Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 7, n. 1, 2020.

Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Os Inteiros de Gauss

Lídia Charra Alves[1]
Universidade Federal do Espírito Santo
Eleonesio Strey[2]
Universidade Federal do Espírito Santo

1 Introdução

Os *inteiros de Gauss* ou *inteiros Gaussianos* são os números complexos da forma $a + bi$, com a e b inteiros e $i = \sqrt{-1}$. O conjunto formado por todos os inteiros de Gauss é denotado por $\mathbb{Z}[i]$ e este, munido das operações de soma e produto usuais, é um anel comutativo com unidade, o qual é conhecido como *anel dos inteiros de Gauss*. Este anel vêm sendo utilizado em algumas aplicações, por exemplo, na teoria de códigos (ver [1] e suas referências). Na próxima seção, apresentamos alguns conceitos e resultados de aritmética em $\mathbb{Z}[i]$. Para elaborar este resumo utilizamos as referências [2] e [3].

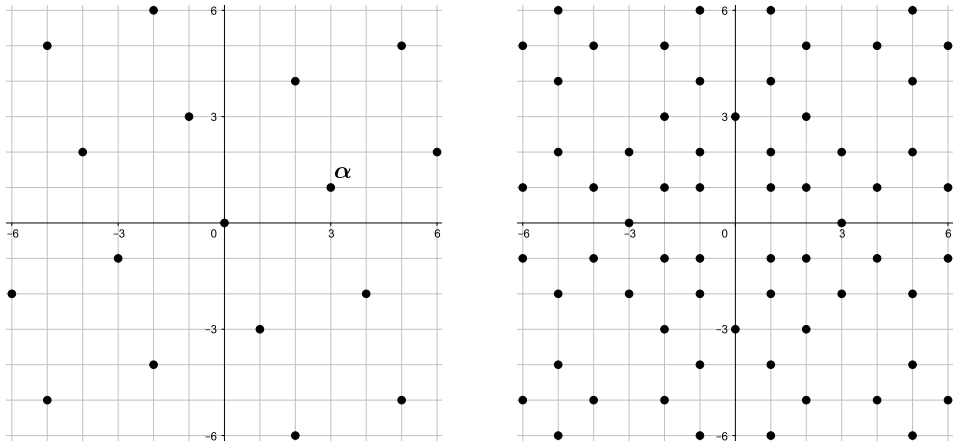
2 Inteiros de Gauss

A *norma* de um inteiro gaussiano α é definida como $N(\alpha) = \alpha\bar{\alpha}$, no qual $\bar{\alpha}$ representa o conjugado de α. Para quaisquer $\alpha, \beta \in \mathbb{Z}[i]$, tem-se $N(\alpha\beta) = N(\alpha)N(\beta)$, isto é, a norma é multiplicativa. Os inteiros de Gauss que possuem inverso multiplicativo são ± 1 e $\pm i$. Dados $\alpha, \beta \in \mathbb{Z}[i]$, dizemos que α é um *múltiplo* de β (ou β é um *divisor* de α) em $\mathbb{Z}[i]$ se, e somente se, $\alpha = \gamma\beta$, para algum $\gamma \in \mathbb{Z}[i]$. Os múltiplos de $\alpha = 3 + i$ estão ilustrados na Figura 1(a). (Divisão Euclidiana) Para quaisquer $\alpha, \beta \in \mathbb{Z}[i]$, com $\alpha \neq 0$, existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que $\beta = \gamma\alpha + \rho$ e $N(\rho) \leq (1/2)N(\alpha)$. Por exemplo, se $\alpha = 3 + i$ e $\beta = -2 + 2i$, podemos escrever $\beta = \gamma_1\alpha + \rho_1$ e $\beta = \gamma_2\alpha + \rho_2$, com $\gamma_1 = i$, $\rho_1 = \beta - \gamma_1\alpha = (-2+2i) - i(3+i) = -1-i$, $\gamma_2 = -1+i$ e $\rho_2 = \beta - \gamma_2\alpha = (-2+2i) - (-1+i)(3+i) = 2$. Note que $N(\rho_1) \leq (1/2)N(\alpha)$ e $N(\rho_2) \leq (1/2)N(\alpha)$, já que $N(\rho_1) = 2$, $N(\rho_2) = 4$ e $N(\alpha) = 10$. Ou seja, ao contrário do que ocorre no conjunto dos números inteiros, na descrição acima o quociente γ e resto ρ não são univocamente determinados.

Um inteiro de Gauss α, com norma maior do que 1 (note que essa condição exclui apenas o elemento neutro e os quatro elementos inversíveis), que possui apenas os fatores triviais $\pm\alpha$ e $\pm i\alpha$ é chamado de *primo Gaussiano*. Por exemplo, 5 não é um primo Gaussiano, pois $5 = (1 + 2i)(1 - 2i)$ (ou seja, $1 + 2i$ e $1 - 2i$ são fatores não triviais de 5).

[1]lidia.charra.alves@gmail.com
[2]eleonesio.strey@ufes.br

Dados dois inteiros a e b quaisquer, pode-se mostrar que: (i) Se a e b são ambos não nulos, $a + bi$ é um primo Gaussiano se, e somente se, $a^2 + b^2$ é um primo em $\mathbb{Z}$; (ii) a é primo em $\mathbb{Z}[i]$ se, e somente se, a é primo em $\mathbb{Z}$ e $|a| \equiv 3 \mod 4$; (iii) bi é primo em $\mathbb{Z}[i]$ se, e somente se, b é primo em $\mathbb{Z}$ e $|b| \equiv 3 \mod 4$. Estes três resultados transferem o problema de verificar se um inteiro de Gauss é um primo Gaussiano para um problema envolvendo apenas números inteiros. Na Figura 1(b) representamos todos os primos Gaussianos $a+bi$, em que $-6 \leq a \leq 6$ e $-6 \leq b \leq 6$.



(a) Múltiplos de $\alpha = 3 + i$ (b) Primos Gaussianos

Figura 1: Múltiplos de α e primos Gaussianos no retângulo $[-6, 6] \times [-6, 6]$.

O anel $\mathbb{Z}[i]$ é um domínio de fatoração única, isto é, todo inteiro de Gauss com norma maior do que 1 pode ser expresso como produto de primos Gaussianos e essa decomposição é única (a menos da ordem e de elementos inversíveis).

Agradecimentos

Os autores agradecem o apoio financeiro da FAPES.

Referências

[1] S. Bouyuklieva. Applications of the Gaussian Integers in Coding Theory. *Proc. of the Inter. Colloquium on Differential Geometry and its Related Fields*, Veliko Tarnovo, p. 3-7. September, 2012.

[2] K. Conrad. The Gaussian Integers. Disponível em: `http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf`. Acesso em: 28 de março de 2019.

[3] G. Fujiwara. Inteiros de Gauss e Inteiros de Eisenstein. *Eureka*, 14:23–31, 2002.