C}$ e para isto basta identificarmos um número real x com o complexo $x + 0i$. Tendo em vista esta identificação, diremos que $\mathbb{R} \subset \mathbb{C}$. Observe que se $z = a + 0i \in \mathbb{R}$ e $w = b + 0i \in \mathbb{R}$ então $z + w$ e $z.w$ estão em $\mathbb{R}$. Portanto $\mathbb{R}$ é um subcorpo de $\mathbb{C}$, isto é, as operações (2.1) e (2.2) estendem as operações de soma e produto de números reais.

Podemos identificar o conjunto dos números complexos com o plano $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ por meio do isomorfismo

$$\begin{array}{rcl} \varphi : \mathbb{R}^2 & \to & \mathbb{C} \\ (x, y) & \mapsto & x + yi \end{array}$$

Assim, podemos definir a soma e o produto de complexos $z_1 = (a_1, b_1)$ e $z_2 = (a_2, b_2)$, respectivamente:

$$z_1 + z_2 = (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \tag{2.3}$$

$$z_1.z_2 = (a_1, b_1).(a_2, b_2) = (a_1.a_2 - b_1.b_2, a_1.b_2 + a_2.b_1) \tag{2.4}$$

A representação dos números complexos por pontos do plano é muito útil e frequente. Por meio dela, o número complexo $z = x + yi$ é identificado como o ponto (x, y), ou com o vetor Oz de componentes x e y. Atualmente, o plano dos números complexos é conhecido como plano de Argand-Gauss.

Dado $z = x + yi \in \mathbb{C}$, definimos

$$Re(z) = x \text{ (parte real de } z)$$
$$Im(z) = y \text{ (parte imaginária de } z).$$

Logo, para todo $z \in \mathbb{C}$ temos $z = Re(z) + Im(z)i$. Na Figura 2.1 apresentamos a representação gráfica de z.

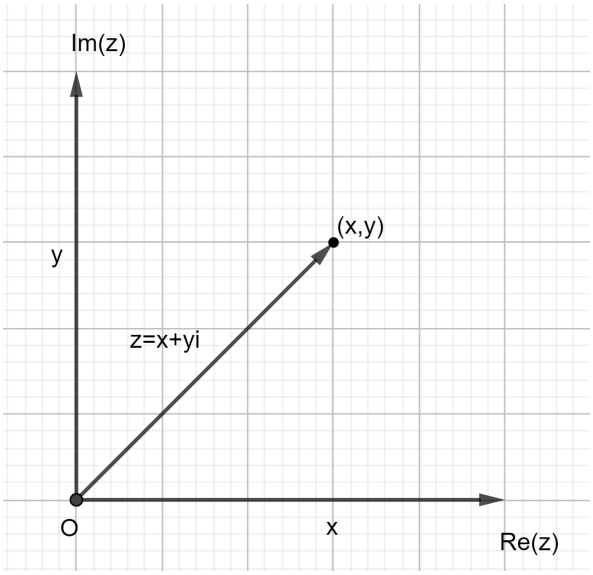

Figura 2.1: Representação gráfica de z

Definição 2.3. *Definimos o módulo, ou valor absoluto ou norma de um número complexo* $z = x + yi$ *como sendo o número não negativo* $|z| = \sqrt{x^2 + y^2}$.

Como se vê (Figura 2.2), $|z|$ é a distância do ponto z à origem.

Definição 2.4. *O complexo conjugado de* $z = x + yi$ *é definido como sendo* $\overline{z} = \overline{x + yi} = x - yi$.

Em termos do módulo e do conjugado, temos:

$$z\overline{z} = (x + yi)(x - yi) = (x^2 + y^2) + (-xy + yx)i = x^2 + y^2,$$

isto é, $z\overline{z} = |z|^2$.

O quociente $z = \frac{z_1}{z_2}$ de dois números complexos z_1 e z_2, $z_2 \neq 0$, é definido pela condição $z.z_2 = z_1$.

Para calcular o quociente basta multiplicar o numerador e o denominador pelo complexo conjugado do denominador, isto é, se $z_1 = x_1 + y_1 i$ e $z_2 = x_2 + y_2 i$ então

$$\frac{z_1}{z_2} = \frac{z_1.\overline{z_2}}{z_2.\overline{z_2}} = \frac{z_1.\overline{z_2}}{|z_2|^2} = \frac{x_1x_2 + y_1y_2 + (y_1x_2 - x_1y_2)i}{x_2^2 + y_2^2}. \tag{2.5}$$

Exemplo 2.5. Considere os números complexos $z_1 = -3 + i$ e $z_2 = 1 - 2i$. Assim,

$$\frac{z_1}{z_2} = \frac{-3+i}{1-2i} = \frac{(-3+i).(1+2i)}{(1-2i).(1+2i)} = \frac{((-3).1 - 1.2) + ((-3).2 + 1.1)i}{(1.1 - (-2).2) + (1.2 + (-2).1)i} = \frac{-5-5i}{5} = -1-i.$$

Para todo z e w em $\mathbb{C}$, tem-se as seguintes propriedades:

1. $|z| = |\overline{z}|$,
2. $\overline{(z+w)} = \overline{z} + \overline{w}$,
3. $\overline{z}.\overline{w} = \overline{zw}$,
4. $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$, $w \neq 0$,
5. $z^{-1} = \frac{\overline{z}}{|z|^2}$, $z \in \mathbb{C}$ - $\{0\}$,
6. $Re(z) = \dfrac{z+\overline{z}}{2}$ e $Im(z) = \dfrac{z-\overline{z}}{2i}$,
7. $|z+w|^2 = |z|^2 + |w|^2 + 2Re\,(z\overline{w})$.

Consideremos agora um número complexo não nulo $z = x + iy$. Se $|z|$ é o segmento de reta que liga 0 a z e θ é o ângulo que $|z|$ faz com o eixo dos x $(0 \leq \theta \leq 2\pi)$ podemos escrever

$$\cos\theta = \frac{x}{\sqrt{x^2+y^2}} = \frac{x}{|z|} \text{ e } \operatorname{sen}\theta = \frac{y}{\sqrt{x^2+y^2}} = \frac{y}{|z|}$$

e, portanto,

$$z = |z|\cos\theta + i|z|\operatorname{sen}\theta = |z|(\cos\theta + i\operatorname{sen}\theta). \tag{2.6}$$

A expressão (2.6) é chamada de **representação polar** do número complexo z. O número θ é chamado de **argumento** de z e denotaremos por $arg(z)$. Na Figura 2.2 representamos geometricamente $|z|$ e $arg(z)$.

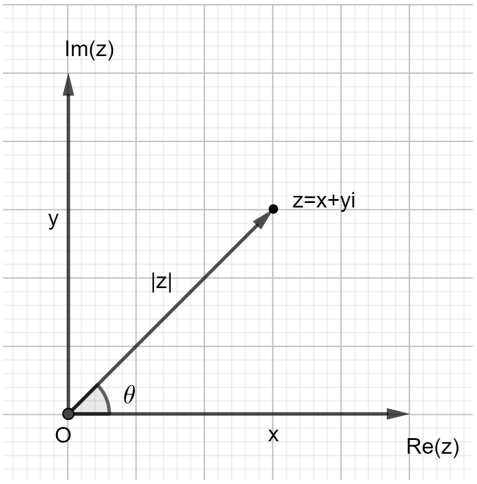

Figura 2.2: Representação gráfica da norma de z e seu argumento.

Podemos determinar θ de maneira única exigindo, por exemplo, que $0 \leq \theta < 2\pi$ ou que $-\pi < \theta \leq \pi$.

Exemplo 2.6. Seja $z_1 = 2-2i$, então $|z_1| = 2\sqrt{2}$ e $arg(z_1) = -\frac{\pi}{4} \pm 2n\pi$ com $n = 0, 1, 2, \cdots$. Logo, uma forma polar desse número complexo é $z_1 = 2\sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i\,\mathrm{sen}\left(-\frac{\pi}{4}\right)\right)$.

Também podemos considerar algum ponto z_0 que não seja a origem $(0, 0)$. A representação

$$z - z_0 = \rho(\cos\phi + i\,\mathrm{sen}\,\phi) \tag{2.7}$$

é a forma polar de $z - z_0$, onde $\rho = |z - z_0|$ e ϕ é o ângulo de inclinação do vetor $\overrightarrow{z - z_0}$.

Para os números complexos

$$z_1 = r_1(\cos\theta_1 + i\,\mathrm{sen}\,\theta_1) \text{ e } z_2 = r_2(\cos\theta_2 + i\,\mathrm{sen}\,\theta_2)$$

segue a multiplicação e divisão, respectivamente:

$$z_1 z_2 = r_1 r_2[\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2)] \tag{2.8}$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i\,\mathrm{sen}(\theta_1 - \theta_2)] \tag{2.9}$$

Além disso, $z_1 = z_2 \Leftrightarrow r_1 = r_2$ e $\theta_1 \equiv \theta_2 (mod\, 2\pi)$.

As igualdades seguem imediatamente considerando as relações conhecidas:

- $\cos(\theta_1 + \theta_2) = \cos\theta_1 \cos\theta_2 - \mathrm{sen}\,\theta_1\,\mathrm{sen}\,\theta_2$
- $\mathrm{sen}(\theta_1 + \theta_2) = \mathrm{sen}\,\theta_1 \cos\theta_2 + \cos\theta_1\,\mathrm{sen}\,\theta_2$
- $\cos(\theta_1 - \theta_2) = \cos\theta_1 \cos\theta_2 + \mathrm{sen}\,\theta_1\,\mathrm{sen}\,\theta_2$

- $\operatorname{sen}(\theta_1 - \theta_2) = \operatorname{sen}\theta_1 \cos\theta_2 - \cos\theta_1 \operatorname{sen}\theta_2$

A fórmula de multiplicação acima estende-se para um número qualquer de fatores. Sendo

$$z_j = r_j(\cos\theta_j + i\operatorname{sen}\theta_j),\ j = 1, 2, ..., n$$

teremos

$$z_1 z_2 ... z_n = r_1 r_2 ... r_n[\cos(\theta_1 + \theta_2 + ... + \theta_n) + i\operatorname{sen}(\theta_1 + \theta_2 + ... + \theta_n)].$$

A demonstração segue por indução. Em particular, quando todos os fatores são iguais e de módulo unitário, obtemos a chamada *Fórmula de De Moivre*:

$$(\cos\theta + i\operatorname{sen}\theta)^n = \cos n\theta + i\operatorname{sen} n\theta. \tag{2.10}$$

Esta fórmula é válida também para expoentes negativos. De fato:

$$(\cos\theta + i\operatorname{sen}\theta)^{-n} = \frac{1}{(\cos\theta + i\operatorname{sen}\theta)^n} = \frac{1}{\cos n\theta + i\operatorname{sen} n\theta} = \cos n\theta - i\operatorname{sen} n\theta,$$

isto é,

$$(\cos\theta + i\operatorname{sen}\theta)^{-n} = \cos(-n\theta) + i\operatorname{sen}(-n\theta). \tag{2.11}$$

As seguintes propriedade se verificam de forma imediata:

1. $|z| \geq 0$ e $|z| = 0$ se, e somente se, $z = 0$;
2. $|Re(z)| \leq |z|$ e $|Im(z)| \leq |z|$,
3. $|z| = |-z|$.

   Desenvolvendo $|z_1 z_2|^2 = (z_1 z_2)(\overline{z_1 z_2}) = (z_1 \bar{z_1})(z_2 \bar{z_2}) = |z_1|^2 |z_2|^2$ segue a propriedade 4:

4. $|z_1 z_2| = |z_1||z_2|$.

   Mostremos agora um resultado importante bem conhecido: a *desigualdade triangular*, ou ainda a propriedade 5:

5. $|z_1 + z_2| \leq |z_1| + |z_2|$.

   Para a demonstração observemos que:

$$\begin{aligned}
|z_1+z_2|^2 &= (z_1+z_2)(\bar{z_1}+\bar{z_2}) \\
&= z_1\bar{z_1}+z_2\bar{z_2}+(z_1\bar{z_2}+\bar{z_1}z_2) \\
&= |z_1|^2+|z_2|^2+z_1\bar{z_2}+\overline{z_1\bar{z_2}} \\
&= |z_1|^2+|z_2|^2+2Re(z_1\bar{z_2}) \\
&\leq |z_1|^2+|z_2|^2+2|Re(z_1\bar{z_2})| \\
&\leq |z_1|^2+|z_2|^2+2|z_1z_2| \\
&= |z_1|^2+|z_2|^2+2|z_1||z_2| \\
&= (|z_1|+|z_2|)^2.
\end{aligned}$$

Extraindo a raiz segue o resultado.

Observamos ainda que $|z_1 - z_2| = |z_1 + (-z_2)| \leq |z_1|+|-z_2|$, e como $|-z_2| = |z_2|$, concluímos outra desigualdade:

6. $|z_1 - z_2| \leq |z_1|+|z_2|$.

Uma terceira desigualdade conhecida é

7. $|z_1|-|z_2| \leq |z_1 + z_2|$.

Para isto basta identificar

$$|z_1| = |(z_1 + z_2) - z_2| \leq |z_1 + z_2|+|z_2| \tag{2.12}$$

e então subtrair $|z_2|$ do primeiro e último membros.

Por último, uma quarta desigualdade:

8. $||z_1|-|z_2|| \leq |z_1 + z_2|$.

Para a verificação basta tomar $|z_1|-|z_2| = a$ e mostrar que $-|z_1 + z_2| \leq a \leq |z_1 + z_2|$. Do item (7) segue que

$$a \leq |z_1 + z_2| \quad \text{e} \quad -a \leq |z_1 + z_2|,$$

ou seja,

$$|a| \leq |z_1 + z_2|,$$

o que conclui o resultado.

2.2 Os Inteiros Gaussianos

O matemático alemão Gauss, investigava questões relacionadas à reciprocidade cúbica e biquadrática ($x^3 \equiv q(mod\, p)$ e $x^4 \equiv q(mod\, p)$, respectivamente,onde p e q são números primos), quando percebeu que essa investigação se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$, o anel dos inteiros gaussianos, do que em $\mathbb{Z}$, o conjunto dos números inteiros.

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 esse novo conjunto com consequências importantes para a 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. O uso que Gauss fez desse novo tipo de número foi de fundamental importância na demonstração do Último Teorema de Fermat.

Definição 2.7. *Seja* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$ *. Os elementos de* $\mathbb{Z}[i]$ *são chamados de inteiros gaussianos.*

Os inteiros gaussianos são a extensão natural dos inteiros para o plano complexo. Como $\mathbb{Z}$ e $\mathbb{Z}[i]$ possuem estruturas parecidas, muitas propriedades que conhecemos de $\mathbb{Z}$ podem ser estendidas para $\mathbb{Z}[i]$. Estudaremos algumas delas.

Como $\mathbb{Z}[i]$ é um subconjunto de $\mathbb{C}$, então eles compartilham das mesmas propriedades de adição e multiplicação, no entanto, $\mathbb{Z}[i]$ não é um corpo, pois veremos (Teorema 2.17) que os únicos elementos de $\mathbb{Z}[i]$ que são invertíveis são $\{1, -1, i, -i\}$.

2.2.1 Representação Gráfica dos Elementos de $\mathbb{Z}[i]$

Já dissemos que o conjunto dos números inteiros de Gauss está contido no conjunto dos números complexos e, por este motivo, é possível representar todos os elementos de $\mathbb{Z}[i]$ no plano cartesiano. Portanto, em geral, podemos representar graficamente cada inteiro gaussiano da forma $a + bi$ no ponto (a, b), de modo que tenhamos a correspondência

$$(a, b) \mapsto a + bi,$$

da mesma forma que fazemos com os números complexos.

No exemplo a seguir veremos como representar graficamente um elemento $z \in \mathbb{Z}[i]$ e todos os seus múltiplos.

Exemplo 2.8. Dado $z = 3 + 2i \in \mathbb{Z}[i]$ vamos representar graficamente todos os seus múltiplos, isto é, os elementos da forma

$$(3 + 2i)(x + yi) = (3 + 2i)x + (3 + 2i)yi = (3 + 2i)x + (-2 + 3i)y,$$

com $x,\ y \in \mathbb{Z}$. Começamos colocando o elemento $z = 3+2i$ no plano cartesiano, na posição $Z = (3, 2)$, enquanto $w = -2 + 3i$ é o ponto $W = (-2, 3)$ (ver Figura 2.3).

Todos os múltiplos de $3 + 2i$ são agora as combinações inteiras de w e z, conforme podemos ver na Figura 2.4, onde os múltiplos de $3 + 2i$, o qual é um vértice de um dos quadrados, acabam por ser os vértices de todos os quadrados.

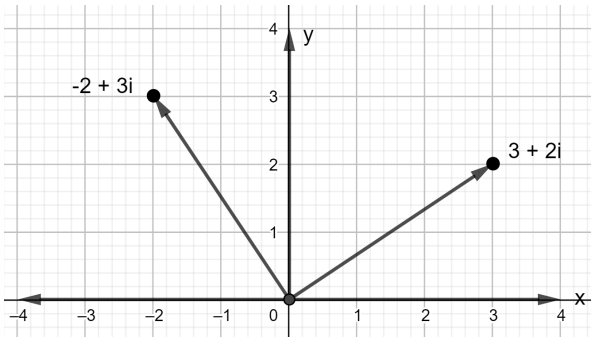

Figura 2.3: Representação dos vetores z e w

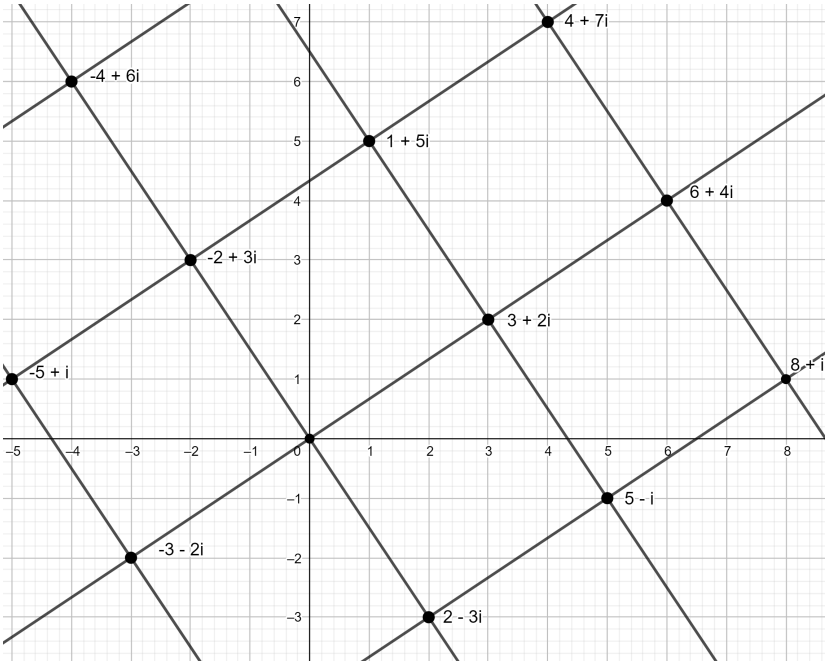

Figura 2.4: Múltiplos de $3 + 2i$

2.2.2 Função Norma em $\mathbb{Z}[i]$

A função norma é muito importante para o estudo dos Inteiros Gaussianos e para nossa extensão do algoritmo RSA. Em $\mathbb{Z}$, a distância de um número até a origem é medido pelo valor absoluto, já em $\mathbb{Z}[i]$, pela norma.

Definição 2.9. *A função $N : \mathbb{Z}[i] \to \mathbb{Z}_+$, tal que para todo $\alpha = a + bi \in \mathbb{Z}[i]$, $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$ é chamada norma.*

Há uma relação direta entre a norma do número complexo α e o valor absoluto do número $\alpha \in \mathbb{Z}[i]$. De fato,

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

Exemplo 2.10. *Interpretação geométrica da norma.* Seja $\alpha = x+yi \in \mathbb{Z}[i]$ e sua norma, $N(\alpha) = r, r \in \mathbb{Z}, r > 0$. Por definição de norma, $N(\alpha) = x^2+y^2$, ou seja, sua representação no plano cartesiano se dá por uma equação da circunferência de raio $\sqrt{r}$ e centro $(0,0)$. Ver Figura2.5.

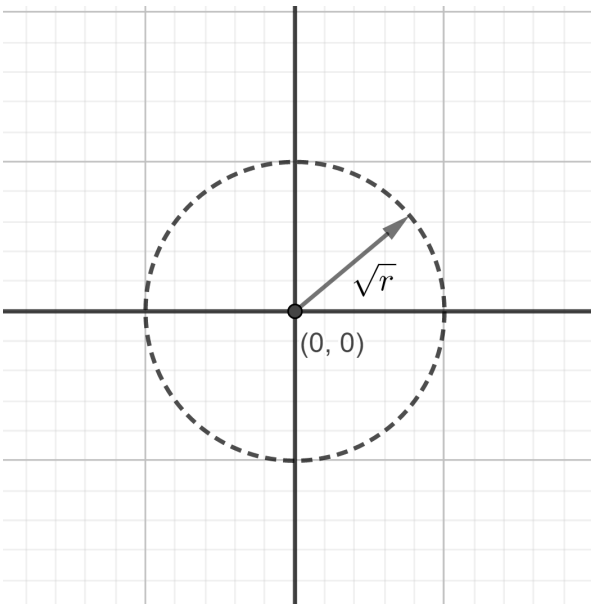

Figura 2.5: Interpretação geométrica da norma

Exemplo 2.11. $N(3+8i) = 3^2+8^2 = 9+64 = 73$.

Teorema 2.12. *Sejam* $\alpha = a+bi$, $\beta = c+di \in \mathbb{Z}[i]$. *Então* $N(\alpha\beta) = N(\alpha)N(\beta)$.

Demonstração. Para $\alpha = a+bi$, $\beta = c+di \in \mathbb{Z}[i]$, temos:

$$\begin{aligned} N(\alpha\beta) &= N((a+bi)(c+di)) = N((ac-bd)+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2 = \\ &= (a^2c^2+b^2d^2+a^2d^2+b^2c^2) = a^2(c^2+d^2)+b^2(c^2+d^2) = (a^2+b^2)(c^2+d^2) = \\ &= N(a+bi)N(c+di) = N(\alpha)N(\beta). \end{aligned}$$

□

Exemplo 2.13. Vamos exemplificar o Teorema 2.12 para um caso particular. Tomando $\alpha = 3+5i$ e $\beta = 2+i$ temos que

$$N(\alpha) = N(3+5i) = 3^2+5^2 = 9+25 = 34$$

e

$$N(\beta) = N(2+i) = 2^2 + 1^2 = 4 + 1 = 5.$$

Logo, $N(\alpha)N(\beta) = 34 \cdot 5 = 170$.

Por outro lado, $\alpha\beta = (3+5i)(2+i) = 1+13i$ e calculando a norma de $\alpha\beta$, temos que

$$N(\alpha\beta) = N(1+13i) = 1^2 + 13^2 = 1 + 169 = 170.$$

Portanto, $N(\alpha\beta) = N(\alpha)N(\beta)$.

Observação: A norma de cada inteiro gaussiano é um inteiro positivo, mas não é verdade que cada inteiro positivo é uma norma, pois normas são inteiros positivos da forma a^2+b^2, e nem todo inteiro é possível escrever dessa maneira, que é o caso dos números 3, 7, 11, entre outros.

2.2.3 Unidades e Associados em $\mathbb{Z}[i]$

Veremos que as unidades e os elementos associados em $\mathbb{Z}[i]$ estão diretamente relacionados com a função norma.

Definição 2.14. *Dizemos que α é invertível em $\mathbb{Z}[i]$, se existir $\beta \in \mathbb{Z}[i]$ tal que $\alpha \cdot \beta = 1$*

A partir de agora, quando dizemos que α é invertível, significa α invertível em $\mathbb{Z}[i]$. Pelo Teorema 2.12, podemos verificar a existência de inteiros gaussianos que possuem inverso multiplicativo, ou seja, $\alpha \cdot \beta = 1$.

Teorema 2.15. *Os únicos inteiros gaussianos que são invertíveis em $\mathbb{Z}[i]$ são ± 1 e $\pm i$.*

Demonstração. Tomemos $\alpha, \beta \in \mathbb{Z}[i]$ tais que $\alpha \cdot \beta = 1$. Aplicando a função norma obtemos $N(\alpha\beta) = N(1)$. Pelo Teorema 2.12 , $N(\alpha)N(\beta) = 1$. Como $N(\alpha)$ e $N(\beta)$ são inteiros positivos diferentes de 0, então $N(\alpha) = N(\beta) = 1$. Tomando $\alpha = a + bi$, segue que

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

O mesmo acontece para β. Portanto, os únicos números possíveis para α e β são $-1, 1, i$ e $-i$, ou seja, os únicos inteiros gaussianos invertíveis em $\mathbb{Z}[i]$ são ± 1 e $\pm i$. □

Fica claro observar o resultado do Teorema 2.15 com a representação geométrica dos inteiros gaussianos α e β com normas iguais a 1. Nesse caso a norma é representada geometricamente por uma circunferência de raio 1 e centro $(0, 0)$, Figura 2.6. Note que os únicos inteiros de Gauss pertencentes a circunferência são ± 1 e $\pm i$.

Definição 2.16. *Chamamos os elementos invertíveis de $\mathbb{Z}[i]$ de unidades.*

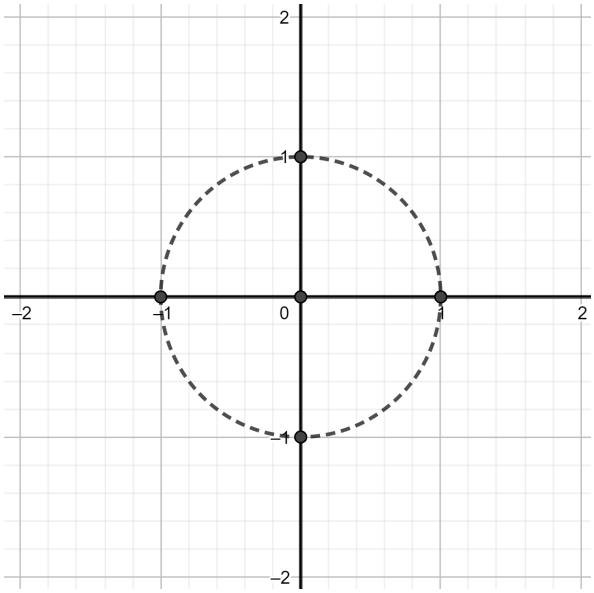

Figura 2.6: Interpretação geométrica do Teorema 2.15

Teorema 2.17. *O elemento $\alpha = a + bi$ é uma unidade em $\mathbb{Z}[i]$ se, e somente se, $N(\alpha) = 1$.*

Demonstração. ($\Rightarrow$) Primeiro suponhamos que $\alpha = a + bi \in \mathbb{Z}[i]$ é uma unidade. Então existe $\beta = c + di \in \mathbb{Z}[i]$ tal que $\alpha \cdot \beta = 1$. Aplicando a função norma na equação temos que $N(\alpha\beta) = N(1)$ e, pelo Teorema 2.12, $N(\alpha)N(\beta) = N(1)$. Logo, $(a^2 + b^2)(c^2 + d^2) = 1$. Como $a^2 + b^2$, $c^2 + d^2 \in \mathbb{Z}_+$, segue que ambos os fatores devem ser iguais a 1. Portanto, $1 = a^2 + b^2 = N(a + bi) = N(\alpha)$.

($\Leftarrow$) Agora, suponhamos para algum $\alpha = a+bi \in \mathbb{Z}[i]$ que $N(\alpha) = 1$. Então $a^2+b^2 = 1$, o que implica que, $a^2 = 1 - b^2$. Como $a^2 \geq 0$, temos que analisar quando $1 - b^2 \geq 0$ e para isso consideremos dois casos:

i) Se $b^2 = 0$ então $b = 0$ e $a^2 = 1 - 0 = 1$. Logo, $a = 1$ ou $a = -1$. Se $a = 1$, então $\alpha = 1 + 0i$. Como $N(1 + 0i) = 1$, segue que $\alpha = 1 + 0i$ é uma unidade em $\mathbb{Z}[i]$. Se $a = -1$, então $\alpha = -1 + 0i$. Como $N(-1 + 0i) = 1$, segue que $\alpha = -1 + 0i$ é uma unidade em $\mathbb{Z}[i]$.

ii) Se $b^2 = 1$ então $a^2 = 1 - 1 = 0$. Logo, $a = 0$ e $b = 1$ ou $b = -1$. Se $b = 1$, então $\alpha = 0 + i$. Como $N(0 + i) = 1$, segue que $\alpha = 0 + i$ é uma unidade em $\mathbb{Z}[i]$. Se $b = -1$, então $\alpha = 0 - i$. Como $N(0 - 0i) = 1$, segue que $\alpha = 0 - i$ é uma unidade em $\mathbb{Z}[i]$.

□

Definição 2.18. *Dizemos que α, $\beta \in \mathbb{Z}[i]$ são associados se $\alpha = u \cdot \beta$ e $N(\alpha) = N(\beta)$, onde $u \in \{-1, 1, i, -i\}$.*

Exemplo 2.19. $3 + 5i$ é associado a $5 - 3i$, pois $3 + 5i = i \cdot (5 - 3i)$.

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

Assim como em $\mathbb{Z}$, falaremos de divisibilidade em $\mathbb{Z}[i]$.

Definição 2.20. *Dados dois inteiros gaussianos α e β, com $\alpha \neq 0$. Diremos que α divide β, escrevendo $\alpha \mid \beta$, quando existir $\omega \in \mathbb{Z}[i]$ tal que $\beta = \alpha \cdot \omega$.*

Exemplo 2.21. Como $-4 + 7i = (1 + 2i)(2 + 3i)$, segue que $(1 + 2i)$ divide $-4 + 7i$.

Exemplo 2.22. $1 + 2i \nmid 4 + 7i$ pois, ao fazermos esta divisão e racionalizar o denominador obtemos:

$$\frac{4+7i}{1+2i} = \frac{(4+7i)(1-2i)}{(1+2i)(1-2i)} = \frac{18-i}{5} = \frac{18}{5} - \frac{1}{5}i \notin \mathbb{Z}[i],$$

pois as partes real e a imaginária não são números inteiros. Portanto, $1 + 2i \nmid 4 + 7i$ em $\mathbb{Z}[i]$.

Veremos sob quais condições $\dfrac{\beta}{\alpha} \in \mathbb{Z}[i]$.

Teorema 2.23. *Dado $\alpha = a + bi \in \mathbb{Z}[i]$ e $c \in \mathbb{Z}$. Então $c \mid \alpha$ se, e somente se, $c \mid a$ e $c \mid b$ em $\mathbb{Z}$.*

Demonstração. Se $c \mid (a + bi)$, então existe $\beta = m + ni \in \mathbb{Z}[i]$ tal que $a + bi = c(m + ni)$. Fazendo a distributiva e comparando as partes reais e imaginárias do inteiro gaussiano, temos que $a = cm$ e $b = cn$, ou seja $c \mid a$ e $c \mid b$.

Reciprocamente, se $c \mid a$ e $c \mid b$ então $a = cm$ e $b = cn$, para algum $m, n \in \mathbb{Z}$. Como $\alpha = a + bi$, substituindo temos $\alpha = (cm) + (cn)i = c(m + ni)$, para algum $c \in \mathbb{Z}$ e $\beta = m + ni \in \mathbb{Z}[i]$. Portanto, $c \mid \alpha$. □

Proposição 2.24. *Se α, β e γ são inteiros gaussianos, $\gamma \mid \alpha$ e $\gamma \mid \beta$, então existem δ, $\eta \in \mathbb{Z}[i]$ tal que $\gamma \mid \alpha\delta + \beta\eta$.*

Demonstração. Se $\gamma \mid \alpha$ e $\gamma \mid \beta$, então $\alpha = \gamma\zeta_1$ e $\beta = \gamma\zeta_2$. Multiplicando as equações por δ e η, respectivamente, obtemos $\alpha\delta = \gamma\zeta_1\delta$ e $\beta\eta = \gamma\zeta_2\eta$. Somando as equações temos que $\alpha\delta + \beta\eta = \gamma(\zeta_1\delta + \zeta_2\eta)$. Portanto, $\gamma \mid \alpha\delta + \beta\eta$.

□

Teorema 2.25. *Para α, $\beta \in \mathbb{Z}[i]$, se $\alpha \mid \beta$ em $\mathbb{Z}[i]$, então $N(\alpha) \mid N(\beta)$ em $\mathbb{Z}$.*

Demonstração. Como $\alpha \mid \beta$, então existe $\gamma \in \mathbb{Z}[i]$, tal que $\beta = \alpha\gamma$. Aplicando a norma nesta equação temos, $N(\beta) = N(\alpha\gamma)$. Pelo Teorema 2.12, $N(\beta) = N(\alpha)N(\gamma)$ e portanto $N(\alpha) \mid N(\beta)$, já que a norma é uma função em $\mathbb{Z}$. □

Exemplo 2.26. Vamos encontrar todos os divisores de $1-3i$ em $\mathbb{Z}[i]$.

Para isso, temos que encontrar os inteiros gaussianos $\alpha = a+bi$, tal que $\alpha \mid 1-3i$. Se $1-3i = \alpha\gamma$, $\gamma \in \mathbb{Z}[i]$, então aplicando a função norma teremos

$$\begin{aligned} N(1-3i) &= N(\alpha\gamma) \\ 10 &= N(\alpha)N(\gamma). \end{aligned}$$

Pelo Teorema 2.25, se $\alpha \mid 1-3i$ então $N(\alpha) \mid 10$, logo $N(\alpha) \in \{1,2,5,10\}$. Fazendo $\alpha = a+bi$, temos:

- se $N(\alpha) = a^2+b^2 = 1$, então $\alpha \in \{\pm 1, \pm i\}$;
- se $N(\alpha) = a^2+b^2 = 2$, então $\alpha \in \{\pm(1+i), \pm(1-i)\}$;
- se $N(\alpha) = a^2+b^2 = 5$, então $\alpha \in \{\pm(1+2i), \pm(1-2i), \pm(2+i), \pm(2-i)\}$ e
- se $N(\alpha) = a^2+b^2 = 10$, então $\alpha \in \{\pm(1+3i), \pm(1-3i), \pm(3+i), \pm(3-i)\}$.

Portanto, encontramos 24 possíveis divisores de $1-3i$. Ao fazermos a verificação, os divisores de $1-3i$ são:

$$\{\pm 1, \pm i, \pm(1+i), \pm(1-i), \pm(1+2i), \pm(2-i), \pm(1-3i), \pm(3+i)\}.$$

Podemos observar na Figura 2.7 a representação de $N(\alpha) \in \{1,2,5,10\}$ nas circunferências C_1, C_2, C_3 e C_4, respectivamente. Os pontos marcados são os inteiros de Gauss α que pertencem as circunferências.

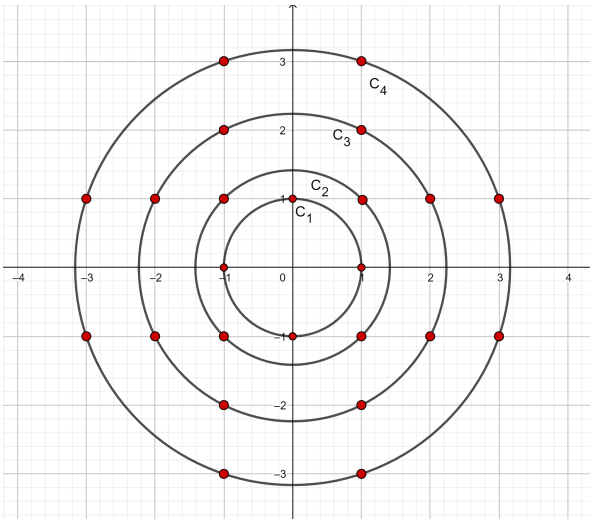

Figura 2.7: Representação gráfica do Exemplo 2.26

Corolário 2.27. *Um inteiro gaussiano tem norma par se, e somente se, é um múltiplo de* $1+i$.

Demonstração. ($\Leftarrow$) Como $N(1+i)=2$, segue que qualquer múltiplo de $1+i$ tem norma par.
($\Rightarrow$) Por outro lado, seja $\alpha = a+bi \in \mathbb{Z}[i]$ com norma par, ou seja, $a^2+b^2 = 2t$, $t \in \mathbb{Z}$. Para a^2+b^2 ser par, a e b devem ser ambos pares ou ambos ímpares. Tomando $a+bi = (1+i)(r+si)$ para alguns $r, s \in \mathbb{Z}$, temos que $a+bi = (r-s)+(r+s)i$, que tem solução $r = \frac{a+b}{2}$ e $s = \frac{b-a}{2}$. Como a e b tem a mesma paridade, r e s são números inteiros. Portanto α é um múltiplo de $1+i$. □

Exemplo 2.28. Seja $\alpha = 5+3i$. Temos que $N(\alpha) = 5^2+3^2 = 34$ e pelo Corolário 2.27, $5+3i$ é múltiplo de $1+i$. Ainda, de acordo com a demonstração do Corolário 2.27, $\gamma \in \mathbb{Z}[i]$ é dado por

$$\gamma = \left(\frac{5+3}{2}\right) + \left(\frac{5-3}{2}\right) = 4+i.$$

Portanto, $5+3i = (1+i)(4+i)$.

Lema 2.29. *Se* $\beta \mid \alpha$ *e* $N(\beta) = 1$ *ou* $N(\beta) = N(\alpha)$*, então ou* β *é uma unidade ou é um associado de* α.

Demonstração. Se $N(\beta) = 1$, então β é uma unidade, pelo Teorema 2.17. Se $N(\beta) = N(\alpha)$, com $\beta \mid \alpha$, então $\alpha = \beta\gamma$ para algum $\gamma \in \mathbb{Z}[i]$. Aplicando a função norma, temos $N(\alpha) = N(\beta)N(\gamma)$. Substituindo, temos

$$\begin{aligned} N(\alpha) &= N(\alpha)N(\gamma) \\ N(\alpha) - N(\alpha)N(\gamma) &= 0 \\ N(\alpha)(1-N(\gamma)) &= 0. \end{aligned}$$

Como a norma de um inteiro gaussiano não nulo é um número inteiro positivo, concluímos que $N(\gamma) = 1$. Portanto, β é um associado de α. □

É importante observar que o Lema 2.29 não afirma que existem apenas $\pm\alpha$ ou $\pm\alpha i$ cuja a norma é igual a $N(\alpha)$. Os números $18i$ e $-4+7i$ possuem normal igual a 65 e ambos não são associados. Na verdade, o Lema 2.29 indica que $\pm\alpha$ ou $\pm\alpha i$ são os únicos inteiros de Gauss que dividem α e tem normal igual a $N(\alpha)$.

2.2.5 Teorema da Divisão em $\mathbb{Z}[i]$

Uma razão pela qual somos capazes de transferir muitas propriedades de $\mathbb{Z}$ para $\mathbb{Z}[i]$ é devido ao próximo teorema.

Teorema 2.30. *(Teorema da Divisão) Para α, $\beta \in \mathbb{Z}[i]$, com $\beta \neq 0$, existem γ, $\delta \in \mathbb{Z}[i]$ de tal forma que $\alpha = \beta\gamma + \delta$ e $\delta = 0$ ou $N(\delta) < N(\beta)$.*

Demonstração. Ao fazermos a divisão de α por β, obtemos $\dfrac{\alpha}{\beta} = x + yi$, onde x e y podem ser inteiros ou racionais. Se x e y forem inteiros então $\gamma = x + yi$ e $\delta = 0$. Se x e y forem racionais então devemos procurar m e n, os inteiros mais próximos de x e y, respectivamente, ou seja, $\mid x - m \mid \leq \dfrac{1}{2}$ e $\mid y - n \mid \leq \dfrac{1}{2}$. Tomando $\gamma = m + ni$ e $\delta = \alpha - \beta\gamma$, temos que

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = N((x+yi) - (m+ni)) = N((x-m) + (y-n)i) = (x-m)^2 + (y-n)^2.$$

Como $\mid x - m \mid \leq \dfrac{1}{2}$ e $\mid y - n \mid \leq \dfrac{1}{2}$, segue que $(x-m)^2 \leq \dfrac{1}{4}$ e $(y-n)^2 \leq \dfrac{1}{4}$. Assim

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = (x-m)^2 + (y-n)^2 \leq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}.$$

Como $N\left(\dfrac{\alpha}{\beta} - \gamma\right) \leq \dfrac{1}{2}$ e $\dfrac{1}{2} < 1$, segue que $N(\dfrac{\alpha}{\beta} - \gamma) < 1$. Multiplicando por $N(\beta)$ esta desigualdade, obtemos

$$\begin{aligned} N\left(\frac{\alpha}{\beta} - \gamma\right) N(\beta) &< N(\beta) \\ N\left(\left(\frac{\alpha}{\beta} - \gamma\right)\beta\right) &< N(\beta) \\ N(\alpha - \beta\gamma) &< N(\beta) \\ N(\delta) &< N(\beta). \end{aligned}$$

□

Exemplo 2.31. Considere $\alpha = 1 + 4i$ e $\beta = 2 - 6i$. Vamos realizar a divisão para encontrar $\alpha = \beta\gamma + \delta$. Como $N(\beta) = 40$, pelo Teorema 2.30 devemos ter $N(\delta) < 40$. Note que

$$\frac{1+4i}{2-6i} = \frac{(1+4i)(2+6i)}{(2-6i)(2+6i)} = \frac{-22+14i}{40} = -\frac{11}{20} + \frac{7}{20}i.$$

Como $-\frac{11}{20} = -0,55$ e $\frac{7}{20} = 0,35$, temos que considerar o maior inteiro mais próximo deles. Logo, $\gamma = -1 + 0i$ e assim segue que

$$1 + 4i = (2 - 6i)(-1 + 0i) + (3 - 2i),$$

já que $\delta = 3 - 2i$ e $N(3 - 2i) = 13$, $N(\delta) < 40$.

Existe uma diferença interessante entre o teorema da divisão em $\mathbb{Z}[i]$ e o teorema da divisão em $\mathbb{Z}$: o quociente e o resto não são únicos em $\mathbb{Z}[i]$.

Exemplo 2.32. Seja $\alpha = 37 + 2i$ e $\beta = 11 + 2i$. Temos que $N(\beta) = 125$. Se realizarmos o algoritmo da divisão em $\mathbb{Z}[i]$ (Teorema 2.30), encontraremos que

$$\alpha = 3\beta + (4 - 4i).$$

Entretanto, também é verdade que

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

O resto em ambos os casos tem norma menor do que 125 (na verdade, menor do que $\frac{125}{2}$).

2.2.6 O Algoritmo de Euclides em $\mathbb{Z}[i]$

Começamos definindo o máximo divisor comum em $\mathbb{Z}[i]$.

Definição 2.33. *Sejam α, β e γ inteiros gaussianos não nulos. Diremos que γ será o máximo divisor comum de α e β, quando:*

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

ii) Se existe $\delta \in \mathbb{Z}[i]$ tal que $\delta \mid \alpha$ e $\delta \mid \beta$, então $N(\delta) \leq N(\gamma)$.

Em outras palavras, o mdc entre dois ou mais inteiros gaussianos será o divisor comum com a maior norma. Indicamos o máximo divisor comum de α e β por $\gamma = mdc(\alpha, \beta)$.

Mesmo sendo análogo o conceito de máximo divisor comum em relação a $\mathbb{Z}$, não existe um valor fixo para $mdc(\alpha, \beta)$. Se γ é um máximo divisor comum de α e β, neste caso, também são (pelo menos) seus múltiplos da unidade: $-\gamma, i\gamma$ e $-i\gamma$. Devido a isso, há a possibilidade de existir maiores divisores. Assim, podemos falar apenas na existência de *um máximo divisor comum*, porém não sobre *o maior divisor comum*.

Teorema 2.34. *Se α, $\beta \in \mathbb{Z}[i]$ e $\alpha = \beta\gamma + \delta$, onde γ e δ são inteiros gaussianos, então $mdc(\alpha, \beta) = mdc(\beta, \delta)$.*

Demonstração. Da relação $\alpha = \beta\gamma + \delta$ podemos concluir que todo divisor de β e γ é um divisor de α, pela Proposição 2.24. Esta mesma relação, escrita da seguinte forma $\delta = \alpha - \beta\gamma$ nos diz que todo divisor de α e β é um divisor de δ. Logo o conjunto de divisores comuns de α e β é igual ao conjunto de divisores de β e δ, o que nos garante que $mdc(\alpha, \beta) = mdc(\beta, \delta)$. □

Teorema 2.35. *(Algoritmo de Euclides) Sejam α, $\beta \in \mathbb{Z}[i]$ e diferentes de zero. Aplicando repetidamente o Teorema 2.30 (Teorema da Divisão), onde o resto é diferente de zero, teremos:*

$$\alpha = \beta\gamma_1 + \delta_1, \textit{ com } N(\delta_1) < N(\beta)$$
$$\beta = \delta_1\gamma_2 + \delta_2, \textit{ com } N(\delta_2) < N(\delta_1)$$
$$\delta_1 = \delta_2\gamma_3 + \delta_3, \textit{ com } N(\delta_3) < N(\delta_2)$$
$$\vdots$$

O último resto diferente de zero é divisível por todos os divisores comuns de α e β e será divisor comum, por isso é um máximo divisor comum de α e β.

Demonstração. Pela divisão euclidiana, temos

$$\alpha = \beta\gamma_1 + \delta_1, \text{ com } N(\delta_1) < N(\beta).$$

Pelo Teorema 2.34, $mdc(\alpha, \beta) = mdc(\beta, \delta_1)$, desta forma temos duas situações:

1. $N(\delta_1) = 0$, neste caso $mdc(\beta, \delta_1) = \beta$.

2. $N(\delta_1) \neq 0$, neste caso fazemos a divisão euclidiana de β por δ_1, obtendo

$$\beta = \delta_1\gamma_2 + \delta_2, \text{ com } N(\delta_2) < N(\delta_1).$$

Segue que $mdc(\beta, \delta_1) = mdc(\delta_1, \delta_2)$. Novamente pode ocorrer duas situações:

1. $N(\delta_2) = 0$, neste caso $mdc(\delta_1, \delta_2) = \delta_1$.

2. $N(\delta_2) \neq 0$, neste caso fazemos a divisão euclidiana de δ_1 por δ_2, obtendo

$$\delta_1 = \delta_2\gamma_3 + \delta_3, \text{ com } N(\delta_3) < N(\delta_2).$$

Segue que

$$mdc(\alpha, \beta) = mdc(\beta, \delta_1) = mdc(\delta_1, \delta_2) = mdc(\delta_2, \beta_3),$$

e assim sucessivamente.

Definindo $\delta_0 = \beta$, existe um valor n natural que $\delta_{n+1} = 0$ e $\delta_n \neq 0$. De fato se tivéssemos para todo n, $\delta_n \neq 0$, teríamos uma sequência infinita em $\mathbb{N}$,

$$N(\delta_0) > N(\delta_1) > N(\delta_2) > ... > 0,$$

o que é um absurdo. Logo,

$$mdc(\alpha, \beta) = mdc(\beta, \delta_1) = mdc(\delta_1, \delta_2) = ... = mdc(\delta_n, \delta_{n+1}) = mdc(\delta_n, 0) = \delta_n.$$

Portanto, o último resto não nulo δ_n deste processo fornece o valor de $mdc(\alpha, \beta)$. □

Exemplo 2.36. Vamos encontrar $mdc(32+9i, 4+11i)$. Aplicando o teorema da divisão (Teorema 2.30) e o Algoritmo de Euclides (Teorema 2.35), encontramos

$$\begin{aligned} 32+9i &= (4+11i)(2-2i)+(2-5i) \\ 4+11i &= (2-5i)(-2+i)+(3-i) \\ 2-5i &= (3-i)(1-i)+(-i) \\ 3-i &= (-i)(1+3i)+0. \end{aligned}$$

Portanto, $mdc(32+9i, 4+11i) = -i$.

Definição 2.37. *Dizemos que α, $\beta \in \mathbb{Z}[i]$ são primos entre si ou coprimos, quando têm as unidades como máximo divisor comum.*

Exemplo 2.38. No Exemplo 2.36, $32+9i$ e $4+11i$ são primos entre si.

Exemplo 2.39. Para calcular $mdc(27+4i, 5-2i)$ basta aplicar o teorema da divisão (Teorema 2.30) e em seguida o Algoritmo de Euclides (Teorema 2.35). Logo, encontramos,

$$\begin{aligned} 27+4i &= (5-2i)(4+3i)+(1-3i) \\ (5-2i) &= (1-3i)(1+i)+1 \\ (1-3i) &= 1(1-3i)+0. \end{aligned}$$

O último resto diferente de zero é 1, então $mdc(27+4i, 5-2i) = 1$ e portanto, $27+4i$ e $5-2i$ são primos entre si.

Nos exemplos apresentados o máximo divisor comum entre dois inteiros gaussianos é uma unidade, mas veremos no resultado que segue que isso nem sempre acontece.

Proposição 2.40. *Dados α, $\beta \in \mathbb{Z}[i]$ e $\gamma = mdc(\alpha, \beta)$ obtido pelo algoritmo de Euclides. Qualquer máximo divisor comum é associado a γ.*

Demonstração. Suponha que $\tilde{\gamma} = mdc(\alpha, \beta)$. Como $\gamma \mid \alpha$ e $\gamma \mid \beta$, segue que

$$\gamma \mid \tilde{\gamma} \Rightarrow N(\gamma) \leq N(\tilde{\gamma}). \tag{2.13}$$

Por outro lado, como $\gamma = (\alpha, \beta)$ e $\tilde{\gamma} \mid \alpha$ e $\tilde{\gamma} \mid \beta$ então

$$\tilde{\gamma} \mid \gamma \Rightarrow N(\tilde{\gamma}) \leq N(\gamma). \tag{2.14}$$

De (2.13) e (2.14), temos que $N(\gamma) = N(\tilde{\gamma})$, assim, γ e $\tilde{\gamma}$ são associados, segundo o Lema 2.29 .

□

Exemplo 2.41. Suponha $\alpha = 11 + 3i$ e $\beta = 1 + 8i$. Pelo teorema de Euclides (Teorema 2.35), temos que

$$\begin{aligned} 11 + 3i &= (1 + 8i)(1 - i) + (2 - 4i) \\ 1 + 8i &= (2 - 4i)(-1 + i) + (-1 + 2i) \\ 2 - 4i &= (-1 + 2i)(-2) + 0. \end{aligned}$$

Neste caso $mdc(\alpha, \beta) = -1 + 2i$.

Agora, vamos utilizar uma outra possibilidade na segunda equação.

$$\begin{aligned} 11 + 3i &= (1 + 8i)(1 - i) + (2 - 4i) \\ 1 + 8i &= (2 - 4i)(-2 + i) + (-1 - 2i) \\ 2 - 4i &= (1 - 2i)(2) + 0. \end{aligned}$$

Neste caso $mdc(\alpha, \beta) = 1 - 2i$.

Note que obtemos dois máximos divisor comum para α e β e segundo a Proposição 2.40, eles são associados. De fato,

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

2.2.7 O Teorema de Bézout em $\mathbb{Z}[i]$

Vimos no Capítulo 1 que em $\mathbb{Z}$ o teorema de Bézout diz que para todo inteiro não nulo a e b em $\mathbb{Z}$ tem-se que $mdc(a, b) = ax + by$, para algum $x,\ y \in \mathbb{Z}$ que são encontrados usando o algoritmo euclidiano. A mesma ideia vale para $\mathbb{Z}[i]$, conforme veremos aqui.

Teorema 2.42. *(Teorema de Bézout) Sejam $\alpha,\ \beta \in \mathbb{Z}[i]$ diferentes de zero e $mdc(\alpha, \beta) = \gamma$. Então $\gamma = \alpha x + \beta y$, para algum $x,\ y \in \mathbb{Z}[i]$.*

Demonstração. Considere o conjunto C sendo todas as combinações lineares de α e β e $n = \alpha x_0 + \beta y_0$, onde n é o elemento de menor norma de C. Suponha por absurdo que $n \nmid \alpha$. Então $\alpha = nq + r$, com $N(r) < N(n)$. Temos que

$$\begin{aligned} r &= \alpha - nq \\ &= \alpha - (\alpha x_0 + \beta y_0)q \\ &= \alpha - \alpha x_0 q - \beta y_0 q \\ &= \alpha(1 - x_0 q) + \beta(-y_0 q). \end{aligned}$$

Então $r \in C$, $N(r) < N(n)$, mas n é o elemento de menor norma em C, portanto, $n \mid \alpha$.

Analogamente, $n \mid \beta$. Assim, n é o divisor comum de α e β. Vamos mostrar que $n = \gamma$. De fato, como $mdc(\alpha, \beta) = \gamma$, então $\gamma \mid \alpha$ e $\gamma\beta$. Logo existem q_1 e $q_2 \in \mathbb{Z}[i]$ tais que $\alpha = \gamma q_1$ e $\beta = \gamma q_2$. Como $n = \alpha x_0 + \beta y_0$, segue que

$$n = (\gamma q_1)x_0 + (\gamma q_2)y_0$$
$$n = \gamma(q_1 x_0 + q_2 y_0).$$

Se $\gamma \mid n$ então $N(\gamma) \mid N(n)$. Como n é o menor elemento de C, $N(\gamma) = N(n)$. Se $\gamma \mid n$ e $N(\gamma) = N(n)$ então γ e n são associados. Isso implica que,

$$\gamma = n \cdot u \Rightarrow \gamma = \alpha x_0 u + \beta y_0 u \Rightarrow \gamma = \alpha x + \beta y,$$

para algum $x, y \in \mathbb{Z}[i]$. □

Corolário 2.43. *Sejam α e β inteiros gaussianos primos entre si. Então existem $x, y \in \mathbb{Z}[i]$ tais que $\alpha x + \beta y = 1$.*

Demonstração. Como α e β são primos entre si, então $mdc(\alpha, \beta) = m$, onde $m \in \{-1, 1, -i, i\}$. Pelo Teorema 2.42, existem $x, y \in \mathbb{Z}[i]$ tais que $\alpha x + \beta y = m$.

Temos quatro casos:

1. Para $m = 1$, então $\alpha x + \beta y = 1$;
2. Para $m = -1$, então $\alpha x + \beta y = -1$, multiplicando a equação por -1, temos que $\alpha(-x) + \beta(-yi) = 1$.
3. Para $m = i$, então $\alpha x + \beta y = i$, multiplicando a equação por $-i$, temos que $\alpha(-xi) + \beta(-yi) = 1$.
4. Para $m = -i$, então $\alpha x + \beta y = -i$, multiplicando a equação por i, temos que $\alpha(xi) + \beta(yi) = 1$.

Portanto, em todos os casos conseguimos escrever $\alpha x + \beta y = 1$. □

Exemplo 2.44. Temos que $27+4i$ e $5-2i$ são primos entre si, pois $mdc(27+4i, 5-2i) = 1$. Agora, escrevendo 1 como uma combinação linear de $27 + 4i$ e $5 - 2i$, conforme o teorema de Bézout (Teorema 2.42) obtemos:

$$1 = 5 - 2i - (1 - 3i)(1 + i)$$
$$1 = 5 - 2i - [(27 + 4i) - (5 - 2i)(4 + 3i)](1 + i)$$
$$1 = 5 - 2i - (27 + 4i)(1 + i) + (5 - 2i)(4 + 3i)(1 + i)$$
$$1 = (5 - 2i)[1 + (4 + 3i)(1 + i)] - (27 + 4i)(1 + i)$$
$$1 = (5 - 2i)[1 + 1 + 7i] + (27 + 4i)(-1 - i)$$
$$1 = (5 + 2i)(2 + 7i) + (27 + 4i)(-1 - i).$$

Logo, $(27+4i)(-1-i)+(5-2i)(2+7i)=1$, com $x=-1-i$ e $y=2+7i$.

Corolário 2.45. *Se $\alpha \mid \beta\gamma$ e α e β são primos entre si, então $\alpha \mid \gamma$.*

Demonstração. Como $\alpha \mid \beta\gamma$ segue que $\beta\gamma = \alpha n$, para algum $n \in \mathbb{Z}[i]$. Sendo α e β primos entre si, pelo Corolário 2.43 temos que existem x, $y \in \mathbb{Z}[i]$, tais que

$$\alpha x + \beta y = 1. \tag{2.15}$$

Multiplicando a Equação 2.15 por γ e sabendo que $\beta\gamma = \alpha n$, temos que $\gamma = \alpha(\gamma x + ny)$, ou seja, $\alpha \mid \gamma$.

□

Teorema 2.46. *Sejam $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ tais que $mdc(\alpha,\beta)=1$ e $\gamma=\alpha\beta$. Então para todo $\delta \in \mathbb{Z}[i]$, $mdc(\gamma,\delta)=1$ se, e somente se, $mdc(\alpha,\delta)=1$ e $mdc(\beta,\delta)=1$.*

Demonstração. ($\Rightarrow$) Sejam α, β, γ em $\mathbb{Z}[i]$ tal que α e β são primos entre si e $\gamma = \alpha\beta$. Suponhamos que $mdc(\alpha,\delta) \neq 1$ ou $mdc(\beta,\delta) \neq 1$. Sem perda de generalidade, tomamos $mdc(\alpha,\delta)=\mu$ para algum $\mu \in \mathbb{Z}[i]$, não unidade. Então $\mu \mid \alpha$ e $\mu \mid \delta$ e além disso, já que $\alpha \mid \gamma$, temos que $\mu \mid \gamma$. Como $\mu \mid \gamma$ e $\mu \mid \delta$, segue que μ é um divisor comum, diferente da unidade, de γ e δ. Assim, γ e δ não são primos entre si, pois $2 \leq N(\mu) \leq N(\gamma)$.
($\Leftarrow$) Agora, suponhamos que $mdc(\alpha,\delta)=1$ e $mdc(\beta,\delta)=1$. Então, $\alpha k_1 + \delta k_2 = 1$ e $\beta k_3 + \delta k_4 = 1$ para algum k_1, k_2, k_3 e $k_4 \in \mathbb{Z}[i]$. Multiplicando as equações membro a membro, temos

$$(\alpha k_1 + \delta k_2)(\beta k_3 + \delta k_4) = 1$$
$$\alpha k_1 \beta k_3 + \alpha k_1 \delta k_4 + \delta k_2 \beta k_3 + \delta k_2 \delta k_4 = 1.$$

Como $\gamma = \alpha\beta$,

$$\gamma(k_1 k_3) + \delta(\alpha k_1 k_4 + k_2 \beta k_3 + k_2 \delta k_4) = 1.$$

Portanto, $mdc(\gamma,\delta)=1$. □

2.2.8 Primos em $\mathbb{Z}[i]$ e Fatoração Única

Nesta seção responderemos a seguinte pergunta: como são caracterizados os primos em $\mathbb{Z}[i]$?

Definição 2.47. *Seja $\alpha \in \mathbb{Z}[i]$. Dizemos que α é composto se existirem $\beta, \gamma \in \mathbb{Z}[i]$ tais que $\alpha = \beta\gamma$ e $N(\beta) > 1$ e $N(\gamma) > 1$. Se α tem somente fatores triviais, dizemos que α é um número primo.*

Ao pensar em números primos é natural perguntar: todo primo em $\mathbb{Z}$ é primo em $\mathbb{Z}[i]$? Nem sempre, vejamos os exemplos que seguem.

Exemplo 2.48. 13 é primo em $\mathbb{Z}$ mas não é primo em $\mathbb{Z}[i]$ pois, $13 = (3+2i)(3-2i)$.

Exemplo 2.49. 7 é primo em $\mathbb{Z}$ e é primo em $\mathbb{Z}[i]$. De fato, suponhamos que 7 é composto, então podemos escrever $7 = \alpha\beta$ com $N(\alpha)$> 1 e $N(\beta) > 1$. Tomando a norma em ambos os membros temos que $N(\alpha)N(\beta) = 49$. Logo, como $N(\alpha)$> 1 e $N(\beta) > 1$ segue que $N(\alpha) = 7$. Se $\alpha = a + bi$ então $N(\alpha) = a^2 + b^2 = 7$, que não tem solução inteira. Portanto, 7 é primo em $\mathbb{Z}[i]$.

Teorema 2.50. *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. Suponha $N(\alpha) = p$, p é primo em $\mathbb{Z}$. Considere qualquer fatoração de α, sendo como $\alpha = \beta\gamma$ para $\beta, \gamma \in \mathbb{Z}[i]$. Aplicando a função Norma, temos que $N(\alpha) = N(\beta)N(\gamma)$, então $N(\beta)N(\gamma) = p$. Como p é primo temos duas possibilidades: ou $N(\beta) = 1$ e $N(\gamma) = p$ ou $N(\beta) = p$ e $N(\gamma) = 1$. Podemos observar que β é uma unidade e γ é um associado de α ou β é um associado de α e γ é uma unidade e, portanto, α possui apenas divisores triviais, ou seja, α é primo. □

Exemplo 2.51. $5 + 2i$ é primo em $\mathbb{Z}[i]$, pois $N(5+2i) = 5^2 + 2^2 = 25 + 4 = 29$ e 29 é primo em $\mathbb{Z}$.

Lema 2.52. *Seja π um primo em $\mathbb{Z}[i]$ e $\alpha\beta \in \mathbb{Z}[i]$. Se $\pi \mid \alpha\beta$, então $\pi \mid \alpha$ ou $\pi \mid \beta$.*

Demonstração. Suponha que $\pi \nmid \alpha$. Então $mdc(\alpha, \pi)$ é uma unidade, isso significa que α e π são primos entre si. Sendo assim, podemos escrevê-los como uma combinação linear, $\alpha x + \pi u = 1$. Multiplicando por β, temos que $\beta\alpha x + \beta\pi y = \beta$. Como $\pi \mid \alpha\beta$ e $\pi \mid \pi$, temos que $\pi \mid (\beta\alpha x + \beta\pi y)$ e, portanto, $\pi \mid \beta$. □

Lema 2.53. *α é primo em $\mathbb{Z}[i]$ se, e somente se, seu conjugado $\overline{\alpha}$ é primo em $\mathbb{Z}[i]$.*

Demonstração. Suponha que α não é primo em $\mathbb{Z}[i]$. Então $\alpha = \gamma\beta$, onde $\gamma, \beta \in \mathbb{Z}[i]$ são divisores não triviais de α. Por conjugação, temos $\overline{\alpha} = \overline{\gamma\beta} = \overline{\gamma}\,\overline{\beta}$ e portanto $\overline{\alpha}$ tem uma fatoração de números não triviais, ou seja, $\overline{\alpha}$ não é primo em $\mathbb{Z}[i]$.

Reciprocamente, suponha que $\overline{\alpha}$ não é primo em $\mathbb{Z}[i]$. Então $\overline{\alpha} = \overline{\gamma}\overline{\beta}$, onde $\overline{\gamma}$ e $\overline{\beta}$ são divisores não triviais de $\overline{\alpha}$. Aplicando a conjugação complexa na igualdade anterior temos:

$$\begin{aligned} \overline{\overline{\alpha}} &= \overline{\overline{\gamma}\,\overline{\beta}} \\ \alpha &= \overline{\overline{\gamma}}\,\overline{\overline{\beta}} \\ \alpha &= \gamma\beta, \end{aligned}$$

com $\gamma, \beta \in \mathbb{Z}[i]$ divisores não triviais de α. Portanto α não é primo em $\mathbb{Z}[i]$. □

Lema 2.54. *Se $\alpha = a + bi$ com $a \cdot b \neq 0$ é primo em $\mathbb{Z}[i]$, então $N(\alpha) = a^2 + b^2$ é primo em $\mathbb{Z}$.*

Demonstração. Note que $N(\alpha) = a^2 + b^2 = (a + bi)(a - bi)$ é um múltiplo de α. Suponha que $N(\alpha) = a^2 + b^2$ não é primo em $\mathbb{Z}$, ou seja,

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

com $m, n \geq 2$. Por hipótese, $\alpha = a + bi$ é primo em $\mathbb{Z}[i]$ e como $\alpha \mid m \cdot n$, segue do Lema 2.52 que $\alpha \mid m$ ou $\alpha \mid n$. Se $\alpha \mid m$ então $m = \gamma \cdot \alpha$, para algum $\gamma \in \mathbb{Z}[i]$, ou seja, m não pode ser associado a α. Logo, multiplicando por n temos

$$\begin{aligned} m \cdot n = \gamma \cdot \alpha \cdot n &= (a + bi)(a - bi) \\ \gamma \cdot n &= (a - bi). \end{aligned}$$

Como n não é uma unidade, então $a - bi$ não é primo em $\mathbb{Z}[i]$, o que é um absurdo. □

Exemplo 2.55. $2 + i$ é primo em $\mathbb{Z}[i]$ e $N(2 + i) = 2^2 + 1^2 = 4 + 1 = 5$ é primo em $\mathbb{Z}$.

Lema 2.56. *Seja $\alpha = a + bi \in \mathbb{Z}[i]$ com $a \cdot b \neq 0$. Então $\alpha = a + bi$ é primo em $\mathbb{Z}[i]$ se, e somente se, $a^2 + b^2 = p$ é um número primo em $\mathbb{Z}$ com $p \equiv 1 (mod\ 4)$ ou $p = 2$.*

Demonstração. ($\Rightarrow$) Suponha que $\alpha = a + bi$ é primo em $\mathbb{Z}[i]$. Usando a aritmética módulo 4 vamos calcular a soma de $a^2 + b^2$ módulo 4:

$$0^2 \equiv 0(\text{ mod } 4),\ 1^2 \equiv 1(\text{ mod } 4),\ 2^2 \equiv 0(\text{ mod } 4) \text{ e } 3^2 \equiv 1(\text{ mod } 4).$$

Logo, um quadrado módulo 4 é igual a 0 ou 1, e sua soma módulo 4 é 0, 1 ou 2, ou seja,

$$p \equiv 0(\text{ mod } 4),\ p \equiv 1(\text{ mod } 4) \text{ ou } p \equiv 2(\text{ mod } 4).$$

Se $p \equiv 0(\text{ mod } 4)$, então $4 \mid p$, logo p não é primo. Pelo Lema 2.54, $p = a^2 + b^2 \equiv 1(\text{ mod } 4)$ ou $p = a^2 + b^2 \equiv 2(\text{ mod } 4)$ e o único primo p, $p \equiv 2(\text{ mod } 4)$ é $p = 2$.
($\Leftarrow$) Suponha que $a^2 + b^2 = p$ é um número primo e que $\alpha = a + bi$ não é primo, ou seja, $a + bi = \gamma \cdot \beta$, para algum $\gamma, \beta \in \mathbb{Z}[i]$. Então,

$$\begin{aligned} N(a + bi) &= N(\gamma \cdot \beta) \\ a^2 + b^2 &= N(\gamma)N(\beta) \\ p &= N(\gamma)N(\beta). \end{aligned}$$

Como p é primo, então $N(\gamma) = 1$ ou $N(\beta) = 1$. Logo γ ou β é uma unidade, o que é um absurdo. Portanto $\alpha = a + bi$ é primo. □

Exemplo 2.57. $2+5i$ é primo em $\mathbb{Z}[i]$, pois $N(2+5i) = 2^2+5^2 = 4+25 = 29$ e $29 \equiv 1(\text{mod } 4)$.

Observação 2.58. 1. Qualquer número que é $\equiv 3\,(mod\,4)$ não é a soma de dois quadrados em $\mathbb{Z}$. De fato, os quadrados módulo 4 são 0 e 1. Fazendo a soma entre eles e a congruência módulo 4 temos:

$$0+0=0\equiv 0\,(mod\,4),\ 1+0=0+1=1\equiv\ (mod\,4)\ e\ 1+1=2\equiv 2\,(mod\,4).$$

2. Se $a+bi$ é um primo em $\mathbb{Z}[i]$ com $a^2+b^2=p=2$, então $a+bi$ é um dos quatro elementos:

   - Se $a=1$ e $b=1$, então $\alpha=1+i$;
   - Se $a=1$ e $b=-1$, então $\alpha=1-i$;
   - Se $a=-1$ e $b=1$, então $\alpha=-1+i$;
   - Se $a=-1$ e $b=-1$, então $\alpha=-1-i$;

3. Considerando elementos da forma a ou bi em $\mathbb{Z}[i]$, podemos ver bi como um associado de b, pois $b=-i(bi)$. Agora os elementos da forma $a+0i$ estão em $\mathbb{Z}[i]$. Note que, se n é um inteiro composto em $\mathbb{Z}$, então n é um inteiro composto em $\mathbb{Z}[i]$, pois para $n=r\cdot s$ como $r,s>1$ em $\mathbb{Z}$, temos $n=r\cdot s=(r+0i)(s+0i)\in\mathbb{Z}[i]$.

Lema 2.59. *Se p é primo em $\mathbb{Z}$ com $p\equiv 3(mod\ 4)$, então p também é primo em $\mathbb{Z}[i]$.*

Demonstração. Suponha que p não é primo em $\mathbb{Z}[i]$. Então $p=\alpha\beta$, onde nem α e nem β são unidades em $\mathbb{Z}[i]$. Logo,

$$\begin{aligned} N(p) &= N(\alpha\beta)=N(\alpha)N(\beta)\\ p^2 &= N(\alpha)N(\beta). \end{aligned}$$

Como $N(\alpha)>1$ e $N(\beta)>1$, temos que $N(\alpha)=N(\beta)=p$. Mas, $N(\alpha)=N(\beta)$ é a soma de dois quadrados e a soma de dois quadrados nunca pode ser congruente a 3 módulo 4 (Observação 2.58, item 1)). Portanto, a hipótese de p não ser primo em $\mathbb{Z}[i]$ é falsa, logo p é primo em $\mathbb{Z}[i]$. □

Exemplo 2.60. 5 não é primo em $\mathbb{Z}[i]$ já que não é congruente a 3 módulo 4. Mas 7 é primo em $\mathbb{Z}[i]$, pois $7\equiv 3(\text{mod }4)$.

Lema 2.61. *Seja p um primo em $\mathbb{Z}$. Se $p\equiv 1(mod\ 4)$, então a congruência $x^2\equiv -1(mod\ p)$ tem solução.*

Demonstração. Considere $p\neq 2$ e o polinômio

$$T^{p-1}-1=(T^{\frac{p-1}{2}}-1)(T^{\frac{p-1}{2}}+1)\text{ módulo }p.$$

Vamos contar as raízes desses polinômios módulo p. Sabemos que um polinômio de grau d não tem mais que d raízes módulo p. Assim,

- $T^{p-1} - 1$, tem $p - 1$ raízes diferentes módulo p
- $T^{\frac{p-1}{2}} - 1$, tem $\frac{p-1}{2}$ raízes diferentes módulo p.

Portanto, $T^{\frac{p-1}{2}} + 1$ tem que ter raízes módulo p, ou seja, deve existir algum inteiro C tal que

$$C^{\frac{p-1}{2}} + 1 \equiv 0 (\text{mod } p),$$

isto é,

$$C^{\frac{p-1}{2}} \equiv -1 (\text{mod } p).$$

Como $p \equiv 1 (\text{mod } 4)$, então $\dfrac{p-1}{2} = 2k$ é par. Portanto, $(C^k)^2 \equiv -1 (\text{mod } p)$, ou seja, $x^2 \equiv -1 (\text{mod } p)$ tem solução. □

Lema 2.62. *Se p é um primo em $\mathbb{Z}$ com $p \equiv 1$(mod 4), então p não é primo em $\mathbb{Z}[i]$, mas tem uma fatoração em primos da forma $p = (a + bi)(a - bi)$.*

Demonstração. Suponha que p é primo em $\mathbb{Z}[i]$. Pelo Lema 2.61, existe $\ell \in \mathbb{Z}$ tal que $p \mid \ell^2 + 1$. Agora, considere esta divisibilidade em $\mathbb{Z}[i]$. Note que $\ell^2 + 1 = (\ell + i)(\ell - i)$, assim $p \mid \ell^2 + 1 = (\ell + i)(\ell - i)$ e temos, pelo Lema 2.61, que $p \mid \ell + i$ ou $p \mid \ell - i$. Portanto, algum $m + ni \in \mathbb{Z}[i]$ satisfaz $\ell \pm i = p(m + ni)$. Olhando para a parte imaginária temos que $pn = \pm 1$, o que é um absurdo pois p é primo em $\mathbb{Z}$. Portanto, p não é primo em $\mathbb{Z}[i]$. Assim, existem fatores não triviais α, $\beta \in \mathbb{Z}[i]$ tais que $p = \alpha\beta$. Aplicando a norma em ambos os membros dessas equação, temos $N(p) = N(\alpha)N(\beta) \Rightarrow p^2 = N(\alpha)N(\beta)$. Portanto, $N(\alpha) = N(\beta) = p$. Escrevendo $\alpha = a + bi$ temos que $p = a^2 + b^2 = (a + bi)(a - bi)$. □

Exemplo 2.63. 5 é primo em $\mathbb{Z}$ e $5 \equiv 1$ (mod 4), então $5 = (2 + i)(2 - i)$.

Exemplo 2.64. 17 é primo em $\mathbb{Z}$ e $17 \equiv 1$(mod 4), então $17 = (4 + i)(4 - i)$.

O resultados dos lemas anteriores fornecem a demonstração do seguinte teorema:

Teorema 2.65. *Os elementos primos em $\mathbb{Z}[i]$ são os seguintes:*

1. *associados dos inteiros da forma $p + 0i$, onde p é primo com $p \equiv 3$(mod 4);*
2. *associados de $1 + i$ e $1 - i$; e*
3. *elementos $a + bi$ tais que $N(a + bi) = a^2 + b^2 = p$ um número primo com $p \equiv 1$(mod 4).*

Demonstração. 1. Segue do Lema 2.59;

2. Segue da Observação 2.58(2); e

3. Segue dos Lemas 2.54, 2.56, 2.61 e 2.62.

□

Lema 2.66. *Seja $\pi \in \mathbb{Z}[i]$. Se $\alpha_1, \alpha_2, \cdots, \alpha_r \in \mathbb{Z}[i]$, com $\pi \mid \alpha_1\alpha_2 \cdots \alpha_r$, então $\pi \mid \alpha_j$, com $1 \leq j \leq r$ e $r \in \mathbb{N}$.*

Demonstração. Faremos a verificação para $r = 2$, visto que para $r > 2$ é um processo simples de indução. Suponha que $\pi \mid \alpha_1\alpha_2$, mas $\pi \nmid \alpha_1$. Logo, π e α_1 são primos entre si. Pelo Corolário 2.45, segue que $\pi \mid \alpha_2$. □

Teorema 2.67. *(Fatoração Única) Qualquer $\alpha \in \mathbb{Z}[i]$, com $N(\alpha) > 1$, tem uma fatoração de primos. Essa fatoração é única a menos da ordem dos fatores e associados.*

Demonstração. A primeira parte da demonstração será feita por indução em $N(\alpha)$. Suponha que $N(\alpha) = 2$, então α é um primo em $\mathbb{Z}[i]$, pelo Teorema 2.50. Agora, vamos supor que $n \geq 2$ e que se $\beta \in \mathbb{Z}[i]$ tal que $1 < N(\beta) < n$ então β é um produto de números primos em $\mathbb{Z}[i]$. Vamos supor que há inteiros gaussianos com norma n. Se temos um número inteiro de Gauss α com norma n, que é composto, então podemos escrever $\alpha = \beta\gamma$. Aplicando a norma, temos $N(\alpha) = N(\beta)N(\gamma)$, onde $N(\beta) < N(\alpha) = n$. Por hipótese indutiva, β e γ são produtos de primos em $\mathbb{Z}[i]$. Portanto, α também é um produto de primos em $\mathbb{Z}[i]$.

Para provar a unicidade também vamos usar indução sobre n. Para $N(\alpha) = 2$ basta tomar $\alpha = \pm 1 \pm i$ que são primos em $\mathbb{Z}[i]$. Agora, suponha que $n \geq 3$ e que $1 < N(\alpha) < n$ com α tendo uma fatoração única. Podemos supor que há inteiros gaussianos com a norma n.

Considere duas fatorações de primos de α:

$$\alpha = \pi_1\pi_2 \cdots \pi_r = \pi_1^{'}\pi_2^{'} \cdots \pi_s^{'}.$$

Como $\pi_1 \mid \alpha$, podemos escrever

$$\pi_1 \mid \pi_1^{'}\pi_2^{'} \cdots \pi_s^{'}.$$

Pelo Lema 2.66, segue que $\pi_1 \mid \pi_j^{'}$, para algum $j = 1, \cdots s$. Podemos supor que $j = 1$, ou seja, $\pi_1 \mid \pi_1^{'}$. Logo, $\pi_1^{'} = \pi_1 \cdot w$, para algum $w \in \mathbb{Z}[i]$. Consequentemente, $\pi_1 = u\pi_1^{'}$ para alguma unidade $u \in \{\pm 1, \pm i\}$. Substituindo a última igualdade na fatoração de α temos:

$$\alpha = u\pi_1^{'}\pi_2 \cdots \pi_r = \pi_1^{'}\pi_2^{'} \cdots \pi_s^{'}. \tag{2.16}$$

Cancelando $\pi_1^{'}$ em ambos os lados, temos:

$$u\pi_2 \cdots \pi_r = \pi_2^{'} \cdots \pi_s^{'}.$$

Considerando $\beta = \pi_2' \cdots \pi_s'$, então $N(\beta) = \dfrac{N(\alpha)}{N(\pi_1')} < N(\alpha)$.

Embora u seja uma unidade, o produto $u\pi_2$ no lado esquerdo de (2.16) é um primo, e portanto (2.16) têm duas fatorações de primos de β, com $(r-1)$ primos do lado esquerdo e $(s-1)$ primos do lado direito. Como $N(\beta) < n$, a hipótese de indução diz que β tem uma fatoração única, então $(r-1) = (s-1)$, o que implica $r = s$. Após nova rotulagem apropriada, temos que $u\pi_2$ e π_2' são múltiplos unitários e π_i, π_i' são múltiplos unitários para $i > 2$. Como $u\pi_2$ e π_2' são múltiplos unitários, segue que π_2 e π_2' são múltiplos unitários. Assim, vemos todo π_i como um múltiplo unitário de π_i', o que conclui a demonstração. □

Exemplo 2.68. Vamos fatorar $3 - 4i$. Sabemos que $N(3-4i) = 25 = 5 \cdot 5$. Já que 5 é a norma de um fator não trivial de $3 - 4i$, podemos escrever $5 = (2+i)(2-i)$. Considerando $\alpha = 2 + i$ e $\beta = 2 - i$, temos as seguintes possibilidades:

1. $\alpha \cdot \alpha = (2+i)(2+i) = 3 + 4i$;
2. $\alpha \cdot \beta = (2+i)(2-i) = 5$;
3. $\beta \cdot \beta = (2-i)(2-i) = 3 - 4i$.

Portanto, a fatoração de $3 - 4i$ é $(2-i)^2$.

Exemplo 2.69. Verifiquemos se $1 - 3i$ é primo.

Podemos verificar calculando $N(1-3i) = 10$. Como a norma de $1 - 3i$ é par, nos indica que um dos fatores de $1 - 3i$ é $1 + i$ (Corolário 2.27). Ao fatorarmos $N(1-3i) = 2 \cdot 5$, temos que $N(1+i) = 2$. Para que $N(\alpha) = 5$, $\alpha = \pm 1 \pm 2i$ ou $\alpha = \pm 2 \pm i$. Fazendo as possíveis combinações de $1 + i$ e α, encontramos:

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

Portanto, $1 - 3i$ não é primo e sua fatoração é $(1+i)(-1-2i)$.

Exemplo 2.70. Vamos determinar a fatoração de $3 + 5i$. Sua norma é 34, cuja fatoração em $\mathbb{Z}$ é $2 \cdot 17$. Já sabemos pelo Corolário 2.27 que um dos fatores de $3 + 5i$ é $1 + i$.

Vamos observar os inteiros gaussianos com norma 17, em seguida iremos multiplicá-los por $1 + i$ para obtermos $3 + 5i$. Representando 17 como a soma de dois quadrados, temos:

$$17 = 4^2 + 1^2 = 1^2 + 4^2.$$

Logo, podemos fatorar em primos gaussianos:

$$17 = (4 + i)(4 - i) \text{ ou } 17 = (1 + 4i)(1 - 4i).$$

Os inteiros gaussianos são primos, pois suas normas são primos em $\mathbb{Z}$. Então temos as seguintes combinações:

- $(1 + i)(4 + i) = 3 + 5i$;
- $(1 + i)(4 - i) = 5 + 3i$;
- $(1 + i)(1 + 4i) = -3 + 5i$;
- $(1 + i)(1 - 4i) = 5 - 3i$.

Portanto, a fatoração de $3 + 5i$ é $(1 + i)(4 + i)$.

2.2.9 Aritmética Modular em $\mathbb{Z}[i]$

Similar ao que acontece em $\mathbb{Z}$, abordaremos aqui a aritmética modular em $\mathbb{Z}[i]$ e suas propriedades.

Definição 2.71. *Sejam α, β e γ inteiros gaussianos. Dizemos que α é congruente a β módulo γ, indicado por $\alpha \equiv \beta \ (mod\ \gamma)$, quando $\gamma \mid (\alpha - \beta)$. ou seja, $\alpha - \beta = \gamma\delta$, para algum $\delta \in \mathbb{Z}[i]$.*

Exemplo 2.72. Vamos verificar que $(16 + 8i) \equiv (3 - i)\ mod\ (7 + i)$.

Pela definição de congruência temos que $(7 + i) \mid (16 + 8i) - (3 - i)$ se existe $\delta \in \mathbb{Z}[i]$ tal que $(16 + 8i) - (3 - i) = (7 + i)\delta$. De fato,

$$\frac{(16 + 8i) - (3 - i)}{(7 + i)} = \delta$$

$$\frac{(13 + 9i)}{(7 + i)} \cdot \frac{(7 - i)}{(7 - i)} = \delta$$

$$\frac{100 + 50i}{50} = \delta$$

$$2 + i = \delta.$$

Como $2 + i \in \mathbb{Z}[i]$, segue que $(16 + 8i) \equiv (3 - i)\ mod\ (7 + i)$.

Assim como nos inteiros, as propriedades da soma e da multiplicação são válidas na congruência para inteiros gaussianos.

Proposição 2.73. *Sejam α, α', β e β' em $\mathbb{Z}[i]$. Se $\alpha \equiv \alpha' \ (mod\, \gamma)$ e $\beta \equiv \beta' \ (mod\, \gamma)$, então:*

1. $\alpha + \beta = \alpha' + \beta' \ (mod\, \gamma)$
2. $\alpha\beta = \alpha'\beta' \ (mod\, \gamma)$

Demonstração. i) Pela definição de congruência, existem δ_1 e δ_2 em $\mathbb{Z}[i]$ tais que $\alpha - \alpha' = \delta_1\gamma$ e $\beta - \beta' = \delta_2\gamma$. Somando as equações membro a membro, temos:

$$\alpha - \alpha' + \beta - \beta' = \delta_1\gamma + \delta_2\gamma$$

$$(\alpha + \beta) - (\alpha' + \beta') = \gamma(\delta_1 + \delta_2),$$

o que implica que $\gamma \mid (\alpha + \beta) - (\alpha' + \beta')$ e portanto $\alpha + \beta = \alpha' + \beta' \ (mod\, \gamma)$.

ii) Multiplicando a primeira equação do item (i) por β e a segunda do item (i) por α', obtemos:

$$\beta(\alpha - \alpha') = \beta(\delta_1\gamma) \text{ e } \alpha'(\beta - \beta') = \alpha'(\delta_2\gamma).$$

Em seguida, somando membro a membro, temos:

$$\begin{aligned} \beta(\alpha - \alpha') + \alpha'(\beta - \beta') &= \beta(\delta_1\gamma) + \alpha'(\delta_2\gamma) \\ \beta\alpha - \beta\alpha' + \alpha'\beta - \alpha'\beta' &= \beta\delta_1\gamma + \alpha'\delta_2\gamma \\ \alpha\beta - \alpha'\beta' &= \gamma(\beta\delta_1 + \alpha'\delta_2) \end{aligned}$$

e portanto, $\gamma \mid \alpha\beta - \alpha'\beta'$, o que implica pela definição de congruência que $\alpha\beta = \alpha'\beta' \ (mod\, \gamma)$. □

Vejamos um exemplo aplicando o item 1. da Proposição 2.73.

Exemplo 2.74. Sejam $(6+16i) \equiv (-10+8i)\ mod\,(3-i)$ e $(-1+12i) \equiv (-2-i)\ mod\,(3-i)$. Somando as congruências, obtemos $(5 + 28i) \equiv (-12 + 7i)\ mod\ (3 - i)$. O que é verdade, pois:

$$\frac{(5 + 28i) - (-12 + 7i)}{(3 - i)} = \frac{(17 + 21i)}{(3 - i)} \cdot \frac{(3 + i)}{(3 + i)} = \frac{51 + 17i + 63i - 21}{10} = \frac{30 + 80i}{10} = 3+8i$$

e $3 + 8i \in \mathbb{Z}[i]$.

Proposição 2.75. *Sejam α, β, γ e $\delta \in \mathbb{Z}[i]$. Então,*

1. *Reflexiva: $\alpha \equiv \alpha \ (mod\, \gamma)$;*

2. *Simétrica: se* $\alpha \equiv \beta \ (mod\ \gamma)$*, então* $\beta \equiv \alpha \ (mod\ \gamma)$*;*

3. *Transitiva: se* $\alpha \equiv \beta \ (mod\ \gamma)$ *e* $\beta \equiv \delta \ (mod\ \gamma)$*, então* $\alpha \equiv \delta \ (mod\ \gamma)$.

Demonstração. i) Temos que $\alpha - \alpha = 0$ e 0 é divisível por γ, ou seja, $\gamma \mid 0$, o que implica que $\gamma \mid \alpha - \alpha$. Logo pela definição de congruência, $\alpha \equiv \alpha \ (mod\ \gamma)$.

ii) Como $\gamma \mid (\alpha - \beta)$ por hipótese, segue que existe k em $\mathbb{Z}[i]$ tal que $\alpha - \beta = \gamma k$. Multiplicando a equação por -1 encontramos $\beta - \alpha = \gamma(-k)$, logo $\gamma \mid (\beta - \alpha)$ e pela definição de congruência, $\beta \equiv \alpha \ (mod\ \gamma)$.

iii) Por hipótese $\gamma \mid (\alpha - \beta)$ e $\gamma \mid (\beta - \delta)$. Logo existem k_1 e k_2 em $\mathbb{Z}[i]$ tais que $\alpha - \beta = \gamma k_1$ e $\beta - \delta = \gamma k_2$. Somando membro a membro as equações temos que

$$\begin{aligned} \alpha - \beta + \beta - \delta &= \gamma k_1 + \gamma k_2 \\ \alpha - \delta &= \gamma(k_1 + k_2), \end{aligned}$$

ou seja, $\gamma \mid \alpha - \delta$ e pela definição de congruência, $\alpha \equiv \delta \ (mod\ \gamma)$. □

Assim, a congruência modular em $\mathbb{Z}[i]$ é uma relação de equivalência.

Teorema 2.76. *Sejam* a, b *e* n *em* $\mathbb{Z}$*. Então* $a \equiv b \ (mod\ n)$ *em* $\mathbb{Z}$*, se e somente se,* $a \equiv b \ (mod\ n)$ *em* $\mathbb{Z}[i]$.

Demonstração. Pela definição de congruência, $a \equiv b \ (mod\ n)$ equivale a $n \mid (a-b)$ em $\mathbb{Z}$, o que implica que $n \mid (a-b)$ em $\mathbb{Z}[i]$. Por outro lado, pelo Teorema 2.23, se $n \mid (a-b)$ em $\mathbb{Z}[i]$ implica que $n \mid (a-b)$ em $\mathbb{Z}$, pois a divisibilidade dos inteiros não muda quando se trabalha em $\mathbb{Z}[i]$. Portanto, $a \equiv b \ (mod\ n)$ em $\mathbb{Z}$ se e somente se, $a \equiv b \ (mod\ n)$ em $\mathbb{Z}[i]$. □

Para permitir que a extensão do algoritmo RSA funcione, precisamos do valor da função de Euler ϕ de um número n em $\mathbb{Z}[i]$, composto pelo produto de dois primos p e q em $\mathbb{Z}[i]$. O teorema a seguir fornece tal valor, no entanto, sua demonstração requer vários resultados sobre classes residuais e que não abordamos aqui, tendo em vista que o foco deste trabalho não é fazer um estudo detalhado dos inteiros gaussianos. Para detalhes desta teoria o leitor pode consultar as referências [10, 11].

Teorema 2.77. *Sejam* p *e* q *em* $\mathbb{Z}[i]$ *primos. Então a função* ϕ *de Euler de* $n = pq$ *é:*

$$\phi(n) = \phi(p)\phi(q) = (N(p) - 1)(N(q) - 1).$$

3 Criptografia RSA

O algoritmo RSA foi inventado em 1977 por Rivest, Samir e Adleman. É um dos mais conhecidos e usados sistema de criptografia de chave pública, que fornece segurança em toda rede. Foi criado a partir de funções matemáticas em $\mathbb{Z}$. Seu sistema baseia-se não somente na segurança de sua chave privada, mas também na sua difícil fatoração. Recentemente alguns estudos, como o de Stillwell (2003), com o objetivo de encontrar um sistema mais seguro e eficiente, provaram que é possível a extensão desse algoritmo para o domínio de números inteiros gaussianos $\mathbb{Z}[i]$, a qual será apresentada no Capítulo 4.

RSA é um algoritmo de criptografia de dados do tipo assimétrico, ou seja, possui uma chave pública em que todos os envolvidos tem acesso e uma chave privada. A primeira é a responsável pela codificação dos dados e deve possuir funções de difícil inversão, uma vez que é isso que garante o sigilo das informações. Para entendermos o método, precisamos analisar cada item, desde a pré-codificação até a decriptação e segurança do método. Começamos a seguir contando um pouco sobre sua história. As principais referências utilizadas para o desenvolvimento deste capítulo foram [1, 5].

3.1 Um Pouco sobre a História

A palavra *criptografia* vem do grego *"kriptos"* e significa oculto. Enviar e receber mensagens ocultas sem que elas fossem interceptadas por terceiros são desejos e anseios que datam desde a muito tempo, tendo registros desde 1900 *a.C.* no Egito. O primeiro exemplo de um código secreto de que se tem notícia foi usado por César para comunicar-se com as legiões em combate pela Europa. Sistemas de criptografia sempre foram utilizados no campo militar. Durante os períodos de guerra a criptografia foi muito utilizada e se desenvolveu, segundo registros históricos. Enigma, a máquina desenvolvida pelos nazistas durante a Segunda Guerra Mundial é um dos melhores códigos já conhecido. A detecção da chave e a quebra do código pelos aliados foi um dos pontos cruciais que marcaram o fim da guerra e a vitória das forças aliadas.

Atualmente, com a chegada da *Internet* e de todas as suas tecnologias de suporte que

utilizam redes, a codificação de mensagens se tornou essencial. Manter o sigilo no envio de e-mails, conversas on-line, transações bancárias, entre outros, é fundamental no nosso mundo digital.

Com o surgimento da criptografia nasce também a criptoanálise, que tem como objetivo decriptar a mensagem criptografada. Muitos métodos surgiram ao longo do anos, mas sempre que estes eram aperfeiçoados, a criptoanálise por sua vez aperfeiçoava-se também para conseguir decriptar o método. Em geral, os sistemas de criptografia eram simétricos, o que significa que o remetente e o destinatário usavam a mesma chave para se comunicar. Isso implica que os dois trocavam com segurança a chave. De fato, isso ainda é possível, mas pode ser difícil, pois talvez o remetente e o destinatário não possam ter um contato seguro para a troca da chave. Assim, tornou-se necessário inventar novos códigos, que fossem difíceis de decifrar, mesmo com a ajuda de um computador.

Essa é a razão a qual levou em 1975, W. Diffie e M. E. Hellman ao início da criação da criptografia de chave pública, com a publicação do projeto intitulado *Novas direções em criptografia* em 1976. O objetivo do trabalho foi criar uma nova forma de comunicação que permitia a troca de informações entre duas pessoas que não tem possibilidade de um contato seguro. Nesse caso, criou-se duas diferentes chaves: a chamada chave pública e a chave secreta, que respectivamente permitem criptografar e descriptografar a mensagem. Porém, eles nunca desenvolveram uma implementação prática de seu método, o qual foi desenvolvido posteriormente em 1977 por Ronald Rivest, Adi Shamir e Leonard Adleman, os quais na época trabalhavam no *Massachussetes Istitute of Technology* (M.I.T). Esses propuseram uma nova ideia chamada *Algoritmo RSA*, baseando a segurança do método no fato de que a fatoração de números inteiros em fatores primos é complexa e leva-se muito tempo para ser encontrada. As letras RSA correspondem às iniciais dos inventores do código.

Essa nova forma de comunicação permite agora a troca de informações entre duas pessoas que nunca tiveram contato anterior e, como o nome sugere, a chave pública pode estar disponível ao público. Como estamos usando duas chaves diferentes, o sistema de criptografia é considerado assimétrico.

A criptografia ao longo dos tempos sempre tentou evitar o problema das interceptações, produzindo uma mensagem ilegível para qualquer pessoa, exceto para o proprietário da chave. Mas, através da criptografia de chave pública, agora também somos capazes de contornar esse problema.

3.2 Pré-Codificação

A primeira etapa a ser realizada é converter a mensagem desejada em uma sequência de números. Essa etapa recebe o nome de *pré-codificação* e consiste em:

(i) Converter a mensagem em uma sequência de números;

(ii) Separar o número, encontrado a partir da conversão da mensagem em números, em blocos cujos valores sejam menores que n (em seguida falaremos como encontrá-lo).

Observação 3.1. 1. Geralmente a tabela de conversão utilizada possui para cada letra da mensagem dois ou mais dígitos para que se evite possíveis ambiguidades. Por exemplo: a letra A é representada pelo número 10, a letra B pelo número 11 e assim sucessivamente.

2. A maneira de se escolher os blocos não precisa ser homogênea (cada bloco pode possuir um número diferente de dígitos).

3. Não podemos começar a sequência com um bloco de zeros, pois isso causaria problemas na hora da decriptação.

Exemplo 3.2. Utilizando a tabela de conversão abaixo, vamos cifrar a seguinte frase, sem diferenciar letras maiúsculas de minúsculas:

Gaby estuda

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

s	t	u	v	w	x	y	z	
28	29	30	31	32	33	34	35	36

Assim, temos o seguinte texto cifrado:

$$1610113436142829301310$$

E podemos, por exemplo, dividir nos seguintes blocos:

$$16 - 10 - 11 - 34 - 36 - 14 - 28 - 29 - 30 - 13 - 10.$$

Note que os blocos não precisam ser divididos possuindo o mesmo número de caracteres.

Exemplo 3.3. Utilizando a tabela de conversão do Exemplo 3.2 vamos cifrar a seguinte frase, sem diferenciar letras maiúsculas de minúsculas:

Bia faz jazz

Assim, temos o seguinte texto cifrado:

$$11181036151035361910 3535$$

Novamente, podemos dividir nos seguintes blocos:

$$11 - 18 - 10 - 36 - 15 - 10 - 35 - 36 - 19 - 10 - 35 - 35.$$

3.3 Geração de Chaves

O processo da geração de chaves do método consiste em:

(iii) Escolher dois números primos distintos p e q;

(iv) Calcular n tal que $n = pq$.

Exemplo 3.4. Os números utilizados aqui são somente para exemplificação, pois são considerados pequenos, o que deixa a segurança do RSA quase nula. Seja $p = 13$ e $q = 17$, então $n = 221$.

Observação 3.5. Note que os blocos separados na seção anterior são todos menores que 221. Assim podemos prosseguir para a próxima etapa.

3.4 Encriptação

Para encriptarmos uma mensagem precisaremos:

(v) Calcular a função de Euler para n;

Pelo Teorema 1.48 $\phi(p) = p^k - p^{k-1}$ e $\phi(q) = q^k - q^{k-1}$. Assim, $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p^k - p^{k-1})(q^k - q^{k-1})$.

Como p e q são números primos, segue pela Proposição 1.50 que $\phi(p) = p - 1$ e $\phi(q) = q - 1$ com $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

Desta forma calculamos $\phi(n) = (p-1)(q-1)$.

(vi) Escolher o menor inteiro positivo $e > 1$ tal que $mdc(\phi(n), e) = 1$. Denominamos e como *componente de enciframento*;

(vii) Formar a *chave pública de encriptação do sistema RSA*, que é dada pelo par de números (n, e);

(viii) Encriptar cada bloco obtido do texto cifrado separadamente, e a mensagem encriptada será a sequência dos blocos encriptados. Isso é muito importante: os blocos já encriptados não poderão ser reunidos de modo a formar um longo número. Se isto for feito, será impossível decriptar a mensagem;

(ix) A encriptação de um bloco b será denotada por $C(b)$, que é o resto da divisão de b^e por n, ou seja,

$$C(b) \equiv b^e \ (mod\ n).$$

Exemplo 3.6. Vamos encriptar a mensagem do Exemplo 3.3. Primeiramente, obtemos a função $\phi(n)$, $n = pq$ com $p = 13$ e $q = 17$, como escolhido no Exemplo 3.4:

$$\phi(n) = (p-1)(q-1) \Rightarrow \phi(n) = (13-1)(17-1) = 12 \cdot 16 = 192.$$

Encontrado o valor de $\phi(n)$, segue que o componente de enciframento e tal que $mdc(192, e) = 1$ é $e = 5$. Assim, temos que a chave pública de encriptação é dada pelo par $(221, 5)$.

A seguir, encriptaremos cada bloco:

Bloco 11 $\longrightarrow$ $(11)^5 \equiv 163\ (mod\ 221)$
Bloco 18 $\longrightarrow$ $(18)^5 \equiv 18\ (mod\ 221)$
Bloco 10 $\longrightarrow$ $(10)^5 \equiv 108\ (mod\ 221)$
Bloco 36 $\longrightarrow$ $(36)^5 \equiv 134\ (mod\ 221)$
Bloco 15 $\longrightarrow$ $(15)^5 \equiv 19\ (mod\ 221)$
Bloco 10 $\longrightarrow$ $(10)^5 \equiv 108\ (mod\ 221)$
Bloco 35 $\longrightarrow$ $(35)^5 \equiv 120\ (mod\ 221)$
Bloco 36 $\longrightarrow$ $(36)^5 \equiv 134\ (mod\ 221)$
Bloco 19 $\longrightarrow$ $(19)^5 \equiv 15\ (mod\ 221)$
Bloco 10 $\longrightarrow$ $(10)^5 \equiv 108\ (mod\ 221)$
Bloco 35 $\longrightarrow$ $(35)^5 \equiv 120\ (mod\ 221)$
Bloco 35 $\longrightarrow$ $(35)^5 \equiv 120\ (mod\ 221)$

Temos como resultado a mensagem encriptada:

$$163 - 18 - 108 - 134 - 19 - 108 - 120 - 134 - 15 - 108 - 120 - 120$$

3.5 Decriptação

Para decriptarmos a mensagem, necessitamos do número n e do inverso de e módulo $\phi(n)$. Denotamos esse número por d. Assim,

$$ed \equiv 1(mod\ \phi(n)).$$

Para determinar d, basta resolver a equação $ed + x\phi(n) = 1$ através do *algoritmo de Euclides estendido*, apresentado no Capítulo 1. Após encontrarmos d, determinamos o resto da divisão. Se $a = C(b)$ é um bloco de mensagem codificada, então $D(a)$ é o resultado da decriptação, que é exatamente o resto da divisão de a^d por n, ou seja,

$$D(a) \equiv a^d(mod\ n).$$

O par (n, d) é denominado *chave privada de decriptação do sistema RSA*. Ao decriptar os blocos de mensagem codificada, é encontrada a mensagem original, ou seja, $D(C(b)) = b$.

Note que para decriptarmos a mensagem, não é necessário sabermos os valores de p e q, mas sim os valores de n e d.

Quando o valor de d for negativo é utilizado o Teorema 1.52 para encontrar um valor positivo para d. Desta forma, para reverter valores negativos de d, escolhemos um $t \in \mathbb{Z}$ tal que $d + \phi(n)t > 0$. Assim, $\tilde{d} = d + \phi(n)t$.

Exemplo 3.7. Vamos decriptar a mensagem do Exemplo 3.6. Para tal, precisamos encontrar d que satisfaça

$$ed \equiv 1 \; mod \; (\phi(n)), \text{ ou seja, } 5d \equiv 1 \; mod(192).$$

Isso é equivalente a resolvermos a seguinte equação:

$$192x + 5d = 1.$$

Pelo algoritmo de Euclides estendido, obtemos

Resto	Quociente	x	d
192	$*$	1	0
5	$*$	0	1
2	38	$(1 - 0.38) = 1$	$(0 - 1.38) = -38$
1	2	$(0 - 1.2) = -2$	$(1 - (-38).2) = 77$
0	2	$*$	$*$

Desta forma, $192 \cdot (-2) + 5 \cdot 77 = 1 \Rightarrow x = -2$ e $d = 77$.

Após encontrado o valor de d, continuamos o processo de decriptação. Para isso, seja $a = C(b)$ um bloco de mensagem codificada. Temos que encontrar $D(a)$ tal que

$$D(a) \equiv a^d (mod \; n).$$

A seguir, decriptaremos cada bloco:

Bloco 163 $\longrightarrow$ $(163)^{77} \equiv 11 \; (mod \; 221)$
Bloco 18 $\longrightarrow$ $(18)^{77} \equiv 18 \; (mod \; 221)$
Bloco 108 $\longrightarrow$ $(108)^{77} \equiv 10 \; (mod \; 221)$
Bloco 134 $\longrightarrow$ $(134)^{77} \equiv 36 \; (mod \; 221)$
Bloco 19 $\longrightarrow$ $(19)^{77} \equiv 15 \; (mod \; 221)$
Bloco 108 $\longrightarrow$ $(108)^{77} \equiv 10 \; (mod \; 221)$
Bloco 120 $\longrightarrow$ $(120)^{77} \equiv 35 \; (mod \; 221)$
Bloco 134 $\longrightarrow$ $(134)^{77} \equiv 36 \; (mod \; 221)$
Bloco 15 $\longrightarrow$ $(15)^{77} \equiv 19 \; (mod \; 221)$
Bloco 108 $\longrightarrow$ $(108)^{77} \equiv 10 \; (mod \; 221)$
Bloco 120 $\longrightarrow$ $(120)^{77} \equiv 35 \; (mod \; 221)$
Bloco 120 $\longrightarrow$ $(120)^{77} \equiv 35 \; (mod \; 221)$

Portanto, a mensagem decodificada fica da forma:

111810361510353619103535,

que é a mensagem original, conforme pode ser visto no Exemplo 3.3.

3.6 Funcionalidade do Sistema

Para mostrar que o sistema RSA realmente funciona, precisamos verificar que se $C(b)$ é um inteiro e $1 \leq b < n$, então $D(C(b)) = b$.

Como $D(C(b))$ e b estão no intervalo de 1 até $n-1$, segue que b e $D(C(b))$ somente serão congruentes módulo n, se forem iguais. Logo, é suficiente mostrarmos que $D(C(b)) \equiv b(mod\ n)$. Por definição, segue que

$$D(C(b)) \equiv (b^e)^d \equiv b^{ed}\ (mod\ n).$$

Como $n = pq$, vamos calcular b^{ed} módulo p e módulo q. Calculemos b^{ed} módulo p. Sendo d o inverso de e módulo $\phi(n)$, segue que

$$ed = 1 + k\phi(n) = 1 + k(p-1)(q-1) \Rightarrow (b^e)^d \equiv b(b^{p-1})^{k(q-1)}\ (mod\ p).$$

Utilizaremos o Teorema 1.45(*Pequeno Teorema de Fermat*). Para isso, vamos supor que p não divide b. Se isso acontece, então $b^{p-1} \equiv 1\ (mod\ p)$, ou seja, $b^{ed} \equiv b\ (mod\ p)$. Assim, podemos afirmar que $b^{ed} - b$ é divisível por p, e analogamente, chega-se ao mesmo resultado para q. Como p e q são primos distintos, segue que $mdc(p, q) = 1$, e assim,

$$pq|(b^{ed} - b) \Longrightarrow b^{ed} \equiv b\ (mod\ n),$$

para qualquer b inteiro, pois $n = pq$. Logo, $D(C(b)) = b$.

3.7 Segurança do RSA

Lembre-se que o RSA é um método de chave pública. Sejam p e q os parâmetros dos sistema que estamos usando e $n = pq$. A chave de codificação corresponde à chave pública do sistema. Portanto, o par (n, e) é acessível a qualquer usuário. O RSA só será seguro se for difícil calcular d quando apenas n e e são conhecidos.

Na prática, só sabemos calcular d aplicando o algoritmo euclidiano estendido a $\phi(n)$ e e. Por outro lado, só sabemos calcular $\phi(n)$ se soubermos fatorar n para obter p e q. Portanto, na prática, só podemos quebrar o código se conseguirmos fatorar n. No entanto, se n for grande, este é um problema difícil, já que não são conhecidos algoritmos rápidos de fatoração.

Um outro ponto importante refere-se à escolha dos primos p e q. É claro que se forem pequenos, o sistema será fácil de quebrar. Se p e q são grandes, mas $|p-q|$ é pequeno, então é fácil fatorar $n = pq$ usando o *algoritmo de Fermat*, que pode ser encontrado em [1], página 40. Por outro lado, o RSA está em uso há anos e, se os primos forem bem escolhidos, o sistema tem se mostrado muito seguro.

4 Criptografia RSA nos Inteiros Gaussianos

Nesse capítulo abordaremos com detalhes a extensão do algoritmo RSA para os inteiros gaussianos. No geral, esse método segue as mesmas etapas do algoritmo RSA em $\mathbb{Z}$, descritas no Capítulo 3. Porém, todas as propriedades descritas no Capítulo 2 devem ser levadas em consideração para termos a certeza que estamos criando um algoritmo funcional e utilizável.

A seguir, abordaremos cada etapa do algoritmo, fazendo as adequações necessárias em $\mathbb{Z}[i]$. Os exemplos aqui apresentados não fornecem uma boa segurança para o método, por isso são somente para exemplificar. Porém com o auxílio de computadores o método pode ser estendido para números maiores, trazendo consequentemente uma maior segurança. A principal referência utilizada para o desenvolvimento deste capítulo foi [10].

4.1 Pré-Codificação

Nessa primeira etapa vamos converter a mensagem desejada em uma sequência de números inteiros de Gauss, utilizando uma tabela de conversão para isso, que não é única. Em seguida, devemos separar em blocos de números a mensagem codificada, de modo que a norma de cada um seja menor que a norma de n (encontraremos n no próximo passo). Uma grande norma significaria que os blocos de números seriam maiores do que n, e com isso nunca obteríamos a mensagem de volta. Chamando de b cada bloco, temos que ter $N(b) < N(n)$.

Observação 4.1.

1. A tabela de conversão utilizada possui para cada letra um inteiro de Gauss z da forma $z = a + bi$, com a e b em $\mathbb{Z}$.

2. Cada bloco foi relacionado a um inteiro de Gauss.

Exemplo 4.2. Utilizando a tabela de conversão abaixo, vamos cifrar a seguinte palavra, sem diferenciar letras maiúsculas de minúsculas:

Lia

a	b	c	d	e	f	g	h	i	j
$1+i$	$2+2i$	$3+3i$	$4+4i$	$5+5i$	$6+6i$	$7+7i$	$8+8i$	$9+9i$	$10+10i$

k	l	m	n	o	p	q	r
$11+11i$	$12+12i$	$13+13i$	$14+14i$	$15+15i$	$16+16i$	$17+17i$	$18+18i$

s	t	u	v	w	x	y	z
$19+19i$	$20+20i$	$21+21i$	$22+22i$	$23+23i$	$24+24i$	$25+25i$	$26+26i$

Assim temos o texto cifrado abaixo, dividido em blocos:

$$12+12i \mid 9+9i \mid 1+i$$

4.2 Geração de Chaves

Nessa etapa precisamos escolher dois números primos distintos p e q em $\mathbb{Z}[i]$, calcular n tal que $n = pq$ e sua norma. Para encontrar p e q utilizaremos o Teorema 2.65 do Capítulo 2.

Exemplo 4.3. Sejam $p = 7+8i$ e $q = 6+i$ primos em $\mathbb{Z}[i]$, pois $N(p) = 113$, $N(q) = 37$ e 113 e 37 são primos em $\mathbb{Z}$ e $113 \equiv 1\ (mod\ 4)$ e $37 \equiv 1\ (mod\ 4)$. Logo, calculando n obtemos:

$$n = (7+8i)(6+i) = 42+7i+48i+8i^2 = 34+55i$$

e a sua norma é dada por $N(n) = 34^2+55^2 = 4181$.

Observação 4.4. Note que os blocos definidos na etapa anterior possuem norma menor que a norma de n:

$$N(12+12i) = 12^2+12^2 = 288 < 4181,$$

$$N(9+9i) = 9^2+9^2 = 162 < 4181$$

e

$$N(1+i) = 1^2+1^2 = 2 < 4181.$$

Assim, podemos seguir para a próxima etapa.

4.3 Encriptação

Para encriptarmos uma mensagem inicialmente calculamos a função de Euler para n, dada pelo Teorema 2.77. Em seguida escolhemos o menor inteiro positivo $e > 1$ tal que

$mdc(\phi(n), e) = 1$, denominado *componente de enciframento*. Assim formamos a *chave pública* do sistema dada pelo par (n, e).

Finalmente a encriptação de cada bloco b será denotada por $C(b)$, que é o resto da divisão de b^e por n, ou seja,

$$C(b) \equiv b^e \ (mod\ n).$$

Para realizar essa etapa utilizaremos o Teorema da Divisão em $\mathbb{Z}[i]$, que é o Teorema 2.30.

Exemplo 4.5. Vamos encriptar a mensagem do Exemplo 4.2 para $n = pq = (7 + 8i)(6 + i)$ dado no Exemplo 4.3.

Primeiro, calculamos a função de Euler para n:

$$\phi(n) = (N(p) - 1)(N(q) - 1) = 112 \cdot 36 = 4032.$$

Encontrado o valor de $\phi(n)$, segue que o componente de enciframento e tal que $mdc(4032, e) = 1$ é $e = 5$. Portanto, a chave pública de encriptação do sistema é dada por $(34 + 55i, 5)$.

A seguir encriptaremos cada bloco:

$$\begin{array}{lcl} \text{Bloco } 12 + 12i & \longrightarrow & (12 + 12i)^5 \equiv (-25 - 9i)\ mod\ (34 + 55i) \\ \text{Bloco } 9 + 9i & \longrightarrow & (9 + 9i)^5 \equiv (-14 + 20i)\ mod\ (34 + 55i) \\ \text{Bloco } 1 + i & \longrightarrow & (1 + i)^5 \equiv (30 + 51i)\ mod\ (34 + 55i) \end{array}$$

Logo, temos como resultado a mensagem encriptada:

$$-25 - 9i \mid \ -14 + 20i \ \mid \ 30 + 51i$$

4.4 Decriptação

O processo de decriptação da mensagem do algoritmo em $\mathbb{Z}[i]$ segue as mesmas etapas da decriptação em $\mathbb{Z}$: basta encontrarmos o inverso de e módulo $\phi(n)$, denominado por d. Para isso fazemos uso do *algoritmo de Euclides estendido*. Em seguida, determinamos o resto da divisão a^d por n, ou seja,

$$D(a) \equiv a^d (mod\ n),$$

onde $a = C(b)$ é um bloco de mensagem codificada e $D(a)$ é o resultado da decriptação. Para a realização desses cálculos, foi utilizado o software matemático *Wolfram/Alpha*.

O par (n, d) é denominado *chave privada de decriptação do sistema RSA*.

Exemplo 4.6. Para decriptarmos a mensagem do Exemplo 4.5, primeiro determinamos d:

$$ed \equiv 1\ mod\ (\phi(n)), \text{ ou seja, } 5d \equiv 1\ mod(4032).$$

O que equivale a resolvermos a seguinte equação:

$$4032x + 5d = 1.$$

Pelo algoritmo de Euclides estendido, temos

Resto	Quociente	x	d
4032	$*$	1	0
5	$*$	0	1
2	806	$(1 - 0.806) = 1$	$(0 - 1.806) = -806$
1	2	$(0 - 1.2) = -2$	$(1 - (-806).2) = 1613$
0	2	$*$	$*$

Assim, $4032 \cdot (-2) + 5 \cdot 1613 = 1$ e $d = 1613$. Logo, nossa chave privada é $(34 + 55i, 1613)$.

A seguir decriptaremos cada bloco, que foi obtido no processo de encriptação:

$$\begin{aligned}
&\text{Bloco } -25 - 19i \quad \longrightarrow \quad (-25 - 19i)^{1613} \equiv (12 + 12i)\ mod\ (34 + 55i)\\
&\text{Bloco } -14 + 20i \quad \longrightarrow \quad (-14 + 20i)^{1613} \equiv (9 + 9i)\ mod\ (34 + 55i)\\
&\text{Bloco } 30 + 51i \quad \longrightarrow \quad (30 + 51i)^{1613} \equiv (1 + i)\ mod\ (34 + 55i)
\end{aligned}$$

Por fim, a mensagem decodificada é:

$$-25 - 9i \mid \ -14 + 20i \ \mid \ 30 + 51i$$

que é a mensagem inicial do Exemplo 4.2.

Observação 4.7. O algoritmo verifica se a mensagem decriptada coincide com a mensagem original, a menos de uma unidade, ou seja, a menos de $-1, i$ e $-i$.

5 Considerações Finais

O campo da criptografia está em constantes transformações, sempre procurando por novos algoritmos que forneçam uma maior segurança ao método. Esse é o motivo de produzir uma versão estendida do algoritmo RSA. Nos últimos vinte anos, houve muitas pesquisas que tentaram encontrar novos conjuntos nos quais a construção do algoritmo RSA fosse possível, segura e utilizável. Quando buscamos um conjunto para utilizar, diferente dos inteiros, é óbvio pensar no conjunto dos números complexos. Infelizmente se trata de um conjunto com muitas propriedades, difícil de analisar. Por esse motivo, foi escolhido inicialmente o conjunto dos inteiros de Gauss.

Assim, além de todos os aspectos de segurança do algoritmo clássico, precisamos considerar algumas novas propriedades que resultaram da introdução dos inteiros gaussianos. Em particular, o conceito de norma fornece novas informações sobre os números que estamos usando para construir o algoritmo e precisamos ver de que forma essa informação pode ser usada por uma terceira pessoa. Sabemos que uma maneira de descobrir a chave privada é encontrar a fatoração de n e, uma vez que n é parte da chave pública, sua norma também está disponível publicamente, pois é facilmente computável. Portanto, devemos tomar precauções na escolha da norma de n. Na verdade, ela deve ser de difícil fatoração. De fato, se aplicarmos a propriedade multiplicativa da norma, tendo uma fatoração de $N(n)$ implica encontrar os valores de $N(p)$ e $N(q)$ e então é possível dar uma lista de valores para p e q, facilitando assim a fatoração de n. Este problema pode ser evitado usando a mesma regra que seguimos para a fatoração de n, ou seja, desde que o valor $N(n)$ seja grande. Isso não é tão difícil de fazer em $\mathbb{Z}[i]$: usando a definição da norma, $N(z) = a^2 + b^2$, para z pertencente a $\mathbb{Z}[i]$, basta escolher a e b de modo que sejam grandes, que é a mesma condição para n. Como trabalhos futuros pode-se fazer a mesma análise para outros anéis da forma $\mathbb{Z}[\sqrt{d}]$, $d \in \mathbb{Z}$.

Índice Remissivo

Referências

[1] COUTINHO. S. C. *Números inteiros e Criptografia RSA*. 2. ed., IMPA, 2011.

[2] HEFEZ, A. *Aritmética*, Coleção PROFMAT, SBM, 2. ed., 2016.

[3] HEFEZ, A. *Elementos de aritmética*, Coleção Textos Universitários, SBM, 2006.

[4] SANTOS, J. P. de O. *Introdução à teoria dos números*. Rio de Janeiro: IMPA, 2000.

[5] SOUZA, B. A. *Teoria dos números e o RSA*. 2004. 66 f. Dissertação (Mestrado em Matemática), Instituto de Matemática, Estatística e Computação Científica, Universidade de Campinas, Campinas, ago. 2004.

[6] FERREIRA, J. *A Construção dos Números,* Coleção Textos Universitários, SBM, 2013.

[7] AVILA, G. *Variáveis complexas e aplicações*. Rio de Janeiro: LCT, 2000.

[8] CONRAD, K. *The gaussian integers.* Notes, 2013. Disponível em: <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf>. Último acesso em 06 nov. 2020.

[9] NETO, A. L. *Funções de uma variável complexa*. Rio de Janeiro: IMPA, 2005.

[10] PINA, A. *RSA in extensions of the ring of integers,* Master Degree, Linnaeus University, Sweden, 2017.

[11] WEINSTEIN, J. *Number Theory Course*, Note for MA 341, May, Spring 2018. Disponível em: <http://math.bu.edu/people/jsweinst/Teaching/MA341Spring18/MA341Notes.pdf>. Último acesso em 06 nov. 2020.

[12] STEIN, R. G. Exploring the gaussian integers. *The Two-Year College Mathematics Journal*, 7(4):4-10, 1976.

[13] STILLWELL, J. *Elements of Number Theory,* New York: Springer-Verlag, 2003.