Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Inteiros de Eisenstein e Aplicações

Renan da Paixão Moura[1]
Universidade Federal do Espírito Santo
Edinaldo Junior Teles de Oliveira[2]
Universidade Federal do Espírito Santo
Eleonesio Strey[3]
Universidade Federal do Espírito Santo

Um *inteiro de Eisenstein* é um número complexo da forma $a + b\omega$, em que a e b são números inteiros e $\omega = (-1 + i\sqrt{3})/2$. O número complexo ω é uma raiz cúbica primitiva da unidade, isto é, $\omega^2 + \omega + 1 = 0$, já que $x^3 - 1 = (x - 1)(x^2 + x + 1)$. A outra raiz cúbica primitiva da unidade é $\omega^2 = -1 - \omega = \overline{\omega}$, onde $\overline{\omega}$ é o conjugado de ω. O conjunto formado por todos os inteiros de *Eisenstein* munido das operações usuais de adição e multiplicação de números complexos é um anel comutativo com unidade, o qual é denotado por $\mathbb{Z}[\omega]$. Em outras palavras, $\mathbb{Z}[\omega]$ consiste de todas as combinações lineares inteiras de 1 e ω. Uma representação dos inteiros de *Eisenstein* no plano cartesiano é apresentada na Figura 1.

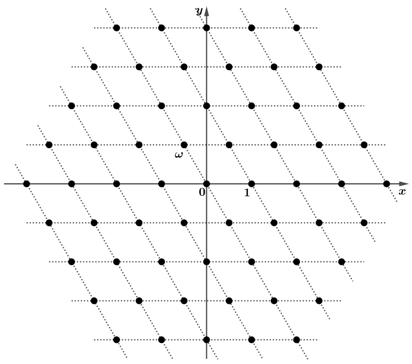

Figura 1: Inteiros de *Eisenstein*

Definimos a *norma* de $a+b\omega$ como $N(a+b\omega) = (a+b\omega)(\overline{a+b\omega}) = a^2 - ab + b^2$. Para quaisquer $z_1, z_2 \in \mathbb{Z}[\omega]$, tem-se $N(z_1 z_2) = N(z_1)N(z_2)$, isto é, a norma é multiplicativa. Os inteiros de *Eisenstein* $\pm 1, \pm\omega$ e $\pm\omega^2$ são os únicos elementos em $\mathbb{Z}[\omega]$ que possuem inverso multiplicativo e são chamados de *unidades* de $\mathbb{Z}[\omega]$. Dados $z_1, z_2 \in \mathbb{Z}[\omega]$, dizemos que z_2 *divide* z_1 em $\mathbb{Z}[\omega]$ (e escrevemos $z_2 | z_1$) se, e somente se, $z_1 = z_3 z_2$ para algum $z_3 \in \mathbb{Z}[\omega]$. Se z_3 é uma unidade, dizemos que z_1 e z_2 são *associados*. Um inteiro de *Eisenstein* z_1, com norma maior do que 1, que possui

[1]rpmoura7@gmail.com
[2]edinaldo_thellys@hotmail.com
[3]eleonesio.strey@ufes.br

apenas os fatores triviais (isto é, fatores com norma igual a 1 ou $N(z_1)$) é chamado *primo de Eisenstein*. Por exemplo, $1+2\omega$, 5 e -11ω são primos de *Eisenstein*. Por outro lado, 3 não é um primo de *Eisenstein*, uma vez que $3 = (1-\omega)(2+\omega)$, ou seja, $1-\omega$ e $2+\omega$ são fatores não triviais de 3 em $\mathbb{Z}[\omega]$. Mais precisamente, seja p um primo positivo, os primos de *Eisenstein* são os inteiros de *Eisenstein* que são associados de um dos seguintes elementos: (i) $1-\omega$; (ii) p, com $p \equiv 2 \mod 3$; (iii) π ou $\bar{\pi}$, onde $N(\pi) = p$ e $p \equiv 1 \mod 3$. Todo inteiro de *Eisenstein*, com norma maior do que 1, pode ser escrito, a menos da ordem e de elementos associados, de forma única como produto de primos de *Eisenstein* (Teorema da Fatoração Única).

Alguns problemas que envolvem números inteiros podem ter suas soluções abordadas a partir da perspectiva dos inteiros de *Eisenstein*. Isto decorre principalmente do fato da norma ser um número inteiro, o que nos permite usar as propriedades dos inteiros de *Eisenstein* como ferramentas para estudar tais problemas. Finalizaremos este resumo apresentando duas destas aplicações.

Exemplo 1. *O número de soluções da equação diofantina* $x^2 - xy + y^2 = n$ *é divisível por* 6.

Solução. Se a equação $x^2 - xy + y^2 = n$ não admite solução, o resultado é trivial. Suponha, então, que ela admite solução. Temos que (x, y) é uma solução da equação se, e somente se, o inteiro de *Eisenstein* $x + y\omega$ possui norma igual a n. Ou seja, existe uma correspondência biunívoca entre o conjunto solução da equação e o conjunto dos inteiros de *Eisenstein* de norma igual n. Por outro lado, o número de elementos deste último conjunto é divisível por 6, pois todo inteiro de *Eisenstein* de norma igual a n divide n em $\mathbb{Z}[\omega]$, n possui um número finito de divisores em $\mathbb{Z}[\omega]$ e cada inteiro de *Eisenstein* de norma n possui outros 5 elementos associados de norma n. Portanto o número de soluções da equação diofantina $x^2 - xy + y^2 = n$ é divisível por 6. ☐

Exemplo 2. *Determine todas as soluções da equação diofantina de* $x^2 - xy + y^2 = 19$.

Solução. Devemos determinar todos os inteiros de *Eisenstein* $x + y\omega$ de norma igual a 19, uma vez que $N(x+y\omega) = x^2 - xy + y^2$. Se $x + y\omega$ tem norma igual a 19, então $(x+y\omega)(\overline{x+y\omega}) = 19$. Como 19 é um primo e $19 \equiv 1 \mod 3$, segue que $x+y\omega$ e $\overline{x+y\omega}$ são primos de *Eisenstein*. Em particular, $5+2\omega$ e $\overline{5+2\omega}$ são primos de *Eisenstein*, pois $N(5+2\omega) = (5+2\omega)(\overline{5+2\omega}) = 19$. Logo, pelo Teorema da Fatoração Única, os inteiros de *Eisenstein* $x + y\omega$ de norma igual a 19 são exatamente os associados de $5+2\omega$ ou $\overline{5+2\omega}$, isto é, $5+2\omega, 3-2\omega, -5-2\omega, -2+3\omega, 2-3\omega, -3-5\omega, 3+5\omega, -3+2\omega, 2+5\omega, -2-5\omega, -5-3\omega$ e $5+3\omega$. Portanto as soluções da equação diofantina $x^2 - xy + y^2 = 19$ são $(5,2), (3,-2), (-5,-2), (-2,3), (2,-3), (-3,-5), (3,5), (-3,2), (2,5), (-2,-5), (-5,-3)$ e $(5,3)$. ☐

Para elaborar este resumo utilizamos as referências [1], [2] e [3].

Agradecimentos

Os autores agradecem o apoio financeiro do Instituto Tim e do CNPq [114341/2020-6].

Referências

[1] Bandara, S. An Exposition of the Eisenstein Integers, Masters Theses, Eastern Illinois University, 2016.

[2] Brito, F. C. A. Resolução de problema via inteiros algébricos, Dissertação de Mestrado, Universidade Federal do Ceará, Fortaleza, 2017.

[3] Lisboa, D. L. Números Inteiros de Eisenstein. Dissertação de Mestrado, Universidade Federal da Paraíba, João Pessoa, 2017