PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1030

Inteiros de Eisenstein

Renan da Paixão Moura[1] Edinaldo Junior Teles de Oliveira Eleonesio Strey

Resumo

Desde os trabalhos de Gauss, vários pesquisadores têm se interessado pelo estudo de anéis que possuam uma aritmética similar à dos inteiros. Dentre eles, destaca-se o anel dos inteiros gaussianos, que é composto pelos números complexos cujas partes real e imaginária são inteiras. Outro exemplo de grande importância neste contexto é o anel dos inteiros de Eisenstein, o qual é o objeto de estudo deste artigo. Neste trabalho, são apresentados os inteiros de Eisenstein, enfocando suas propriedades algébricas, além de fornecer interpretações geométricas de alguns resultados.

Palavras-chave: Inteiros de Eisenstein; Teorema da Divisão em $\mathbb{Z}[\omega]$; Teorema de Bézout em $\mathbb{Z}[\omega]$; Fatoração Única em $\mathbb{Z}[\omega]$.

Abstract

Since the works of Gauss, several researchers have been interested in the study of rings that have an arithmetic similar to that of integers. Among them, the ring of Gaussian integers stands out, which is composed of complex numbers that have a real part and an integer imaginary part. Another example of great importance in this context is the Eisenstein ring of integers, which is the object of study of this article. In this work, Eisenstein's integers will be presented, focusing on their algebraic properties, in addition to providing geometric interpretations of some results.

Keywords: Eisenstein Integers; Division Theorem in $\mathbb{Z}[\omega]$; Bezout's Theorem in $\mathbb{Z}[\omega]$; Unique Factorization in $\mathbb{Z}[\omega]$.

1. Introdução

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 símbolos,

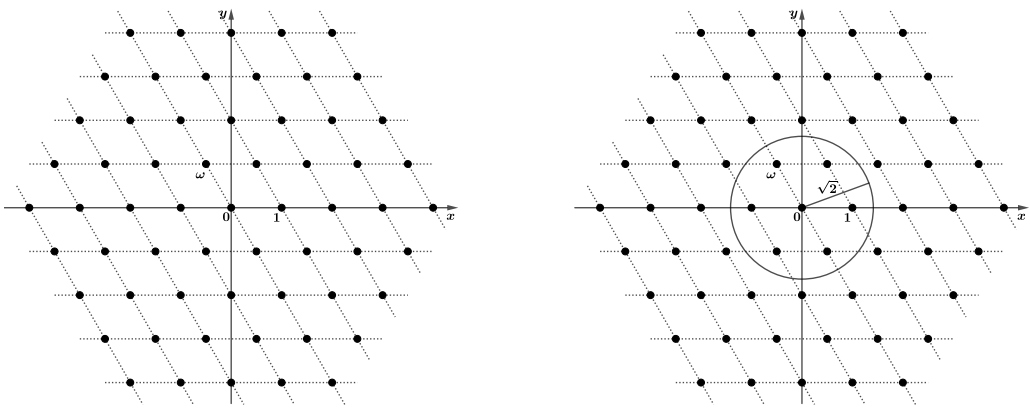
$$\mathbb{Z}[\omega] = \{a + b\omega;\ a, b \in \mathbb{Z}\}.$$

De maneira alternativa, podemos descrever $\mathbb{Z}[\omega]$ como sendo o conjunto formado por todas as combinações lineares inteiras de 1 e ω. Um número complexo $x + iy$, onde x e y são números

[1]Parcialmente apoiado pelo Instituto Tim e pelo CNPq [119064/2021-9].

reais, é representado geometricamente pelo par ordenado (x, y) no plano complexo. Em particular, um inteiro de Eisenstein da forma $a + b\omega$, em que a e b são números inteiros, é representado por $(\mathrm{Re}(a + b\omega), \mathrm{Im}(a + b\omega))$, isto é, $(a - b/2, b\sqrt{3}/2)$. Uma representação dos inteiros de Eisenstein no plano complexo é apresentada na Figura 1(a). Dois inteiros de Eisenstein $a + b\omega$ e $c + d\omega$ são ditos *iguais* se, e somente se, $a = c$ e $b = d$. Essa última definição coincide com o conceito de igualdade de números complexos.

Definição 1. Definimos a *norma* em $\mathbb{Z}[\omega]$ como a função $N : \mathbb{Z}[\omega] \to \mathbb{Z}_+$ que associa a cada inteiro de Eisenstein $\alpha = a + b\omega$, o valor inteiro não negativo $N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = a^2 - ab + b^2$.



(a) Inteiros de Eisenstein. (b) Não existem inteiros de Eisenstein de norma 2.

Figura 1: Representação dos Inteiros de Eisenstein no Plano Complexo.

Observação 1. Seja n um inteiro positivo. Um inteiro de Eisenstein α tem norma igual a n se, e somente se, $(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))$ pertence à circunferência centrada na origem de raio $\sqrt{n}$. A norma de um inteiro de Eisenstein é um inteiro não negativo, mas nem todo inteiro não negativo é norma de algum inteiro de Eisenstein, isto é, a função norma não é sobrejetora. Por exemplo, não existem inteiros de Eisenstein de norma igual a 2, conforme ilustrado na Figura 1(b).

Teorema 1. *A função norma é multiplicativa, isto é,* $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$, $\forall \alpha, \beta \in \mathbb{Z}[\omega]$.

Demonstração. Para quaisquer $\alpha, \beta \in \mathbb{Z}[\omega]$, tem-se

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

Logo, a função norma é multiplicativa. Isso conclui a demonstração. □

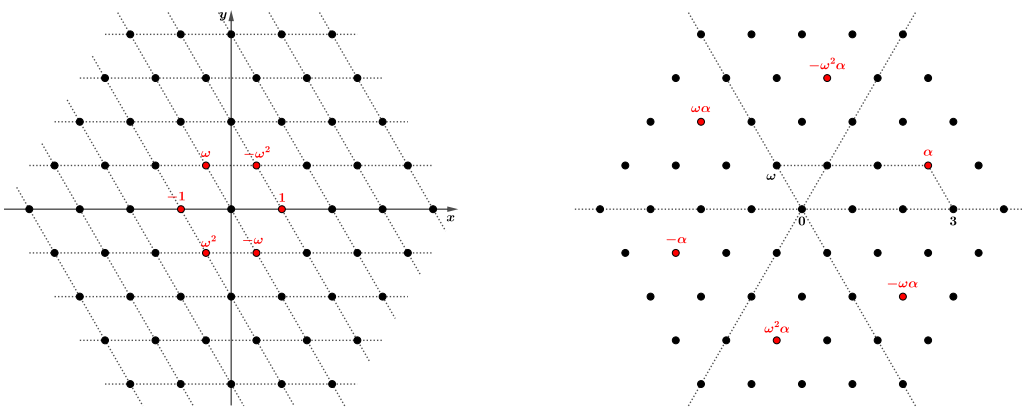
Definição 2. Um inteiro de Eisenstein α é dito *invertível* em $\mathbb{Z}[\omega]$, se existir um elemento $\beta \in \mathbb{Z}[\omega]$ tal que $\alpha \cdot \beta = 1$. Os elementos invertíveis em $\mathbb{Z}[\omega]$ também são chamados de *unidades* de $\mathbb{Z}[\omega]$, ou simplesmente de *unidades*, se estiver subentendido que estamos nos referindo às unidades de $\mathbb{Z}[\omega]$. Denotaremos por $U(\mathbb{Z}[\omega])$ o conjunto das unidades de $\mathbb{Z}[\omega]$.

Teorema 2. *Os únicos inteiros de Eisenstein que são invertíveis em* $\mathbb{Z}[\omega]$ *são* $\pm 1, \pm\omega$ *e* $\pm\omega^2$. *Isto é, o conjunto das unidades de* $\mathbb{Z}[\omega]$ *é* $\mathrm{U}(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$.

Demonstração. É fácil ver que $\pm 1, \pm\omega$ e $\pm\omega^2$ são invertíveis em $\mathbb{Z}[\omega]$. Reciprocamente, se $u = a+b\omega$ é um elemento invertível em $\mathbb{Z}[\omega]$. Então existe $v \in \mathbb{Z}[\omega]$ tal que $u \cdot v = 1$. Aplicando a norma em ambos os lados dessa última igualdade e usando a multiplicidade da norma, obtemos $N(u)\cdot N(v) = 1$. Como $N(u)$ e $N(v)$ são inteiros não negativos, segue que $N(u) = N(v) = 1$. Assim, $a^2 - ab + b^2 = 1$, uma vez que $u = a + b\omega$. Considerando $a^2 - ab + (b^2 - 1) = 0$ como uma equação de segundo grau com incógnita "a", vemos que esta equação só tem solução real quando $b^2 - 4(b^2 - 1) \geq 0$, isto é, se $-2/\sqrt{3} \leq b \leq 2/\sqrt{3}$. Como b é um número inteiro, os possíveis valores para b são $-1, 0$ e 1. Vamos analisar cada um dos casos. Quando $b = -1$, teremos $a^2 + a = 0$; desse modo, $a = 0$ ou $a = -1$, e, assim, $u = -\omega$ ou $u = -1 - \omega = \omega^2$. Se $b = 0$, teremos $a^2 - 1 = 0$, o que implica $a = 1$ ou $a = -1$; desse modo $u = 1$ ou $u = -1$. Por último, se $b = 1$, teremos $a^2 - a = 0$, e assim $a = 0$ ou $a = 1$; logo, $u = \omega$ ou $u = 1 + \omega = -\omega^2$. Portanto $\mathrm{U}(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$. □

Definição 3. Dois inteiros de Eisenstein α e β são ditos *associados* se $\beta = \mu \cdot \alpha$ para algum $\mu \in \mathrm{U}(\mathbb{Z}[\omega])$ (isto é, se $\beta = \pm\alpha$, $\beta = \pm\omega\alpha$ ou $\beta = \pm\omega^2\alpha$).

Exemplo 1. As unidades de $\mathbb{Z}[\omega]$ estão ilustradas na Figura 2(a). Os associados de $\alpha = 3 + \omega$ são os inteiros de Eisenstein $\alpha = 3 + \omega$, $-\alpha = -3 - \omega$, $\omega\alpha = -1 + 2\omega$, $-\omega\alpha = 1 - 2\omega$, $\omega^2\alpha = -2 - 3\omega$ e $-\omega^2\alpha = 2 + 3\omega$, os quais estão ilustrados na Figura 2(b).



(a) Unidades de $\mathbb{Z}[\omega]$ (b) Associados de $\alpha = 3 + \omega$

Figura 2: Unidades de $\mathbb{Z}[\omega]$ e associados de $\alpha = 3 + \omega$.

Corolário 1. *Sejam* α *e* β *são inteiros de Eisenstein. Temos que:*

(i) α *é invertível se, e somente se,* $N(\alpha) = 1$.

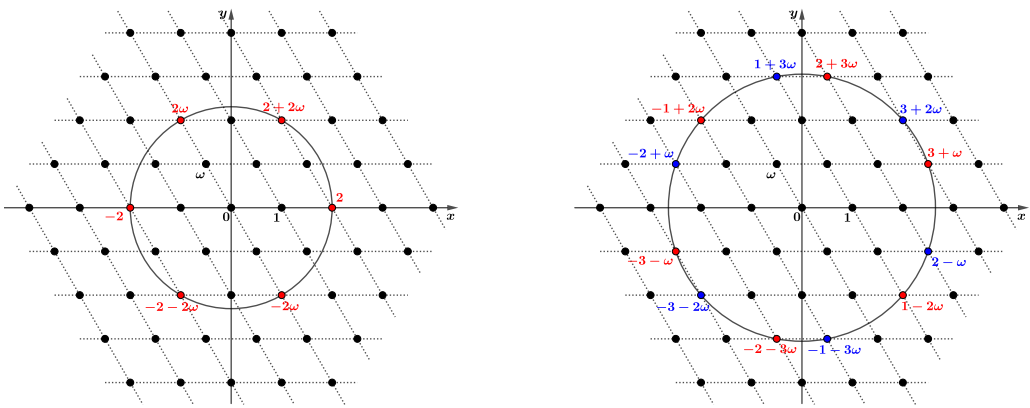
(ii) Se α *e* β *são associados, então* $N(\alpha) = N(\beta)$.

Demonstração. Consequência imediata do Teorema 2. □

Observação 2. Um inteiro de Eisenstein α não nulo possui exatamente seis associados, a saber $\pm\alpha, \pm\omega\alpha$ e $\pm\omega^2\alpha$. Por outro lado, o Corolário 1 garante que elementos associados possuem a mesma norma. Logo, para cada inteiro positivo n, o número de inteiros de Eisenstein de norma igual a n é múltiplo de 6.

Observação 3. A recíproca do Item *(ii)* do Corolário 1 não é verdadeira, uma vez que $3+\omega$ e $3+2\omega$ possuem a mesma norma, mas não são associados (Exemplo 2).

Exemplo 2. Os inteiros de Eisenstein de norma igual a 4 e norma igual a 7 estão ilustrados nas Figuras 3(a) e 3(b), respectivamente. Os elementos de norma igual a 4 são os associados de 2 e os de norma igual a 7 são os associados de $3+\omega$ (destacados em vermelho) e $3+2\omega$ (destacados em azul).



(a) Norma igual a 4

(b) Norma igual a 7

Figura 3: Inteiros de Eisenstein de norma igual a 4 e igual a 7.

Definição 4. Sejam α e β inteiros de Eisenstein. Dizemos que β *divide* α (ou β é um *divisor* de α, ou ainda, α é um *múltiplo* de β), e escrevemos $\beta \mid \alpha$, se existir um elemento $\gamma \in \mathbb{Z}[\omega]$ tal que $\alpha = \gamma \cdot \beta$. Caso contrário, dizemos que β *não divide* α (ou β *não é um divisor* de α, ou ainda, α *não é um múltiplo* de β) e escrevemos $\beta \nmid \alpha$.

Exemplo 3. Para verificar se $2-\omega$ divide $4+6\omega$, basta verificar se existe um inteiro de Eisenstein $a+b\omega$ tal que $4+6\omega = (2-\omega)(a+b\omega)$, ou seja, $4+6\omega = (2a+b)+(-a+3b)\omega$. Como não existem inteiros a e b que satisfazem simultaneamente $2a+b=4$ e $-a+3b=6$, segue que $(2-\omega) \nmid (4+6\omega)$.

Observação 4. Os múltiplos de um inteiro de Eisenstein β são os elementos da forma $(m+n\omega)\cdot\beta$, com $m, n \in \mathbb{Z}$. Como $(m+n\omega)\cdot\beta = m\beta + n(\omega\beta)$, segue que os múltiplos de β são as combinações lineares inteiras de β e $\omega\beta$.

Exemplo 4. Os múltiplos de $\beta = 3+\omega$ estão destacados em vermelho na Figura 4. Eles são as combinações lineares inteiras de $3+\omega$ e $\omega\beta = \omega(3+\omega) = 3\omega+\omega^2 = 3\omega+(-1-\omega) = -1+2\omega$.

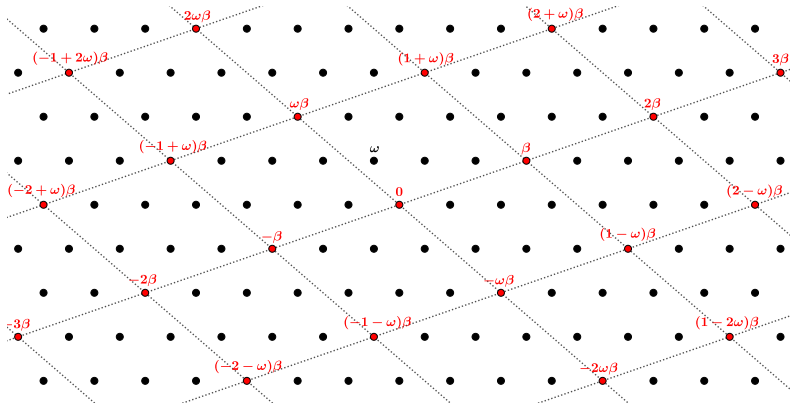


Figura 4: Múltiplos de $\beta = 3 + \omega$.

Teorema 3. *Um inteiro de Eisenstein* $a + b\omega$ *é divisível por um inteiro* c *se, e somente se,* $c \mid a$ *e* $c \mid b$ *em* $\mathbb{Z}$.

Demonstração. Sejam a, b e c inteiros tais que $a + b\omega$ é divisível por c. Assim, existem inteiros m e n de modo que $a + b\omega = c(m + n\omega) = cm + (cn)\omega$. Logo, $a = cm$ e $b = cn$, isto é, $c \mid a$ e $c \mid b$. Reciprocamente, se $c \mid a$ e $c \mid b$ em $\mathbb{Z}$, então existem inteiros m e n tais que $a = cm$ e $b = cn$. Assim $a + b\omega = cm + cn\omega = c(m + n\omega)$ e, consequentemente, $c \mid (a + b\omega)$. □

Teorema 4. *Se* $\alpha \mid \beta$ *em* $\mathbb{Z}[\omega]$*, então* $N(\alpha) \mid N(\beta)$ *em* $\mathbb{Z}$.

Demonstração. Sejam $\alpha, \beta \in \mathbb{Z}[\omega]$ tais que $\alpha \mid \beta$. Assim, existe um elemento $\gamma \in \mathbb{Z}[\omega]$ tal que $\beta = \alpha\gamma$. Aplicando a norma em ambos os lados dessa última igualdade e usando o fato de que a norma é multiplicativa, obtemos $N(\beta) = N(\alpha\gamma) = N(\alpha)N(\gamma)$. Portanto $N(\alpha) \mid N(\beta)$ em $\mathbb{Z}$. □

Exemplo 5. Como $N(-2-3\omega) = (-2)^2 - (-2)\cdot(-3) + (-3)^2 = 7$, $N(10-3\omega) = 10^2 - 10\cdot(-3) + (-3)^2 = 139$ e $7 \nmid 139$ em $\mathbb{Z}$, o Teorema 4 garante que $(-2-3\omega) \nmid (10-3\omega)$ em $\mathbb{Z}[\omega]$.

Observação 5. A recíproca do Teorema 4 não é verdadeira, ou seja, existem inteiros de Eisenstein α e β tais que $N(\alpha) \mid N(\beta)$ e $\alpha \nmid \beta$. Por exemplo, $N(2-\omega) = 7$ divide $N(4+6\omega) = 28$, porém $(2-\omega) \nmid (4+6\omega)$, como visto no Exemplo 3.

Teorema 5. *Se* α *e* β *são inteiros de Eisenstein tais que* α *é não nulo,* β *é um divisor de* α *e* $N(\beta) = N(\alpha)$*, então* α *e* β *são associados.*

Demonstração. Como $\beta \mid \alpha$, segue que existe um elemento $\gamma \in \mathbb{Z}[\omega]$ tal que $\alpha = \beta\gamma$. Aplicando a norma em ambos os lados dessa última igualdade e usando a multiplicidade da norma, obtemos $N(\alpha) = N(\beta)N(\gamma)$. Assim, $N(\alpha) = N(\alpha)N(\gamma)$, pois $N(\beta) = N(\alpha)$. Como $\alpha \neq 0$, segue que $N(\gamma) = 1$, isto é, γ é uma unidade. Portanto α e β são associados. □

Teorema 6. *Sejam* α *e* β *inteiros de Eisenstein não nulos. Se* $\alpha \mid \beta$ *e* $\beta \mid \alpha$*, então* α *e* β *são associados.*

Demonstração. Como $\alpha \mid \beta$ e $\beta \mid \alpha$, segue que existem $\gamma_1, \gamma_2 \in \mathbb{Z}[\omega]$ tais que $\beta = \gamma_1\alpha$ e $\alpha = \gamma_2\beta$. A partir disso, obtemos $\alpha = \gamma_2\beta = \gamma_2(\gamma_1\alpha)$ e, consequentemente, $1 = \gamma_2\gamma_1$ (pois $\alpha \neq 0$). Aplicando a norma em ambos os lados dessa última igualdade e usando a multiplicidade da norma, obtemos $1 = \mathrm{N}(\gamma_2)\mathrm{N}(\gamma_1)$, o que implica que $\mathrm{N}(\gamma_1) = \mathrm{N}(\gamma_2) = 1$, isto é, γ_1 e γ_2 são unidades. Portanto, α e β são associados. □

2. Teorema da Divisão

Nesta seção apresentaremos o Teorema da Divisão para inteiros de Eisenstein.

Teorema 7 (Teorema da Divisão)**.** *Para $\alpha, \beta \in \mathbb{Z}[\omega]$, com $\beta \neq 0$, existem $\gamma, \rho \in \mathbb{Z}[\omega]$ tais que $\alpha = \gamma\beta + \rho$ e $\mathrm{N}(\rho) < \mathrm{N}(\beta)$.*

Demonstração. Sejam α e β inteiros de Eisenstein com $\beta \neq 0$. Se $\beta \mid \alpha$, então existe um elemento $\gamma \in \mathbb{Z}[\omega]$ tal que $\alpha = \gamma\beta + 0$. Observe que $\mathrm{N}(0) \leq \mathrm{N}(\beta)$, logo obtemos o resultado desejado. Por outro lado, se $\beta \nmid \alpha$, então existem $\mathrm{x}, \mathrm{y} \in \mathbb{Q}$ tais que $\alpha/\beta = \mathrm{x} + \mathrm{y}\omega$. Agora, escolhemos inteiros m e n tais que

$$|\mathrm{x} - \mathrm{m}| \leq \frac{1}{2} \quad \text{e} \quad |\mathrm{y} - \mathrm{n}| \leq \frac{1}{2}, \tag{1}$$

e definimos $\gamma = \mathrm{m} + \mathrm{n}\omega$ e $\rho = \alpha - \beta\gamma = \beta(\alpha/\beta - \gamma)$. Como para todo número complexo da forma $\mathrm{z} = \mathrm{c} + \mathrm{d}\omega$ tem-se $|\mathrm{z}|^2 = |\mathrm{c} + \mathrm{d}\omega|^2 = \mathrm{c}^2 - \mathrm{cd} + \mathrm{d}^2$, segue que

$$\begin{aligned}\left|\frac{\alpha}{\beta} - \gamma\right|^2 &= |(\mathrm{x} + \mathrm{y}\omega) - (\mathrm{m} + \mathrm{n}\omega)|^2 \\ &= |(\mathrm{x} - \mathrm{m}) + (\mathrm{y} - \mathrm{n})\omega|^2 \\ &= (\mathrm{x} - \mathrm{m})^2 - (\mathrm{x} - \mathrm{m})(\mathrm{y} - \mathrm{n}) + (\mathrm{y} - \mathrm{n})^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}.\end{aligned}$$

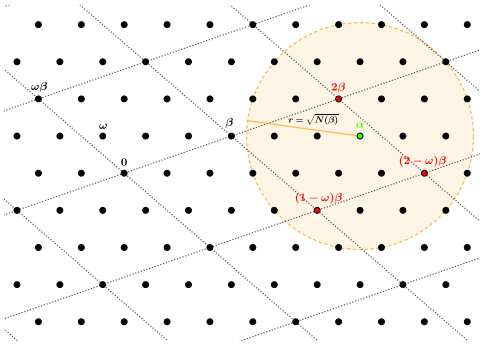
Como $\rho = \beta(\alpha/\beta - \gamma)$ e $\beta \neq 0$, segue que $\mathrm{N}(\rho) = |\rho|^2 = |\beta|^2 \cdot \left|\alpha/\beta - \gamma\right|^2 \leq 3/4 \cdot |\beta|^2 < |\beta|^2 = \mathrm{N}(\beta)$. Portanto existem $\gamma, \rho \in \mathbb{Z}[\omega]$ tais que $\alpha = \gamma\beta + \rho$ e $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. □

Observação 6. Dois inteiros m e n satisfazem as desigualdades descritas em (1) se, e somente se, não existem inteiros mais próximos de x e y do que m e n, respectivamente.

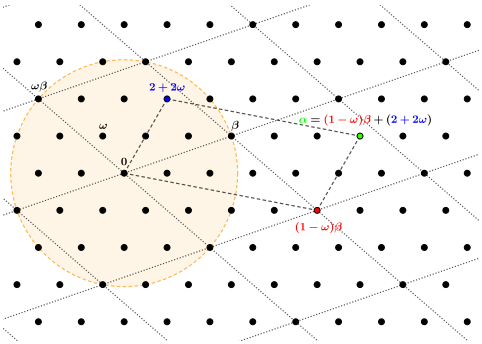
Exemplo 6. Sejam $\alpha = 6+\omega$ e $\beta = 3+\omega$. Dizer que um inteiro de Einsentein ρ satisfaz $\mathrm{N}(\rho) < \mathrm{N}(\beta)$ significa que ρ, representado no plano complexo pelo par ordenado $(\mathrm{Re}(\rho), \mathrm{Im}(\rho))$, pertence ao interior do círculo centrado na origem de raio $\sqrt{\mathrm{N}(\beta)}$. Por outro lado, na Figura 5(a) observamos que existem exatamente três múltiplos de β que estão a uma distância de α estritamente menor do que $\sqrt{\mathrm{N}(\beta)}$, a saber, $(1-\omega)\beta$, $(2-\omega)\beta$ e 2β. Isso nos permite concluir que existem exatamente três maneiras de escrever $\alpha = \gamma\beta+\rho$ com $\mathrm{N}(\rho) < \mathrm{N}(\beta)$, a saber, $\alpha = (1-\omega)\beta+(2+2\omega)$, $\alpha = (2-\omega)\beta+(-1+\omega)$ e $\alpha = 2\beta + (-\omega)$, as quais estão ilustradas nas Figuras 5(b), 5(c) e 5(d), respectivamente. Todas as afirmações feitas neste exemplo podem ser comprovadas algebricamente.

Observação 7. O Exemplo 6 ilustra o fato de que, ao contrário do que ocorre com a divisão nos inteiros, os elementos γ e ρ do Teorema 7 não são únicos.

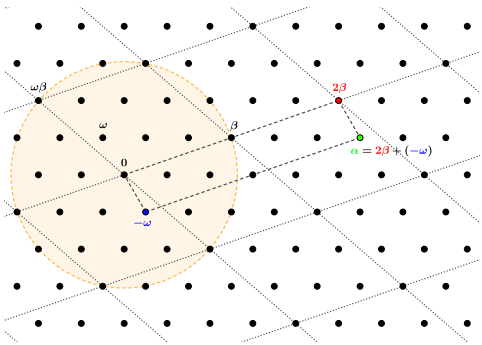
Dados inteiros de Eisenstein α e β, com $\beta \neq 0$, o Teorema 7 garante a existência de inteiros de Eisenstein γ e ρ tais que $\alpha = \gamma\beta + \rho$ e $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. No enunciado do teorema não há informação



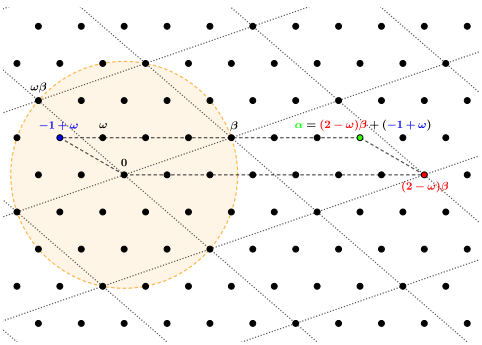
(a) Múltiplos de β próximos de α.



(b) $\alpha = (1-\omega)\beta + (2+2\omega)$



(c) $\alpha = 2\beta + (-\omega)$



(d) $\alpha = (2-\omega)\beta + (-1+\omega)$

Figura 5: Divisão de α por β.

de como encontrá-los, mas a demonstração do teorema fornece implicitamente um método para determinar, ao menos, um par (γ, ρ) que satisfaz as condições do teorema. Esse método será ilustrado no exemplo a seguir.

Exemplo 7. Considere novamente os inteiros de Eisenstein $\alpha = 6+\omega$ e $\beta = 3+\omega$ do Exemplo 6. Como $\overline{\beta} = \overline{3+\omega} = 3+\overline{\omega} = 3+(-1-\omega) = 2-\omega$ e $\mathrm{N}(\beta) = 7$, segue que

$$\frac{\alpha}{\beta} = \frac{\alpha\cdot\bar{\beta}}{\beta\cdot\bar{\beta}} = \frac{(6+\omega)(2-\omega)}{\mathrm{N}(\beta)} = \frac{13-3\omega}{7} = \frac{13}{7} - \frac{3}{7}\omega.$$

Agora, observe que os inteiros $\mathrm{m} = 2$ e $\mathrm{n} = 0$ satisfazem as condições

$$\left|\frac{13}{7} - \mathrm{m}\right| \leq \frac{1}{2} \quad \text{e} \quad \left|-\frac{3}{7} - \mathrm{n}\right| \leq \frac{1}{2},$$

pois 2 e 0 são os inteiros mais próximos de 13/7 e –3/7, respectivamente. Logo, pela demonstração do Teorema 7, $\gamma = 2+0\cdot\omega$ e $\rho = \alpha - \beta\mathrm{q} = (6+\omega) - (3+\omega)(2+0\cdot\omega) = -\omega$ satisfazem as condições

desejadas, ou seja, $\alpha = 2\beta + (-\omega)$ e $N(-\omega) < N(\beta)$. No Exemplo 6 vimos que existem exatamente três maneiras de dividir α por β, e a solução encontrada aqui é obviamente uma delas (Ver Figura 5(c)).

Exemplo 8. Sejam $\alpha = 5 + 6\omega$ e $\beta = 2\omega$. Como $N(\beta) = 4$ e $\overline{\beta} = -2 - 2\omega$, segue que

$$\frac{\alpha}{\beta} = \frac{\alpha \cdot \bar{\beta}}{\beta \cdot \bar{\beta}} = \frac{(5+6\omega)(-2-2\omega)}{N(\beta)} = \frac{2-10\omega}{4} = \frac{1}{2} - \frac{5}{2}\omega. \tag{2}$$

Existem exatamente dois inteiros que satisfazem a desigualdade $|1/2 - m| \leq 1/2$, a saber, $m = 0$ e $m = 1$, e dois inteiros que satisfazem $|-5/2 - n| \leq 1/2$, a saber, $n = -3$ e $n = -2$. Ou seja, seguindo os passos da demonstração do Teorema 7, obtemos quatro pares de inteiros de Eisenstein (γ, ρ) satisfazendo $\alpha = \gamma\beta + \rho$ e $N(\rho) < N(\beta)$ que são $(-2\omega, 1+2\omega)$, $(-3\omega, -1)$, $(1-2\omega, 1)$ e $(1-3\omega, -1-2\omega)$. Em outras palavras, o método descrito implicitamente na demonstração do teorema, nesse caso, fornece quatro formas distintas de dividir α por β, a saber,

$$\alpha = (-2\omega)\beta + (1+2\omega) = (-3\omega)\beta - 1 = (1-2\omega)\beta + 1 = (1-3\omega)\beta + (-1-2\omega).$$

Por outro lado, os únicos múltiplos de β que pertencem ao interior do círculo centrado em α e raio $r = \sqrt{N(\beta)}$ são $-2\omega\beta$, $-3\omega\beta$, $(1-2\omega)\beta$ e $(1-3\omega)\beta$ (Figura 6). Logo, as únicas formas de dividir α por β são as quatro apresentadas acima.

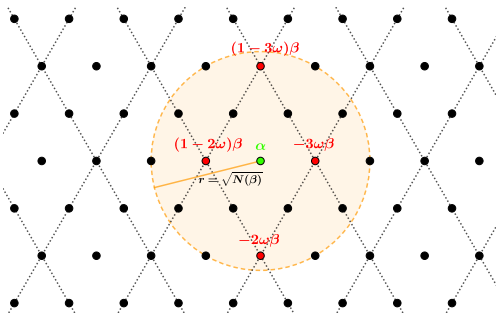


Figura 6: Múltiplos de β próximos de α

3. Algoritmo de Euclides

Iniciaremos introduzindo o conceito de máximo divisor comum.

Definição 5. Sejam $\alpha, \beta \in \mathbb{Z}[\omega]$ tais que $\alpha \neq 0$ ou $\beta \neq 0$. Um divisor comum de α e β de norma máxima é chamado *máximo divisor comum de* α *e* β.

Observação 8. Se δ é um máximo divisor comum de α e β, então (pelo menos) seus múltiplos unitários $\pm\delta$, $\pm\omega\delta$ e $\pm\omega^2\delta$ também são máximos divisores comuns de α e β. Apesar do conceito de máximo divisor comum em $\mathbb{Z}[\omega]$ ser análogo ao conceito de máximo divisor comum em $\mathbb{Z}$ (Tal fato será demonstrado na próxima seção - Corolário 3), aqui não temos um elemento específico que seja chamado de "o máximo divisor comum de α e β".

Teorema 8 (Algoritmo de Euclides)**.** *Sejam $\alpha, \beta \in \mathbb{Z}[\omega]$ com $\alpha \neq 0$ e $\beta \neq 0$. Se o Teorema da Divisão for aplicado sucessivamente para se obter*

$$\begin{aligned} \alpha &= \gamma_1\beta + \rho_1 && \mathrm{N}(\rho_1) < \mathrm{N}(\beta) \\ \beta &= \gamma_2\rho_1 + \rho_2 && \mathrm{N}(\rho_2) < \mathrm{N}(\rho_1) \\ \rho_1 &= \gamma_3\rho_2 + \rho_3 && \mathrm{N}(\rho_3) < \mathrm{N}(\rho_2) \\ &\vdots \\ \rho_{n-2} &= \gamma_n\rho_{n-1} + \rho_n && \mathrm{N}(\rho_n) < \mathrm{N}(\rho_{n-1}) \\ \rho_{n-1} &= \gamma_{n+1}\rho_n + 0, \end{aligned}$$

então ρ_n (isto é, o último resto não nulo) é um máximo divisor comum de α e β.

Demonstração. Essa prova pode ser feita de forma análoga à demonstração do Algoritmo de Euclides para números inteiros. Para mais detalhes, confira a referência [6]. □

Observação 9. A partir das igualdades do Teorema 8 é possível concluir que qualquer divisor comum de α e β também divide ρ_n.

Exemplo 9. Sejam $\alpha = 8 - 3\omega$ e $\beta = 4 + \omega$. Como

$$\begin{aligned} 8 - 3\omega &= (2 - 2\omega)(4 + \omega) + (-2 + \omega) && \mathrm{N}(-2 + \omega) < \mathrm{N}(4 + \omega) \\ 4 + \omega &= (-2 - \omega)(-2 + \omega) + (-1) && \mathrm{N}(-1) < \mathrm{N}(-2 + \omega) \\ -2 + \omega &= (2 - \omega)(-1) + 0, \end{aligned}$$

o Algoritmo de Euclides garante que -1 é um máximo divisor comum de α e β.

Teorema 9. *Sejam α e β inteiros de Eisenstein não nulos e δ é um máximo divisor comum de α e β obtido via Algoritmo de Euclides. Se δ' é um máximo divisor comum de α e β, então δ e δ' são associados.*

Demonstração. Sejam α e β inteiros de Eisenstein não nulos, δ um máximo divisor comum de α e β obtido via Algoritmo de Euclides e δ' um máximo divisor comum de α e β. Da Observação 9, segue que $\delta' \mid \delta$, uma vez que δ' é um divisor comum de α e β. Assim, existe $\gamma \in \mathbb{Z}[\omega]$ não nulo tal que $\delta = \delta' \cdot \gamma$, pois $\delta \neq 0$. Como a norma é multiplicativa e $\gamma \neq 0$, segue que $\mathrm{N}(\delta) = \mathrm{N}(\delta') \cdot \mathrm{N}(\gamma) \geq \mathrm{N}(\delta')$. Por outro lado, temos $\mathrm{N}(\delta) = \mathrm{N}(\delta')$, pois um máximo divisor comum de α e β é um divisor comum de norma máxima. Portanto $\mathrm{N}(\gamma) = 1$ e consequentemente δ e δ' são associados. □

Corolário 2. *Sejam α e β inteiros de Eisenstein não nulos. Se δ_1 e δ_2 são máximos divisores comuns de α e β, então δ_1 e δ_2 são associados.*

Demonstração. Sejam α e β inteiros de Eisenstein não nulos, δ_1 e δ_2 máximos divisores comuns de α e β e δ um máximo divisor comum de α e β obtido via Algoritmo de Euclides. O Teorema 9 garante que existem $\mu_1, \mu_2 \in \mathrm{U}(\mathbb{Z}[\omega])$ tais que $\delta = \mu_1\delta_1$ e $\delta_2 = \mu_2\delta$. Donde segue que $\delta_2 = \mu_2\mu_1\delta_1$. Mas, $\mathrm{N}(\mu_2\mu_1) = \mathrm{N}(\mu_2)\mathrm{N}(\mu_1) = 1 \cdot 1 = 1$. Logo, δ_1 e δ_2 são associados. □

Observação 10. O Corolário 2 e a Observação 8 garantem que se δ é um máximo divisor comum de α e β obtido via Algoritmo de Euclides, então os máximos divisores comuns α e β são $\pm\delta, \pm\omega\delta$ e $\pm\omega^2\delta$. Em particular, os máximos divisores comuns α e β podem ser obtidos a partir de um máximo divisor comum fornecido pelo algoritmo de Euclides.

Definição 6. Dizemos que α e β *são primos entre si* ou *relativamente primos* quando os inteiros de Eisenstein α e β tem uma unidade como um máximo divisor comum.

Observação 11. Dois inteiros de Eisenstein α e β são relativamente primos se, e somente se, seus máximos divisores comuns são $\pm 1, \pm\omega$ e $\pm\omega^2$.

Exemplo 10. No Exemplo 9 vimos que -1 é um máximo divisor comum de $8-3\omega$ e $4+\omega$. Como -1 é uma unidade de $\mathbb{Z}[\omega]$, segue que $8-3\omega$ e $4+\omega$ são relativamente primos. Os máximos divisores comuns de $8-3\omega$ e $4+\omega$ são $\pm 1, \pm\omega$ e $\pm\omega^2$.

4. Teorema de Bézout

Nesta seção apresentaremos o Teorema de Bézout e alguns de seus corolários.

Teorema 10 (Teorema de Bézout)**.** *Sejam α e β inteiros de Eisenstein, não ambos nulos, e seja δ um máximo divisor comum de α e β. Então, existem $\sigma, \lambda \in \mathbb{Z}[\omega]$ tais que $\alpha\sigma + \beta\lambda = \delta$.*

Demonstração. Sejam $A = \{\alpha\sigma + \beta\lambda;\ \sigma, \lambda \in \mathbb{Z}[\omega]\}$ e $B = \{N(\gamma);\ \gamma \in A \text{ e } \gamma \neq 0\}$. Sejam n_0 o menor elemento de B (a existência desse elemento é garantida pelo Princípio da Boa Ordenação [4], uma vez que $B \neq \emptyset$ e $B \subset \mathbb{Z}_+$) e $\gamma_0 \in A$ tais que $\gamma_0 \neq 0$ e $n_0 = N(\gamma_0)$. Provaremos que $\gamma_0 \mid \alpha$ e $\gamma_0 \mid \beta$ (isto é, γ_0 é um divisor comum de α e β). Se $\gamma_0 \nmid \alpha$, então existem $q, r \in \mathbb{Z}[\omega]$ tais que $\alpha = \gamma_0 q + r$, $r \neq 0$ e $N(r) < N(\gamma_0)$. Como $\gamma_0 \in A$, existem $\sigma_0, \lambda_0 \in \mathbb{Z}[\omega]$ tais que $\gamma_0 = \alpha\sigma_0 + \beta\lambda_0$. Então,

$$r = \alpha - \gamma_0 q = \alpha - (\alpha\sigma_0 + \beta\lambda_0)q = \alpha - \alpha\sigma_0 q - \beta\lambda_0 q = \alpha(1 - \sigma_0 q) + \beta(-\lambda_0 q).$$

Assim, $r \in A$ (Absurdo!). Isto contradiz a minimalidade de γ_0. Logo, $\gamma_0 \mid \alpha$. Analogamente, podemos mostrar que $\gamma_0 \mid \beta$. Portanto γ_0 é um divisor comum de α e β. Agora, mostraremos que γ_0 é um divisor comum de norma máxima. De fato, seja γ um divisor comum de α e β. Assim, existem $\upsilon_1, \upsilon_2 \in \mathbb{Z}[\omega]$ tais que $\alpha = \gamma\upsilon_1$ e $\beta = \gamma\upsilon_2$ e, consequentemente,

$$\gamma_0 = \alpha\sigma_0 + \beta\lambda_0 = (\gamma\upsilon_1)\sigma_0 + (\gamma\upsilon_2)\lambda_0 = \gamma(\upsilon_1\sigma_0 + \upsilon_2\lambda_0).$$

Isso mostra que $\gamma \mid \gamma_0$ e, pelo Teorema 4, $N(\gamma) \mid N(\gamma_0)$ em $\mathbb{Z}$. Como $N(\gamma_0) \geq 1$, pois $\gamma_0 \neq 0$, segue que $N(\gamma) \leq N(\gamma_0)$. Logo, γ_0 é um máximo divisor comum de α e β. Para concluir a demonstração, basta aplicar o Corolário 2 e usar o fato de que $\gamma_0 \in A$. □

O próximo resultado mostra que o conceito de máximo divisor comum em $\mathbb{Z}[\omega]$ é análogo ao de máximo divisor comum nos inteiros.

Corolário 3. *Sejam α e β inteiros de Eisenstein tais que $\alpha \neq 0$ ou $\beta \neq 0$. Temos que δ é um máximo divisor comum de α e β se, e somente se, as seguintes condições são verificadas:*

(i) O elemento δ é um divisor comum de α e β.

(ii) Se γ é um divisor comum de α e β, então γ é um divisor de δ.

Demonstração. Sejam α e β inteiros de Eisenstein, não ambos nulos, e δ é um máximo divisor comum de α e β. Evidentemente, por definição, δ é um divisor comum de α e β. Agora, se γ é um divisor comum de α e β, existem $\upsilon_1, \upsilon_2 \in \mathbb{Z}[\omega]$ tais que $\alpha = \gamma\upsilon_1$ e $\beta = \gamma\upsilon_2$. Por outro lado,

sejam $\sigma, \lambda \in \mathbb{Z}[\omega]$ tais que $\alpha\sigma + \beta\lambda = \delta$ (a existência desses elementos é garantida pelo Teorema de Bézout). Logo,

$$\delta = \alpha\sigma + \beta\lambda = (\gamma\upsilon_1)\sigma + (\gamma\upsilon_2)\lambda = \gamma(\upsilon_1\sigma + \upsilon_2\lambda).$$

Isso mostra que γ é um divisor de δ. Reciprocamente, sejam α e β inteiros de Eisenstein, não ambos nulos, e δ um divisor comum de α e β tal que para qualquer γ que divide α e β temos que γ também divide δ. Como $\mathrm{N}(\delta) \geq 1$, aplicando o Teorema 4, temos que δ é um divisor comum de α e β de norma máxima. Portanto δ é um máximo divisor comum de α e β. □

Corolário 4. *Sejam α e β inteiros de Eisenstein. Temos que α e β são relativamente primos se, e somente se, existem inteiros de Eisenstein σ e λ tais que $\alpha\sigma + \beta\lambda = 1$.*

Demonstração. Se α e β são relativamente primos, então 1 é um máximo divisor comum de α e β. Portanto, pelo Teorema de Bézout, existem inteiros de Eisenstein σ e λ tais que $\alpha\sigma + \beta\lambda = 1$. Reciprocamente, se existem inteiros de Eisenstein σ e λ tais que $\alpha\sigma + \beta\lambda = 1$, então qualquer divisor comum de α e β é também um divisor de 1 e, portanto, é uma unidade de $\mathbb{Z}[\omega]$. Logo, α e β são relativamente primos. □

Exemplo 11. No Exemplo 9 mostramos que -1 é um máximo divisor comum de $\alpha = 8 - 3\omega$ e $\beta = 4 + \omega$. Além disso, temos que

$$-2 + \omega = (8 - 3\omega) - (4 + \omega)(2 - 2\omega) \tag{3}$$

$$\text{e} \quad -1 = (4 + \omega) - (-2 + \omega)(-2 - \omega). \tag{4}$$

Substituindo (3) em (4), obtemos

$$\begin{aligned} -1 &= (4 + \omega) - [(8 - 3\omega) - (4 + \omega)(2 - 2\omega)](-2 - \omega) \\ &= (4 + \omega) - (8 - 3\omega)(-2 - \omega) + (4 + \omega)(2 - 2\omega)(-2 - \omega) \\ &= (8 - 3\omega)(-2 - \omega)(-1) + (4 + \omega)[1 + (2 - 2\omega)(-2 - \omega)] \\ &= (8 - 3\omega)(2 + \omega) + (4 + \omega)(-5). \end{aligned}$$

Finalmente, multiplicando ambos os lados da igualdade obtida acima por -1, obtemos

$$1 = (8 - 3\omega)(-2 - \omega) + (4 + \omega)(5).$$

Corolário 5. *Sejam α, β e γ inteiros de Eisenstein relativamente primos. Se $\alpha \mid \beta\gamma$, então $\alpha \mid \gamma$.*

Demonstração. Se $\alpha \mid \beta\gamma$, então $\beta\gamma = \alpha\phi$, para algum $\phi \in \mathbb{Z}[\omega]$. Como α e β são relativamente primos, pelo Corolário 4, existem $\sigma, \lambda \in \mathbb{Z}[\omega]$ tais que $\alpha\sigma + \beta\lambda = 1$. Multiplicando ambos os lados dessa última igualdade por γ e usando a igualdade $\beta\gamma = \alpha\phi$, obtemos $\gamma = \gamma\alpha\sigma + \gamma\beta\lambda = \gamma\alpha\sigma + \gamma\alpha\phi = \alpha(\gamma\sigma + \gamma\phi)$. Portanto $\alpha \mid \gamma$. □

Corolário 6. *Sejam α e β inteiros de Eisenstein relativamente primos. Se $\alpha \mid \gamma$ e $\beta \mid \gamma$ em $\mathbb{Z}[\omega]$, então $\alpha\beta \mid \gamma$.*

Demonstração. Se $\alpha \mid \gamma$ e $\beta \mid \gamma$, então existem inteiros de Eisenstein ϕ e θ tais que $\gamma = \alpha\phi$ e $\gamma = \beta\theta$. Porém, α e β são relativamente primos, isto é, existem $\sigma, \lambda \in \mathbb{Z}[\omega]$ tais que $\alpha\sigma + \beta\lambda = 1$. Logo, $\gamma = \gamma\alpha\sigma + \gamma\beta\lambda = (\beta\theta)\alpha\sigma + (\alpha\phi)\beta\lambda = (\alpha\beta)(\theta\sigma + \phi\lambda)$. Portanto $\alpha\beta \mid \gamma$. □

Corolário 7. *Sejam α, β e γ inteiros de Eisenstein. Temos que $\alpha\beta$ e γ são relativamente primos se, e somente se, α e γ são relativamente primos e β e γ são relativamente primos.*

Demonstração. ($\Rightarrow$) Se $\alpha\beta$ e γ são relativamente primos, existem inteiros de Eisenstein σ e λ tais que $(\alpha\beta)\sigma + \gamma\lambda = 1$ (Corolário 4). Como $\alpha(\beta\sigma) + \gamma\lambda = 1$ e $\beta\sigma \in \mathbb{Z}[\omega]$, segue que α e γ são relativamente primos. Analogamente, da igualdade $\beta(\alpha\sigma) + \gamma\lambda = 1$, obtemos que β e γ são relativamente primos, já que $\alpha\sigma \in \mathbb{Z}[\omega]$. ($\Leftarrow$) Como α e γ são relativamente primos, existem inteiros de Eisenstein σ e λ tais que $\alpha\sigma + \gamma\lambda = 1$ (Corolário 4). Além disso, como β e γ também são relativamente primos, existem inteiros de Eisenstein σ' e λ' tais que $\beta\sigma' + \gamma\lambda' = 1$. Logo, $(\alpha\sigma + \gamma\lambda)(\beta\sigma' + \gamma\lambda') = 1$, isto é, $\alpha\sigma\beta\sigma' + \alpha\sigma\gamma\lambda' + \gamma\lambda\beta\sigma' + \gamma\lambda\gamma\lambda' = 1$, ou melhor, $\alpha\beta(\sigma\sigma') + \gamma(\alpha\sigma\lambda' + \lambda\beta\sigma' + \gamma\lambda\lambda') = 1$. Portanto $\alpha\beta$ e γ são relativamente primos. □

5. Primos de Eisenstein

Nesta seção mostraremos que os primos de Eisenstein são irredutíveis em $\mathbb{Z}[\omega]$ e vice-versa. Além disso, será apresentada uma caracterização dos primos de Eisenstein em termos dos primos em $\mathbb{Z}$.

Definição 7. Um inteiro de Eisenstein π de norma maior que 1 é dito *primo de Eisenstein* se toda vez que $\pi \mid \alpha\beta$, com $\alpha, \beta \in \mathbb{Z}[\omega]$, tem-se que $\pi \mid \alpha$ ou $\pi \mid \beta$. Um inteiro de Eisenstein π de norma maior que 1 é denominado *composto* em $\mathbb{Z}[\omega]$ se ele não é um primo de Eisenstein.

Definição 8. Um inteiro de Eisenstein π de norma maior que 1 é dito *irredutível* em $\mathbb{Z}[\omega]$ se seus únicos divisores são as unidades de $\mathbb{Z}[\omega]$ e seus próprios associados. Um inteiro de Eisenstein de norma maior que 1 é dito *redutível* em $\mathbb{Z}[\omega]$ se ele não for irredutível.

Observação 12. O Teorema 5 garante que se um inteiro de Eisenstein α é redutível em $\mathbb{Z}[\omega]$, então α possui divisores com norma estritamente entre 1 e $N(\alpha)$.

Teorema 11. *Seja π um inteiro de Eisenstein. Então, π é um primo de Eisenstein se, e somente se, π é irredutível em $\mathbb{Z}[\omega]$.*

Demonstração. ($\Rightarrow$) Seja α um inteiro de Eisenstein que divide π. Assim, existe $\beta \in \mathbb{Z}[\omega]$ tal que $\pi = \alpha\beta$ e, em particular, $\pi \mid \alpha\beta$. Como π é um primo de Eisenstein, segue que $\pi \mid \alpha$ ou $\pi \mid \beta$. Se $\pi \mid \alpha$, o Teorema 6 garante que α e π são associados, pois $\alpha \mid \pi$. Analogamente, se $\pi \mid \beta$ tem-se que β e π são associados e, nesse caso, existe $u \in U(\mathbb{Z}[\omega])$ tal que $\pi = u\beta$. Como $u\beta = \pi = \alpha\beta$, segue que $\alpha = u$. Portanto α é uma unidade. Isso mostra que π é irredutível em $\mathbb{Z}[\omega]$. ($\Leftarrow$) Seja π um inteiro de Eisenstein irredutível em $\mathbb{Z}[\omega]$. Suponha que $\pi \mid \alpha\beta$, com $\alpha, \beta \in \mathbb{Z}[\omega]$. Se $\pi \nmid \alpha$, então apenas as unidades de $\mathbb{Z}[\omega]$ são divisores comuns de π e α, pois π é irredutível. Logo, π e α são relativamente primos e, pelo Corolário 5, $\pi \mid \beta$. Analogamente, pode-se mostrar que se $\pi \nmid \beta$, então $\pi \mid \alpha$. Isso mostra que π é um primo de Eisenstein. □

Exemplo 12. O elemento $2-4\omega$ é redutível em $\mathbb{Z}[\omega]$, pois $2-4\omega = 2\cdot(1-2\omega)$, $1 < N(2) < N(2-4\omega)$ e $1 < N(1-2\omega) < N(2-4\omega)$. Pelo Teorema 11, $2-4\omega$ não é um primo de Eisenstein.

Exemplo 13. O inteiro de Eisenstein 3 é composto em $\mathbb{Z}[\omega]$. Para provar isso, é suficiente mostrar que existem inteiros de Eisenstein de norma igual a 3, uma vez que se α é um inteiro de Eisenstein de norma igual a 3, então $\alpha\overline{\alpha} = 3$, $1 < N(\alpha) < N(3)$ e $1 < N(\overline{\alpha}) < N(3)$. Com efeito, escrevendo $\alpha = a + b\omega$ com $a, b \in \mathbb{Z}$, temos que $a^2 - ab + b^2 = 3$. Considerando $a^2 - ab + (b^2 - 3) = 0$ como uma equação de segundo grau com incógnita "a", vemos que esta equação só tem solução real quando $b^2 - 4(b^2 - 3) \geq 0$, isto é, se $-2 \leq b \leq 2$. Assim, os possíveis valores inteiros para b são $-2, -1, 0, 1$

e 2. Vamos analisar cada um dos casos. Se $b = -2$, então $a^2 + 2a + 1 = 0$ e, logo, $a = -1$. Quando $b = -1$, teremos $a^2 + a - 2 = 0$ e, desse modo, $a = 1$ ou $a = -2$. No caso em que $b = 0$, teremos a equação $a^2 - 3 = 0$, a qual não possui solução inteira. Além disso, se $b = 1$, teremos $a^2 - a - 2 = 0$ e, logo, $a = -1$ ou $a = 2$. Por fim, se $b = 2$, então $a^2 - 2a + 1 = 0$ e, consequentemente, $a = 1$. Portanto os inteiros de Eisenstein de norma igual a 3 são $-1-2\omega, 1-\omega, -2-\omega, -1+\omega, 2+\omega$ e $1+2\omega$. Tomando $\alpha = 1 - \omega$, temos que $\overline{\alpha} = (1 - (-1)) - (-\omega) = 2 + \omega$. Logo, podemos escrever $3 = (1 - \omega)(2 + \omega)$, em que $1 < N(1 - \omega) = N(2 + \omega) = 3 < N(3)$. Portanto 3 é redutível em $\mathbb{Z}[\omega]$ e, pelo Teorema 11, 3 é composto em $\mathbb{Z}[\omega]$.

Observação 13. A partir do exemplo anterior podemos concluir que os únicos inteiros de Eisenstein de norma 3 são $-1 - 2\omega, 1 - \omega, -2 - \omega, -1 + \omega, 2 + \omega$ e $1 + 2\omega$. Além disso, é possível concluir que esses seis elementos são associados, pois um inteiro de Eisenstein possui seis associados e elementos associados têm a mesma norma.

Exemplo 14. O inteiro 2 é um primo de Eisenstein. De fato, suponha por absurdo que 2 é redutível em $\mathbb{Z}[\omega]$. Assim, existem inteiros de Eisenstein α e β tais que $2 = \alpha\beta$, com $1 < N(\alpha) < 4$. Aplicando a norma em ambos os lados e usando a multiplicidade da norma, obtemos $N(\alpha)N(\beta) = 4$. A partir disso, concluímos que $N(\alpha) = 2$, uma vez que $1 < N(\alpha) < 4$. Logo, escrevendo $\alpha = a + b\omega$, com $a, b \in \mathbb{Z}$, temos que $a^2 - ab + b^2 = 2$, isto é, $a^2 - ab + (b^2 - 2) = 0$. A equação $a^2 - ab + (b^2 - 2) = 0$ com incógnita "a" tem solução real somente se $b^2 - 4(b^2 - 2) \geq 0$, isto é, $b^2 \leq 8/3$. Por outro lado, os únicos valores inteiros para b que satisfazem $b^2 \leq 8/3$ são $-1, 0$ e 1. Nesse caso, as equações correspondentes são $a^2 + a - 1 = 0$, $a^2 - 2 = 0$ e $a^2 - a - 1 = 0$, respectivamente. Como essas três equações não possuem soluções inteiras, segue que 2 é irredutível em $\mathbb{Z}[\omega]$. Isso mostra que 2 é um primo de Eisenstein (Teorema 11).

Observação 14. No exemplo anterior foi mostrado que não existe um par de inteiros (a, b) que satisfaz a igualdade $a^2 - ab + b^2 = 2$, isto é, não existem inteiros de Eisenstein de norma igual a 2.

Teorema 12. *Seja α um inteiro de Eisenstein. Se $N(\alpha)$ é primo em $\mathbb{Z}$, então α é um primo de Eisenstein.*

Demonstração. Sejam α um inteiro de Eisenstein e p um primo positivo tal que $N(\alpha) = p$. Suponha, por absurdo, que α seja irredutível. Assim, existem $\beta, \gamma \in \mathbb{Z}[\omega]$ de modo que $\alpha = \beta\gamma$ é uma fatoração não trivial (isto é, $1 < N(\beta) < N(\alpha)$ e $1 < N(\gamma) < N(\alpha)$). Aplicando a norma em ambos os lados dessa última igualdade e usando a multiplicidade da norma, obtemos $p = N(\beta)N(\gamma)$. Como p é primo, segue que $N(\beta) = 1$ ou $N(\gamma) = 1$. Logo, β é uma unidade ou γ é uma unidade. Isso contradiz o fato de $\alpha = \beta\gamma$ ser uma fatoração não trivial. Portanto α é irredutível em $\mathbb{Z}[\omega]$ e, consequentemente, α é um primo de Eisenstein. □

Exemplo 15. O elemento $1 + 2\omega$ é um primo de Eisenstein, uma vez que $N(1 + 2\omega) = 3$.

Observação 15. É importante ressaltar que a recíproca do teorema é falsa. Por exemplo, 2 é um primo de Eisenstein, mas $N(2) = 4$.

O próximo teorema fornece uma caracterização dos inteiros de Eisenstein em termos dos primos em $\mathbb{Z}$. A notação $a \equiv b \mod m$ significa que a e b são *congruentes* módulo m. Dados inteiros a, b e $m > 1$, dizemos que a e b são congruentes módulo m quando $m \mid (a - b)$ em $\mathbb{Z}$.

Teorema 13. *Os primos de Eisenstein são os elementos*

(i) p, *e seus associados, onde* p *é um primo positivo tal que* $p \equiv 2 \mod 3$ *e*

(ii) π, *onde* $\mathrm{N}(\pi) = \mathrm{p}$ *com* p *um primo positivo tal que* $\mathrm{p} = 3$ *ou* $\mathrm{p} \equiv 1 \mod 3$.

Demonstração. Ver ([2], Página 31). □

Exemplo 16. O Item *(i)* do Teorema 13 garante que os elementos 2, 5 e seus respectivos associados são primos de Eisenstein, pois 2 e 5 são primos positivos congruentes a 2 módulo 3. Os associados de 2 e 5 estão destacados em verde na Figura 7. O Item *(ii)* do mesmo teorema garante que os elementos de norma igual a 19 são também primos de Eisenstein, pois 19 é um primo positivo congruente a 1 módulo 3. Os primos de Eisenstein de norma igual a 19 estão ilustrados em vermelho na Figura 7.

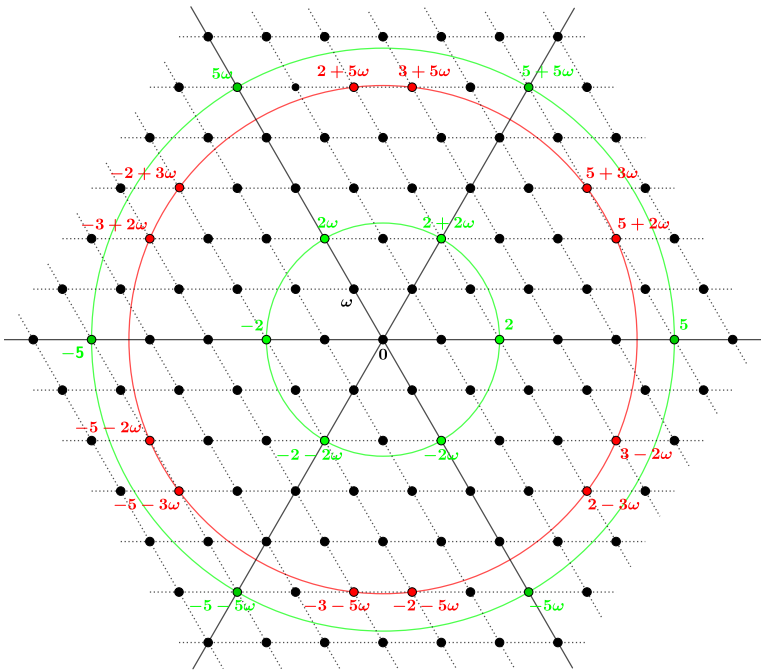


Figura 7: Primos de Eisenstein de norma igual a $4, 19$ e 25.

Quais são os primos de Eisenstein de norma menor ou igual a 31? O Teorema 13 fornece a resposta dessa pergunta. São os elementos de norma igual a $\mathrm{p}^2 \leq 31$, em que p é um primo positivo congruente a 2 módulo 3 (isto é, $\mathrm{p} = 2$ ou $\mathrm{p} = 5$), e os de norma igual a $\mathrm{p} \leq 31$, em que $\mathrm{p} = 3$ ou p é um primo positivo congruente a 1 módulo 3 (isto é, $\mathrm{p} \in \{3, 7, 13, 19, 31\}$). Em outras palavras, são os inteiros de Eisenstein que pertencem à união das circunferências centradas na origem do plano complexo e de raios $\sqrt{3}, 4, \sqrt{7}, \sqrt{13}, \sqrt{19}, 25$ e $\sqrt{31}$. Os primos de Eisenstein de norma menor ou igual a 31 e as circunferências mencionadas estão ilustrados na Figura 8. Os elementos obtidos a partir do item *(i)* do teorema estão destacados na cor verde, e os caracterizados pelo item *(ii)* estão destacados em vermelho.

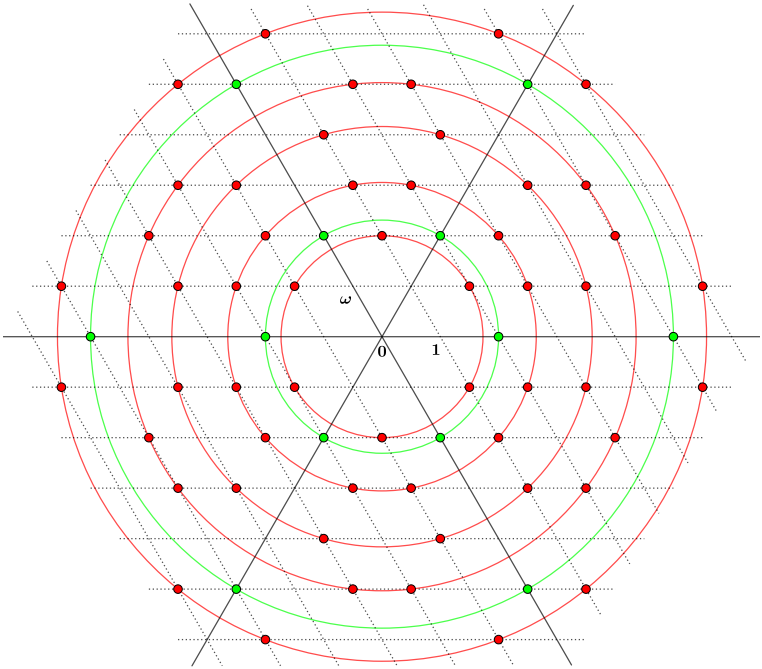


Figura 8: Primos de Eisenstein de norma menor ou igual a 31.

Na próxima tabela estão listados os primos de Eisenstein de norma menor ou igual a 31.

Norma	Primos de Eisenstein
3	$2+\omega, 1+2\omega, -1+\omega, -2-\omega, -1-2\omega$ e $1-\omega$
4	$2, 2+2\omega, 2\omega, -2, -2-2\omega$ e -2ω.
7	$3+\omega, 3+2\omega, 2+3\omega, 1+3\omega, -1+2\omega, -2+\omega,$ $-3-\omega, -3-2\omega, -2-3\omega, -1-3\omega, 1-2\omega$ e $2-\omega$.
13	$4+\omega, 4+3\omega, 3+4\omega, 1+4\omega, -1+3\omega, -3+\omega,$ $-4-\omega, -4-3\omega, -3-4\omega, -1-4\omega, 1-3\omega$ e $3-\omega$.
19	$5+2\omega, 5+3\omega, 3+5\omega, 2+5\omega, -2+3\omega, -3+2\omega,$ $-5-2\omega, -5-3\omega, -3-5\omega, -2-5\omega, 2-3\omega$ e $3-2\omega$.
25	$5, 5+5\omega, 5\omega, -5, -5-5\omega$ e -5ω.
31	$6+\omega, 6+5\omega, 5+6\omega, 1+6\omega, -1+5\omega, -5+\omega,$ $-6-\omega, -6-5\omega, -5-6\omega, -1-6\omega, 1-5\omega$ e $5-\omega$.

Tabela 1: Primos de Eisenstein de norma menor ou igual a 31.

Por fim, apresentamos a Figura 9, na qual estão ilustrados todos os primos de Eisenstein de norma menor ou igual a 169. Tal figura pode ser construída utilizando um procedimento análogo ao que

foi discutido acima.

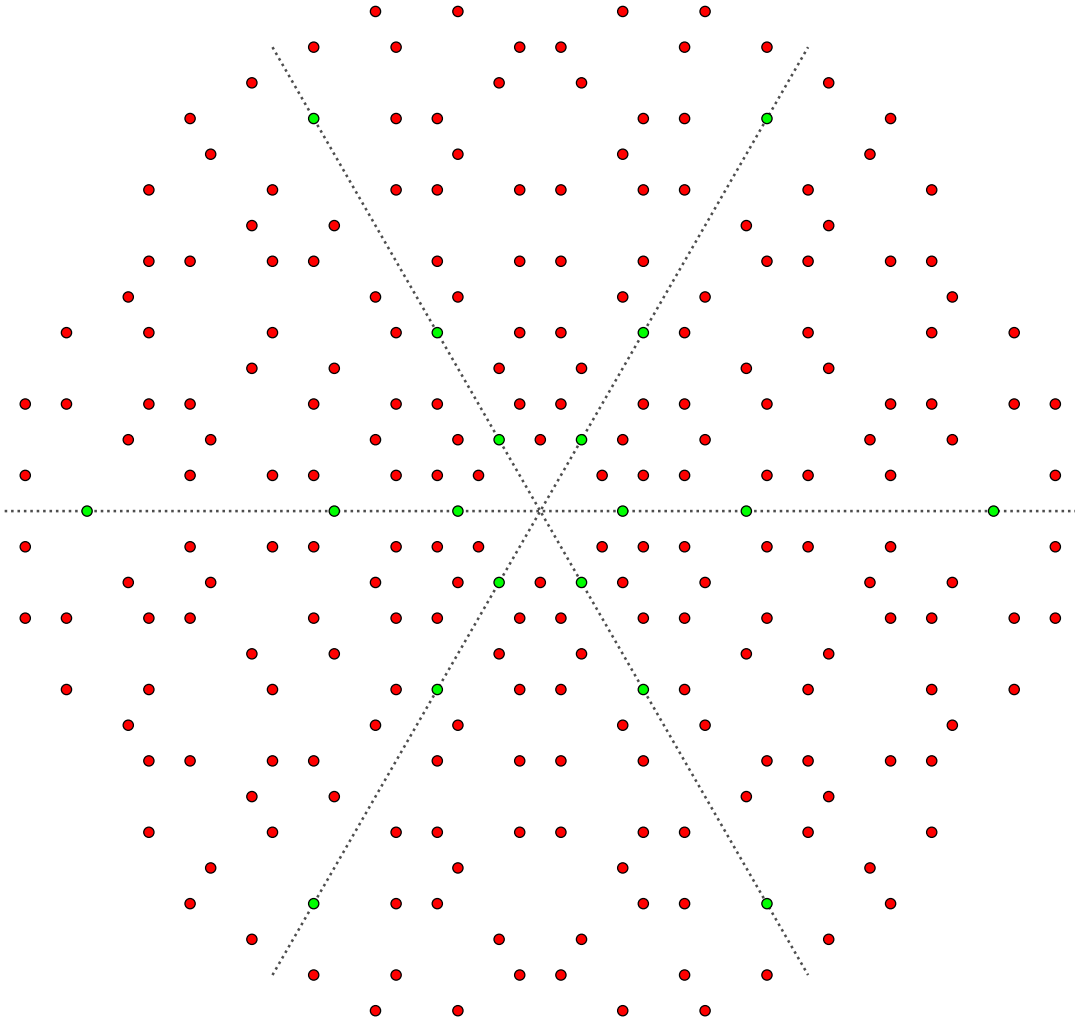


Figura 9: Primos de Eisenstein de norma menor ou igual a 169

Observação 16. Os primos de 1 até n podem ser determinados utilizado o Crivo de Eratóstenes. Para mais detalhes, confira a referência [4].

Corolário 8. *Não existe um inteiro de Eisenstein* α *tal que* $\mathrm{N}(\alpha) = \mathrm{p}$ *e* p *é um primo positivo com* $\mathrm{p} \equiv 2 \mod 3$.

Demonstração. Suponha, por absurdo, que exista um inteiro de Eisenstein α tal que $\mathrm{N}(\alpha) = \mathrm{p}$ e p é um primo positivo com $\mathrm{p} \equiv 2 \mod 3$. Como p é primo, o Teorema 12 garante que α é um primo

de Eisenstein. No entanto, $p \neq 3$, $p \not\equiv 1 \mod 3$ e α não é um associado de um primo positivo q congruente a 2 módulo 3 (caso contrário, teríamos $N(\alpha) = q^2$). Pelo Teorema 13, α não é um primo de Eisenstein. Temos um absurdo e, portanto, concluímos que não existe inteiro de Eisenstein α tal que $N(\alpha) = p$ e p é um primo positivo com $p \equiv 2 \mod 3$. □

Corolário 9. *Se α é um inteiro de Eisenstein, p é um primo positivo, $p \equiv 2 \mod 3$ e $N(\alpha) = p^2$, então α é um primo de Eisenstein.*

Demonstração. Sejam α um inteiro de Eisenstein e p um primo positivo tal que $p \equiv 2 \mod 3$ e $N(\alpha) = p^2$. Suponha, por absurdo, que α seja composto em $\mathbb{Z}[\omega]$. Pelo Teorema 11, segue que α é redutível em $\mathbb{Z}[\omega]$, isto é, existem inteiros de Eisenstein β_1 e β_2 tais que $\beta_1\beta_2 = \alpha$ e $1 < N(\beta_1), N(\beta_2) < N(\alpha)$. Aplicando a norma em ambos os lados da igualdade $\beta_1\beta_2 = \alpha$ e usando a multiplicidade da norma, obtemos $N(\beta_1)N(\beta_2) = N(\alpha) = p^2$. Como p é primo e $1 < N(\beta_1), N(\beta_2) < p^2$, segue que $N(\beta_2) = N(\beta_1) = p$, o que contradiz o Corolário 8. Portanto α é um primo de Eisenstein. □

Corolário 10. *Um inteiro de Eisenstein α é composto em $\mathbb{Z}[\omega]$ se, e somente se, $N(\alpha)$ é composto em $\mathbb{Z}$ e $\sqrt{N(\alpha)}$ não é um primo congruente a 2 módulo 3.*

Demonstração. ($\Rightarrow$) Seja α um inteiro de Eisenstein composto. O Teorema 12 garante que $N(\alpha)$ é composto em $\mathbb{Z}$. Além disso, como α é composto em $\mathbb{Z}[\omega]$, segue do Corolário 9 que não existe um primo positivo p tal que $p \equiv 2 \mod 3$ e $N(\alpha) = p^2$. Portanto $\sqrt{N(\alpha)}$ não é um primo congruente a 2 módulo 3. ($\Leftarrow$) Seja α um inteiro de Eisenstein tal que $N(\alpha) = n$ é composto em $\mathbb{Z}$ e $\sqrt{N(\alpha)}$ não é um primo congruente a 2 módulo 3. Assim, $n \neq 3$ e n não é um primo positivo congruente a 1 módulo 3, uma vez que n é composto em $\mathbb{Z}$. Além disso, como $\sqrt{N(\alpha)}$ não é um primo congruente a 2 módulo 3, para qualquer primo positivo q tal que $q \equiv 2 \mod 3$, tem-se $N(\alpha) \neq q^2$. Logo, α não é um associado de um primo congruente a 2 módulo 3. Pelo Teorema 13, α é um inteiro de Eisenstein composto. □

Exemplo 17. O Corolário 10 pode ser usado para mostrar que um determinado inteiro de Eisenstein α é composto. Por exemplo, $4 + 5\omega$, $5 + 5\omega$, 7 e 13 são inteiros de Eisenstein compostos, pois $N(4 + 5\omega) = 21$, $N(5 + 5\omega) = 25, N(7) = 49$ e $N(13) = 169$ são números inteiros compostos e $\sqrt{21}$, $\sqrt{25}, \sqrt{49}$ e $\sqrt{169}$ não são primos congruentes a 2 módulo 3.

6. Fatoração Única

O objetivo desta seção é mostrar que, a menos da ordem e de elementos associados, a fatoração de um inteiro de Eisenstein de norma maior do que 1 como produto de primos de Eisenstein é única. Em algumas demonstrações será utilizado o princípio de indução matemática. Para mais detalhes sobre essa técnica de demonstração sugerimos a referência [5].

Teorema 14. *Todo inteiro de Eisenstein de norma maior do que 1 ou é um primo de Eisenstein ou pode ser escrito como um produto de primos de Eisenstein.*

Demonstração. Como não existem inteiros de Eisenstein de norma igual a 2 (Exemplo 14), basta provar o resultado para inteiros de Eisenstein de norma maior ou igual a 3. A prova será por indução sobre a norma. Inicialmente observe que todo inteiro de Eisenstein de norma igual a 3 é um primo de Eisenstein (Teorema 12). Agora, seja $n \geq 4$ e suponha que cada inteiro de Eisenstein α tal que $3 \leq N(\alpha) < n$ ou é um primo de Eisenstein ou pode ser escrito como produto de primos

de Eisenstein. Se não existem inteiros de Eisenstein de norma igual a n, não há nada a provar. Resta, então, estudar o caso em que existem inteiros de Eisenstein de norma igual a n. Seja α um inteiro de Eisenstein de norma igual a n. Se α é um primo de Eisenstein temos o resultado desejado. Por outro lado, se α não é um primo de Eisenstein, então α é redutível, ou seja, podemos escrever $\alpha = \beta\gamma$, na qual $1 < N(\beta), N(\gamma) < N(\alpha) = n$. Dessa forma, pela hipótese de indução, segue que cada um dos elementos β e γ ou é um primo de Eisenstein ou pode ser escrito como um produto de primos de Eisenstein. Portanto α é também um produto de primos de Eisenstein. □

Lema 1. *Sejam $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}[\omega]$ e π um primo de Eisenstein. Se $\pi \mid \alpha_1\alpha_2\cdots\alpha_r$, então π divide α_j para algum $1 \leq j \leq r$.*

Demonstração. Esta prova será omitida e pode ser feita por indução sobre r. □

Teorema 15 (Fatoração Única)**.** *Todo inteiro de Eisenstein de norma maior do que 1 ou é um primo de Eisenstein ou, a menos da ordem e de elementos associados, pode ser fatorado de forma única como produto de primos de Eisenstein.*

Demonstração. O Teorema 14 garante que todo inteiro de Eisenstein de norma maior do que 1, ou é um primo de Eisenstein ou pode ser escrito como um produto de primos de Eisenstein. A prova da unicidade (a menos da ordem e de elementos associados) será feita por indução sobre a norma. Primeiramente observe que não existem inteiros de Eisenstein de norma igual a 2 (Observação 1) e todo inteiro de Eisenstein de norma igual a 3 é um primo de Eisenstein (Teorema 12). Seja $n \geq 4$ e suponha que todo inteiro de Eisenstein de norma k, com $3 \leq k < n$, seja um primo de Eisenstein ou tenha, a menos da ordem e de elementos associados, uma fatoração única como produto de primos de Eisenstein. Se não há inteiros de Eisenstein de norma igual a n, não temos nada a provar. Suponha que α seja um inteiro de Eisenstein de norma igual a n. Se n é primo, então α é um primo de Eisenstein. Se n composto e α é um primo de Eisenstein, temos o resultado. Se, porém, n composto e α é um inteiro de Eisenstein composto, considere as seguintes fatorações de α

$$\alpha = \pi_1\pi_2\cdots\pi_r = \pi'_1\pi'_2\cdots\pi'_s,$$

onde π_i e π'_j são primos de Eisenstein, para todo $1 \leq i \leq r$ e $1 \leq j \leq s$. Como $\pi_1 \mid \alpha$, temos que $\pi_1 \mid \pi'_1\pi'_2\cdots\pi'_s$ e, pelo Lema 1, segue que $\pi_1 \mid \pi'_j$ para algum $j \in \{1, 2, \ldots, s\}$. Podemos supor, sem perda de generalidade, que $\pi_1 \mid \pi'_1$. Assim, como π_1 e π'_1 são primos de Eisenstein, existe $u \in U(\mathbb{Z}[\omega])$ tal que $\pi'_1 = u\pi_1$. Logo, podemos escrever

$$\alpha = \pi_1\pi_2\cdots\pi_r = u\pi_1\pi'_2\cdots\pi'_s.$$

Assim, $\pi_2\cdots\pi_r = u\pi'_2\cdots\pi'_s$. Seja $\beta = \pi_2\cdots\pi_r = u\pi'_2\cdots\pi'_s$. Temos que $N(\beta) = N(\alpha)/N(\pi_1) < N(\alpha) = n$, pois $N(\pi_1) > 1$, uma vez que π_1 é um primo de Eisenstein. Como u é uma unidade e π'_2 é um primo de Eisenstein, temos que $u\pi'_2$ também é um primo de Eisenstein. Assim, temos duas fatorações em produtos de primos de Eisenstein para β. No entanto, como $N(\beta) < n$, pela hipótese de indução, segue que β é um primo de Eisenstein ou, a menos da ordem e de elementos associados, tem uma fatoração única em produto de primos de Eisenstein. Desse modo, como $\pi'_1 = u\pi_1$, concluímos que a menos da ordem e de elementos associados α pode ser fatorado de forma única como produto de primos de Eisenstein. □

Exemplo 18. No Exemplo 13 vimos que $3 = (1-\omega)(2+\omega)$. Por outro lado, também é possível fatorar 3 da forma $3 = (-1-2\omega)(1+2\omega)$. Em ambos os casos, os fatores são primos de Eisenstein, já que todos possuem norma igual a 3. Observe que são fatorações distintas, mas isso obviamente não contradiz o Teorema 15, uma vez que $1+2\omega = \omega(1-\omega)$ e $-1-2\omega = \omega^2(2+\omega)$.

Exemplo 19. O número de soluções da equação diofantina $x^2 - xy + y^2 = n$ é divisível por 6. De fato, 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 inteiros de Eisenstein de norma igual a n é múltiplo de 6 (Observação 2). Portanto o número de soluções da equação diofantina $x^2 - xy + y^2 = n$ é divisível por 6.

Exemplo 20. O objetivo deste exemplo é determinar as soluções da equação diofantina $x^2 - xy + y^2 = 19$. Para isso, basta determinar 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 $5 + 2\omega$ e os associados de $\overline{5 + 2\omega}$, 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 $5 + 3\omega$ (esses elementos estão ilustrados em vermelho na Figura 7). 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 $(5, 3)$.

As principais referências utilizadas para elaboração deste artigo foram [1], [3], [6], [7] e [8].

Agradecimentos

Agradecemos ao/à parecerista pelas importantes considerações, as quais contribuíram para melhorar este artigo.

Referências

[1] Bandara, S. P. *An Exposition of the Eisenstein Integers*. Masters Theses, Eastern Illinois University, Charleston, Illinois, 2016. Disponível em: <https://thekeep.eiu.edu/cgi/viewcontent.cgi?article=3459&context=theses>. Acesso em: 09 de dezembro de 2021.

[2] Brito, F. C. A. *Resolução de problema via inteiros algébricos*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Centro de Ciências, Universidade Federal do Ceará, Fortaleza, 2017.

[3] Conrad, K. *The Gaussian Integers*. Disponível em: <http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf>. Acesso em: 09 de dezembro de 2021.

[4] Hefez, A. *Curso de Álgebra*. vol. 1. 5ª ed. Coleção Matemática Universitária. Rio de Janeiro: Impa. 2016.

[5] Hefez, A. *Indução Matemática*. Rio de Janeiro: Obmep. 2009. Disponível em: <http://www.obmep.org.br/docs/apostila4.pdf>. Acesso em: 22 de junho de 2022.

[6] Lisboa, D. L. *Números Inteiros de Eisenstein*. Dissertação (Mestrado Profissional em Matemática) - Centro de Ciências Exatas e da Natureza (CCEN), Universidade Federal da Paraíba, João Pessoa, 2017.

[7] Pontes, R. S. *Equações polinomiais: soluções algébricas, geométricas e com o auxílio de derivadas*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Centro de Ciências Exatas e da Natureza (CCEN), Universidade Federal da Paraíba, João Pessoa, 2013.

[8] Santos, J. P. O. *Introdução à teoria dos números*. Coleção Matemática Universitária. Rio de Janeiro: Impa. 1998.

Renan da Paixão Moura
Universidade Federal do Espírito Santo
<rpmoura7@gmail.com>

Edinaldo Junior Teles de Oliveira
Universidade Federal do Espírito Santo
<edinaldo_thellys@hotmail.com>

Eleonesio Strey
Universidade Federal do Espírito Santo
<eleonesio.strey@ufes.br>

Recebido: 14/12/2021
Publicado: 22/08/2022