Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

Os Inteiros Gaussianos via Matrizes [†]

por

Fabrício de Paula Farias Barbosa

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto / 2015
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Os Inteiros Gaussianos via Matrizes

por

Fabrício de Paula Farias Barbosa

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva -UFPB (Orientador)

Prof. Dr. João Bosco Batista Lacerda - UFPB

Prof. Dr. Jamilson Ramos Campos - UFPB

Agosto / 2015

Agradecimentos

Agradeço a Deus por me ajudar nas horas em que, no meu isolamento, pensava em desistir dando-me forças para continuar.

Aos meus pais que acreditaram no meu potencial e investiram no meu crescimento pessoal, fazendo que a cada dia me tornasse uma pessoa melhor.

A minha irmã e amiga que, à sua maneira, fazia com que não desistisse.

Em especial aos meus amigos Helder e Morais que por meio de "brigas", risadas e palavras de conforto, fizemos a nossa jornada.

A minha filha e esposa, Maria Luísa e Aluska, que veio no final da caminhada, e fez o seu papel de oxigenar meus pulmões nos últimos metros.

A todo corpo docente que em muitas vezes foram não educadores e sim amigos que apontam o caminho certo.

Ao meu orientador Prof. Dr. Antônio de Andrade e Silva que indicou o tema desse trabalho, acompanhou o seu desenvolvimento ajudando sempre que foi solicitado.

A CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior e SBM - Sociedade Brasileira de Matemática, pela oportunidade oferecida aos professores da rede pública.

Dedicatória

Dedico esse trabalho a todos que contribuíram direta ou indiretamente para esta nova caminhada.

Resumo

Nosso estudo tem como objetivo apresentar uma categoria especial de números, os inteiros Gaussianos, suas propriedades e operações, ter uma visão geral sobre esses números, sua história e surgimento. Também estudaremos números primos Gaussianos, suas propriedades e aplicação com representação em linguagem matricial do tipo 2×2.

Palavras Chaves: Inteiros de Gauss, Números Primos Gaussianos, Fatoração Única e Matrizes.

Abstract

Our study aims to present a special category of numbers, the Gaussian integers, their properties and operations, have an overview about these numbers, their history and emergence. We will also study Gaussian prime numbers, their properties and application in matrix language representation of 2×2 type.

Keywords: Gaussian Integers, Gaussian Primes numbers, unique factorization and matrix.

Sumário

Notações

Notações Gerais

- $\mathbb{N}$ é o conjunto dos números naturais
- $\mathbb{Z}$ é o conjunto dos números inteiros
- $\mathbb{Z}_+$ é o conjunto dos números inteiros positivos
- $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ é o conjunto dos números inteiros menos o 0
- $\mathbb{Q}$ é o conjunto dos números racionais
- $\mathbb{R}$ é o conjunto dos números reais
- $\mathbb{C}$ é o conjunto dos números complexos
- $\mathbb{Z}[i]$ é o anel dos inteiros Gaussianos
- $\mathcal{U}(\mathbb{Z}[i])$ é o grupo das unidades de $\mathbb{Z}[i]$
- R é um anel comutativo com identidade
- $M_2(R)$ é o anel das matrizes 2×2 sobre R
- $\mathbf{A}$ representa uma matriz
- $\mathrm{N}(\mathbf{A})$ é a norma de $\mathbf{A}$
- $\mathbf{A}^t$ representa a matriz transposta
- $\det(\mathbf{A})$ é o determinante de $\mathbf{A}$
- $\mathrm{Tr}(\mathbf{A})$ é o traço de $\mathbf{A}$
- $\mathbf{J}$ representa a matriz

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

- $|$ é a operação divide
- $\nmid$ é a operação não divide
- $\equiv$ relação de congruência
- mdc é o máximo divisor comum

Introdução

De acordo com os axiomas de Cantor-Dedekind para representar os números reais $\mathbb{R}$, geometricamente, podem ser identificados com os pontos de uma reta do seguinte modo: fixemos sobre a reta um ponto O (a origem) e escolhamos um outro ponto U sobre a mesma reta e uma unidade de comprimento 1, de modo que 1 seja igual ao comprimento do segmento de reta OU. Não obstante, necessitamos de um plano para representar um número complexo, ou seja, chamamos o eixo das abscissas de eixo real e o eixo das ordenadas de eixo imaginário. Portanto, o número complexo $z = x + yi$ é representado sobre o plano cartesiano como o ponto de coordenadas (x, y). Esta interpretação foi introduzida e usada em 1796 por Gauss. O plano cartesiano chama-se de plano complexo (Gaussiano). Ainda podemos ver cada ponto (x, y) do plano complexo como um "**vetor**" (segmento de reta orientado) de origem $(0, 0)$ e extremidade (x, y). Neste caso, se $x \neq 0$, então $m = yx^{-1}$ é a inclinação do vetor. A representação geométrica de números complexos como pontos no plano é de grande importância prática.

A resolução de problemas tais como

$$x^3 \equiv q \pmod{p} \text{ e } x^4 \equiv q \pmod{p},$$

com p e q números primos, motivaram Gauss em 1825 a introduzir os número inteiros complexos da forma

$$\alpha = a + bi, \;\; a, b \in \mathbb{Z},$$

chamados de *números inteiros Gaussianos*, como um subanel dos números complexos $\mathbb{C}$ e denotado por $\mathbb{Z}[i]$, ou seja,

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

No presente trabalho, vamos estudar os principais conceitos e resultados relacionados aos inteiros e primos Gaussianos via matrizes 2×2 especiais, do tipo:

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

de modo que esse estudo possa ser tratado no ensino médio.

No Capítulo 1 veremos as principais definições e resultados sobre matrizes 2×2 e determinantes (sobre anel comutativo com identidade) que serão necessárias para o desenvolvimento deste trabalho. Não obstante, todas as definições e resultados continuam válidos para matrizes $n \times n$.

Já no Capitulo 2 apresentaremos definições, propriedades e teoremas relacionados aos números inteiros Gaussianos, representados pelos elementos do conjunto $\mathbb{Z}[i]$, os quais apresentam semelhanças com as propriedades dos números inteiros, e apresentaremos o Algorítimo da Divisão para matrizes de ordem 2.

Por fim, no Capitulo 3 abordaremos os primos Gaussianos detalhando suas propriedades e teoremas, como o da sua fatoração única e o do critério de sua primalidade.

Capítulo 1

Resultados e Conceitos Básicos sobre Matriz e Determinante

Neste capitulo faremos uma breve revisão sobre matrizes de ordem 2, seus conceitos e operações. As Matrizes são ferramentas da Álgebra Linear muito úteis para resolução de sistemas lineares. O leitor interessado em mais detalhes pode consultar as referências Boldrine[2], Hoffman-Kunze [7] e Lipschutz[9].

1.1 Matrizes

Em tudo que segue, salvo menção explícita em contrário, R representa um anel comutativo com identidade.

Um arranjo de quatro elementos $a, b, c, d \in R$ em que

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ ou } \mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

chama-se uma *matriz* 2×2 sobre R (lê-se "**matriz dois por dois**") ou simplesmente uma *matriz quadrada* de ordem 2 sobre R. Em algum sentido, uma matriz 2×2 pode ser vista como uma generalização dos nossos "pares" ordenados (x, y), e pode ser vista de dois modos: vendo como duas linhas

$$(a, b) \text{ e } (c, d),$$

as quais chamam-se primeira e segunda linha de $\mathbf{A}$, respectivamente, ou vendo como duas colunas

$$\begin{pmatrix} a \\ c \end{pmatrix} \text{ e } \begin{pmatrix} b \\ d \end{pmatrix},$$

as quais chamam-se primeira e segunda coluna de $\mathbf{A}$, respectivamente. É usual denotar uma matriz por

$$\mathbf{A} = (a_{ij}).$$

Os elementos $a_{ij} \in R$ chamam-se de *entradas* da matriz. Neste caso, formalmente, uma matriz 2×2 é uma função

$$f : \{1, 2\} \times \{1, 2\} \to R$$

definida como $f(i, j) = a_{ij}$.

Duas matrizes

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \text{ e } \mathbf{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

são *iguais*, em símbolos, $\mathbf{A} = \mathbf{B}$ se, e somente se,

$$a_{11} = b_{11}, \;\; a_{12} = b_{12}, \;\; a_{21} = b_{21} \text{ e } a_{22} = b_{22}.$$

Vamos denotar por $M_2(R)$ o conjunto de todas as matrizes de ordem 2 sobre R. Assim, é fácil verificar que $M_2(R)$, munido com as operações de adição

$$\mathbf{A} + \mathbf{B} = (a_{ij} + b_{ij})$$

e multiplicação por escalar

$$c\mathbf{A} = (ca_{ij}), \;\; \forall \;\; c \in R,$$

satisfaz as seguintes condições:

1. $\mathbf{A} + (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) + \mathbf{C}$, para quaisquer $\mathbf{A}, \mathbf{B}, \mathbf{C} \in M_2(R)$.
2. Existe $\mathbf{O} \in M_2(R)$ tal que $\mathbf{A} + \mathbf{O} = \mathbf{O} + \mathbf{A} = \mathbf{A}$, para qualquer $\mathbf{A} \in M_2(R)$.
3. Para cada $\mathbf{A} \in M_2(R)$, existe $-\mathbf{A} \in M_2(R)$ tal que
$$\mathbf{A} + (-\mathbf{A}) = -\mathbf{A} + \mathbf{A} = \mathbf{O}.$$
4. $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$, para quaisquer $\mathbf{A}, \mathbf{B} \in M_2(R)$.
5. $c(\mathbf{A} + \mathbf{B}) = c\mathbf{A} + c\mathbf{B}$, para quaisquer $\mathbf{A}, \mathbf{B} \in M_2(R)$ e $c \in R$.
6. $(c + d)\mathbf{A} = c\mathbf{A} + d\mathbf{A}$, para quaisquer $c, d \in R$ e $\mathbf{A} \in M_2(R)$.
7. $c(d\mathbf{A}) = (cd)\mathbf{A}$, para quaisquer $c, d \in R$ e $\mathbf{A} \in M_2(R)$.
8. $1 \cdot \mathbf{A} = \mathbf{A}$, para qualquer $\mathbf{A} \in M_2(R)$.

Neste caso, diremos que o terno $(M_2(R), +, \cdot)$ é um *módulo* sobre R.

Já equipamos o conjunto $M_2(R)$ com uma estrutura de módulo. Agora, equiparemos $M_2(R)$ com uma estrutura de "álgebra". Para isto, sejam $\mathbf{A} = (a_{ij}), \mathbf{B} = (b_{ij}) \in M_2(R)$. O *produto* de $\mathbf{A}$ por $\mathbf{B}$ é definido como

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

O produto de matriz satisfaz as seguintes condições:

1. $\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}$, para quaisquer $\mathbf{A}, \mathbf{B}, \mathbf{C} \in M_2(R)$.
2. $\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$, para quaisquer $\mathbf{A}, \mathbf{B}, \mathbf{C} \in M_2(R)$.
3. $(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$, para quaisquer $\mathbf{A}, \mathbf{B}, \mathbf{C} \in M_2(R)$.
4. Existe $\mathbf{I} \in M_2(R)$ tal que $\mathbf{A} \cdot \mathbf{I} = \mathbf{I} \cdot \mathbf{A} = \mathbf{A}$, para qualquer $\mathbf{A} \in M_2(R)$.
5. $c(\mathbf{AB}) = (c\mathbf{A})\mathbf{B} = \mathbf{A}(c\mathbf{B})$, para quaisquer $\mathbf{A}, \mathbf{B} \in M_2(R)$ e $c \in R$.

Neste caso, diremos que o terno $(M_2(R), +, \cdot)$ é um *anel* com identidade com a matriz identidade $\mathbf{I}$ não comutativo sobre R. Além disso, $(M_2(R), +, \cdot)$ é uma *algébra* sobre R.

As matrizes

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

chamam-se *matrizes unitárias*.

Seja $\mathbf{A} = (a_{ij}) \in M_2(R)$. Então:

1. $\mathbf{A} = a_{11}\mathbf{E}_{11} + a_{12}\mathbf{E}_{12} + a_{21}\mathbf{E}_{21} + a_{22}\mathbf{E}_{22}$.
2. $\mathbf{E}_{ii}^2 = \mathbf{E}_{ii}$ e $\mathbf{E}_{ij}^2 = \mathbf{O}$, se $i \neq j$.
3. $\mathbf{E}_{11} + \mathbf{E}_{22} = \mathbf{I}$, com $\mathbf{I}$ a *matriz identidade* ou a *matriz unidade*.
4. $\mathbf{E}_{km}\mathbf{A} = a_{m1}\mathbf{E}_{k1} + a_{m2}\mathbf{E}_{k2}$.
5. $\mathbf{AE}_{km} = a_{1k}\mathbf{E}_{1m} + a_{2k}\mathbf{E}_{2m}$.
6. $\mathbf{E}_{ij}\mathbf{AE}_{km} = a_{jk}\mathbf{E}_{im}$.

A *transposta* da matriz

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(R)$$

é a matriz

$$\mathbf{A}^t = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix},$$

isto é, $\mathbf{A}^t$ é a matriz obtida escrevendo-se as linhas de $\mathbf{A}$ como colunas. Os elementos a_{11} e a_{22} formam a *diagonal principal* da matriz $\mathbf{A}$. Diremos que $\mathbf{A} = (a_{ij}) \in M_2(R)$ é uma *matriz diagonal* se $a_{ij} = 0$ quando $i \neq j$.

A matriz transposta satisfaz as seguintes propriedades:

1. $(\mathbf{A} + \mathbf{B})^t = (\mathbf{A})^t + (\mathbf{B})^t$, para quaisquer $\mathbf{A}, \mathbf{B} \in M_2(R)$.
2. $(c\mathbf{A})^t = c\mathbf{A}^t$, para qualquer $\mathbf{A} \in M_2(R)$ e $c \in R$.
3. $(\mathbf{A}^t)^t = \mathbf{A}$, para qualquer $\mathbf{A} \in M_2(R)$.
4. $(\mathbf{AB})^t = \mathbf{B}^t\mathbf{A}^t$, para quaisquer $\mathbf{A}, \mathbf{B} \in M_2(R)$.

1.2 Determinantes

Seja

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

uma matriz em $M_2(R)$. Definimos o *determinante* de $\mathbf{A}$ como o elemento

$$ad - bc \in R$$

que será denotado por

$$|\mathbf{A}| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \text{ ou } \det(\mathbf{A}).$$

É útil usar a seguinte notação para o determinante: se $\mathbf{C}_1$ e $\mathbf{C}_2$ são as colunas de $\mathbf{A}$, então

$$\det(\mathbf{A}) = \det(\mathbf{C}_1, \mathbf{C}_2).$$

Seja $\mathbf{A} \in M_2(R)$. Então o determinante satisfaz as seguintes propriedades:

1. $\det(\mathbf{A}) = \det(\mathbf{A}^t)$.
2. $\det(\mathbf{C}_1 + \mathbf{C'}_1, \mathbf{C}_2) = \det(\mathbf{C}_1, \mathbf{C}_2) + \det(\mathbf{C'}_1, \mathbf{C}_2)$.

3. $\det(c\mathbf{C}_1, \mathbf{C}_2) = c\det(\mathbf{C}_1, \mathbf{C}_2)$, para todo $c \in R$.

4. $\det(\mathbf{C}_1, \mathbf{C}_1) = 0$.

5. $\det(\mathbf{C}_1 + c\mathbf{C}_2, \mathbf{C}_2) = \det(\mathbf{C}_1, \mathbf{C}_2)$, para todo $c \in R$.

6. $\det(\mathbf{C}_1, \mathbf{C}_2) = -\det(\mathbf{C}_2, \mathbf{C}_1)$.

É importante observar que as propriedades valem de modo natural para a segunda coluna, por exemplo $\det(\mathbf{C}_1, c\mathbf{C}_2) = c\det(\mathbf{C}_1, \mathbf{C}_2)$. Como uma ilustração provaremos à condição (2). Sejam

$$\mathbf{C}_1 = \begin{pmatrix} a \\ c \end{pmatrix}, \ \mathbf{C'}_1 = \begin{pmatrix} x \\ y \end{pmatrix} \text{ e } \mathbf{C}_2 = \begin{pmatrix} b \\ d \end{pmatrix},$$

Então

$$\begin{aligned} \det(\mathbf{C}_1 + \mathbf{C'}_1, \mathbf{C}_2) &= \begin{vmatrix} a+x & b \\ c+y & d \end{vmatrix} \\ &= (a+x)d - (c+y)b \\ &= (ad - bc) + (dx - by) \\ &= \det(\mathbf{C}_1, \mathbf{C}_2) + \det(\mathbf{C'}_1, \mathbf{C}_2), \end{aligned}$$

A condição 2 e 3 prova que a função determinante $\det : M_2(R) \to R$ definida como

$$\det(\mathbf{A}) = \det(\mathbf{C}_1, \mathbf{C}_2)$$

é uma *forma bilinear* sobre R.

Teorema 1.1 (Binet-Cauchy) *Sejam* $\mathbf{A}, \mathbf{B} \in M_2(R)$. *Então*

$$\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B}).$$

Prova. Sejam

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ e } \mathbf{B} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Então

$$\begin{aligned} \det(\mathbf{A})\det(\mathbf{B}) &= (ad - bc)(ps - qr) \\ &= adps - adqr - bcps + bcqr \\ &= acpq + adps + bcqr + bdrs - acpq - adqr - bcps - bdrs \\ &= (ap + br)(cq + ds) - (aq + bs)(cp + dr) \\ &= \det(\mathbf{AB}), \end{aligned}$$

que é o resultado desejado. ■

A função $\mathrm{Tr} : M_2(R) \to R$ definida como

$$\mathrm{Tr}(\mathbf{A}) = a + d, \ \forall \ \mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$$

chama-se *função traço*.

Sejam $\mathbf{A}, \mathbf{B} \in M_2(R)$. Então a função traço satisfaz as seguintes condições:

1. $\mathrm{Tr}(c\mathbf{A} + \mathbf{B}) = c\mathrm{Tr}(\mathbf{A}) + \mathrm{Tr}(\mathbf{B})$, para todo $c \in R$.
2. $\mathrm{Tr}(\mathbf{AB}) = \mathrm{Tr}(\mathbf{BA})$.
3. $\mathrm{Tr}(\mathbf{A}) = \mathrm{Tr}(\mathbf{A}^t)$.

A condição 1 prova que a função traço é uma forma linear sobre $\mathbf{R}$.

O conjunto

$$\mathcal{U}(R) = \{u \in R : uv = vu = 1, \ \text{para algum} \ v \in R\}$$

chama-se *conjunto das unidades* de R. Por exemplo,

$$\mathcal{U}(\mathbb{Z}) = \{-1, 1\}.$$

Seja $\mathbf{A} \in M_2(R)$. Diremos que $\mathbf{A}$ é uma *matriz invertível* se existir $\mathbf{B} \in M_2(R)$ tal que

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}.$$

É comum denotar $\mathbf{B} = \mathbf{A}^{-1}$ onde a matriz $\mathbf{B}$ chamá-la *matriz inversa* de $\mathbf{A}$. O conjunto

$$\mathcal{U}(M_2(R)) = \mathrm{GL}_2(R)$$

é um grupo chamado de grupo linear geral.

Note que se

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R),$$

então pode ser verificado diretamente que

$$\mathbf{A}^2 - \mathrm{Tr}(\mathbf{A})\mathbf{A} + \det(\mathbf{A})\mathbf{I} = \mathbf{0},$$

ou seja, $\mathbf{A}$ *anula* ou $\mathbf{A}$ é um *raiz* do polinômio

$$f = x^2 - \mathrm{Tr}(\mathbf{A})x + \det(\mathbf{A}) \in R[x].$$

Portanto, se $\mathbf{A} \in \mathrm{GL}_2(R)$, então $\Delta = \det(\mathbf{A}) \in \mathcal{U}(R)$ e

$$\mathbf{A}^{-1} = \Delta^{-1}(\mathrm{Tr}(\mathbf{A})\mathbf{I} - \mathbf{A}).$$

Por exemplo, se

$$\mathbf{A} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Z}),$$

então $\mathbf{A} \notin \mathrm{GL}_2(\mathbb{Z})$, pois $\det(\mathbf{A}) = 2 \notin \mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.

Consideremos o sistema de equações lineares não homogêneo

$$\begin{cases} ax + by &= r \\ cx + dy &= s \end{cases} \quad \text{ou} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix}.$$

O método tradicional de resolver esse sistema é o seguinte: multiplicando a primeira equação por d, a segunda por $-b$ e somando, obtemos

$$(ad - bc)x = dr - bs.$$

De modo análogo, obtemos

$$(ad - bc)y = as - cr.$$

Portanto, se $\Delta = \det(\mathbf{A}) \in \mathcal{U}(R)$, então teremos a **Regra de Cramer**

$$x = \Delta^{-1} \begin{vmatrix} r & b \\ s & d \end{vmatrix} \text{ e } y = \Delta^{-1} \begin{vmatrix} a & r \\ c & s \end{vmatrix}.$$

Note que se

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix} \text{ ou } \mathbf{AX} = \mathbf{R}$$

e $\det(\mathbf{A}) \in \mathcal{U}(R)$, então

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} r \\ s \end{pmatrix} \text{ ou } \mathbf{X} = \mathbf{A}^{-1}\mathbf{R}.$$

Capítulo 2

Os Inteiros Gaussianos

Neste capitulo estudaremos várias definições, propriedades e teoremas relacionados aos números inteiros Gaussianos, os quais são representados pelo conjunto $\mathbb{Z}[i]$. Os inteiros Gaussianos podem ser considerados um tipo particular de números complexos e é formado pelas matrizes da forma

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

onde $a, b \in \mathbb{Z}$, com uma série de propriedades semelhantes aos números inteiros $\mathbb{Z}$.

Gauss, ao definir número inteiro como elemento do conjunto $\mathbb{Z}[i]$, observou que muito da teoria de Euclides sobre fatoração de números inteiros poderia ser aplicada nesse novo conjunto por ele definido. Assim, desenvolveu uma teoria de fatoração em primos para $\mathbf{A} \in \mathbb{Z}[i]$ e essa decomposição é única, igual aos elementos do conjunto dos números inteiros $\mathbb{Z}$, dando com isso uma fundamental contribuição para a demonstração do último teorema de Fermat (Hefez [6]).

2.1 Os Inteiros Gaussianos

O conjunto

$$\mathbb{Z}[i] = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

munido com operações de soma e multiplicação induzidas pelo anel $M_2(\mathbb{Z})$ é um anel comutativo com identidade, chamado de *anel dos inteiros Gaussianos*. Pondo

$$\mathbf{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathbb{Z}[i],$$

obtemos

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a\mathbf{I} + b\mathbf{J}, \ \ \forall \ a, b \in \mathbb{Z},$$

a qual chama-se *forma normal* de $\mathbf{A}$. Observe que a função $\sigma : \mathbb{Z} \to \mathbb{Z}[i]$ definida como

$$\sigma(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a\mathbf{I}$$

claramente preserva as operações dos aneis e é injetora. Assim, podemos identificar o anel $\mathbb{Z}$ com o subanel

$$R = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z} \right\}$$

de $\mathbb{Z}[i]$. Neste caso, a nossa multiplicação sobre $\mathbb{Z}[i]$ estende a multiplicação sobre $\mathbb{Z}$, ou seja,

$$a\mathbf{I}b\mathbf{I} = ab\mathbf{I}$$

e $\mathbf{I}$ é o elemento identidade para a multiplicação sobre $\mathbb{Z}[i]$.

O conjunto

$$\mathbb{Q}[i] = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}$$

munido com operações de soma e multiplicação induzidas pelo anel $M_2(\mathbb{Q})$ é um corpo. Note que se $\mathbf{A} \in \mathbb{Q}[i]$, com $\mathbf{A} \neq \mathbf{O}$, então $\Delta = \det(\mathbf{A}) \in \mathcal{U}(\mathbb{Q}) = \mathbb{Q} - \{0\}$ e

$$\mathbf{A}^{-1} = \Delta^{-1}(\mathrm{Tr}(\mathbf{A})\mathbf{I} - \mathbf{A}).$$

Em particular, se

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

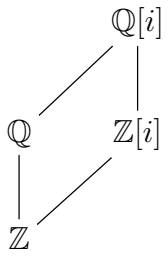
então

$$\mathbf{A}^{-1} = \Delta^{-1}(\mathrm{Tr}(\mathbf{A})\mathbf{I} - \mathbf{A}) = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{b}{a^2+b^2} \\ -\frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in \mathbb{Q}[i].$$

Além disso, é fácil verificar que $\mathbb{Z}[i]$ é um subanel (domínio de integridade) de $\mathbb{Q}[i]$ e que

$$\mathbb{Q}[i] = \{\mathbf{B}^{-1}\mathbf{A} : \mathbf{A}, \mathbf{B} \in M_2(\mathbb{Q}), \text{ com } \mathbf{B} \in \mathcal{U}(M_2(\mathbb{Q}))\}.$$

Neste caso, diremos que $\mathbb{Q}[i]$ é o *corpo quociente* (ver [10]) de $\mathbb{Z}[i]$, confira diagrama abaixo.



Seja

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{Z}[i].$$

Então a matriz transposta

$$\mathbf{A}^t = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a\mathbf{I} - b\mathbf{J} \in \mathbb{Z}[i]$$

chama-se *conjugada* de $\mathbf{A}$. Em particular, se $\mathbf{A}$ é invertível, então

$$\mathbf{A}^{-1} = \frac{1}{a^2+b^2}\mathbf{A}^t.$$

Observe que a função $\phi : \mathbb{Z}[i] \to \mathbb{Z}[i]$ definida como

$$\phi(\mathbf{A}) = \mathbf{A}^t$$

é bijetora e satisfaz as seguintes condições:

1. $\phi(\mathbf{A}+\mathbf{B}) = \phi(\mathbf{A}) + \phi(\mathbf{B})$.
2. $\phi(\mathbf{AB}) = \phi(\mathbf{B})\phi(\mathbf{A})$.
3. $\phi^2 = I$.

Consideremos a identificação

$$\mathbb{Z}_+ \longleftrightarrow R_+ = \{a\mathbf{I} : a \in \mathbb{Z}_+\} \text{ e } a \leq b \Leftrightarrow a\mathbf{I} \leq b\mathbf{I}.$$

A função $\mathrm{N} : \mathbb{Z}[i] \to R_+$ definida como

$$\mathrm{N}(\mathbf{A}) = \det(\mathbf{A})\mathbf{I}, \ \forall \ \mathbf{A} \in \mathbb{Z}[i]$$

chama-se *norma*. Observe que

$$\mathrm{N}(\mathbf{A}) = (a^2+b^2)\mathbf{I} = \mathbf{A}\mathbf{A}^t, \ \forall \ \mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{Z}[i].$$

Além disso, pelo Teorema 1.1,

$$\mathrm{N}(\mathbf{A}) = \mathrm{N}(\mathbf{A}^t) \text{ e } \mathrm{N}(\mathbf{AB}) = \mathrm{N}(\mathbf{A})\mathrm{N}(\mathbf{B}), \ \forall \ \mathbf{A},\mathbf{B} \in \mathbb{Z}[i].$$

Neste caso,

$$\mathrm{N}(\mathbf{A}) \leq \mathrm{N}(\mathbf{A})\mathrm{N}(\mathbf{B}), \ \forall \ \mathbf{A},\mathbf{B} \in \mathbb{Z}[i],$$

pois

$$\mathrm{N}(\mathbf{A}) = 0 \Leftrightarrow \mathbf{A} = \mathbf{O}.$$

Proposição 2.1 *Seja*

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{Z}[i].$$

Então as seguintes condições são equivalentes:

1. $\mathbf{A} \in \mathcal{U}(\mathbb{Z}[i])$;
2. $N(\mathbf{A}) = \mathbf{I}$, *ou seja,* $a^2 + b^2 = 1$;
3. $\mathbf{A} \in \{-\mathbf{I}, \mathbf{I}, -\mathbf{J}, \mathbf{J}\} = \{\mathbf{J}^k : k = 0, 1, 2, 3\}$.

Prova. $(1 \Rightarrow 2)$ Suponhamos que $\mathbf{A} \in \mathcal{U}(\mathbb{Z}[i])$. Então existe $\mathbf{B} \in \mathbb{Z}[i]$ tal que

$$\mathbf{AB} = \mathbf{I}.$$

Assim, $\mathrm{N}(\mathbf{A})\mathrm{N}(\mathbf{B}) = \mathbf{I}$. Como $a^2 + b^2 \in \mathbb{Z}_+$ temos que $0 < a^2 + b^2 \leq 1$. Portanto, $\mathrm{N}(\mathbf{A}) = \mathbf{I}$.

$(2 \Rightarrow 3)$ Suponhamos que $\mathrm{N}(\mathbf{A}) = \mathbf{I}$ e que

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Então

$$a^2 + b^2 = 1.$$

Assim, $|a| \leq 1$ e $|b| \leq 1$. Logo, $a, b \in \{-1, 0, 1\}$. Portanto, $b = 0$ e $a = \pm 1$ ou $a = 0$, $b = \pm 1$. Consequentemente,

$$\mathbf{A} \in \{-\mathbf{I}, \mathbf{I}, -\mathbf{J}, \mathbf{J}\} = \{\mathbf{J}^k : k = 0, 1, 2, 3\}.$$

$(3 \Rightarrow 1)$ É imediata. ∎

2.2 Algoritmo da Divisão

Nesta seção vamos provar que o anel dos inteiros Gaussianos $\mathbb{Z}[i]$ possui quase todas as propriedades do anel dos inteiros $\mathbb{Z}$. Como veremos, 2 perde a primalidade em $\mathbb{Z}[i]$.

Sejam $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$, com $\mathbf{A} \neq \mathbf{O}$. Diremos que $\mathbf{A}$ *divide* $\mathbf{B}$ se existir $\mathbf{Q} \in \mathbb{Z}[i]$ tal que

$$\mathbf{B} = \mathbf{QA}.$$

Como veremos esta definição nos permite estudar o máximo divisor comum (mdc), primos Gaussianos, etc. Observe que $\mathbf{I}$ divide $\mathbf{A}$ e $\mathbf{A}$ divide $\mathbf{O}$, para todo $\mathbf{A} \in \mathbb{Z}[i]$. A notação usada é $\mathbf{A} \mid \mathbf{B}$ se $\mathbf{A}$ divide $\mathbf{B}$ e $\mathbf{A} \nmid \mathbf{B}$, caso contrário.

Exemplo: Sejam

$$\mathbf{A} = \begin{pmatrix} 7 & -25 \\ 25 & 7 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 57 & -11 \\ 11 & 57 \end{pmatrix} \in \mathbb{Z}[i].$$

Mostre que $\mathbf{A}$ divide $\mathbf{B}$. $\diamond$ **Solução**. Devemos provar que existe

$$\mathbf{Q} = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in \mathbb{Z}[i]$$

tal que

$$\mathbf{B} = \mathbf{QA}.$$

Mas, isso é equivalente ao sistema

$$\begin{cases} 7x - 25y &= 57 \\ 25x + 7y &= 11 \end{cases}$$

possuir solução em $\mathbb{Z}$. Pela Regra de Cramer, o sistema possui solução se, e somente se,

$$x = \frac{7 \cdot 57 + 25 \cdot 11}{7 \cdot 7 + 25 \cdot 25} \in \mathbb{Z} \text{ e } y = \frac{7 \cdot 11 - 25 \cdot 57}{7 \cdot 7 + 25 \cdot 25} \in \mathbb{Z}.$$

Neste caso, $x = 1$ e $y = -2$. Portanto, $\mathbf{A}$ divide $\mathbf{B}$.

Em geral, um critério para examinar as condições de divisibilidade em $\mathbb{Z}[i]$ é como segue. Sejam

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \mathbf{B} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathbb{Z}[i].$$

Então $\mathbf{A}$ divide $\mathbf{B}$ se, e somente se, existe

$$\mathbf{Q} = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in \mathbb{Z}[i]$$

tal que

$$\mathbf{B} = \mathbf{QA}.$$

Mas, isso é equivalente ao sistema

$$\begin{cases} ax - by &= c \\ bx + ay &= d \end{cases}$$

possuir solução em $\mathbb{Z}$. Pela Regra de Cramer, o sistema possui solução se, e somente se,

$$x = \frac{ac + bd}{a^2 + b^2} \in \mathbb{Z} \text{ e } y = \frac{ad - bc}{a^2 + b^2} \in \mathbb{Z}.$$

Exemplo: Se

$$\mathbf{A} = \begin{pmatrix} 14 & -3 \\ 3 & 14 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 57 & -11 \\ 11 & 57 \end{pmatrix} \in \mathbb{Z}[i],$$

então $\mathbf{A}$ não divide $\mathbf{B}$, pois

$$\frac{ac+bd}{a^2+b^2} = \frac{831}{205} \notin \mathbb{Z}.$$

$\diamond$

Em particular, se $\mathbf{A} = a\mathbf{I}$, para todo $a \in \mathbb{Z}$, então $\mathbf{A}$ divide $\mathbf{B}$ se, e somente se,

$$x = \frac{c}{a} \in \mathbb{Z} \text{ e } y = \frac{d}{a} \in \mathbb{Z}$$

se, e somente se, a divide c e d em $\mathbb{Z}$.

Observe que, dados $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$, com $\mathbf{A} \neq \mathbf{O}$, se $\mathbf{A}$ divide $\mathbf{B}$, então $\mathrm{N}(\mathbf{A})$ divide $\mathrm{N}(\mathbf{B})$ em $\mathbb{Z}$. Mas, a recíproca é falsa, por exemplo, se

$$\mathbf{A} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 3 & -1 \\ 1 & 3 \end{pmatrix} \in \mathbb{Z}[i],$$

então $\mathrm{N}(\mathbf{A}) = 5\mathbf{I}$ divide $\mathrm{N}(\mathbf{B}) = 10\mathbf{I}$ em $\mathbb{Z}$. No entanto, $\mathbf{A}$ não divide $\mathbf{B}$, pois

$$\frac{7}{5} \notin \mathbb{Z}.$$

Finalmente, seja $\mathbf{A} \in \mathbb{Z}[i]$. Então $\mathrm{N}(\mathbf{A})$ é igual a um número par se, e somente se, $\mathbf{I} + \mathbf{J}$ divide $\mathbf{A}$.

É pertinente notar que estas observações nos levam de forma prática e rápida decidir se um dado inteiro Gaussiano divide ou não um outro inteiro Gaussiano.

Sejam $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$. Diremos que $\mathbf{A}$ é *associado* a $\mathbf{B}$ se existir $\mathbf{U} \in \mathcal{U}(\mathbb{Z}[i])$ tal que

$$\mathbf{B} = \mathbf{U}\mathbf{A}.$$

Vamos resumir esses resultados na seguinte proposição:

Proposição 2.2 *Sejam* $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$. *Então*:

1. *Se* $\mathbf{A}$ *divide* $\mathbf{B}$, *então* $N(\mathbf{A})$ *divide* $N(\mathbf{B})$ *em* $\mathbb{Z}$.
2. *Se* $\mathbf{A}$ *divide* $\mathbf{B}$ *e* $\mathbf{B}$ *divide* $\mathbf{A}$, *então* $\mathbf{A}$ *e* $\mathbf{B}$ *são associados.*
3. *Se* $a\mathbf{I}$ *divide* $b\mathbf{I}$, *então* a *divide* b *em* $\mathbb{Z}$.
4. *Se* $\mathbf{A}$ *divide* $\mathbf{B}$, *então* $\mathbf{A}^t$ *divide* $\mathbf{B}^t$.

5. *Se* $\mathbf{A}$ *divide* $\mathbf{B}$ *e* $\mathbf{A}$ *não é uma unidade e nem associado a* $\mathbf{B}$*, então*

$$\mathbf{I} < N(\mathbf{A}) < N(\mathbf{B}).$$

A função $f : \mathbb{R} \to \mathbb{Z}$ definida como

$$f(x) = \lfloor x \rfloor = (x-1, x] \cap \mathbb{Z}$$

chama-se *função maior inteiro* sobre $\mathbb{R}$. Note que

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}$$

e

$$0 \leq x - \lfloor x \rfloor < 1$$

chama-se *parte fracionária* de x.

Note que não podemos estender a relação de ordem sobre $\mathbb{Z}$ para $\mathbb{Z}[i]$. Por exemplo, não vale a Lei da Tricotomia em $\mathbb{Z}[i]$. Caso contrário, se $\mathbf{J} < \mathbf{O}$, então $\mathbf{O} < -\mathbf{J}$. Assim,

$$\mathbf{O} < (-\mathbf{J})^2 = -\mathbf{I},$$

o que é impossível. Se $\mathbf{J} > \mathbf{O}$, então

$$\mathbf{O} < \mathbf{J}^2 = -\mathbf{I},$$

o que também é impossível. Mas, uma comparação fraca entre os elementos de $\mathbb{Z}[i]$ pode ser efetuado por comparação de normas, a qual é dada pelo seguinte teorema:

Teorema 2.1 (Algoritmo da Divisão) *Sejam* $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$*, com* $\mathbf{B} \neq \mathbf{O}$*. Então existem* $\mathbf{Q}, \mathbf{R} \in \mathbb{Z}[i]$ *tais que*

$$\mathbf{A} = \mathbf{QB} + \mathbf{R}, \ \textit{com} \ \mathbf{R} = \mathbf{O} \ \textit{ou} \ N(\mathbf{R}) < N(\mathbf{B}).$$

Prova. Sejam

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \mathbf{B} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathbb{Z}[i].$$

Então podemos escrever

$$\mathbf{B}^{-1}\mathbf{A} = \frac{1}{c^2+d^2}\mathbf{B}^t\mathbf{A} = \begin{pmatrix} \frac{ac+bd}{c^2+d^2} & \frac{-(ad-bc)}{c^2+d^2} \\ \frac{ad-bc}{c^2+d^2} & \frac{ac+bd}{c^2+d^2} \end{pmatrix} = \begin{pmatrix} x & -y \\ y & x \end{pmatrix},$$

onde $x, y \in \mathbb{Q}$, pois $\mathbf{B} \neq \mathbf{O}$. Pondo $r = \lfloor x \rfloor, s = \lfloor y \rfloor \in \mathbb{Z}$, obtemos

$$|x - r| \leq \frac{1}{2} \ \text{e} \ |y - s| \leq \frac{1}{2}.$$

Assim,

$$\mathrm{N}\left(\begin{pmatrix} x & -y \\ y & x \end{pmatrix} - \begin{pmatrix} r & -s \\ s & r \end{pmatrix}\right) = \mathrm{N}\left(\begin{pmatrix} x-r & -(y-s) \\ y-s & x-r \end{pmatrix}\right) \leq \frac{1}{4}\mathbf{I} < \mathbf{I}.$$

Logo, escolhendo

$$\mathbf{Q} = \begin{pmatrix} r & -s \\ s & r \end{pmatrix} \text{ e } \mathbf{R} = \mathbf{A} - \mathbf{QB},$$

teremos $\mathbf{R} = \mathbf{O}$ ou

$$\mathrm{N}(\mathbf{R}) = \mathrm{N}(\mathbf{B}(\mathbf{B}^{-1}\mathbf{A} - \mathbf{Q})) = \mathrm{N}(\mathbf{B})\mathrm{N}(\mathbf{B}^{-1}\mathbf{A} - \mathbf{Q}) < \mathrm{N}(\mathbf{B}),$$

que é o resultado desejado. ■

Exemplo: Determine o quociente e o resto de

$$\mathbf{A} = \begin{pmatrix} 4 & -5 \\ 5 & 4 \end{pmatrix} \in \mathbb{Z}[i] \text{ e } \mathbf{B} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \mathbb{Z}[i].$$

◇

Solução. Como

$$\mathbf{B}^{-1}\mathbf{A} = \begin{pmatrix} \frac{9}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{9}{2} \end{pmatrix}$$

temos que escolher

$$\mathbf{Q} = \begin{pmatrix} r & -s \\ s & r \end{pmatrix}$$

tal que

$$\left|\frac{9}{2} - r\right| \leq \frac{1}{2} \text{ e } \left|\frac{1}{2} - s\right| \leq \frac{1}{2}.$$

Assim, $r \in \{4, 5\}$ e $s \in \{0, 1\}$. Portanto, as possíveis soluções $(\mathbf{Q}, \mathbf{R})$, com

$$\mathbf{Q} = \begin{pmatrix} r & -s \\ s & r \end{pmatrix} \text{ e } \mathbf{R} = \mathbf{A} - \mathbf{QB},$$

são

$$(4\mathbf{I}, \mathbf{J}), (4\mathbf{I} + \mathbf{J}, \mathbf{I}), (5\mathbf{I}, -\mathbf{I}) \text{ e } (5\mathbf{I} + \mathbf{J}, -\mathbf{J}).$$

Lema 2.1 *Sejam $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$, com $\mathbf{B} \neq \mathbf{O}$. Então o quociente $\mathbf{Q}$ e o resto $\mathbf{R}$ do Algoritmo da Divisão são únicos se, e somente se,*

$$N(\mathbf{A} + \mathbf{B}) \leq \max\{N(\mathbf{A}), N(\mathbf{B})\}.$$

Prova. Suponhamos que

$$\mathrm{N}(\mathbf{A}+\mathbf{B}) > \max\{\mathrm{N}(\mathbf{A}), \mathrm{N}(\mathbf{B})\}.$$

Então

$$\mathbf{A} = \mathbf{O}(\mathbf{A}+\mathbf{B}) + \mathbf{A} \text{ e } \mathbf{A} = \mathbf{I}(\mathbf{A}+\mathbf{B}) + (-\mathbf{B}),$$

com

$$\mathrm{N}(\mathbf{A}) < \mathrm{N}(\mathbf{A}+\mathbf{B}) \text{ e } \mathrm{N}(-\mathbf{B}) = \mathrm{N}(\mathbf{B}) < \mathrm{N}(\mathbf{A}+\mathbf{B}).$$

Portanto, o quociente e o resto não são únicos.

Reciprocamente, sejam $\mathbf{Q}, \mathbf{Q}_1, \mathbf{R}, \mathbf{R}_1 \in \mathbb{Z}[i]$ tais que

$$\mathbf{A} = \mathbf{Q}\mathbf{B} + \mathbf{R}, \text{ com } \mathbf{R} = \mathbf{O} \text{ ou } \mathrm{N}(\mathbf{R}) < \mathrm{N}(\mathbf{B}).$$

e

$$\mathbf{A} = \mathbf{Q_1}\mathbf{B} + \mathbf{R}_1, \text{ com } \mathbf{R}_1 = \mathbf{O} \text{ ou } \mathrm{N}(\mathbf{R}_1) < \mathrm{N}(\mathbf{B}).$$

Então

$$\mathbf{R} - \mathbf{R}_1 = (\mathbf{Q}_1 - \mathbf{Q})\mathbf{B}.$$

Assim,

$$\mathrm{N}(\mathbf{B}) \leq \mathrm{N}((\mathbf{Q}_1 - \mathbf{Q})\mathbf{B}) = \mathrm{N}(\mathbf{R} - \mathbf{R}_1) \leq \max \mathrm{N}(\mathbf{R}), \mathrm{N}(\mathbf{R}_1) < \mathrm{N}(\mathbf{B}),$$

o que é impossível, a menos que

$$\mathbf{R} - \mathbf{R}_1 = \mathbf{O} \text{ ou } \mathbf{Q}_1 - \mathbf{Q} = \mathbf{O},$$

ou seja, $\mathbf{R} = \mathbf{R}_1$ e $\mathbf{Q} = \mathbf{Q}_1$. ■

Exemplo: Determine o quociente e o resto de

$$\mathbf{A} = \begin{pmatrix} 7 & -11 \\ 11 & 7 \end{pmatrix} \in \mathbb{Z}[i] \text{ e } \mathbf{B} = \begin{pmatrix} 3 & -5 \\ 5 & 3 \end{pmatrix} \in \mathbb{Z}[i].$$

◇

Solução. Como

$$\mathbf{A} + \mathbf{B} = \begin{pmatrix} 10 & -16 \\ 16 & 10 \end{pmatrix}$$

temos que

$$\mathrm{N}(\mathbf{A}+\mathbf{B}) > \max\{\mathrm{N}(\mathbf{A}), \mathrm{N}(\mathbf{B})\}.$$

Assim,

$$\mathbf{A} = \mathbf{Q}\mathbf{B} + \mathbf{R},$$

com $\mathbf{Q} = 2\mathbf{I}$ e $\mathbf{R} = \mathbf{I} + \mathbf{J}$, é uma das soluções possíveis.

Lema 2.2 *Seja $f : \mathbb{N} \longrightarrow \mathbb{N}$ uma função (sequência) decrescente. Então existe $n_0 \in \mathbb{N}$ tal que $f(n) = f(n_0)$, para todo $n \in \mathbb{N}$, com $n \geq n_0$.*

Prova. Seja

$$S = f(\mathbb{N}) = \{f(n) : n \in \mathbb{N}\}.$$

Então $S \notin \emptyset$. Assim, pelo Princípio da Boa Ordenação, existe $s_0 \in S$ tal que $s_0 \leq s$, para todo $s \in S$. Como $s_0 \in S$ temos que existe $n_0 \in \mathbb{N}$ tal que $f(n_0) = s_0$. Assim, $f(n) \leq f(n_0) = s_0$, para todo $n \in \mathbb{N}$, com $n \geq n_0$, pois f é decrescente. Por outro lado, $s_0 \leq f(n)$, para todo $n \in \mathbb{N}$, com $n \geq n_0$. Portanto, $f(n) = f(n_0)$, para todo $n \in \mathbb{N}$, com $n \geq n_0$. ■

Com base no Teorema 2.1, o *Algoritmo de Euclides* pode ser generalizado para $\mathbb{Z}[i]$, do seguinte modo

$$\begin{array}{rcll}
\mathbf{A} & = & \mathbf{Q}_1\mathbf{B} + \mathbf{R}_1, & \text{com } \mathbf{R}_1 = \mathbf{O} \text{ ou } \mathrm{N}(\mathbf{R}_1) < \mathrm{N}(\mathbf{B}) \\
\mathbf{B} & = & \mathbf{Q}_2\mathbf{R}_1 + \mathbf{R}_2, & \text{com } \mathbf{R}_2 = \mathbf{O} \text{ ou } \mathrm{N}(\mathbf{R}_2) < \mathrm{N}(\mathbf{R}_1) \\
\mathbf{R}_1 & = & \mathbf{Q}_3\mathbf{R}_2 + \mathbf{R}_3, & \text{com } \mathbf{R}_3 = \mathbf{O} \text{ ou } \mathrm{N}(\mathbf{R}_3) < \mathrm{N}(\mathbf{R}_4) \\
 & \vdots & & \\
\mathbf{R}_{n-2} & = & \mathbf{Q}_n\mathbf{R}_{n-1} + \mathbf{R}_n, & \text{com } \mathbf{R}_n = \mathbf{O} \text{ ou } \mathrm{N}(\mathbf{R}_n) < \mathrm{N}(\mathbf{R}_{n-1}) \\
\mathbf{R}_{n-1} & = & \mathbf{Q}_{n+1}\mathbf{R}_n, & \text{com } \mathbf{R}_{n+1} = \mathbf{O},
\end{array}$$

pois, pelo Lema 2.2, a sequência

$$\{\mathrm{N}(\mathbf{B}), \mathrm{N}(\mathbf{R}_1), \mathrm{N}(\mathbf{R}_2), \ldots\}$$

termina.

Sejam $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$, não ambos nulo. Diremos que $\mathbf{D} \in \mathbb{Z}[i]$ é um *máximo divisor comum* de $\mathbf{A}$ e $\mathbf{B}$ se as seguintes condições são satisfeitas:

1. $\mathbf{D} \mid \mathbf{A}$ e $\mathbf{D} \mid \mathbf{B}$.
2. Se $\mathbf{D}_1 \mid \mathbf{A}$ e $\mathbf{D}_1 \mid \mathbf{B}$, então $\mathbf{D}_1 \mid \mathbf{D}$.

Observe que se $\mathbf{D}, \mathbf{D}_1 \in \mathbb{Z}[i]$ são dois máximos divisores comuns de $\mathbf{A}$ e $\mathbf{B}$, respectivamente, então, pelas condições (1) e (2), $\mathbf{D}_1 \mid \mathbf{D}$ e $\mathbf{D} \mid \mathbf{D}_1$. Assim, $\mathbf{D}$ é associado a $\mathbf{D}_1$. Portanto, a menos de associados,

$$\mathbf{D} = \mathrm{mdc}(\mathbf{A}, \mathbf{B})$$

é único. Portanto, não há perda de generalidade, em escolher

$$\mathbf{D} = \begin{pmatrix} r & -s \\ s & r \end{pmatrix}, \text{ com } r > 0 \text{ e } s \geq 0.$$

Diremos que $\mathbf{A}$ e $\mathbf{B}$ são *relativamente primos* quando

$$\mathrm{mdc}(\mathbf{A}, \mathbf{B}) = \mathbf{I}.$$

Lema 2.3 *Sejam* $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i] - \{\mathbf{O}\}$. *Se*

$$\mathbf{A} = \mathbf{QB} + \mathbf{R}, \text{ com } \mathbf{R} = \mathbf{O} \text{ ou } N(\mathbf{R}) < N(\mathbf{B}),$$

então

$$mdc(\mathbf{A}, \mathbf{B}) = mdc(\mathbf{B}, \mathbf{R}) = mdc(\mathbf{B}, \mathbf{A} - \mathbf{QB}).$$

Prova. Pela sua simplicidade sua demonstração fica como sugestão de exercício. ■

Teorema 2.2 (Bézout) *Sejam* $\mathbf{A}, \mathbf{B} \in \mathbb{Z}[i]$, *não ambos nulos. Então existem* $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}[i]$ *tais que*

$$mdc(\mathbf{A}, \mathbf{B}) = \mathbf{AX} + \mathbf{BY}.$$

Prova. Basta usar o Lema 2.3 e o Algoritmo de Euclides de trás para frente. ■

Exemplo: Sejam

$$\mathbf{A} = \begin{pmatrix} 7 & -11 \\ 11 & 7 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 3 & -5 \\ 5 & 3 \end{pmatrix} \in \mathbb{Z}[i].$$

Determine $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}[i]$ tais que

$$\text{mdc}(\mathbf{A}, \mathbf{B}) = \mathbf{AX} + \mathbf{BY}.$$

◇

Solução. Já vimos, no Exemplo 2.2, que:

$$\mathbf{A} = \mathbf{Q}_1\mathbf{B} + \mathbf{R}_1,$$

com $\mathbf{Q}_1 = 2\mathbf{I}$ e $\mathbf{R}_1 = \mathbf{I} + \mathbf{J}$. É fácil verificar que

$$\mathbf{B} = \mathbf{Q}_2\mathbf{R}_1, \text{ em que } \mathbf{Q}_2 = \begin{pmatrix} 4 & -1 \\ 1 & 4 \end{pmatrix}.$$

Assim,

$$\mathbf{R}_1 = \mathbf{A} - \mathbf{Q}_1\mathbf{B} = \mathbf{AX} + \mathbf{BY},$$

com $\mathbf{X} = \mathbf{I}$ e $\mathbf{Y} = -\mathbf{Q}_1$. Portanto, $\text{mdc}(\mathbf{A}, \mathbf{B}) = \mathbf{I} + \mathbf{J}$.

Exemplo: Sejam

$$\mathbf{A} = \begin{pmatrix} 32 & -9 \\ 9 & 32 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 4 & -11 \\ 11 & 4 \end{pmatrix} \in \mathbb{Z}[i].$$

Determine $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}[i]$ tais que

$$\text{mdc}(\mathbf{A}, \mathbf{B}) = \mathbf{AX} + \mathbf{BY}.$$

◇

Solução. Como

$$\mathbf{B}^{-1}\mathbf{A} = \begin{pmatrix} \frac{227}{137} & \frac{316}{137} \\ -\frac{316}{137} & \frac{227}{137} \end{pmatrix} = \begin{pmatrix} 2-\frac{47}{137} & 2+\frac{42}{137} \\ -2-\frac{42}{137} & 2-\frac{47}{137} \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix} + \frac{1}{137}\begin{pmatrix} -47 & 42 \\ -42 & -47 \end{pmatrix}$$

temos que

$$\mathbf{A} = \mathbf{Q}_1\mathbf{B} + \mathbf{R}_1,$$

com

$$\mathbf{Q}_1 = \begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix} \text{ e } \mathbf{R}_1 = \frac{1}{137}\mathbf{B}\begin{pmatrix} -47 & 42 \\ -42 & -47 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ -5 & 2 \end{pmatrix}.$$

De modo análogo,

$$\begin{aligned} \mathbf{B} &= \mathbf{Q}_2\mathbf{R}_1 + \mathbf{R}_2, \text{ com } \mathbf{Q}_2 = \begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix} \text{ e } \mathbf{R}_2 = \begin{pmatrix} 3 & 1 \\ -1 & 3 \end{pmatrix} \\ \mathbf{R}_1 &= \mathbf{Q}_3\mathbf{R}_2 + \mathbf{R}_3, \text{ com } \mathbf{Q}_3 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \text{ e } \mathbf{R}_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ \mathbf{R}_2 &= \mathbf{Q}_4\mathbf{R}_3, \qquad \text{com } \mathbf{Q}_4 = \begin{pmatrix} 1 & -3 \\ 3 & 1 \end{pmatrix}. \end{aligned}$$

Assim, com alguns cálculos, obtemos

$$\text{mdc}(\mathbf{A},\mathbf{B}) = \mathbf{I} = \mathbf{AX} + \mathbf{BY}, \text{ com } \mathbf{X} = 3\mathbf{I} \text{ e } \mathbf{Y} = \begin{pmatrix} -5 & -7 \\ 7 & -5 \end{pmatrix}.$$

Portanto, $\mathbf{A}$ e $\mathbf{B}$ são relativamente primos. ■

Lema 2.4 *Sejam* $\mathbf{A},\mathbf{B},\mathbf{C} \in \mathbb{Z}[i]$. *Se* $mdc(\mathbf{A},\mathbf{B}) = \mathbf{I}$ *e* $mdc(\mathbf{A},\mathbf{C}) = \mathbf{I}$. *Então*

$$mdc(\mathbf{A},\mathbf{BC}) = \mathbf{I}.$$

Prova. Temos que existem $\mathbf{X},\mathbf{Y},\mathbf{V},\mathbf{W} \in \mathbb{Z}[i]$ tais que

$$\mathbf{AX} + \mathbf{BY} = \mathbf{I} \text{ e } \mathbf{AV} + \mathbf{CW} = \mathbf{I}.$$

Assim,

$$\mathbf{I} = (\mathbf{AX} + \mathbf{BY})(\mathbf{AV} + \mathbf{CW})$$

implica que

$$\mathbf{I} = \mathbf{A}(\mathbf{AXV} + \mathbf{BYV} + \mathbf{CXW}) + \mathbf{BC}(\mathbf{YW}).$$

Portanto, $\text{mdc}(\mathbf{A},\mathbf{BC}) = \mathbf{I}$.

Proposição 2.3 *Sejam* $\mathbf{A},\mathbf{B},\mathbf{C} \in \mathbb{Z}[i]$. *Se* $\mathbf{A} \mid \mathbf{C}$, $\mathbf{B} \mid \mathbf{C}$ *e* $mdc(\mathbf{A},\mathbf{B}) = \mathbf{I}$. *Então*

$$\mathbf{AB} \mid \mathbf{C}.$$

Prova. Temos que existem $\mathbf{S}, \mathbf{T}, \mathbf{X}, \mathbf{Y} \in \mathbb{Z}[i]$ tais que

$$\mathbf{C} = \mathbf{AS}, \ \ \mathbf{C} = \mathbf{BT} \ \text{ e } \ \mathbf{AX} + \mathbf{BY} = \mathbf{I}.$$

Assim,

$$\mathbf{C} = \mathbf{ACX} + \mathbf{BCY} = (\mathbf{TX} + \mathbf{SY})\mathbf{AB}.$$

Portanto, $\mathbf{AB} \mid \mathbf{C}$. ■

Capítulo 3

Os Primos Gaussianos

Neste capitulo abordaremos de maneira detalhada os primos Gaussianos, suas propriedades e teoremas.

3.1 Fatoração Única

Seja $\mathbf{P} \in \mathbb{Z}[i]$. Diremos que $\mathbf{P}$ é um *primo Gaussiano* em $\mathbb{Z}[i]$ se as seguintes condições são satisfeitas:

1. $\mathbf{P} \neq \mathbf{O}$ e $\mathbf{P} \notin \mathcal{U}(\mathbb{Z}[i])$.
2. Se $\mathbf{P} \mid \mathbf{AB}$, então $\mathbf{P} \mid \mathbf{A}$ ou $\mathbf{P} \mid \mathbf{B}$ ou ambos.

Note que a condição (2) é equivalente a:

$$\mathbf{P} = \mathbf{AB} \Rightarrow \mathbf{A} \in \mathcal{U}(\mathbb{Z}[i]) \text{ ou } \mathbf{B} \in \mathcal{U}(\mathbb{Z}[i]),$$

ou seja, se $\mathbf{A} \mid \mathbf{P}$, então

$$\mathbf{A} \in \mathcal{U}(\mathbb{Z}[i]) \text{ ou } \mathbf{A} \text{ é associado a } \mathbf{P}.$$

Por exemplo, $\mathbf{P} = \mathbf{I} + \mathbf{J}$ é um primo Gaussiano, pois

$$\mathbf{P} = \mathbf{AB} \Rightarrow \mathrm{N}(\mathbf{A})\mathrm{N}(\mathbf{B}) = 2\mathbf{I}.$$

Assim, $\mathrm{N}(\mathbf{A}) = \mathbf{I}$ ou $\mathrm{N}(\mathbf{B}) = \mathbf{I}$. Portanto, $\mathbf{A} \in \mathcal{U}(\mathbb{Z}[i])$ ou $\mathbf{B} \in \mathcal{U}(\mathbb{Z}[i])$. No entanto, 2 é um número primo em $\mathbb{Z}$, mas $2\mathbf{I}$ não é um primo Gaussiano, pois

$$2\mathbf{I} = (\mathbf{I} + \mathbf{J})(\mathbf{I} - \mathbf{J}) = \mathbf{J}(\mathbf{I} - \mathbf{J})^2 = -\mathbf{J}(\mathbf{I} + \mathbf{J})^2.$$

Observe que $\mathbf{P}$ é um primo Gaussiano se, e somente se, $\mathbf{P}^t$ também o é, pois

$$\mathbf{P} = \mathbf{AB} \Leftrightarrow \mathbf{P}^t = \mathbf{A}^t\mathbf{B}^t.$$

É pertinente observar que $\mathbf{P}$ é um primo Gaussiano se, e somente se, $\mathbf{P}$ possui exatamente oito divisores, a saber,

$$\pm\mathbf{I},\ \pm\mathbf{J},\ \pm\mathbf{P} \text{ e } \pm\mathbf{JP}.$$

Portanto, se $\mathbf{A} \in \mathbb{Z}[i]$ não é divisível por um primo Gaussiano $\mathbf{P}$, então $\text{mdc}(\mathbf{A}, \mathbf{P}) = \mathbf{I}$.

Proposição 3.1 *Para qualquer $\mathbf{A} \in \mathbb{Z}[i]$, com $N(\mathbf{A}) = a\mathbf{I}$ e $a \geq 2$, existe um primo Gaussiano $\mathbf{P}$ que divide $\mathbf{A}$.*

Prova. Seja

$$S = \{a \in \mathbb{N}-\{1\} : \exists\ \mathbf{A} \in \mathbb{Z}[i],\ \text{com } \mathrm{N}(\mathbf{A}) = a\mathbf{I} \text{ e } \mathbf{Q} \nmid \mathbf{A},\ \forall \text{ primo Gaussiano } \mathbf{Q}\}.$$

Então $S = \emptyset$. De fato, se $S \neq \emptyset$, então, pelo Princípio da Boa Ordenação, S contém um menor elemento, digamos $d \in S$. Seja $\mathbf{D} \in \mathbb{Z}[i]$ tal que $\mathrm{N}(\mathbf{D}) = d\mathbf{I}$. Como $\mathbf{D}$ divide $\mathbf{D}$ temos que $\mathbf{D}$ não é um primo Gaussiano. Assim,

$$\mathbf{D} = \mathbf{BC},\ \text{com } \mathrm{N}(\mathbf{B}) = b\mathbf{I},\ \mathrm{N}(\mathbf{C}) = c\mathbf{I} \text{ e } 1 < b, c < d.$$

Logo, $b \notin S$. Neste caso, existe um primo Gaussiano $\mathbf{P}$ tal que $\mathbf{P}$ divide $\mathbf{B}$. Por definição, $\mathbf{P}$ divide $\mathbf{D}$. Portanto, $d \notin S$, o que é uma contradição. Consequentemente, existe um primo Gaussiano $\mathbf{P}$ que divide $\mathbf{A}$. ■

Seja $\mathbf{A} \in \mathbb{Z}[i]$. Diremos que $\mathbf{A}$ é *redutível* sobre $\mathbb{Z}[i]$ se ele não for um primo Gaussiano.

Teorema 3.1 *Seja $\mathbf{A} \in \mathbb{Z}[i]$ redutível. Então $\mathbf{A}$ contém um divisor primo Gaussiano $\mathbf{P}$ tal que*

$$N(\mathbf{P}) \leq \sqrt{N(\mathbf{A})}.$$

Prova. Seja

$$S = \{a \in \mathbb{N}-\{1\} : \exists\ \mathbf{A} \in \mathbb{Z}[i],\ \text{com } \mathrm{N}(\mathbf{A}) = a\mathbf{I} \text{ e } \mathbf{Q} \mid \mathbf{A},\ \text{com } \mathbf{Q} \text{ Primo Gausiano}\}.$$

Então, pela Proposição 3.1, $S \neq \emptyset$. Assim, pelo Princípio da Boa Ordenação, S contém um menor elemento, digamos $p \in S$. Seja $\mathbf{P} \in \mathbb{Z}[i]$ tal que $\mathrm{N}(\mathbf{P}) = p\mathbf{I}$. Então existe $\mathbf{B} \in \mathbb{Z}[i]$ tal que $\mathbf{A} = \mathbf{PB}$. É claro que $\mathrm{N}(\mathbf{P}) \leq \mathrm{N}(\mathbf{B})$ e

$$\mathrm{N}(\mathbf{P})^2 \leq \mathrm{N}(\mathbf{P})\mathrm{N}(\mathbf{B}) = \mathrm{N}(\mathbf{A}).$$

Portanto, $\mathrm{N}(\mathbf{P}) \leq \sqrt{\mathrm{N}(\mathbf{A})}$. ■

Teorema 3.2 *Qualquer* $\mathbf{A} \in \mathbb{Z}[i]$, *com* $N(\mathbf{A}) = a\mathbf{I}$ *e* $a \geq 2$, *pode ser fatorado como um produto finito de primos Gaussianos.*

Prova. Seja

$$S = \{a \in \mathbb{N} - \{1\} : \exists\ \mathbf{A} \in \mathbb{Z}[i],\ \text{com}\ \mathrm{N}(\mathbf{A}) = a\mathbf{I}\ \text{e}\ \mathbf{A} \neq \mathbf{P}_1 \cdots \mathbf{P}_n\}.$$

Então $S = \emptyset$. De fato, se $S \neq \emptyset$, então, pelo Princípio da Boa Ordenação, S contém um menor elemento, digamos $b \in S$. Seja $\mathbf{B} \in \mathbb{Z}[i]$ tal que $\mathrm{N}(\mathbf{B}) = b\mathbf{I}$. Então, pela Proposição 3.1, $\mathbf{B} = \mathbf{PC}$, para algum primo Gaussiano $\mathbf{P} \in \mathbb{Z}[i]$. Assim, $1 < c < b$, com $\mathrm{N}(\mathbf{C}) = c\mathbf{I}$. Logo, $c \notin S$ e $\mathbf{C} \in \mathcal{U}(\mathbb{Z}[i])$ ou existem primos Gaussianos $\mathbf{P}_1, \ldots, \mathbf{P}_m \in \mathbb{Z}[i]$ tais que

$$\mathbf{C} = \mathbf{P}_1 \cdots \mathbf{P}_m$$

Portanto, $\mathbf{B}$ é associado a $\mathbf{P}$ ou

$$\mathbf{B} = \mathbf{P}_1\mathbf{P}_1 \cdots \mathbf{P}_m,$$

o que é impossível. ■

Lema 3.1 (Euclides) *Sejam* $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{Z}[i]$. *Se* $\mathbf{A} \mid \mathbf{BC}$ *e* $mdc(\mathbf{A}, \mathbf{B}) = \mathbf{I}$, *então* $\mathbf{A} \mid \mathbf{C}$.

Prova. Temos que existem $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}[i]$ tais que

$$\mathbf{AX} + \mathbf{BY} = \mathbf{I}.$$

Assim,

$$\mathbf{C} = \mathbf{CI} = \mathbf{C}(\mathbf{AX} + \mathbf{BY}) = (\mathbf{AC})\mathbf{X} + (\mathbf{BC})\mathbf{Y}.$$

Como $\mathbf{A} \mid \mathbf{AC}$ e $\mathbf{A} \mid \mathbf{BC}$ temos que $\mathbf{A} \mid \mathbf{C}$. ■

Teorema 3.3 *Sejam* $\mathbf{P}, \mathbf{P}_1, \ldots, \mathbf{P}_n \in \mathbb{Z}[i]$ *primos Gaussianos. Se*

$$\mathbf{P} \mid \mathbf{P}_1 \cdots \mathbf{P}_n,$$

então $\mathbf{P}$ *é associado a* $\mathbf{P}_k$, *para algum* $k \in \{1, \ldots, n\}$.

Prova. Suponhamos que

$$\mathbf{P} \mid \mathbf{P}_1 \cdots \mathbf{P}_n,$$

mas

$$\mathbf{P} \neq \mathbf{U}_k\mathbf{P}_k,\ \text{onde}\ \mathbf{U}_k \in \mathcal{U}(\mathbb{Z}[i])\ \text{e}\ k = 1, \ldots, n-1.$$

Então, é fácil verificar que,

$$\mathrm{mdc}(\mathbf{P}, \mathbf{P}_k) = \mathbf{I},\ \ k = 1, \ldots, n-1.$$

Assim, pelo Lema **??**,

$$\mathrm{mdc}(\mathbf{P}, \mathbf{P}_1 \cdots \mathbf{P}_{n-1}) = \mathbf{I}.$$

Logo, pelo Lema 3.1, $\mathbf{P} \mid \mathbf{P}_n$. Portanto, $\mathbf{P}$ é associado a $\mathbf{P}_n$. ■

Teorema 3.4 (Fatoração Única) *Qualquer* $\mathbf{A} \in \mathbb{Z}[i]$, *com* $N(\mathbf{A}) = a\mathbf{I}$ *e* $a \geq 2$, *pode ser fatorado de modo único como um produto finito de primos Gaussianos, a menos da ordem e unidades.*

Prova. Basta provar a unicidade. Suponhamos que $\mathbf{A} \in \mathbb{Z}[i]$, com $\mathrm{N}(\mathbf{A}) = a\mathbf{I}$ e $a \geq 2$,

$$\mathbf{A} = \mathbf{P}_1 \cdots \mathbf{P}_m \text{ e } \mathbf{A} = \mathbf{Q}_1 \cdots \mathbf{Q}_n.$$

Então

$$\mathbf{P}_1 \cdots \mathbf{P}_m = \mathbf{Q}_1 \cdots \mathbf{Q}_n \text{ e } \mathbf{P}_1 \mid \mathbf{Q}_1 \cdots \mathbf{Q}_n.$$

Note que $m > 1$, pois se $m = 1$, então $\mathbf{A}$ já seria um primo Gaussiano. Assim, pelo Teorema 3.3, $\mathbf{P}_1$ é associado a $\mathbf{Q}_k$, para algum $k \in \{1, \ldots, n\}$. Reindexando, se necessário, de modo que $\mathbf{Q}_1 = \mathbf{U}_1\mathbf{P}_1$, para algum $\mathbf{U}_1 \in \mathcal{U}(\mathbb{Z}[i])$. Logo, pela lei do cancelamento,

$$\mathbf{P}_2 \cdots \mathbf{P}_m = \mathbf{U}_1\mathbf{Q}_2 \cdots \mathbf{Q}_n.$$

Agora, vamos usar indução sobre $\max\{m, n\}$. Se $m > n$, então

$$\mathbf{P}_{n+1} \cdots \mathbf{P}_m = \mathbf{U},$$

o que é impossível. Se $m < n$, então

$$\mathbf{U} = \mathbf{Q}_{m+1} \cdots \mathbf{Q}_n,$$

o que é impossível. Portanto, $m = n$ e

$$\mathbf{P}_2 \cdots \mathbf{P}_n$$

é no máximo uma reordenação de

$$\mathbf{Q}_2 \cdots \mathbf{Q}_n,$$

ou seja, a menos da ordem e unidades. ■

Exemplo: Determine a fatoração de $\mathbf{A} = 20\mathbf{I} \in \mathbb{Z}[i]$. ⋄

Solução. Como $\mathrm{N}(\mathbf{A}) = 400\mathbf{I}$ temos, pelo Teorema 3.1, que os possíveis divisores primos Gaussianos de $\mathbf{A}$ devem ter norma $\mathrm{N}(\mathbf{D}) = 2\mathbf{I}$ ou $\mathrm{N}(\mathbf{D}) = 5\mathbf{I}$. Com alguns cálculos, que veremos na próxima secção, obtemos

$$\mathbf{A} = -(\mathbf{I} + \mathbf{J})^4(\mathbf{I} + 2\mathbf{J})(\mathbf{I} - 2\mathbf{J}),$$

■

3.2 Critérios de Primalidade

Nesta seção veremos que a melhor maneira de identificar os primos Gaussianos é através de comparação com os números primos em $\mathbb{Z}$.

Proposição 3.2 *Seja* $\mathbf{P} \in \mathbb{Z}[i]$ *um primo Gaussiano. Então* $\mathbf{P} \mid p\mathbf{I}$, *para algum número primo* $p \in \mathbb{Z}$.

Prova. Como $\mathrm{N}(\mathbf{P}) = a\mathbf{I}$, onde $a \in \mathbb{Z}$, temos que

$$\mathrm{N}(\mathbf{P}) = (p_1 \cdots p_n)\mathbf{I}$$

é sua fatoração em números primos. Sendo $\mathrm{N}(\mathbf{P}) = \mathbf{P}\mathbf{P}^t$, teremos

$$\mathbf{P} \mid (p_1 \cdots p_n)\mathbf{I}.$$

Assim, por definição, $\mathbf{P} \mid p_k\mathbf{I}$, para algum $k \in \{1, \ldots, n\}$. ■

Lema 3.2 *Sejam* $\mathbf{A} \in \mathbb{Z}[i]$ *e* $p \in \mathbb{Z}$ *um número primo. Se* $N(\mathbf{A}) = p\mathbf{I}$, *então* $\mathbf{A}$ *é um primo Gaussiano.*

Prova. Sejam $\mathbf{B}, \mathbf{C} \in \mathbb{Z}[i]$ tais que $\mathbf{A} = \mathbf{BC}$. Então

$$p\mathbf{I} = \mathrm{N}(\mathbf{A}) = \mathrm{N}(\mathbf{B})\mathrm{N}(\mathbf{C}) \Rightarrow \mathrm{N}(\mathbf{B}) \in \mathcal{U}(\mathbb{Z}[i]) \text{ ou } \mathrm{N}(\mathbf{C}) \in \mathcal{U}(\mathbb{Z}[i]).$$

Então, pela Proposição 2.1, $\mathbf{B} \in \mathcal{U}(\mathbb{Z}[i])$ ou $\mathbf{C} \in \mathcal{U}(\mathbb{Z}[i])$. Portanto, $\mathbf{A}$ é um primo Gaussiano. ■

Observe que a recíproca do Lema 3.1 é falsa, pois como veremos $\mathbf{P} = 3\mathbf{I}$ é um primo Gaussiano, mas $\mathrm{N}(\mathbf{P}) = 9\mathbf{I}$ e 9 não é um número primo em $\mathbb{Z}$.

Proposição 3.3 *Seja* $p \in \mathbb{Z}$ *um número primo. Então as seguintes condições são equivalentes*:

1. $\mathbf{A} = p\mathbf{I}$ *é redutível sobre* $\mathbb{Z}[i]$;
2. $\mathbf{A} = \mathbf{P}\mathbf{P}^t$, *para algum primo Gaussiano* $\mathbf{P} \in \mathbb{Z}[i]$;
3. $\mathbf{A} = (a^2 + b^2)\mathbf{I}$, *ou seja,* $\mathbf{A}$ *é soma de dois quadrados.*

Prova. $(1 \Rightarrow 2)$ Suponhamos que $\mathbf{A}$ seja redutível sobre $\mathbb{Z}[i]$. Então existem $\mathbf{B}, \mathbf{C} \in \mathbb{Z}[i]$ tais que

$$\mathbf{A} = \mathbf{BC}, \text{ com } \mathbf{I} < \mathrm{N}(\mathbf{B}), \mathrm{N}(\mathbf{C}) < \mathrm{N}(\mathbf{A}).$$

Como

$$p^2\mathbf{I} = \mathrm{N}(\mathbf{A}) = \mathrm{N}(\mathbf{B})\mathrm{N}(\mathbf{C})$$

temos que $\mathrm{N}(\mathbf{B}) = p\mathbf{I}$. Assim, pelo Lema 3.2, $\mathbf{B} = \mathbf{P}$ é um primo Gaussiano. Por outro lado,

$$\mathbf{C} = \frac{1}{p}\mathbf{P}^t\mathbf{A} = \mathbf{P}^t.$$

Portanto, $\mathbf{A} = \mathbf{P}\mathbf{P}^t$, para algum primo Gaussiano $\mathbf{P}$.

$(2 \Rightarrow 3)$ Seja

$$\mathbf{P} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{Z}[i]$$

um primo Gaussiano. Então

$$\mathbf{A} = \mathbf{P}\mathbf{P}^t = (a^2 + b^2)\mathbf{I},$$

ou seja, $\mathbf{A}$ é soma de dois quadrados.

$(3 \Rightarrow 1)$ Suponhamos que $\mathbf{A} = (a^2 + b^2)\mathbf{I}$. Então $\mathbf{A} = \mathbf{P}\mathbf{P}^t$, com

$$\mathbf{P} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{Z}[i].$$

Como $\mathrm{N}(\mathbf{P}) = \mathrm{N}(\mathbf{P}^t)$ e

$$p^2\mathbf{I} = \mathrm{N}(\mathbf{A}) = \mathrm{N}(\mathbf{P})\mathrm{N}(\mathbf{P}^t)$$

temos que $\mathrm{N}(\mathbf{P}) = p\mathbf{I}$. Portanto, $\mathbf{A}$ é redutível sobre $\mathbb{Z}[i]$. ■

Teorema 3.5 (Fermat) *Sejam $a, p \in \mathbb{Z}$, com p um número primo. Se $mdc(a, p) = 1$, então*

$$p \mid a^{p-1} - 1 \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}.$$

Conclua que

$$p \mid a^p - a \Leftrightarrow a^p \equiv a \pmod{p}.$$

Prova. Sabendo que o conjunto

$$\mathbb{Z}_p^\bullet = \{1, \ldots, p-1\}$$

munido com as operações

$$a \oplus b \equiv r \pmod{p} \text{ e } a \odot b \equiv r \pmod{p}, \ \forall \ a, b \in \mathbb{Z}_p^\bullet,$$

em que r é o resto da divisão por p, é um corpo. A função $\sigma : \mathbb{Z}_p^\bullet \to \mathbb{Z}_p^\bullet$ definida como

$$\sigma(x) = ax$$

é claramente bijetora. Assim,

$$\mathbb{Z}_p^\bullet = \sigma(\mathbb{Z}_p^\bullet) = \{a, \ldots, a(p-1)\}.$$

Logo,

$$a \cdot 2a \cdots a(p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p},$$

pois $\text{mdc}(k, p) = 1$, com $k = 1, \ldots, p-1$. Portanto,

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

Finalmente, se $p \mid a$, então

$$a \equiv 0 \pmod{p} \Rightarrow a^p \equiv a \pmod{p},$$

que é o resultado desejado. ■

Teorema 3.6 (Wilson) *Seja $p \in \mathbb{Z}$ um número primo. Então*

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

Prova. Consideremos o polinômio

$$f(x) = x^{p-1} - 1 - \prod_{k=1}^{p-1}(x-k) = c_0 + c_1 x + \cdots + c_{p-2}x^{p-2}.$$

Então, pelo Teorema 3.5, a equação

$$f(x) \equiv 0 \pmod{p}$$

possui pelo menos $p-1$ soluções, a saber, $x \in \mathbb{Z}_p^\bullet$. Assim,

$$c_m \equiv 0 \pmod{p}, \;\; m = 0, \ldots, p-2.$$

Como

$$c_0 = -1 - (-1)^{p-1}(p-1)!$$

temos que

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

que é o resultado desejado. ■

Note que o Teorema 3.6 fornece um critério de primalidade: se $n \in \mathbb{Z}$, então n é um número primo se, e somente se,

$$n \mid (n-1)! + 1,$$

ou seja, basta calcular $(n-1)!+1$ e verificar se este número é divisível por n, não obstante, este critério não é eficiente.

É bem conhecido que a equação

$$x^2+1=0$$

não possui solução em $\mathbb{R}$, mas possui soluções em $\mathbb{C}$. Por analogia, ela possui duas soluções em $\mathbb{Z}_5^\bullet$, a saber, 2 e $-2=3$, mas não possui solução em $\mathbb{Z}_7^\bullet$. O próximo resultado caracteriza as soluções desta equação:

Proposição 3.4 (Fermat) *Seja $p \in \mathbb{Z}$ um número primo. Então as seguintes condições são equivalentes*:

1. *p é soma de dois quadrados*;
2. *$p=2$ ou $p \equiv 1 \pmod 4$*;
3. *A equação $x^2+1 \equiv 0 \pmod p$ possui solução.*

Prova. $(1 \Rightarrow 2)$ Suponhamos que p seja soma de dois quadrados e que $p>2$, digamos $p=a^2+b^2$. Então a e b possuem paridade diferentes. Assim,

$$p=a^2+b^2=(2m)^2+(2n+1)^2 \Rightarrow p \equiv 1 \pmod 4.$$

$(2 \Rightarrow 3)$ Se $p=2$, então nada há para ser provado. Suponhamos que $p=4m+1$, para algum $m \in \mathbb{N}$. Se x e y são soluções desta equação, então

$$x^2 \equiv y^2 \pmod p \Rightarrow y \equiv x \pmod p \text{ ou } y \equiv -x \pmod p.$$

Como $k \equiv -(p-k) \pmod p$, com $k=1,\ldots,p-1$, temos, pelo Teorema 3.6, que

$$\begin{aligned}(p-1)!+1 &= (p-1)\cdots(p-2m)(2m)(2m-1)\cdots 2\cdot 1+1\\ &\equiv (2m)^2(2m-1)^2\cdots 2^2\cdot 1^2+1 \equiv 0 \pmod p.\end{aligned}$$

Portanto, $x=(2m)(2m-1)\cdots 2\cdot 1$ é uma solução da equação.

$(3 \Rightarrow 1)$ Suponhamos que equação $x^2+1 \equiv 0 \pmod p$ possua uma solução, digamos $a \in \mathbb{Z}$. Então

$$a^2+1 \equiv 0 \pmod p \Leftrightarrow p\mathbf{I} \mid (a^2+1)\mathbf{I}.$$

Assim,

$$p\mathbf{I} \mid (a\mathbf{I}+\mathbf{J})(a\mathbf{I}-\mathbf{J}).$$

Note que

$$p\mathbf{I} \nmid (a\mathbf{I}+\mathbf{J}) \text{ e } p\mathbf{I} \nmid (a\mathbf{I}-\mathbf{J}).$$

De fato, se

$$p\mathbf{I} \mid (a\mathbf{I} + \mathbf{J}),$$

então existe

$$\mathbf{A} = \begin{pmatrix} b & -c \\ c & b \end{pmatrix} \in \mathbb{Z}[i]$$

tal que

$$a\mathbf{I} + \mathbf{J} = p\mathbf{A} \Rightarrow pc = 1,$$

o que é impossível. Logo, $p\mathbf{I}$ é redutível. Portanto, pela Proposição 3.3, p é soma de dois quadrados. ■

Note que se $p \in \mathbb{Z}$, com $p > 2$, é um número primo, então é fácil verificar que

$$p \equiv 1 \pmod 4 \text{ ou } p \equiv 3 \pmod 4.$$

Com base nisto vamos apresentar os critérios de primalidade em $\mathbb{Z}[i]$.

Teorema 3.7 *Seja*

$$\mathbf{P} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{Z}[i], \ \forall \ a, b \in \mathbb{Z}^*.$$

Então $\mathbf{P}$ *é um primo Gaussiano se, e somente se,* $N(\mathbf{P}) = p\mathbf{I}$*, para algum número primo* $p \in \mathbb{Z}$*.*

Prova. (1) Suponhamos que $\mathbf{P}$ seja um primo Gaussiano. Então

$$\mathbf{P}\mathbf{P}^t = \mathrm{N}(\mathbf{P}) = (a^2 + b^2)\mathbf{I}.$$

Se $a^2 + b^2$ não fosse um número primo, então existiriam $m, n \in \mathbb{Z}$ tais que

$$a^2 + b^2 = mn, \text{ com } 1 < m, n < a^2 + b^2.$$

Além disso, podemos supor que $\mathrm{mdc}(\mathbf{P}, \mathbf{P}^t) = \mathbf{I}$. Caso contrário, $\mathbf{P}$ e $\mathbf{P}^t$ seriam associados, o qual implica que $a = \pm b = \pm 1$ e $a^2 + b^2 = 2$. Assim, a prova acabou. Como $\mathbf{P}$ é um primo Gaussiano e $\mathbf{P} \mid mn\mathbf{I}$ temos que $\mathbf{P} \mid m\mathbf{I}$ ou $\mathbf{P} \mid n\mathbf{I}$. Logo, existe $\mathbf{A} \in \mathbb{Z}[i]$ tal que $m\mathbf{I} = \mathbf{A}\mathbf{P}$. Isto implica que $m\mathbf{I} = \mathbf{A}^t\mathbf{P}^t$, de modo que $\mathbf{P}^t \mid m\mathbf{I}$. Neste caso, $\mathbf{P}\mathbf{P}^t \mid m\mathbf{I}$, pois $\mathrm{mdc}(\mathbf{P}, \mathbf{P}^t) = \mathbf{I}$ e $m = a^2 + b^2 = 1$, $n = 1$, o que é uma contradição. Portanto, $\mathrm{N}(\mathbf{P}) = p\mathbf{I}$, para algum número primo $p \in \mathbb{Z}$.

A recíproca segue do Lema 3.2. ■

Teorema 3.8 *Seja* $\mathbf{P} \in \mathbb{Z}[i]$*. Então* $\mathbf{P}$ *é um primo Gaussiano se, e somente se,* $\mathbf{P} = p\mathbf{I}$*, para algum número primo* $p \in \mathbb{Z}$ *da forma* $p = 4n + 3$*.*

Prova. Suponhamos que $\mathbf{P}$ seja um primo Gaussiano. Então, pela Proposição 3.2, $\mathbf{P} \mid p\mathbf{I}$, para algum número primo $p \in \mathbb{Z}$. Assim, pela Proposição 3.3, $\mathbf{P}$ não é a soma de dois quadrados. Portanto, pela Proposição 3.4, $\mathbf{P} = p\mathbf{I}$, para algum número primo $p \in \mathbb{Z}$ da forma $p = 4n + 3$.

Reciprocamente, suponhamos que

$$p\mathbf{I} = \mathbf{AB}.$$

Então

$$p^2\mathbf{I} = \mathrm{N}(p\mathbf{I}) = \mathrm{N}(\mathbf{A})\mathrm{N}(\mathbf{B}).$$

Se $\mathrm{N}(\mathbf{A}) = \mathbf{I}$ ou $\mathrm{N}(\mathbf{B}) = \mathbf{I}$, então $\mathbf{A} \in \mathcal{U}(\mathbb{Z}[i])$ ou $\mathbf{B} \in \mathcal{U}(\mathbb{Z}[i])$ e $p\mathbf{I}$ é um primo Gaussiano. Caso contrário,

$$p\mathbf{I} = \mathrm{N}(\mathbf{A}) \text{ e } p\mathbf{I} = \mathrm{N}(\mathbf{B}).$$

Seja

$$\mathbf{A} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{Z}[i].$$

Então

$$a^2 + b^2 = p \text{ ou } a^2 + b^2 \equiv 3 \pmod 4.$$

Como

$$a^2 \equiv 0, 1 \pmod 4, \ \forall \ a \in \mathbb{Z},$$

temos que

$$a^2 + b^2 \equiv 0, 1, 2 \pmod 4,$$

o que é impossível. Portanto, $p\mathbf{I}$ é um primo Gaussiano. ■

Podemos concluir que os primos Gaussianos são aqueles das seguintes três classes e seus associados:

1. $\mathbf{I} + \mathbf{J}$;
2. Os fatores primos Gaussianos dos números primos da forma $4n+1$, para algum $n \in \mathbb{N}$;
3. Os primos Gaussianos associados aos números primos da forma $(4n + 3)$, para algum $n \in \mathbb{N}$.

Exemplo: Determine a fatoração de $\mathbf{A} = 30\mathbf{I} \in \mathbb{Z}[i]$. ⋄
Solução. Como $\mathrm{N}(\mathbf{A}) = 900\mathbf{I}$ temos, pelo Teorema 3.1, que os possíveis divisores primos Gaussianos de $\mathbf{A}$ devem ter norma $\mathrm{N}(\mathbf{D}) = 2\mathbf{I}$, $\mathrm{N}(\mathbf{D}) = 3\mathbf{I}$ ou $\mathrm{N}(\mathbf{D}) = 5\mathbf{I}$. Neste caso,

$$\mathbf{A} = 2\mathbf{I}3\mathbf{I}5\mathbf{I} = \mathbf{J}(\mathbf{I} + \mathbf{J})^2 3\mathbf{I}(\mathbf{I} + 2\mathbf{J})(\mathbf{I} - 2\mathbf{J}),$$

pois

$$5 \equiv 1 \pmod 4 \Rightarrow 5\mathbf{I} = (\mathbf{I}+2\mathbf{J})(\mathbf{I}-2\mathbf{J})$$

e $3 \equiv 3 \pmod 4$. ■

Lema 3.3 *Para cada $n \in \mathbb{Z}_+$, o conjunto de números primos da forma $4n+3$ é infinito.*

Prova. Suponhamos, por absurdo, que exista um número finito de primos da forma $4n+3$, digamos

$$3, 7, 11, \ldots, p_m.$$

Seja $a = 4(3 \cdot 7 \cdot 11 \cdots p_m) + 3$. Como todo número primo ímpar é da forma $4r+1$ ou $4r+3$ e

$$(4r+1)(4r+1) = 4(4r^2+2r)+1 = 4s+1$$

temos que existe um número primo p da forma $4n+3$ tal que p divide a. É fácil verificar que $p \neq 3, 7, 11$ e p_i, o que é uma contradição. ■

Corolário 3.1 *O conjunto de primos Gaussianos é infinito.*

Prova. Consequência direta do Teorema 3.8 e do Lema 3.3. ■

Vamos usar os resultados apresentados neste capítulo para obter um algoritmo de fatoração para um inteiro Gaussiano qualquer.

Seja $\mathbf{A} \in \mathbb{Z}[i]$, com $\mathrm{N}(\mathbf{A}) = n\mathbf{I}$, para algum $n \in \mathbb{N}$. Então qualquer fator primo Gaussiano de $\mathbf{A}$ é claramente um fator de $n\mathbf{I} = \mathbf{A}\mathbf{A}^t$. Assim, os fatores primos Gaussianos de $n\mathbf{I}$ podem ser obtidos dos fatores primos de n. De fato, seja

$$n = 2^r p_1^{r_1} \cdots p_k^{r_k} q_1^{s_1} \cdots q_m^{s_m}$$

a fatoração de n, em que os p's são números primos da forma $4u+1$ e os q's são números primos da forma $4u+3$. Seja

$$\mathbf{P}_j = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \ \ j = 1, \ldots, k,$$

o fator primo Gaussiano associado ao número primo p_j. Então

$$\mathbf{P}_j \mathbf{P}_j^t = p_j \mathbf{I} \text{ ou } a^2 + b^2 = p_j, \ \ j = 1, \ldots, k,$$

e

$$n\mathbf{I} = (-\mathbf{J})^r (\mathbf{I}+\mathbf{J})^{2r} \mathbf{P}_1^{r_1} (\mathbf{P}_1^t)^{r_1} \cdots \mathbf{P}_k^{r_k} (\mathbf{P}_k^t)^{r_k} \mathbf{Q}_1^{s_1} \cdots \mathbf{Q}_m^{s_m}.$$

Como $n\mathbf{I} = \mathbf{A}\mathbf{A}^t$ temos que

$$\mathbf{A} = \mathbf{J}^t (\mathbf{I}+\mathbf{J})^u \mathbf{P}_1^{u_1} (\mathbf{P}_1^t)^{u_1'} \cdots \mathbf{P}_k^{u_k} (\mathbf{P}_k^t)^{u_k'} \mathbf{Q}_1^{v_1} \cdots \mathbf{Q}_m^{v_m},$$

onde $t \in \{0,1,2,3\}$ e $u, u_j, u_j', v_j \in \mathbb{Z}_+$. Assim,

$$\mathrm{N}(\mathbf{A}) = 2^u p_1^{u_1+u_1'} \cdots p_k^{u_k+u_k'} q_1^{2v_1} \cdots q_m^{2v_m}\mathbf{I}.$$

Sendo $\mathrm{N}(\mathbf{A}) = n\mathbf{I}$, teremos

$$\begin{aligned} u &= r \\ u_i + u_i' &= r_i, \ \ i = 1, \ldots, k, \\ 2v_j &= s_j, \ \ j = 1, \ldots, m. \end{aligned}$$

Logo, os inteiros

$$u = r, \ \ v_1 = \frac{1}{2}s_1, \ldots, v_m = \frac{1}{2}s_m$$

são unicamente determinados. Além disso, os fatores primos da forma $4w+3$ possuem expoentes pares na fatoração de n.

Vamos determinar os expoentes u_i e u_i', $i = 1, \ldots, k$. Seja

$$k_i = \max\{m \in \mathbb{Z}_+ : p_i^m\mathbf{I} \mid \mathbf{A}\},$$

ou seja,

$$k_i = \max\{m \in \mathbb{Z}_+ : p_i^m \mid c \ \text{ e } \ p_i^m \mid d\}, \ \text{ onde } \ \mathbf{A} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathbb{Z}[i].$$

Então

$$p_i^{k_i}\mathbf{P}_i \mid \mathbf{A} \Rightarrow \begin{cases} u_i &= r_i - k_i \\ u_i' &= k_i \end{cases}$$

ou

$$p_i^{k_i}\mathbf{P}_i \nmid \mathbf{A} \Rightarrow \begin{cases} u_i &= k_i \\ u_i' &= r_i - k_i \end{cases}$$

Com efeito, se

$$\mathbf{B} = (p_i^{k_i}\mathbf{I})^{-1}\mathbf{A},$$

então

$$\mathbf{P}_i \nmid \mathbf{B} \ \text{ ou } \ \mathbf{P}_i^t \nmid \mathbf{B}.$$

Caso contrário,

$$\mathbf{P}_i\mathbf{P}_i^t \mid \mathbf{B}, \ \text{ pois } \ \mathrm{mdc}(\mathbf{P}_i, \mathbf{P}_i^t) = \mathbf{I}.$$

Assim,

$$p_i^{k_i+1}\mathbf{I} \mid \mathbf{A},$$

o que contradiz a maximalidade de k_i. Se

$$\mathbf{P}_i \mid \mathbf{B},$$

então

$$\mathbf{P}_i^t \nmid \mathbf{B}.$$

Neste caso, $p_i^{k_i}\mathbf{I} = \mathbf{P}_i^{k_i}(\mathbf{P}_i^t)^{k_i}$ e

$$p_i^{k_i}\mathbf{P}_i \mid \mathbf{A} \Rightarrow \left\{ \begin{array}{rcl} u_i & = & r_i - k_i \\ u_i^{,} & = & k_i. \end{array} \right.$$

O outro caso é análogo.

Finalmente, o expoente t segue da divisão de $\mathbf{A}$ pelo produto dos primos Gaussianos cujos expoentes já foram determinados.

Exemplo: Determine a fatoração de

$$\mathbf{A} = \begin{pmatrix} 22 & -7 \\ 7 & 22 \end{pmatrix} \in \mathbb{Z}[i].$$

◇

Solução. Como $\mathrm{N}(\mathbf{A}) = 533\mathbf{I} = (13 \cdot 41)\mathbf{I}$ temos que $p_1 = 13 = 2^2 + 3^2$ e $p_2 = 41 = 4^2 + 5^2$ são os fatores primos de 533. Neste caso,

$$\mathbf{A} = \mathbf{J}^t\mathbf{P}_1^{u_1}(\mathbf{P}_1^t)^{u_1^{,}}\mathbf{P}_2^{u_2}(\mathbf{P}_2^t)^{u_2^{,}},$$

em que

$$\mathbf{P}_1 = \begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix} \text{ e } \mathbf{P}_2 = \begin{pmatrix} 4 & -5 \\ 5 & 4 \end{pmatrix}.$$

É fácil verificar que $k_1 = k_2 = 0$, por exemplo,

$$13\mathbf{I} \nmid \mathbf{A}.$$

Note que

$$\mathbf{P}_1^{-1}\mathbf{A} = \frac{1}{13}\begin{pmatrix} 2 & 3 \\ -3 & 2 \end{pmatrix}\begin{pmatrix} 22 & -7 \\ 7 & 22 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ -4 & 5 \end{pmatrix} \in \mathbb{Z}[i].$$

Assim, $u_1 = r_1 - k_1 = 1 - 0 = 1$ e $u_1^{,} = k_1 = 0$. De modo análogo,

$$\mathbf{P}_2^{-1}\mathbf{A} = \frac{1}{41}\begin{pmatrix} 4 & 5 \\ -5 & 4 \end{pmatrix}\begin{pmatrix} 22 & -7 \\ 7 & 22 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -2 & 3 \end{pmatrix} \in \mathbb{Z}[i]$$

e $u_2 = r_2 - k_2 = 1 - 0 = 1$ e $u_2^{,} = k_2 = 0$.

Finalmente,

$$\mathbf{P}_2^{-1}\mathbf{P}_1^{-1}\mathbf{A} = \frac{1}{41}\begin{pmatrix} 4 & 5 \\ -5 & 4 \end{pmatrix}\begin{pmatrix} 5 & 4 \\ -4 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{Z}[i]$$

e $t = 3$. Portanto,

$$\mathbf{A} = \mathbf{J}^3\mathbf{P}_1\mathbf{P}_2.$$

Observe que esta fatoração não é única, por exemplo,

$$\mathbf{A} = \mathbf{P}_1\mathbf{P}_3, \text{ onde } \mathbf{P}_3 = \begin{pmatrix} 5 & 4 \\ -4 & 5 \end{pmatrix} \in \mathbb{Z}[i],$$

é outra fatoração. ■

Referências Bibliográficas

[1] Almeida, C. V. A., *Números Primos Gaussianos para o Ensino Médio*, (Trabalho de Coclusão de Curso-PROFMAT-2014/UFPB)8

[2] Boldrini, J. L. [et al], *Álgebra Linear*, (Editora HARBRA Ltda, UNICAMP, São Paulo, 1980).

[3] Boyer, C. B., *História da Matemática*, (Editora Blücher Ltda., Editora da USP, São Paulo, 1974).

[4] Conrad, K. The Gaussian Integers.

[5] Eves, H. Introdução à História da Matemática, Campinas, São Paulo: Editora da UNICAMP. (2004)

[6] Hefez, A. *Elementos da Aritmética*, (Textos Universitários, Segunda Edição, São Paulo: SBM. 2006)

[7] Hoffman, K. e Kunze, R., *Álgebra Linear*, (Editora Polígono, São Paulo, 1971).

[8] LeVeque, W. J. *Elementary Theory of Numbers*, (Editora Dover Publications, Inc., New York, 1990).

[9] Lipschutz, S., *Álgebra Linear*, (Editora McGraw-Hill do Brasil Ltda, Rio de Janeiro, 1971).

[10] Silva, A. de A. e, *Álgebra Linear*, (Editora Universitária/UFPB, 2007).

[11] Soares, Marcio G., *Cálculo de uma variável complexa*, (Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2001).