



Inteiros Gaussianos

Lídia Charra Alves 

Renan da Paixão Moura 

Eleonesio Strey 

Resumo

O presente trabalho tem como objetivo abordar e desenvolver alguns resultados de aritmética dos inteiros gaussianos, que são os números complexos cujas partes real e imaginária são inteiras. Dentre os conceitos e resultados abordados, destacamos o Teorema da Divisão, o Teorema da Fatoração Única, uma caracterização dos primos gaussianos em termos dos números primos e uma breve introdução à aritmética modular nos inteiros gaussianos.

Palavras-chave: Inteiros Gaussianos; Divisibilidade em $\mathbb{Z}[i]$; Primos Gaussianos; Aritmética Modular em $\mathbb{Z}[i]$.

Abstract

This work aims to approach and develop some arithmetic results of Gaussian integers, which are complex numbers whose real and imaginary parts are integers. Among the concepts and results discussed, we highlight the Division Theorem, the Unique Factorization Theorem, a characterization of Gaussian primes in terms of prime numbers and a brief introduction to modular arithmetic in Gaussian integers.

Keywords: Gaussian Integers; Divisibility in $\mathbb{Z}[i]$; Gaussian Primes; Modular Arithmetic in $\mathbb{Z}[i]$.

1. Introdução

Desde os trabalhos de Gauss muitos pesquisadores têm se interessado pelo estudo de anéis que são análogos ao anel dos inteiros, nos quais os conceitos da aritmética também podem ser desenvolvidos. Dentre eles, destacamos o anel dos inteiros gaussianos, cujo estudo tem origem nas investigações de Gauss a respeito das reciprocidades cúbica e biquadrática. O que torna esse anel interessante é o fato de que muitos resultados da aritmética nos inteiros gaussianos são análogos aos resultados da aritmética nos inteiros e, além disso, podem ser ilustrados geometricamente. Para a elaboração deste artigo foram usadas as referências [1], [2], [3], [4], [5], [6], [8] e [9].

Inicialmente, apresentaremos as definições de norma e múltiplo, que nos permitirão desenvolver alguns resultados a respeito da divisibilidade no anel dos inteiros gaussianos, tais como o Teorema da Divisão para inteiros gaussianos e algumas de suas interpretações geométricas. Em seguida, trataremos a definição de primos gaussianos e uma caracterização desses elementos em termos dos números primos. Também trataremos o conceito de congruência e uma interpretação geométrica da aritmética modular nesse anel.

¹Parcialmente apoiado pelo Instituto Tim e pelo CNPq 104171/2023-5.

2. Inteiros Gaussianos

Os *inteiros gaussianos* ou *inteiros de Gauss* são os números complexos da forma $a + bi$, com a e b inteiros e $i = \sqrt{-1}$. O conjunto formado por todos os inteiros gaussianos é denotado por $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Este conjunto munido das operações usuais de adição e multiplicação de números complexos é um anel de integridade, o qual é conhecido como *anel dos inteiros gaussianos*. Uma representação dos inteiros gaussianos no plano cartesiano é apresentada na Figura 1.

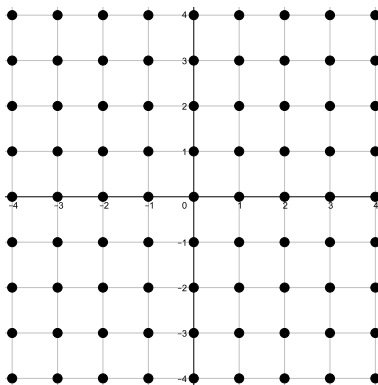


Figura 1: Inteiros gaussianos

Definição 1. A *norma* de um inteiro gaussiano $\alpha = a + bi$ é definida por

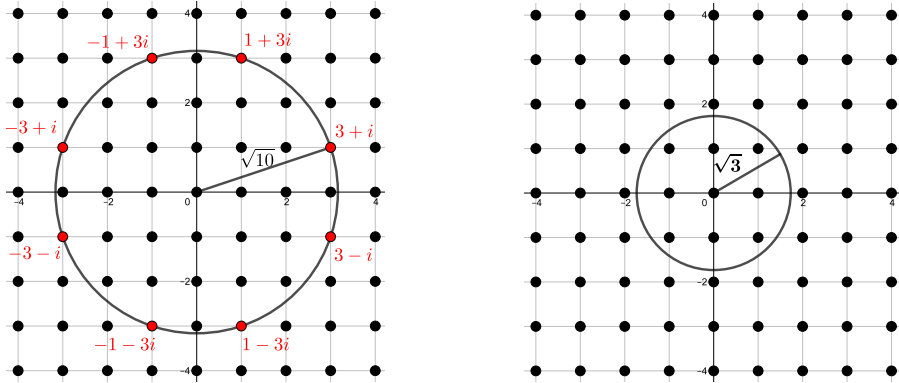
$$N(\alpha) = \alpha\bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2.$$

A norma de um inteiro gaussiano é igual à norma de seu conjugado. Além disso, a norma de qualquer inteiro gaussiano é um inteiro não negativo, uma vez que $a^2 + b^2 \geq 0$ e $a^2 + b^2 \in \mathbb{Z}$ quaisquer que sejam os inteiros a e b . Dados um inteiro gaussiano $a + bi$ e um inteiro n não negativo, tem-se que $N(a + bi) = n$ se, e somente se, o ponto (a, b) pertence à circunferência centrada na origem de raio \sqrt{n} .

Exemplo 1. Na Figura 2(a) estão destacados em vermelho todos os inteiros gaussianos de norma igual a 10. A norma de um inteiro gaussiano é sempre um inteiro não negativo, porém nem todo inteiro não negativo é norma de algum inteiro gaussiano. Por exemplo, conforme ilustrado na Figura 2(b), não existem inteiros gaussianos de norma igual a 3. Para verificar este fato algebricamente, basta notar que a equação $a^2 + b^2 = 3$ não admite solução nos inteiros.

Teorema 1. Para quaisquer inteiros gaussianos α_1 e α_2 , tem-se $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$. Em outras palavras, a norma é multiplicativa.

Demonstração. Basta observar que, quaisquer que sejam os inteiros gaussianos α_1 e α_2 , tem-se $N(\alpha_1\alpha_2) = \alpha_1\alpha_2\overline{\alpha_1\alpha_2} = (\alpha_1\alpha_2)(\overline{\alpha_1}\overline{\alpha_2}) = (\alpha_1\overline{\alpha_1})(\alpha_2\overline{\alpha_2}) = N(\alpha_1)N(\alpha_2)$. \square



(a) Inteiros gaussianos de norma igual a 10.

(b) Não existem elementos de norma igual a 3.

Figura 2: Norma de um inteiro gaussiano

Definição 2. Um inteiro gaussiano α é dito *invertível* em $\mathbb{Z}[i]$ se existir um inteiro gaussiano β tal que $\alpha\beta = 1$. Os elementos invertíveis em $\mathbb{Z}[i]$ também são chamados de *unidades* de $\mathbb{Z}[i]$.

Teorema 2. Os inteiros gaussianos invertíveis são ± 1 e $\pm i$.

Demonstração. Seja α um inteiro gaussiano invertível, então existe um inteiro gaussiano β tal que $\alpha\beta = 1$. Aplicando a norma em ambos os lados dessa igualdade e usando a multiplicidade da norma, obtemos $N(\alpha)N(\beta) = N(1) = 1$ e conseqüentemente $N(\alpha) = 1$, uma vez que $N(\alpha)$ e $N(\beta)$ são inteiros não negativos. Escrevendo $\alpha = a + bi$, com a e b inteiros, temos $a^2 + b^2 = 1$. Logo, os possíveis valores para o par (a, b) são $(1, 0)$, $(-1, 0)$, $(0, 1)$ e $(0, -1)$. Portanto, $\alpha = \pm 1$ ou $\alpha = \pm i$. \square

Observação 1. As unidades de $\mathbb{Z}[i]$ são os inteiros gaussianos de norma igual a 1 (Figura 3(a)).

Definição 3. Dois inteiros gaussianos α e β são ditos *associados* se $\alpha = \mu\beta$ para alguma unidade μ de $\mathbb{Z}[i]$, isto é, se $\alpha = \pm\beta$ ou $\alpha = \pm i\beta$.

Elementos associados têm a mesma norma. De fato, se α e β são associados, então $\alpha = \mu\beta$ para alguma unidade μ de $\mathbb{Z}[i]$. Aplicando a norma em ambos os lados dessa igualdade e usando a multiplicidade da norma, temos $N(\alpha) = N(\mu)N(\beta) = 1 \cdot N(\beta) = N(\beta)$.

Exemplo 2. Na Figura 3(b) estão representados os associados de $\beta = 3 + i$, a saber, $\beta = 3 + i$, $i\beta = -1 + 3i$, $-\beta = -3 - i$ e $-i\beta = 1 - 3i$.

Definição 4. Sejam $\alpha, \beta \in \mathbb{Z}[i]$. Dizemos que β *divide* α (ou β é um *divisor* de α , ou ainda, α é um *múltiplo* de β) em $\mathbb{Z}[i]$, e escrevemos $\beta \mid \alpha$, se $\alpha = \gamma\beta$, para algum $\gamma \in \mathbb{Z}[i]$. 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 $1 + 2i$ divide $2 - 4i$, basta verificar se existe um inteiro gaussiano $a + bi$ tal que $2 - 4i = (a + bi)(1 + 2i)$, isto é, $2 - 4i = (a - 2b) + (2a + b)i$. Como não existem inteiros a e b que satisfazem simultaneamente $a - 2b = 2$ e $2a + b = -4$, segue que $(1 + 2i) \nmid (2 - 4i)$.

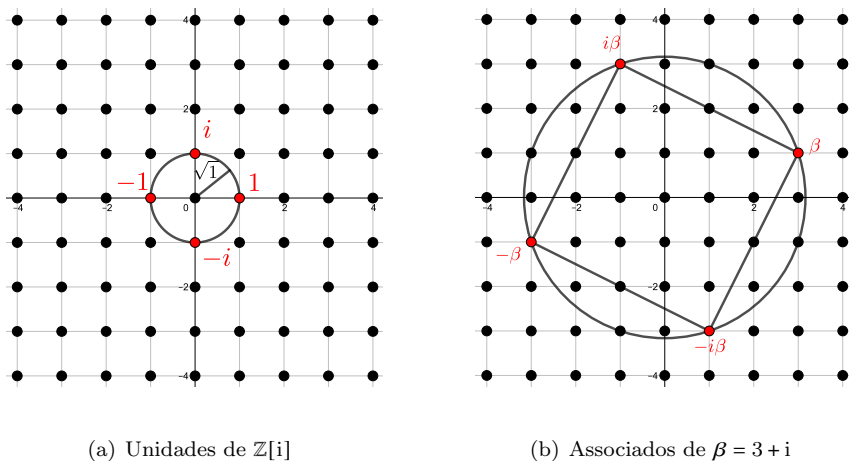


Figura 3: Unidades de $\mathbb{Z}[i]$ e associados de $\beta = 3 + i$

Dados dois inteiros gaussianos α e β , temos que α é um múltiplo de β se, e somente se, existem inteiros m e n tais que $\alpha = (m + ni)\beta = m \cdot \beta + n \cdot i\beta$. Em outras palavras, os múltiplos de β são as combinações lineares inteiras de β e $i\beta$.

Exemplo 4. Na Figura 4, destacamos em vermelho os múltiplos de $\beta = 3 + i$ que pertencem ao retângulo $[-6, 6] \times [-6, 6]$.

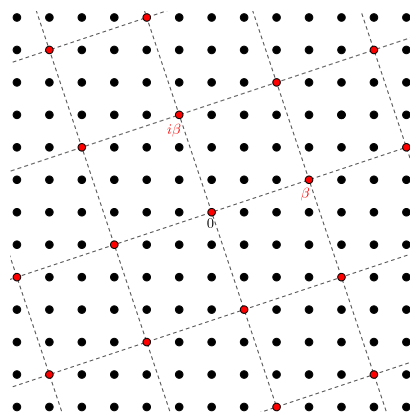


Figura 4: Múltiplos de $\beta = 3 + i$

Teorema 3. Sejam α e β inteiros gaussianos, com α não nulo. Se $\beta \mid \alpha$ em $\mathbb{Z}[i]$ e $N(\beta) = N(\alpha)$, então α e β são associados.

Demonstração. Sejam α e β inteiros gaussianos, com α não nulo. Se $\beta \mid \alpha$ em $\mathbb{Z}[i]$, então $\alpha = \beta\gamma$ para algum inteiro gaussiano $\gamma \neq 0$. Aplicando a norma em ambos os lados dessa última igualdade

e usando a multiplicidade da norma, obtemos $N(\alpha) = N(\beta)N(\gamma)$. Como $N(\beta) = N(\alpha)$ e $\alpha \neq 0$, segue que $N(\gamma) = 1$. Portanto, α e β são associados. \square

O teorema a seguir é um importante resultado que relaciona a divisibilidade em $\mathbb{Z}[i]$ com a norma de um inteiro gaussiano.

Teorema 4. *Sejam α e β inteiros gaussianos. Se $\beta \mid \alpha$ em $\mathbb{Z}[i]$, então $N(\beta) \mid N(\alpha)$ em \mathbb{Z} .*

Demonstração. Sejam α e β inteiros gaussianos tais que $\beta \mid \alpha$ em $\mathbb{Z}[i]$. Desse modo, existe um inteiro gaussiano γ tal que $\alpha = \beta\gamma$. Aplicando a norma em ambos os lados da igualdade e usando a multiplicidade da norma, obtemos $N(\alpha) = N(\beta)N(\gamma)$. Portanto, $N(\beta) \mid N(\alpha)$ em \mathbb{Z} . \square

Exemplo 5. O Teorema 4 garante que $\alpha = 1 + 2i$ não divide $\beta = 2 - 3i$, pois $N(\beta) = 13$ não é divisível por $N(\alpha) = 5$. Note que a recíproca do teorema não é verdadeira, uma vez que $N(1 + 2i) = 5$ divide $N(2 - 4i) = 20$, porém $(1 + 2i) \nmid (2 - 4i)$ (Exemplo 3).

Corolário 1. *A norma de um inteiro gaussiano α é par se, e somente se, α é um múltiplo de $1 + i$.*

Demonstração. Seja α um inteiro gaussiano de norma par. Escreva $\alpha = a + bi$ e note que $N(\alpha) = a^2 + b^2$ é par. Afirmamos que os inteiros a e b têm a mesma paridade. De fato, suponha, sem perda de generalidade, que a seja par e b seja ímpar. Logo, existem inteiros k e q tais que $a = 2k$ e $b = 2q + 1$. Consequentemente $a^2 + b^2 = (2k)^2 + (2q + 1)^2 = 4k^2 + 4q^2 + 4q + 1 = 2(2k^2 + 2q^2 + 2q) + 1$. Assim, como $2k^2 + 2q^2 + 2q$ é um inteiro, concluímos que $a^2 + b^2$ é ímpar, o que é um absurdo. Desse modo, como a e b têm a mesma paridade, segue que $c = (a+b)/2$ e $d = (b-a)/2$ são inteiros. Para concluir que $(1 + i) \mid (a + bi)$, basta observar que $a + bi = (c + di)(1 + i)$. Reciprocamente, seja α um múltiplo de $1 + i$, isto é, $\alpha = \gamma(1 + i)$, para algum inteiro gaussiano γ . Aplicando a norma em ambos os lados dessa última igualdade e usando a multiplicidade da norma, obtemos $N(\alpha) = N(\gamma)N(1 + i) = 2N(\gamma)$, já que $N(1 + i) = 2$. Como $N(\gamma)$ é um inteiro, segue que $N(\alpha)$ é par. \square

3. Teorema da Divisão

Nesta seção apresentaremos o Teorema da Divisão para inteiros gaussianos e traremos uma interpretação geométrica deste resultado. Para isso, inicialmente, abordaremos uma versão modificada do Teorema da Divisão para inteiros.

Teorema 5. *Dados dois inteiros a e b , com $b > 0$, existem inteiros q e r tais que $a = bq + r$ e $|r| \leq b/2$.*

Demonstração. Sejam a e b inteiros, com $b > 0$. O Teorema da Divisão nos inteiros (confira [9]) garante que existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$. Se $0 \leq r \leq b/2$ não há o que demonstrar. Se $b/2 < r < b$, basta observar que $a = (q + 1)b + (r - b)$ e $-b/2 \leq r - b < 0$. \square

Teorema 6 (Teorema da Divisão). *Dados dois inteiros gaussianos α e β , com $\beta \neq 0$, existem inteiros gaussianos γ e θ tais que $\alpha = \beta\gamma + \theta$ e $N(\theta) < N(\beta)$.*

Demonstração. Para quaisquer inteiros gaussianos α e β , com $\beta \neq 0$, podemos escrever

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{\alpha\bar{\beta}}{N(\beta)} = \frac{a + bi}{N(\beta)},$$

em que $a = \operatorname{Re}(\alpha\bar{\beta})$ e $b = \operatorname{Im}(\alpha\bar{\beta})$. Aplicando o Teorema 5, obtemos inteiros q_1, q_2, r_1 e r_2 tais que $a = N(\beta)q_1 + r_1$, $b = N(\beta)q_2 + r_2$, $|r_1| \leq (1/2)N(\beta)$ e $|r_2| \leq (1/2)N(\beta)$. Assim,

$$\frac{\alpha}{\beta} = \frac{(N(\beta)q_1 + r_1) + (N(\beta)q_2 + r_2)i}{N(\beta)} = q_1 + q_2i + \frac{r_1 + r_2i}{N(\beta)}.$$

Multiplicando ambos os lados da igualdade acima por β e tomando $\gamma = q_1 + q_2i$, obtemos

$$\alpha = \beta\gamma + \frac{r_1 + r_2i}{\beta}.$$

Agora, defina $\theta = \alpha - \beta\gamma = (r_1 + r_2i)/\bar{\beta}$ e note que $\theta \in \mathbb{Z}[i]$, pois $\mathbb{Z}[i]$ é um anel e $\alpha, \beta, \gamma \in \mathbb{Z}[i]$. Como $|r_1| \leq (1/2)N(\beta)$ e $|r_2| \leq (1/2)N(\beta)$, segue que

$$\begin{aligned} N(\theta) &= N\left(\frac{r_1 + r_2i}{\bar{\beta}}\right) = N\left(\frac{(r_1 + r_2i)\beta}{\beta\bar{\beta}}\right) = N\left(\frac{(r_1 + r_2i)\beta}{N(\beta)}\right) \\ &= \frac{(r_1^2 + r_2^2)N(\beta)}{N(\beta)^2} = \frac{r_1^2 + r_2^2}{N(\beta)} \leq \frac{(1/4)N(\beta)^2 + (1/4)N(\beta)^2}{N(\beta)} = \frac{1}{2}N(\beta). \end{aligned}$$

Isso conclui a demonstração □

Observação 2. Da demonstração do Teorema 6, obtemos que dados dois inteiros gaussianos α e β , com $\beta \neq 0$, sempre existem inteiros gaussianos γ e θ tais que

$$\alpha = \beta\gamma + \theta \text{ e } N(\theta) \leq (1/2)N(\beta).$$

Ao contrário do que ocorre nos inteiros, neste contexto o quociente e o resto da divisão não são necessariamente únicos. A demonstração do Teorema 6 fornece implicitamente um método para determinar, ao menos, um par (γ, θ) que satisfaz as condições do teorema. Note que $a = N(\beta)q_1 + r_1$, com $|r_1| \leq (1/2)N(\beta)$, implica $q_1 = a/N(\beta) - r_1/N(\beta)$, com $|r_1|/N(\beta) \leq 1/2$. Além disso,

$$\begin{aligned} \frac{1}{2} \geq \frac{r_1}{N(\beta)} \geq -\frac{1}{2} &\Leftrightarrow -\frac{1}{2} \leq -\frac{r_1}{N(\beta)} \leq \frac{1}{2} \\ &\Leftrightarrow \frac{a}{N(\beta)} - \frac{1}{2} \leq \frac{a}{N(\beta)} - \frac{r_1}{N(\beta)} \leq \frac{a}{N(\beta)} + \frac{1}{2} \\ &\Leftrightarrow \frac{a}{N(\beta)} - \frac{1}{2} \leq q_1 \leq \frac{a}{N(\beta)} + \frac{1}{2} \\ &\Leftrightarrow q_1 \in \left[\frac{a}{N(\beta)} - \frac{1}{2}, \frac{a}{N(\beta)} + \frac{1}{2} \right]. \end{aligned} \tag{1}$$

Analogamente, a partir da igualdade $b = N(\beta)q_2 + r_2$, na qual $|r_2| \leq (1/2)N(\beta)$, obtemos

$$q_2 \in \left[\frac{b}{N(\beta)} - \frac{1}{2}, \frac{b}{N(\beta)} + \frac{1}{2} \right]. \tag{2}$$

Portanto, para obter inteiros gaussianos γ e θ tais que $\alpha = \beta\gamma + \theta$ e $N(\theta) \leq (1/2)N(\beta)$, basta escolher q_1 e q_2 satisfazendo as condições (1) e (2). Em particular, basta escolher q_1 como sendo o inteiro (ou um dos inteiros) mais próximo de $a/N(\beta)$ e q_2 o inteiro (ou um dos inteiros) mais próximo de $b/N(\beta)$.

Exemplo 6. Sejam $\alpha = 5 + 2i$ e $\beta = 3 + i$. Dizer que um inteiro gaussiano θ satisfaz $N(\theta) \leq (1/2)N(\beta)$ significa que θ pertence ao círculo centrado na origem de raio $\sqrt{N(\beta)}/2$. Na Figura 5, observamos que existem exatamente dois múltiplos de β que estão a uma distância menor ou igual a $\sqrt{N(\beta)}/2$ de α , a saber, β e 2β . Isso permite-nos escrever $\alpha = \beta\gamma + \theta$, com $N(\theta) \leq (1/2)N(\beta)$, de duas maneiras diferentes, sendo elas $\alpha = \beta + (2 + i)$ e $\alpha = 2\beta - 1$, as quais estão ilustradas nas Figuras 6(a) e 6(b), respectivamente.

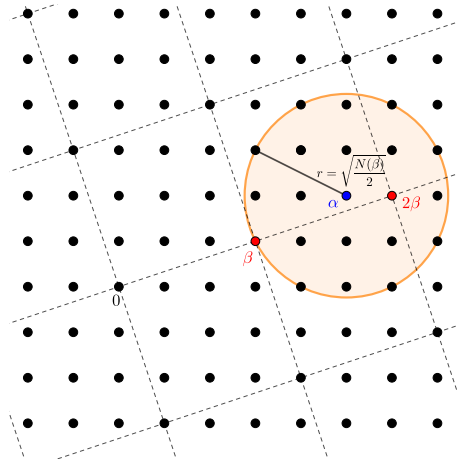
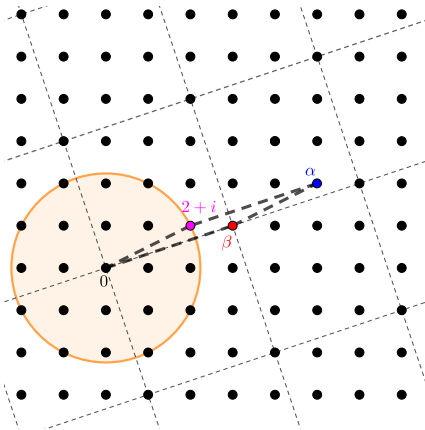
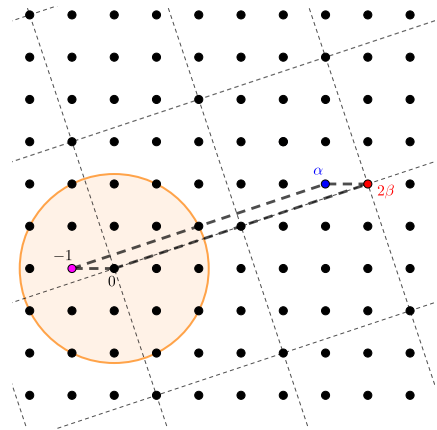


Figura 5: Múltiplos de β vizinhos de α



(a) $\alpha = \beta + (2 + i)$.



(b) $\alpha = 2\beta - 1$.

Figura 6: Teorema da Divisão para $\alpha = 5 + 2i$ e $\beta = 3 + i$.

Para encontrar algebricamente uma destas soluções, utilizando o método descrito implicitamente na demonstração do Teorema 6, iniciamos determinando a parte real e a parte imaginária do

número complexo α/β ,

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{N(\beta)} = \frac{(5+2i)(3-i)}{10} = \frac{17+i}{10} = \frac{17}{10} + \frac{1}{10}i.$$

Em seguida, tomamos γ como sendo o inteiro gaussiano cuja parte real é o inteiro mais próximo de $17/10$ e a parte imaginária é o inteiro mais próximo de $1/10$ (isto é, $\gamma = 2+0i = 2$) e $\theta = \alpha - \beta\gamma = (5+2i) - (3+i)(2) = -1$.

4. Primos Gaussianos

Nesta seção serão apresentadas definições e resultados que caracterizam os primos gaussianos. Mostraremos que todo inteiro gaussiano de norma maior do que 1 pode ser escrito como um produto de primos gaussianos e, a menos da ordem e de elementos associados, tal fatoração é única.

Definição 5. Seja α um inteiro gaussiano tal que $N(\alpha) > 1$. Dizemos que α é um *primo gaussiano* se seus únicos divisores são os triviais (isto é, $\pm 1, \pm i, \pm \alpha$ e $\pm i\alpha$). Se α possui um fator não trivial, dizemos que α é *composto* em $\mathbb{Z}[i]$.

Observação 3. Se β é um fator não trivial de um inteiro gaussiano α , então $1 < N(\beta) < N(\alpha)$.

Exemplo 7. O inteiro 3 é um primo gaussiano. De fato, suponha por absurdo que 3 seja composto em $\mathbb{Z}[i]$. Assim, existem inteiros gaussianos α e β tais que $\alpha\beta = 3$, $N(\alpha) > 1$ e $N(\beta) > 1$. Aplicando a norma em ambos os lados da igualdade e usando a multiplicidade da norma, obtemos $N(\alpha)N(\beta) = 9$. Logo, α é um inteiro gaussiano de norma igual a 3, o que é um absurdo (ver Exemplo 1). Portanto, 3 é um primo gaussiano.

Exemplo 8. O inteiro 5 é composto em $\mathbb{Z}[i]$, pois pode ser expresso como $5 = (1+2i)(1-2i)$ e $1+2i$ é um fator não trivial de 5, uma vez que $N(1+2i) = 1^2 + 2^2 = 5 \neq 25 = 5^2 + 0^2 = N(5)$.

Teorema 7. Se α é um inteiro gaussiano e $N(\alpha)$ é um primo, então α é um primo gaussiano.

Demonstração. Seja α um inteiro gaussiano tal que $N(\alpha)$ é um número primo e sejam β e γ inteiros gaussianos tais que $\alpha = \beta\gamma$. Aplicando a norma em ambos os lados dessa última igualdade e usando a multiplicidade da norma, obtemos $N(\alpha) = N(\beta)N(\gamma)$. Como $N(\alpha)$, $N(\beta)$ e $N(\gamma)$ são inteiros positivos e $N(\alpha)$ é um primo, segue que $N(\beta) = 1$ e $N(\gamma) = N(\alpha)$ ou então $N(\gamma) = 1$ e $N(\beta) = N(\alpha)$. Isto mostra que α só admite fatores triviais e, logo, α é um primo gaussiano. \square

A recíproca do Teorema 7 não é verdadeira, uma vez que 3 é um primo gaussiano e $N(3) = 9$ não é um primo.

Teorema 8. Todo inteiro gaussiano de norma maior do que 1 ou é um primo gaussiano ou pode ser escrito como um produto de primos gaussianos.

Demonstração. Seja α um inteiro gaussiano tal que $N(\alpha) > 1$. A demonstração será feita utilizando o princípio de indução matemática (ver [7]). Note que todo inteiro de norma igual a 2 é um primo gaussiano (Teorema 7). Seja $n \geq 3$ e suponha que todo inteiro gaussiano de norma igual a k , com $2 \leq k < n$, é um primo gaussiano ou pode ser escrito como um produto de primos gaussianos. Se não existirem inteiros gaussianos com norma igual a n , não há o que demonstrar. Suponha que α

seja um inteiro gaussiano de norma igual a n . Se n é primo, o Teorema 7 garante que α é um primo gaussiano. Se n é composto e α é um primo gaussiano, temos o resultado. Se, porém, n composto e α é um inteiro gaussiano composto, então existem inteiros gaussianos β e γ , com $N(\beta) > 1$ e $N(\gamma) > 1$, tais 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, $N(\alpha) > N(\beta) > 1$ e $N(\alpha) > N(\gamma) > 1$. Pela hipótese de indução, cada um dos elementos β e γ ou é um primo gaussiano ou pode ser escrito como um produto de primos gaussianos. Logo, α é um produto de primos gaussianos. Portanto, todo inteiro gaussiano α com norma maior que 1 ou é um primo gaussiano ou pode ser escrito como um produto de primos gaussianos. \square

O Teorema 8 garante-nos apenas a possibilidade de fatoração de um inteiro gaussiano. O resultado a seguir ajudar-nos-á a demonstrar a unicidade.

Teorema 9. *Seja π um primo gaussiano. Se $\alpha_1, \dots, \alpha_r$ são inteiros gaussianos tais que $\pi \mid \alpha_1\alpha_2 \dots \alpha_r$, então π divide α_j , para algum $j \in \{1, 2, \dots, r\}$.*

Demonstração. Tal resultado pode ser provado por indução sobre r . Para mais detalhes, confira a referência [3]. \square

Teorema 10 (Teorema da Fatoração Única). *Todo inteiro gaussiano de norma maior do que 1 ou é um primo gaussiano ou, a menos da ordem e de elementos associados, pode ser fatorado de forma única como produto de primos gaussianos.*

Demonstração. O Teorema 8 garante que todo inteiro gaussiano de norma maior do que 1 ou é um primo gaussiano ou pode ser escrito como um produto de primos gaussianos. A prova da unicidade (a menos da ordem e de elementos associados) será feita por indução sobre a norma. Note que todo inteiro gaussiano de norma igual a 2 é um primo gaussiano (Teorema 7). Seja $n \geq 3$ e suponha que todo inteiro gaussiano de norma k , com $2 \leq k < n$, é um primo gaussiano ou, a menos da ordem e de elementos associados, pode ser fatorado de forma única como produto de primos gaussianos. Se não existirem inteiros gaussianos de norma igual a n , não há o que demonstrar. Suponha que α seja um inteiro gaussiano de norma igual a n . Se n é primo, o Teorema 7 garante que α é um primo gaussiano. Se n é composto e α é um primo gaussiano, temos o resultado. Se, porém, n é composto e α é um inteiro gaussiano composto, considere as seguintes fatorações de α

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

em que π_i e π'_j são primos gaussianos, 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 Teorema 9, segue que $\pi_1 \mid \pi'_j$ para algum $j \in \{1, 2, \dots, s\}$. Podemos supor, sem perda de generalidade, que $\pi_1 \mid \pi'_1$. Assim, como π_1 e π'_1 são primos gaussianos, existe $u \in \{\pm 1, \pm i\}$ tal que $\pi'_1 = u\pi_1$. Logo, π_1 e π'_1 são primos gaussianos associados e podemos escrever $\alpha = \pi_1\beta$, em que $\beta = \pi_2 \cdots \pi_r = u\pi'_2 \cdots \pi'_s$. Aplicando a hipótese de indução, temos que β é um primo gaussiano ou, a menos da ordem e de elementos associados, pode ser fatorado de forma única como produto de primos gaussianos, pois $N(\beta) = N(\alpha)/N(\pi_1) < N(\alpha) = n$. Isso conclui a demonstração. \square

Exemplo 9. O inteiro gaussiano $7 - 3i$ é múltiplo de $1 + i$, pois $N(7 - 3i) = 58$ é par (Corolário 1). Como

$$\frac{7 - 3i}{1 + i} = \frac{7 - 3i}{1 + i} \cdot \frac{1 - i}{1 - i} = \frac{4 - 10i}{2} = 2 - 5i,$$

segue que $7 - 3i = (1 + i)(2 - 5i)$. Por outro lado, $1 + i$ e $2 - 5i$ são primos gaussianos, pois $N(1 + i) = 2$ e $N(2 - 5i) = 29$ são primos (Teorema 7). Logo, o Teorema 10 garante que, a menos da ordem, as fatorações não triviais de $7 - 3i$ são $7 - 3i = (1 + i)(2 - 5i)$, $7 - 3i = (1 - i)(5 + 2i)$, $7 - 3i = (-1 + i)(-5 - 2i)$ e $7 - 3i = (-1 - i)(-2 + 5i)$.

Teorema 11. *Se π é um primo gaussiano, então existe um primo positivo p tal que $\pi \mid p$.*

Demonstração. Seja π um primo gaussiano. Como $N(\pi) > 1$, segue do Teorema Fundamental da Aritmética que $N(\pi)$ pode ser expresso como um produto de primos positivos, ou seja, existem primos positivos p_1, \dots, p_r tais que $N(\pi) = p_1 p_2 \dots p_r$. Pela definição de norma, temos $N(\pi) = \pi \bar{\pi}$ e, com isso, sabemos que $\pi \mid N(\pi)$. Assim, temos que π é um primo gaussiano tal que $\pi \mid p_1 p_2 \dots p_r$. Portanto, pelo Teorema 9, segue que $\pi \mid p_j$, para algum $j \in \{1, \dots, r\}$. \square

Teorema 12. *Um primo positivo p é composto em $\mathbb{Z}[i]$ se, e somente se, pode ser expresso como uma soma de dois quadrados.*

Demonstração. Seja p um primo positivo. Se p é composto em $\mathbb{Z}[i]$, então existem inteiros gaussianos α e β tais que $p = \alpha\beta$, $N(\alpha) > 1$ e $N(\beta) > 1$. Aplicando a norma em ambos os lados da igualdade e usando a multiplicidade da norma, obtemos $p^2 = N(\alpha)N(\beta)$. Como p é um número primo positivo e $N(\alpha), N(\beta) > 1$, segue que $N(\alpha) = p$. Escrevendo $\alpha = a + bi$, com $a, b \in \mathbb{Z}$, temos que $p = N(\alpha) = a^2 + b^2$. Reciprocamente, suponha que existam inteiros a e b tais que $p = a^2 + b^2$. Considere o inteiro gaussiano $\alpha = a + bi$ e observe que $N(\alpha) = \alpha \bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2$. Logo, $p = (a + bi)(a - bi)$, em que $a + bi$ é um fator não trivial. Portanto, p é composto em $\mathbb{Z}[i]$. \square

Exemplo 10. O inteiro 5 é um primo positivo que é composto em $\mathbb{Z}[i]$ (Exemplo 8). Logo, pelo Teorema 12, 5 pode ser expresso como soma de dois quadrados ($5 = 1^2 + 2^2$).

Teorema 13. *Se um primo positivo p diferente de 2 é composto em $\mathbb{Z}[i]$, então ele pode ser expresso como produto de dois primos gaussianos, os quais são conjugados, possuem norma p e não são associados.*

Demonstração. Seja p um primo positivo composto em $\mathbb{Z}[i]$. O Teorema 12 garante que existem inteiros a e b tais que $p = a^2 + b^2 = (a + bi)(a - bi)$. Os elementos $a + bi$ e $a - bi$ possuem norma igual a p e, conseqüentemente, são primos gaussianos (Teorema 7). Como $a + bi$ e $a - bi$ são conjugados, resta mostrar que não são associados. Suponha, por absurdo, que $a + bi = \mu \cdot (a - bi)$, em que μ é uma unidade de $\mathbb{Z}[i]$. Se $\mu = 1$, então $a + bi = a - bi$. Logo, $b = 0$ e, conseqüentemente, $p = a^2$, o que nos leva a uma contradição, pois p é primo. Analogamente, se $\mu = -1$, então $a + bi = -(a - bi)$. Assim, $a = 0$ e, conseqüentemente, $p = b^2$, o que também é uma contradição. Se $\mu = i$ ou $\mu = -i$, temos $a + bi = i(a - bi) = b + ia$ e $a + bi = -i(a - bi) = -b - ai$, respectivamente. Nesses casos, $b^2 = a^2$ e, com isso, $p = 2a^2$, o que é um absurdo, pois p é um primo diferente de 2. \square

Teorema 14. *Os associados de um primo gaussiano também são primos gaussianos.*

Demonstração. Seja π um primo gaussiano e μ uma unidade. Observe que $N(\mu\pi) = N(\mu)N(\pi) = N(\pi) > 1$. Suponha, por absurdo, que $\mu\pi$ seja um inteiro gaussiano composto. Logo, existem inteiros gaussianos α e β tais que $\mu\pi = \alpha\beta$ com $1 < N(\alpha) < N(\pi)$ e $1 < N(\beta) < N(\pi)$. Como μ é uma unidade, por definição, existe um inteiro gaussiano μ^{-1} tal que $\mu^{-1}\mu = 1$. Multiplicando ambos os lados da igualdade $\mu\pi = \alpha\beta$ por μ^{-1} , temos $\mu^{-1}\mu\pi = \mu^{-1}\alpha\beta$, isto é, $\pi = \mu^{-1}\alpha\beta$. Note que μ^{-1} é uma unidade, pois se aplicarmos a norma em ambos os lados da igualdade $\mu^{-1}\mu = 1$ e usarmos a

multiplicidade da norma, obtemos $N(\mu^{-1})N(\mu) = 1$, ou seja, $N(\mu^{-1}) = 1$. Logo, $\pi = (\mu^{-1}\alpha)\beta$ é uma fatoração não trivial de π , uma vez que $1 < N(\mu^{-1}\alpha) = N(\mu^{-1})N(\alpha) = 1 \cdot N(\alpha) = N(\alpha) < N(\pi)$, o que é um absurdo, pois π é um primo gaussiano. Portanto, $\mu\pi$ é um primo gaussiano. \square

O próximo resultado, que é do contexto de números inteiros, será de suma importância para a apresentação da demonstração de uma caracterização dos inteiros gaussianos em termos dos primos em \mathbb{Z} (Teorema 16). A notação $a \equiv b \pmod m$ significa que a e b sejam *congruentes* módulo m , isto é, $m \mid (a - b)$ em \mathbb{Z} .

Teorema 15. *Seja p um primo positivo. As seguintes condições são equivalentes:*

- i) $p = 2$ ou $p \equiv 1 \pmod 4$;
- ii) a congruência $x^2 \equiv -1 \pmod p$ possui uma solução;
- iii) existem inteiros a e b tais que $p = a^2 + b^2$.

Demonstração. Seja p um primo positivo.

i) \Rightarrow ii) Se $p = 2$, então $x = 1$ é solução da congruência $x^2 \equiv -1 \pmod p$. No caso em que $p \equiv 1 \pmod 4$, sabemos que existe um inteiro k tal que $p - 1 = 4k$. Considere então a fatoração polinomial $T^{p-1} - 1 = (T^{(p-1)/2} - 1)(T^{(p-1)/2} + 1)$ com coeficientes módulo p . O Pequeno Teorema de Fermat (ver [9]), garante que o polinômio do lado esquerdo da igualdade possui $p - 1$ raízes distintas módulo p , o que implica que o polinômio do lado direito também possui $p - 1$ raízes distintas módulo p . Como o polinômio $T^{(p-1)/2} - 1$ possui grau $(p - 1)/2$, ele tem no máximo $(p - 1)/2$ raízes módulo p . Logo, o polinômio $T^{(p-1)/2} + 1$ também deve possuir raízes módulo p , ou seja, existe inteiro c tal que $c^{(p-1)/2} + 1 \equiv 0 \pmod p$. Desse modo, temos $c^{[(4k+1)-1]/2} \equiv -1 \pmod p$, isto é $(c^k)^2 \equiv -1 \pmod p$. Isso mostra que $x = c^k$ é uma solução da congruência $x^2 \equiv -1 \pmod p$.

ii) \Rightarrow iii) Seja $x \in \mathbb{Z}$ tal que $x^2 \equiv -1 \pmod p$, isto é, $p \mid (x^2 + 1)$ em \mathbb{Z} . Considerando esta divisibilidade em $\mathbb{Z}[i]$, temos $p \mid (x + i)(x - i)$. Suponha, por absurdo, que p seja um primo gaussiano. Assim, pelo Teorema 9, $p \mid (x + i)$ ou $p \mid (x - i)$ em $\mathbb{Z}[i]$. Logo, existe um inteiro gaussiano $m + ni$, em que m e n são inteiros, que satisfaz $p(m + ni) = x + i$ ou $p(m + ni) = x - i$. Donde segue que $pn = 1$ ou $pn = -1$, o que é um absurdo, pois n é inteiro e p é primo. Portanto, p é composto em $\mathbb{Z}[i]$ e, pelo Teorema 12, p pode ser expresso como soma de dois quadrados.

iii) \Rightarrow i) Sejam a e b inteiros tais que $p = a^2 + b^2$. Se p é par, então $p = 2$. Por outro lado, se p é ímpar, então $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$. Vamos mostrar que $p \not\equiv 3 \pmod 4$. De fato, seja k um inteiro qualquer. Temos 4 possibilidades quando consideramos a congruência módulo 4. Se $k \equiv 0 \pmod 4$, então $k^2 \equiv 0 \pmod 4$. No caso em que $k \equiv 1 \pmod 4$, temos $k^2 \equiv 1 \pmod 4$. Se $k \equiv 2 \pmod 4$, vale que $k^2 \equiv 4 \pmod 4$ e, como $4 \equiv 0 \pmod 4$, temos $k^2 \equiv 0 \pmod 4$. Por fim, se $k \equiv 3 \pmod 4$, então $k^2 \equiv 9 \pmod 4$ e, conseqüentemente, $k^2 \equiv 1 \pmod 4$, pois $9 \equiv 1 \pmod 4$. Logo, $k^2 \equiv 0 \pmod 4$ ou $k^2 \equiv 1 \pmod 4$. Isso implica que ao somarmos os quadrados de dois inteiros nunca obteremos um inteiro congruente a 3 módulo 4. Portanto, $p = 2$ ou $p \equiv 1 \pmod 4$. \square

Agora apresentaremos uma caracterização dos primos gaussianos.

Teorema 16. *Dados dois inteiros a e b quaisquer, temos que:*

- i) a é um primo gaussiano se, e somente se, a é primo e $|a| \equiv 3 \pmod 4$;

ii) bi é um primo gaussiano se, e somente se, b é primo e $|b| \equiv 3 \pmod{4}$;

iii) Se a e b são ambos não nulos, $a+bi$ é um primo gaussiano se, e somente se, a^2+b^2 é primo.

Demonstração. Sejam a e b inteiros quaisquer.

i) Se a é um primo gaussiano, então $N(a) > 1$. Suponha, por absurdo, que a não seja primo. Como $a \neq 0$, $a \neq 1$ e $a \neq -1$ (pois $N(a) > 1$), temos que a é composto em \mathbb{Z} . Pelo Teorema 11, existe um primo positivo p tal que $a \mid p$. Como p é um primo positivo e a é um inteiro, segue que $a = \pm p$, ou seja, $|a|$ é um primo positivo. Isso mostra que a é primo. Agora, suponha por absurdo que $|a| \not\equiv 3 \pmod{4}$. Temos que $|a| \equiv 1 \pmod{4}$ ou $|a| = 2$, pois $|a|$ é um primo positivo. Pelo Teorema 15, $|a|$ pode ser escrito como soma de dois quadrados, ou seja, existem inteiros m e n tais que $|a| = m^2 + n^2 = (m+ni)(m-ni)$ e, conseqüentemente, $a = (m+ni)(m-ni)$ ou $a = -(m+ni)(m-ni)$. Como a é um primo gaussiano, seus únicos divisores são os triviais. Assim, $m^2 + n^2 = 1$, pois um dos fatores deve ter norma igual a 1. Logo, $a = \pm 1$ ou $a = \pm i$, o que é um absurdo, já que a é um primo gaussiano. Portanto, $|a| \equiv 3 \pmod{4}$. Reciprocamente, seja a um primo tal que $|a| \equiv 3 \pmod{4}$. Se $a > 0$, então $a \equiv 3 \pmod{4}$ e, pelo Teorema 15, a não pode ser expresso como uma soma de dois quadrados. Portanto, pelo Teorema 12, temos que a é um primo gaussiano. Se $a < 0$, então $|a| = -a$ e, com isso, $-a \equiv 3 \pmod{4}$. Como $-a > 0$, o caso anterior garante que $-a$ é um primo gaussiano. Portanto, pelo Teorema 14, a também é um primo gaussiano, uma vez que é um associado de $-a$.

ii) Suponha bi um primo gaussiano. Observe que $bi(-i) = b$, ou seja, b é um associado de bi . Logo, b é um primo gaussiano (Teorema 14). Pelo Item (i), o inteiro b é primo e $|b| \equiv 3 \pmod{4}$. Reciprocamente, suponha que b seja primo e $|b| \equiv 3 \pmod{4}$. Assim, pelo item (i), segue que b é um primo gaussiano e, conseqüentemente, bi é um primo gaussiano (Teorema 14).

iii) Seja $a+bi$ um primo gaussiano, em que a e b são ambos não nulos. Suponha, por absurdo, que $a^2 + b^2$ seja composto em \mathbb{Z} . Pelo Teorema Fundamental da Aritmética, existem primos positivos q_1, \dots, q_n tais que $a^2 + b^2 = q_1 \cdots q_n$. Como $a^2 + b^2 = N(a+bi) = (a+bi)(a-bi)$, segue que $(a+bi) \mid q_1 \cdots q_n$. O Teorema 9 garante que existe $r \in \{1, \dots, n\}$ tal que $(a+bi) \mid q_r$, uma vez que $a+bi$ é um primo gaussiano. Suponha, sem perda de generalidade, que $q_1 = (a+bi)\beta$, com $\beta \in \mathbb{Z}[i]$. Como $q_1 \neq 0$, temos que $\beta \neq 0$. Se $N(\beta) = 1$, então q_1 e $a+bi$ são associados, o que não é possível, pois $q_1 \in \mathbb{Z}$, $a \neq 0$ e $b \neq 0$. Logo, $N(\beta) > 1$ e, conseqüentemente, q_1 não é um primo gaussiano, uma vez que β e $a+bi$ são fatores não triviais de q_1 . Assim, o Item i) garante que $q_1 = 2$ ou $q_1 \equiv 1 \pmod{4}$, pois q_1 é primo. Portanto, pelo Teorema 15, existem inteiros m e n tais que $m^2 + n^2 = q_1$, ou seja, $(m+ni)(m-ni) = q_1 = (a+bi)\beta$, com $m+ni$ e $m-ni$ primos gaussianos (pois $m^2 + n^2 = q_1$ é primo). Como $a+bi$ é um primo gaussiano, pelo Teorema 9, segue que $(a+bi) \mid (m+ni)$ ou $(a+bi) \mid (m-ni)$. Logo, $a+bi$ é associado de $m+ni$ ou de $m-ni$, pois $a+bi$, $m+ni$ e $m-ni$ são primos gaussianos. Conseqüentemente, $N(a+bi) = N(m+ni)$ ou $N(a+bi) = N(m-ni)$. Em ambos os casos, $a^2 + b^2 = m^2 + n^2 = q_1$, sendo $a^2 + b^2$ composto em \mathbb{Z} e q_1 é primo em \mathbb{Z} , o que é um absurdo. Portanto, $a^2 + b^2$ é primo em \mathbb{Z} . Reciprocamente, suponha que $N(a+bi) = a^2 + b^2$ é um primo em \mathbb{Z} e note que, pelo Teorema 7, segue que $a+bi$ é um primo gaussiano. \square

Exemplo 11. Os Itens i) e ii) do Teorema 16 garantem que 3 , -3 , $3i$ e $-3i$ são primos gaussianos. O Item iii) do mesmo teorema garante que $\pm 1 \pm 2i$ e $\pm 2 \pm i$ são primos gaussianos, pois possuem norma igual a 5. Não existem outros primos gaussianos de norma igual 5, conforme pode-se verificar na Figura 7. Quais são os primos gaussianos de norma menor ou igual a 60? O Teorema 16 fornece a resposta dessa pergunta. São os elementos de norma igual a $p^2 \leq 60$, em que p é um primo positivo congruente a 3 módulo 4 (isto é, $p = 3$ ou $p = 7$), e os de norma igual a $p \leq 60$, onde p é um primo que pode ser escrito como soma de quadrados de dois inteiros positivos (pelo Teorema 15,

$p = 2$ ou $p \equiv 1 \pmod{4}$, ou seja, $p \in \{2, 5, 13, 17, 29, 37, 41, 53\}$). Em outras palavras, são os inteiros gaussianos que pertencem à união das circunferências centradas na origem do plano complexo de raios $\sqrt{2}, \sqrt{5}, 3, \sqrt{13}, \sqrt{17}, \sqrt{29}, \sqrt{37}, \sqrt{41}, 7$ e $\sqrt{53}$. Os primos gaussianos de norma menor ou igual a 60 e as circunferências mencionadas estão ilustrados na Figura 7. Os elementos obtidos a partir dos itens i) e ii) do teorema estão destacados na cor verde e os caracterizados pelo item iii) estão destacados em vermelho. Na Tabela 1 estão listados os primos gaussianos de norma menor ou igual a 60.

Norma	Primos gaussianos
2	$1 + i, -1 - i, -1 + i$ e $1 - i$.
5	$1 + 2i, -1 - 2i, -2 + i, 2 - i, 1 - 2i, -1 + 2i, 2 + i$ e $-2 - i$.
9	$3, -3, 3i$ e $-3i$.
13	$2 + 3i, -2 - 3i, -3 + 2i, 3 - 2i, 2 - 3i, -2 + 3i, 3 + 2i$ e $-3 - 2i$.
17	$1 + 4i, -1 - 4i, -4 + i, 4 - i, 1 - 4i, -1 + 4i, 4 + i$ e $-4 - i$.
29	$2 + 5i, -2 - 5i, -5 + 2i, 5 - 2i, 2 - 5i, -2 + 5i, 5 + 2i$ e $-5 - 2i$.
37	$1 + 6i, -1 - 6i, -6 + i, 6 - i, 1 - 6i, -1 + 6i, 6 + i$ e $-6 - i$.
41	$4 + 5i, -4 - 5i, -5 + 4i, 5 - 4i, 4 - 5i, -4 + 5i, 5 + 4i$ e $-5 - 4i$.
49	$7, -7, 7i$ e $-7i$.
53	$2 + 7i, -2 - 7i, -7 + 2i, 7 - 2i, 2 - 7i, -2 + 7i, 7 + 2i$ e $-7 - 2i$.

Tabela 1: Primos gaussianos de norma menor ou igual a 60.

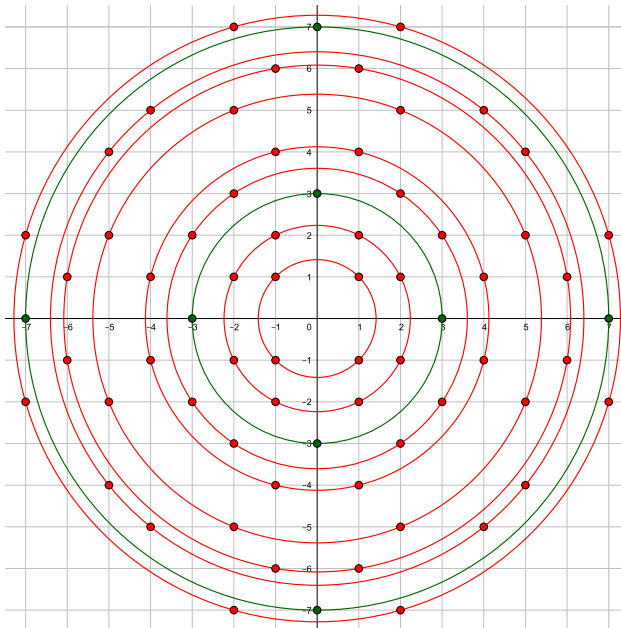


Figura 7: Primos gaussianos de norma menor ou igual a 60.

Observação 4. Os números primos de 1 até n podem ser determinados utilizando o Crivo de Eratóstenes. Para mais detalhes, confira a referência [5].

5. Aritmética Modular

Nesta seção apresentaremos uma breve introdução à aritmética modular em $\mathbb{Z}[i]$.

Definição 6. Sejam α , β e γ inteiros gaussianos, com γ não nulo. Dizemos que α é *congruente* a β módulo γ , e escrevemos $\alpha \equiv \beta \pmod{\gamma}$, quando $\gamma \mid (\alpha - \beta)$. Se $\gamma \nmid (\alpha - \beta)$, dizemos que α é *incongruente* a β módulo γ e escrevemos $\alpha \not\equiv \beta \pmod{\gamma}$.

Exemplo 12. Observe que $20 + 2i \equiv 6 + 5i \pmod{4 + 5i}$ (isto é, $4 + 5i \mid [(20 + 2i) - (6 + 5i)]$), pois

$$\frac{(20 + 2i) - (6 + 5i)}{4 + 5i} = \frac{14 - 3i}{4 + 5i} = \frac{(14 - 3i)(4 - 5i)}{(4 + 5i)(4 - 5i)} = \frac{41 - 82i}{N(4 + 5i)} = \frac{41 - 82i}{41} = 1 - 2i \in \mathbb{Z}[i].$$

Teorema 17. Sejam $\alpha, \beta, \mu, \delta, \theta$ e γ inteiros gaussianos, com γ não nulo. Temos que

- i) $\alpha \equiv \alpha \pmod{\gamma}$.
- ii) Se $\alpha \equiv \beta \pmod{\gamma}$, então $\beta \equiv \alpha \pmod{\gamma}$.
- iii) Se $\alpha \equiv \beta \pmod{\gamma}$ e $\beta \equiv \mu \pmod{\gamma}$ então $\alpha \equiv \mu \pmod{\gamma}$.
- iv) Se $\alpha \equiv \beta \pmod{\gamma}$ e $\delta \equiv \theta \pmod{\gamma}$, então $\alpha + \delta \equiv \beta + \theta \pmod{\gamma}$.
- v) Se $\alpha \equiv \beta \pmod{\gamma}$ e $\delta \equiv \theta \pmod{\gamma}$, então $\alpha \cdot \delta \equiv \beta \cdot \theta \pmod{\gamma}$.

Demonstração. A demonstração segue diretamente da Definição 6. □

Definição 7. Sejam α, β e γ inteiros gaussianos, com γ não nulo. Dizemos que β é um *resíduo* de α módulo γ se $\alpha \equiv \beta \pmod{\gamma}$.

Exemplo 13. O objetivo deste exemplo é determinar, ao menos, um resíduo de $4 + 3i$ módulo $3 + i$ cuja norma é menor do que a norma de $3 + i$. Dividindo $4 + 3i$ por $3 + i$, obtemos

$$\frac{4 + 3i}{3 + i} = \frac{(4 + 3i)(3 - i)}{N(3 + i)} = \frac{3}{2} + \frac{1}{2}i.$$

Aplicando o método implícito na demonstração do Teorema 6, encontramos os quocientes $1, 1 + i, 2, 2 + i$ e, respectivamente, os restos $1 + 2i, 2 - i, -2 + i, -1 - 2i$. Portanto, $4 + 3i$ é congruente a $1 + 2i, 2 - i, -2 + i$ e $-1 - 2i$ módulo $3 + i$, ou seja, $1 + 2i, 2 - i, -2 + i, -1 - 2i$ são resíduos de $4 + 3i$ módulo $3 + i$ que possuem a norma menor do que $N(3 + i)$.

Definição 8. Um conjunto de inteiros gaussianos $\{\beta_1, \dots, \beta_r\}$ é um *sistema completo de resíduos* módulo γ se são válidas as seguintes afirmações

- i) $\beta_i \not\equiv \beta_j \pmod{\gamma}$, se $i \neq j$.
- ii) Para todo inteiro gaussiano α tem-se $\alpha \equiv \beta_i \pmod{\gamma}$, para algum $i \in \{1, \dots, r\}$.

Teorema 18. Se $R = \{\beta_1, \beta_2, \dots, \beta_r\}$ e $S = \{\alpha_1, \alpha_2, \dots, \alpha_s\}$ são sistemas completos de resíduos módulo γ , então $r = s$.

Demonstração. Sejam $R = \{\beta_1, \beta_2, \dots, \beta_r\}$ e $S = \{\alpha_1, \alpha_2, \dots, \alpha_s\}$ sistemas completos de resíduos módulo γ . Suponha, por absurdo, que $r \neq s$ e assumamos, sem perda de generalidade, que $s > r$. Como R é um sistema completo de resíduos módulo γ , para cada $j \in \{1, 2, \dots, s\}$, existe um $i \in \{1, 2, \dots, r\}$ tal que $\alpha_j \equiv \beta_i \pmod{\gamma}$. Mas $s > r$ e, pelo Princípio da Casa dos Pombos (ver referência [9]), existem índices $j_1, j_2 \in \{1, 2, \dots, s\}$ distintos tais que $\alpha_{j_1} \equiv \beta_{i_0} \pmod{\gamma}$ e $\alpha_{j_2} \equiv \beta_{i_0} \pmod{\gamma}$ para algum $i_0 \in \{1, 2, \dots, r\}$. Desse modo, $\alpha_{j_1} \equiv \alpha_{j_2} \pmod{\gamma}$, com $j_1 \neq j_2$, o que é um absurdo, pois S é um sistema completo de resíduos módulo γ . Portanto, $r = s$. \square

Observação 5. O número de elementos de um sistema completo de resíduos módulo γ será denotado por $n(\gamma)$.

Para visualizar geometricamente elementos congruentes módulo β , basta plotar os inteiros gaussianos no plano complexo, destacar os múltiplos de β e, em seguida, revestir o plano por quadrados, de forma que os múltiplos de β sejam os vértices desses quadrados. Elementos congruentes módulo β estão localizados nas mesmas posições relativas dentro dos diferentes quadrados. Isso será ilustrado no próximo exemplo.

Exemplo 14. Seja $\beta = 3 + i$. Os múltiplos de β estão destacados em vermelho na Figura 8. Os pontos de mesma cor representam inteiros gaussianos congruentes módulo β enquanto que de cores diferentes representam elementos incongruentes módulo β . Qualquer conjunto que contenha exatamente um elemento de cada cor é um sistema completo de resíduos módulo β . Reciprocamente, qualquer sistema completo de resíduos contém exatamente um elemento de cada cor. Em cada um dos quadrados que revestem o plano complexo temos um sistema completo de resíduos. O número de elementos de qualquer sistema completo de resíduos módulo β é $n(\beta) = 10$.

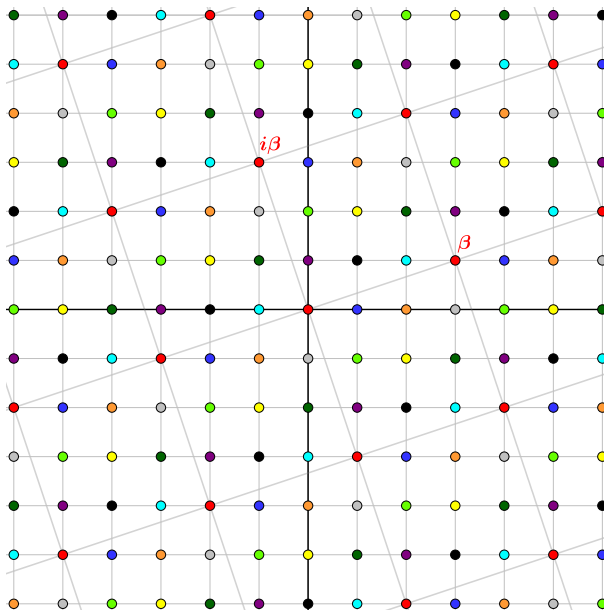


Figura 8: Aritmética módulo $3+i$

Uma curiosidade é que as dez cores estão presentes no eixo real. Isso significa que existe um sistema completo de resíduos módulo β que contém apenas números inteiros. Por exemplo, $\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$ é um sistema completo de resíduos módulo β . Isso não vale em geral e será abordado mais adiante (Exemplo 15 e Corolário 2).

Observação 6. Para $\beta = 3 + i$, tem-se $n(\beta) = N(\beta)$. Mostraremos que não se trata de uma coincidência, isto é, a igualdade é verdadeira para qualquer inteiro gaussiano não nulo (Teorema 22).

Teorema 19. *Sejam α e β inteiros gaussianos e γ um primo gaussiano. Temos que $\alpha\beta \equiv 0 \pmod{\gamma}$ se, e somente se, $\alpha \equiv 0 \pmod{\gamma}$ ou $\beta \equiv 0 \pmod{\gamma}$.*

Demonstração. Sejam α e β inteiros gaussianos e γ um primo gaussiano. Suponha que $\alpha\beta \equiv 0 \pmod{\gamma}$, isto é, $\gamma \mid \alpha\beta$. Pelo Teorema 9, temos que $\gamma \mid \alpha$ ou $\gamma \mid \beta$, ou seja, $\alpha \equiv 0 \pmod{\gamma}$ ou $\beta \equiv 0 \pmod{\gamma}$. Reciprocamente, se $\alpha \equiv 0 \pmod{\gamma}$ ou $\beta \equiv 0 \pmod{\gamma}$, então $\gamma \mid \alpha$ ou $\gamma \mid \beta$. Logo, $\gamma \mid \alpha\beta$ e, portanto, $\alpha\beta \equiv 0 \pmod{\gamma}$. \square

Teorema 20. *Sejam a, b e c inteiros, com $c > 1$. Então $a \equiv b \pmod{c}$ em \mathbb{Z} se, e somente se, $a \equiv b \pmod{c}$ em $\mathbb{Z}[i]$.*

Demonstração. Sejam a, b e c inteiros. Se $a \equiv b \pmod{c}$ em \mathbb{Z} , então $c \mid (a - b)$ em \mathbb{Z} . Como todo inteiro é um inteiro gaussiano, segue que $c \mid (a - b)$ em $\mathbb{Z}[i]$, ou seja, $a \equiv b \pmod{c}$ em $\mathbb{Z}[i]$. Reciprocamente, se $a \equiv b \pmod{c}$ em $\mathbb{Z}[i]$, então existe um inteiro gaussiano $\gamma = m + ni$ tal que $a - b = c(m + ni) = cm + cni$. Como a e b são inteiros, temos que $a - b$ é um inteiro e , consequentemente, $cm + cni$ é um inteiro. Logo, $cn = 0$ e, como $c \neq 0$, segue que $n = 0$. Assim, $\gamma = m + 0i$ é um inteiro, o que implica que $c \mid (a - b)$ em \mathbb{Z} . Portanto, $a \equiv b \pmod{c}$ em \mathbb{Z} . \square

Teorema 21. *Qualquer conjunto contendo $n(\alpha)$ elementos incongruentes módulo α é um sistema completo de resíduos módulo α .*

Demonstração. Considere o conjunto $\{\beta_1, \beta_2, \dots, \beta_{n(\alpha)}\}$, em que $\beta_i \not\equiv \beta_j \pmod{\alpha}$ sempre que $i \neq j$. Seja $\{\gamma_1, \gamma_2, \dots, \gamma_{n(\alpha)}\}$ um sistema completo de resíduos módulo α . Assim, para cada β_i , $1 \leq i \leq n(\alpha)$, temos que $\beta_i \equiv \gamma_j \pmod{\alpha}$ para algum $1 \leq j \leq n(\alpha)$. Note que cada γ_j está associado a um único β_i , uma vez que se $\beta_{i_1} \equiv \gamma_j \pmod{\alpha}$ e $\beta_{i_2} \equiv \gamma_j \pmod{\alpha}$, então $\beta_{i_1} \equiv \beta_{i_2} \pmod{\alpha}$ e, consequentemente, $i_1 = i_2$. Logo, como ambos os conjuntos possuem $n(\alpha)$ elementos, temos que para cada γ_j existe um β_i tal que $\gamma_j \equiv \beta_i \pmod{\alpha}$. Agora, seja δ um inteiro gaussiano qualquer. Como $\{\gamma_1, \gamma_2, \dots, \gamma_{n(\alpha)}\}$ é um sistema completo de resíduos módulo α , segue que $\delta \equiv \gamma_{j_0} \pmod{\alpha}$ para algum $1 \leq j_0 \leq n(\alpha)$. E, como $\gamma_{j_0} \equiv \beta_{i_0} \pmod{\alpha}$ para algum $1 \leq i_0 \leq n(\alpha)$, temos, pelo Teorema 17, que $\delta \equiv \beta_{i_0} \pmod{\alpha}$. Portanto, $\{\beta_1, \beta_2, \dots, \beta_{n(\alpha)}\}$ é um sistema completo de resíduos módulo α . \square

Lema 1. *Se m é um inteiro não nulo, então $n(m) = m^2$.*

Demonstração. Seja m um inteiro não nulo. Os elementos da forma $a + bi$, com $0 \leq a \leq m - 1$ e $0 \leq b \leq m - 1$, constituem um sistema completo de resíduos módulo m . Assim, como a e b podem assumir m valores cada, esse sistema completo de resíduos tem m^2 elementos. Portanto, $n(m) = m^2$. \square

Lema 2. *Se γ é um inteiro gaussiano não nulo, então $n(\bar{\gamma}) = n(\gamma)$.*

Demonstração. Seja γ um inteiro gaussiano não nulo. Congruências módulo γ podem ser convertidas em congruências módulo $\bar{\gamma}$ e vice-versa. De fato, sejam α e β inteiros gaussianos tais que $\alpha \equiv \beta \pmod{\gamma}$, temos que $\gamma \mid (\alpha - \beta)$. Assim, existe $\theta \in \mathbb{Z}[i]$ tal que $\alpha - \beta = \theta\gamma$. Donde segue que $\bar{\alpha} - \bar{\beta} = \bar{\theta}\bar{\gamma}$. Logo, $\bar{\gamma} \mid (\bar{\alpha} - \bar{\beta})$ e, conseqüentemente, $\bar{\alpha} \equiv \bar{\beta} \pmod{\bar{\gamma}}$. Isso mostra que $\alpha \equiv \beta \pmod{\gamma}$ se, e somente se, $\bar{\alpha} \equiv \bar{\beta} \pmod{\bar{\gamma}}$, uma vez que $\bar{\bar{z}} = z$ para todo $z \in \mathbb{C}$. A partir disso, podemos concluir que o conjunto formado pelos conjugados dos elementos de um sistema completo de resíduos módulo γ é um sistema completo de resíduos módulo $\bar{\gamma}$. Portanto, $n(\gamma) = n(\bar{\gamma})$. \square

Lema 3. Se α e β são inteiros gaussianos não nulos, então $n(\alpha\beta) = n(\alpha)n(\beta)$.

Demonstração. Sejam $\{x_1, \dots, x_r\}$ um sistema completo de resíduos módulo α e $\{y_1, \dots, y_s\}$ um sistema completo de resíduos módulo β , temos $n(\alpha) = r$ e $n(\beta) = s$. Vamos mostrar que o conjunto $\{x_i + \alpha y_j; 1 \leq i \leq r \text{ e } 1 \leq j \leq s\}$ é um sistema completo de resíduos módulo $\alpha\beta$. Seja γ um inteiro gaussiano qualquer. Como $\{x_1, \dots, x_r\}$ é um sistema completo de resíduos módulo α , segue que $\gamma \equiv x_i \pmod{\alpha}$, para algum $i = 1, \dots, r$. Assim, existe um inteiro gaussiano θ tal que $\gamma - x_i = \theta\alpha$. Além disso, como $\{y_1, \dots, y_s\}$ é um sistema completo de resíduos módulo β , temos que $\theta \equiv y_j \pmod{\beta}$, para algum $j = 1, \dots, s$. Logo, existe um inteiro gaussiano κ tal que $\theta - y_j = \beta\kappa$. Com isso, obtemos $\gamma - x_i = \alpha y_j + \alpha\beta\kappa$ e concluímos que $\gamma \equiv x_i + \alpha y_j \pmod{\alpha\beta}$, pois $\alpha\beta \mid [\gamma - (x_i + \alpha y_j)]$. Agora suponha que

$$x_i + \alpha y_j \equiv x'_i + \alpha y'_j \pmod{\alpha\beta}.$$

Nesse caso, temos $\alpha\beta \mid [(x_i + \alpha y_j) - (x'_i + \alpha y'_j)]$ e, conseqüentemente, $\alpha \mid [(x_i + \alpha y_j) - (x'_i + \alpha y'_j)]$. Assim, $x_i + \alpha y_j \equiv x'_i + \alpha y'_j \pmod{\alpha}$ e, como $\alpha y_j \equiv 0 \pmod{\alpha}$ e $\alpha y'_j \equiv 0 \pmod{\alpha}$, segue que $x_i \equiv x'_i \pmod{\alpha}$. Logo, $i = i'$, pois x_i e x'_i são elementos de um sistema completo de resíduos módulo α . Usando que $\alpha\beta \mid [(x_i + \alpha y_j) - (x'_i + \alpha y'_j)]$ e $x_i = x'_i$, temos que $\alpha\beta \mid [\alpha(y_j - y'_j)]$ e, conseqüentemente, $\beta \mid (y_j - y'_j)$. Ou seja, $y_j \equiv y'_j \pmod{\beta}$, o que implica que $j = j'$, pois y_i e y'_i são elementos de um sistema completo de resíduos módulo β . Portanto, $\{x_i + \alpha y_j; 1 \leq i \leq r \text{ e } 1 \leq j \leq s\}$ é um sistema completo de resíduos módulo $\alpha\beta$ e, conseqüentemente, $n(\alpha\beta) = rs = n(\alpha)n(\beta)$. \square

Teorema 22. Se γ é um inteiro gaussiano não nulo, então $n(\gamma) = N(\gamma)$.

Demonstração. Seja γ um inteiro gaussiano não nulo. O Lema 3 garante que $n(\gamma\bar{\gamma}) = n(\gamma)n(\bar{\gamma})$. Aplicando o Lema 2, obtemos $n(\gamma\bar{\gamma}) = n(\gamma)^2$. Por outro lado, o Lema 1 garante que $n(\gamma\bar{\gamma}) = (\gamma\bar{\gamma})^2 = N(\gamma)^2$, uma vez que $\gamma\bar{\gamma} = N(\gamma)$ é um número inteiro. Logo, $N(\gamma)^2 = n(\gamma)^2$. Como $N(\gamma)$ e $n(\gamma)$ são inteiros positivos (pois $\gamma \neq 0$), segue que $N(\gamma) = n(\gamma)$. \square

Teorema 23. Sejam a, b, d, j e ℓ inteiros, com $\text{mdc}(a, b) = d \geq 1$. Se $\beta = a + bi$ e $j \equiv \ell \pmod{\beta}$, então

$$j \equiv \ell \pmod{\frac{N(\beta)}{d}}.$$

Demonstração. Sejam a, b e d inteiros, com $\text{mdc}(a, b) = d \geq 1$. Assim, existem inteiros a' e b' tais que $a = a'd$, $b = b'd$ e $\text{mdc}(a', b') = 1$. Agora, sejam j e ℓ inteiros e $\beta = a + bi$ tais que $j \equiv \ell \pmod{\beta}$. Isto implica que existe um inteiro gaussiano θ tal que $j - \ell = \theta\beta$. Logo, como j e ℓ são inteiros, segue que $\theta\beta$ é um inteiro. Escrevendo $\theta = m + ni$, em que $m, n \in \mathbb{Z}$, temos que $\theta\beta = (m + ni)(a + bi) = (am - bn) + (an + bm)i$. Dessa forma, para que $(am - bn) + (an + bm)i$ seja um inteiro, é necessário que $an + bm = 0$, isto é, $an = -bm$. Donde segue que $a'n = -b'm$. Como a' e b' são primos entre si, existe um inteiro k tal que $m = ka'$ e $n = -kb'$. Logo, $\theta = m + ni = ka' - (kb')i = k(a' - b'i)$ e, conseqüentemente, $j - \ell = \theta\beta = k(a' - b'i)\beta = (k/d)(a - bi)\beta = [(k/d)\bar{\beta}]\beta = k \cdot N(\beta)/d$. Portanto, $j \equiv \ell \pmod{[N(\beta)/d]}$. \square

O próximo resultado garante, se $\beta = a + bi$ e $\text{mdc}(a, b) = 1$, a existência de um sistema completo de resíduos módulo β composto apenas por números inteiros e outro por inteiros gaussianos cuja parte real é igual a zero.

Corolário 2. *Seja $\beta = a + bi$ um inteiro gaussiano. Se $\text{mdc}(a, b) = 1$, então $\{0, 1, 2, \dots, N(\beta) - 1\}$ e $\{0, i, 2i, \dots, (N(\beta) - 1)i\}$ são sistemas completos de resíduos módulo β .*

Demonstração. Seja $\beta = a + bi$ um inteiro gaussiano, em que a e b são inteiros e $\text{mdc}(a, b) = 1$. Sejam $j, \ell \in \{0, 1, \dots, N(\beta) - 1\}$, com $j \neq \ell$. Temos que $j \not\equiv \ell \pmod{N(\beta)}$, pois $0 < |j - \ell| < N(\beta)$. Aplicando o Teorema 23, obtemos $j \not\equiv \ell \pmod{\beta}$. Isso mostra que os elementos do conjunto $\{0, 1, 2, \dots, N(\beta) - 1\}$ são dois a dois incongruentes módulo β . Como o número de elementos desse conjunto é $N(\beta)$, e $N(\beta) = n(\beta)$ (Teorema 22), o Teorema 21 garante que se trata de um sistema completo de resíduos módulo β . A prova da outra parte é trivial e será omitida. \square

O exemplo a seguir mostra que a hipótese do Corolário 2 (isto é, $\text{mdc}(a, b) = 1$) é necessária.

Exemplo 15. Seja $\beta = 2 + 2i$. Na Figura 9, de forma análoga ao Exemplo 14, os múltiplos de β estão destacados em vermelho, pontos de mesma cor representam inteiros gaussianos congruentes

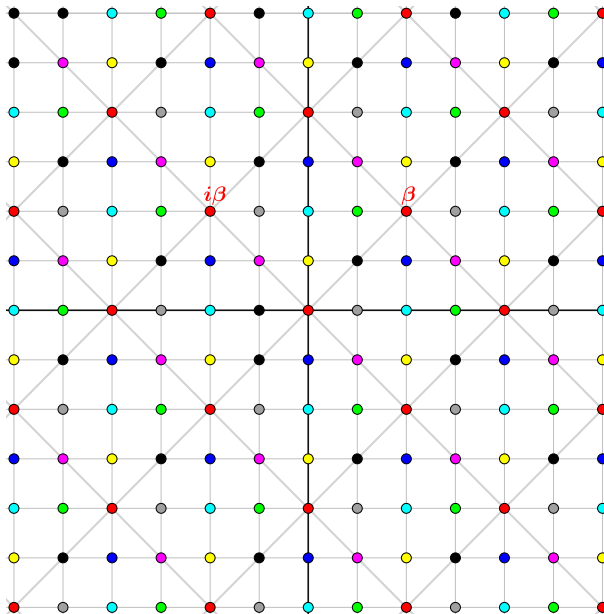


Figura 9: Aritmética módulo $2 + 2i$

módulo β enquanto que elementos de cores diferentes são incongruentes módulo β . O número de elementos de qualquer sistema completo de resíduos módulo β é $n(\beta) = 8$. Não existe um sistema completo de resíduos módulo β no eixo real (somente quatro cores no eixo real) e nem no eixo imaginário (somente quatro cores no eixo imaginário). Isso não contradiz o Corolário 2, uma vez que $\beta = 2 + 2i$ e $\text{mdc}(2, 2) = 2 \neq 1$.

Agradecimentos

Agradecemos aos pareceristas pelas importantes considerações, as quais contribuíram para o aprimoramento da versão final deste artigo.

Referências

- [1] Alves, L. C.; Strey, E. *Os Inteiros de Gauss*. Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 7, n° 1, 2020.4
- [2] Batista, P. H. A. *A teoria elementar dos inteiros de Gauss*. Dissertação (Mestrado Profissional em Matemática) - Instituto de Matemática e Estatística, Universidade Federal de Goiás, Goiânia, 2019.
- [3] Conrad, K. *The Gaussian Integers*. Disponível em: <<http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf>>. Acesso em: 13 de fevereiro de 2023.
- [4] Fujiwara, G. *Inteiros de Gauss e Inteiros de Eisenstein*. Eureka, n.14, p.23–31, 2002.
- [5] Hefez, A. *Curso de Álgebra*. vol. 1. 5ª ed. Coleção Matemática Universitária. Rio de Janeiro: IMPA. 2016.
- [6] Hefez, A. *Elementos de Aritmética*. Coleção Textos Universitários. Rio de Janeiro: SBM, 2006.
- [7] 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.
- [8] Moura, R. P.; Oliveira, E. J. T.; Strey, E. “Inteiros de Eisenstein”. *Revista Professor de Matemática Online (PMO)*, v. 10, n° 3, p.420–439, 2022. Disponível em: <<https://doi.org/10.21711/2319023x2022/pmo1030>>. Acesso em: 03 de maio de 2023.
- [9] Santos, J. P. O. *Introdução à teoria dos números*. Coleção Matemática Universitária. Rio de Janeiro: Impa. 1998.

Lídia Charra Alves
Universidade Federal do Espírito Santo
<lidia.charra.alves@gmail.com>

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

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

Recebido: 16/05/2023
Publicado: 25/08/2023