INTEIROS DE GAUSS:
os números primos complexos

Gabriela Moura Ferreira
Discente do Curso de Licenciatura em Matemática – Uni-FACEF
gabi.gabrielamouraferreira@gmail.com

Antônio Carlos da Silva Filho
Doutor em Física e Docente do Uni-FACEF
acdasf@bol.com.br

Resumo: Com o avanço matemático no decorrer dos anos, especificamente no campo de Teoria dos Números Algébricos, o conceito de números primos ultrapassou os campos dos conjuntos dos números Naturais e Inteiros. Entre 1808 e 1825, Carl F. Gauss definiu um conjunto, posteriormente denominado Inteiros de Gauss, onde se verifica a validade de propriedades que são usadas no domínio dos números inteiros e, ainda, possui propriedades específicas para trabalhar com seus elementos complexos. O artigo direciona o estudo do tópico, inicialmente com a definição de inteiros gaussianos, norma, unidade, divisão euclidiana, Lema de Euclides e fatoração única. Com os assuntos pontuais compreendidos, é feita a abordagem dos números primos complexos, suas definições e demonstrações.

Palavras-chave: Primos. Inteiros de Gauss. Primos de Gauss. Primos complexos.

1 Introdução

O estudo dos números primos tem seduzido os matemáticos ao longo destes últimos séculos. Uma das razões pelas quais o tema atingiu maior destaque é o atual problema matemático não resolvido considerado um dos mais importantes da história, a Hipótese de Riemann, apresentada pela primeira vez em 1859, elaborada por aquele de quem recebe o nome, o matemático alemão Bernhard Riemann.

> A hipótese de Riemann é o problema da longitude da matemática. Sua solução nos dará a perspectiva de mapear as águas nebulosas do grande oceano dos números, representando somente o início da nossa compreensão sobre esses elementos da natureza. Se conseguirmos desvendar o segredo da navegação pelos primos, quem sabe o que haverá mais além, ainda por descobrir? (DU SAUTOY, 2004)

Diferente dos demais problemas matemáticos não comprovados, mas também não refutados, que usualmente recebem o nome de conjectura, o proposto por Riemann hoje é chamado de hipótese, pois sua prova validará diversos outros trabalhos, não somente na área de matemática, mas também na física e na

computação, que dependem exclusivamente da mesma para estarem provados, uma vez que também não foram refutados.

Desde os primórdios, os matemáticos identificaram a importância da classificação dos números de acordo com as propriedades que eles apresentam perante a natureza. Primeiramente, estabeleceu-se que os números inteiros são divididos em duas categorias: primos e compostos.

No conjunto dos números naturais, um número primo *p* é aquele que só pode ser dividido por *p* ou por *1*. Se aumentarmos o universo para o conjunto dos números inteiros, um número *p* será considerado primo se só puder ser dividido por *p*, *-p*, *1* ou *-1*. Os números compostos são aqueles formados pela multiplicação de números primos.

Inicialmente, os gregos se preocuparam em provar que os números inteiros só poderiam ser classificados desta maneira, pois não haveria nenhum número pária que não fosse primo ou composto. Em seguida, Euclides explica o que pode ser considerado como o primeiro momento brilhante de raciocínio matemático, a verdade simples e fundamental sobre os números primos: há um número infinito deles. Ele foi o responsável por demonstrar a maneira de se construir um número que não pudesse ser gerado por qualquer lista finita de primos que lhe fosse dada.

Ainda assim, por muitos anos a pergunta mais importante sobre os números primos foi, e ainda é: como saber qual será o próximo? De que maneira eles se comportam? Na tentativa de desvendar as propriedades dos números primos, entre 1808 e 1825, o célebre matemático Carl Friedrich Gauss, estava investigando propriedades relacionadas à reciprocidade cúbica e à reciprocidade quadrática. Durante o período, Gauss percebeu que determinados números complexos da forma $a + bi$, com a e b inteiros e $i = (-1)^{\frac{1}{2}}$, eram raízes de polinômios da forma $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$, onde todos os coeficientes dos termos $x^k, com\ 0 \leq k \leq n$, são números inteiros.

Homenageando Gauss, esses números complexos foram chamados posteriormente de números inteiros de Gauss ou números inteiros gaussianos. A forma como foram aplicados, em conjunto com o fato de muito da teoria de Euclides sobre as propriedades dos números inteiros poder ser transportada para a nova aplicação, foram essenciais para desencadear o vasto campo matemático conhecido como Teoria dos Números Algébricos. Neste campo, dos Inteiros de Gauss, pode-se

fazer uma generalização da definição dos números primos, que é (GETHNER et al., 1998):

(1) Se *a, b ≠ 0*, então *a + b*i* é um Primo de Gauss se, e somente se, $a^2 + b^2 = p$, onde *p* é um número primo no campo dos números inteiros;

(2) Um inteiro gaussiano da forma *a* ou *a*i*, com a pertencendo ao conjunto dos números inteiros, é um Primo de Gauss se, e somente se, *a* é um número primo e o resto da divisão do módulo de *a* por *4* for *3*.

2 Os Inteiros de Gauss

Em Teoria dos Números Algébricos, há uma importante classificação dos números em dois grupos, números algébricos e números transcendentes. Para que um número seja considerado algébrico ele deve ser raiz de uma equação polinomial da forma $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$ onde todos os coeficientes dos termos $x^k, com\ 0 \leq k \leq n$, são inteiros. Exemplos de números algébricos:

$$i \rightarrow x^2 + 1 = 0 \ ; \sqrt{2} \rightarrow x^2 - 2 = 0$$

Quando um número não atende à condição necessária para ser um inteiro algébrico, ele é classificado como número transcendente (PACCI e RODRIGUES, 2013). Todos os números transcendentes são números irracionais, porém a recíproca não é válida pois, como vimos no exemplo acima, $\sqrt{2}$ é um número irracional que ao mesmo tempo é um inteiro algébrico, comprovando que não necessariamente um número irracional será transcendente. Podemos citar como exemplos de números transcendentes o número de Euler (*e*), e o número π.

Os números Inteiros de Gauss estão contidos no conjunto dos números algébricos, ou seja, satisfazem a condição de serem raízes de uma equação polinomial com os coeficientes inteiros e, ainda, são números complexos específicos, que possuem parte real e parte imaginária pertencentes ao conjunto dos números inteiros, além da unidade imaginária *i* equivaler a $\sqrt{-1}$. A representação é feita pelo conjunto $Z_{[i]} = \{a + bi \ / \ a, b \in \mathbb{Z} \ e \ i^2 = -1\}$.

Os números inteiros gaussianos possuem algumas propriedades e particularidades de suma importância para o desenvolvimento do conceito de número primo complexo (COSTA, 2016). Dentre elas, verificaremos: Norma, Unidades, Divisão Euclidiana, Lema de Euclides e Fatoração Única.

A Norma, estabelece que: $\forall z \in \mathbb{Z}_+, N(z) = z.\bar{z}$, onde $\bar{z}$ é o conjugado do complexo z. Sabemos que para um determinado número complexo da forma $z = a + bi$, o conjugado dele é definido como $\bar{z} = a - bi$. E como dados dois números complexos da mesma forma pré-determinada, denominados *a* e *b*, temos que: $\overline{ab} = \bar{a}\,.\,\bar{b}$, então $N(a).N(b) = a.\bar{a}\,.\,b.\bar{b} = a.b.\bar{a}\,.\,\bar{b} = ab.\overline{ab} = N(ab)$ o que nos comprova a propriedade multiplicativa da norma.

Dentro do conjunto dos Inteiros de Gauss, todo elemento $z \neq (0,0)$ possui um inverso z' tal que $z.z^{-1} = 1$, o que implica em $N(z.z') = N(z).N(z') = 1$ como demonstraremos a seguir:

1- Considerando primeiramente que z.z'=1, temos que:

$$z.z' = 1 \rightarrow \overline{zz'} = 1 \rightarrow N(z.z') = (1)^2.(1)^2 = 1$$

2- Agora, considerando z=a+bi, ficamos com:

$$z' = \frac{a - bi}{a^2 + b^2}$$

$$|z|^2 = a^2 + b^2 = N(z)$$

$$|z'|^2 = \frac{a^2}{(a^2+b^2)^2} + \frac{b^2}{(a^2+b^2)^2} = \frac{1}{a^2+b^2} \Rightarrow N(z).N(z') = (a^2+b^2).\left(\frac{1}{a^2+b^2}\right) = 1$$

Assim, mostramos também que se N(z) = a^2+b^2 = 1, então teremos duas possibilidades de valores para a e b em $Z_{[i]}$, resultando em quatro possíveis números complexos que são unidade dos Inteiros de Gauss:

$$\begin{cases} a = \pm 1 \; e \; b = 0 \begin{cases} Z_1 = 1 \\ Z_2 = -1 \end{cases} \\ a = a \; e \; b = \pm 1 \begin{cases} Z_3 = i \\ Z_4 = -i \end{cases} \end{cases}$$

Portanto, $x \in Z_{[i]}$ é $unidade \leftrightarrow N(x) = 1$.

Tratando agora da Divisão Euclidiana, precisamos ter o conhecimento inicial do conceito de divisibilidade, que nada mais é que: para $a, b \in Z_{[i]}, a|b \; se \; \exists c \in Z_{[i]} \; tal \; que \; b = ac$. Partindo deste ponto, a existência de $q, r \in Z_{[i]}, \forall a, b \in Z_{[i]}, b \neq 0 / a = bq + r, sendo \; 0 \leq N(r) < N(b)$.

A demonstração se dá através da divisão de a por b, representada como b|a (lê-se b divide a), sendo que $a = x + yi \; e \; b = z + wi \; com \; x, y, z \; e \; w \in \mathbb{Z}$. Vejamos:

$$\frac{a}{b} = \frac{x+yi}{z+wi} = \frac{x+yi}{z+wi} \cdot \frac{z-wi}{z-wi} \Leftrightarrow \frac{xz - xwi + yzi - ywi^2}{z^2+w^2} = \frac{xz+yw}{z^2+w^2} + \frac{yz-xw}{z^2+w^2} i$$

Considerando que *m* é o inteiro mais próximo de $\frac{xz+yw}{z^2+w^2}$ e *n* o inteiro mais próximo de $\frac{yz-xw}{z^2+w^2}$ teremos que $\left|m - \frac{xz+yw}{z^2+w^2}\right|, \left|n - \frac{yz-xw}{z^2+w^2}\right| \leq \frac{1}{2}$ e ainda, considerando que $q = (m + ni)$ teremos:

$$r = a - bq = b\left(\frac{a}{b} - q\right) = b\left[\left(\frac{xz+yw}{z^2+w^2} + \left(\frac{yz-xw}{z^2+w^2}\right) i\right) - m + ni\right] \Rightarrow$$

$$\Rightarrow N(r) \leq N(b)\left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) = \frac{N(b)}{2} < N(b)$$

O Lema de Euclides nos diz que se *p* é um primo de Gauss, então sendo $a, b \in Z_{[i]}, p|ab \Rightarrow p|a \; ou \; p|b$ (PISSINI e MAIOCHI, 2013). Para que um número seja primo de Gauss, é necessário que o mesmo não possa ser escrito na forma de produto entre de dois inteiros de Gauss cujas normas sejam maiores que 1. Estando compreendida a divisão euclidiana, é possível realizar a demonstração do lema através de sucessivas aplicações da mesma.

Uma das propriedades mais utilizadas para resolução de problemas com números inteiros, é a fatoração única, que pode ser provada para os inteiros gaussianos seguindo as etapas de, primeiramente, verificar que todo inteiro de Gauss z, com N(z) > 1, pode ser escrito como o produto de um ou mais primos de Gauss. Tomando N(z) = 2, temos o próprio 2 um número primo e pela norma ser multiplicativa, então z é um número primo.

Agora, ao considerarmos N(z) > 2, passamos a ter duas possibilidades. A primeira é, se z for um número primo, imediatamente temos a prova da fatoração. E, se z não for um número primo, ficaremos com:

$$z = a.b \Rightarrow N(z) = N(a).N(b) \; ; N(a) > 1 \; e \; N(b) > 1 \therefore N(a) < N(z) \; e \; N(b) < N(z)$$

Através de indução finita, podemos supor que se N(x) < N(z), teremos x um número fatorável, o que implica em a e b fatoráveis, assim como o próprio z. Gauss realizou a comprovação de que a fatoração é única para o anel dos gaussianos, assim como para os inteiros (SCHAFASCHEK, 2016). De forma sucinta,

temos as operações de adição e multiplicação, bem como a fatoração única, aplicáveis aos Inteiros de Gauss. Agora, se tratando de divisibilidade, a complexidade é maior, como entenderemos a seguir.

3 Os primos de Gauss

Para que possamos compreender quais números inteiros de Gauss apresentarão a característica de número primo de Gauss, é importante seguir o raciocínio de que, para um número *p* ser considerado primo, no conjunto $\mathbb{Z}$, ele precisa, necessariamente, ser divisível apenas por *p*, *-p*, *1* ou *-1*. Quando expandimos a possibilidade de que um número *p* seja primo, no conjunto $Z_{[i]}$, um número que é primo em $\mathbb{Z}$ pode não ser primo em $Z_{[i]}$. Veja o exemplo a seguir:

$$(1-2i).(1+2i) = 1+2i-2i-4i^2 = 1-4.(-1) = 1+4 = 5$$

O número 5, quando considerado no conjunto dos números inteiros, é um número primo, mas se o considerarmos dentro do conjunto dos inteiros gaussianos, como mostrado acima, não podemos classificá-lo como primo, uma vez que pode ser decomposto em um produto de dois inteiros de Gauss.

Por definição, um número inteiro de Gauss será um número primo de Gauss se, e somente se, dividir exatamente um primo inteiro (tanto o valor positivo, como seu oposto negativo), em $\mathbb{Z}$. Assim, tomaremos *p* como um primo inteiro e positivo e N(π) um primo, também em $\mathbb{Z}$. π é um primo de Gauss pois, se π é fatorável, N(π) também é fatorável. Temos três possíveis casos:

1- Se *p* é par, então só podemos ter *p* = 2 e, como π = a + bi, $a^2+b^2 = 2 \Leftrightarrow \pi = \pm 1 \pm i$, obtendo assim, o quatro números primos de Gauss: 1+i, 1-i, -1+i e -1-i.

2- Se *p* for ímpar e da forma $p \equiv 3(mód.4)$, teremos $x \in \mathbb{Z} \Rightarrow x^2 \equiv 0\ ou\ 1\ (mód.4)$ e, se existisse $\pi = c+di$, com c e d ∈ $\mathbb{Z}$ e $1 < N(\pi) < p^2$. Temos que $p = \pi\varphi$ e, por *p* ser um primo inteiro, $\varphi = c-di$. Levando a $p = c^2+d^2 \equiv 0,1\ ou\ 2\ (mód.4)$ o que é absurdo, uma vez que $p = 4k+3$. Assim, *p* é um primo de Gauss.

3- Se *p* for ímpar e da forma $p \equiv 1(mód.4)$, então, sendo $x = 1 \times 2 \times \ldots \times \frac{(p-1)}{2}$ teremos que $x^2 \equiv 1 \times 2 \times \ldots \times \frac{(p-1)}{2} \times 1 \times 2 \times \ldots \times \frac{(p-1)}{2} \equiv 1 \times 2 \times \ldots \times \frac{(p-1)}{2} \times \frac{(p+1)}{2} \times \ldots \times (p-2) \times (p-1) \equiv 1 \times (p-1) \equiv -1(mód.p)$. Logo, $p|x^2+1 = (x+i)(x-i)$. Como π é um

primo de Gauss que divide *p*, então $\pi \in \mathbb{Z}$, $\pi|x + i$ ou $\pi|x - i \Rightarrow \pi|1$, o que é um absurdo. Portanto $\pi \notin Z_{[i]}$ tal que $p = \pi\varphi$. Seja $\pi = a + bi$ e $\varphi = c + di$, com a, b, c, d $\in \mathbb{Z}$. Como p é primo em $\mathbb{Z}$, então mdc(a;b) = mdc(c;d) = 1. Temos $p = (a + bi)(c + di) = ac - bd + (bc + ad)i$. Como $p \in \mathbb{Z}$, então $bc = -ad \Rightarrow (a = c$ e $b = -d)$ ou $(a = -c$ e $b = d) \Leftrightarrow \varphi = \pm \pi$. Como $p > 0$, então $\varphi = \pi \Rightarrow N(\pi) = p$, logo π é primo (e π e seu conjugado são os únicos primos de Gauss que dividem *p*).

4 Considerações finais

Assim, concluímos que para um número inteiro de Gauss ser considerado um número primo de Gauss, ou seja, um número primo no domínio do Conjunto dos Complexos, $\mathbb{C}$, é necessário que aconteça uma das duas opções:

1- Se $a, b \neq 0$, então $a + b*i$ é um Primo de Gauss se, e somente se, $a^2 + b^2 = p$, onde *p* é um número primo no campo dos números inteiros;
2- Um inteiro gaussiano da forma *a* ou *a*i*, com a pertencendo ao conjunto dos números inteiros, é um Primo de Gauss se, e somente se, *a* é um número primo e o resto da divisão do módulo de *a* por *4* for *3*.

E, de todas as propriedades vistas a cerca do anel dos gaussianos, podemos apresentar da seguinte maneira, suas propriedades:

1- As unidades, ou seja, os elementos inversíveis são: ±1 e ±i;
2- O Domínio é Fatorial, ou seja, para qualquer que seja *a* pertencente ao domínio e não pertencente ao conjunto das unidades do domínio, pela comprovação da fatoração única para os inteiros gaussianos, mantém-se a integridade do domínio, sendo o mesmo irredutível, uma vez que a propriedade da fatoração única é válida;
3- Através da norma $N(a+bi) = a^2+b^2$ pode se tornar um Domínio Euclidiano, uma vez que o algoritmo de Euclides para a divisão pode ser aplicado.

Referências

CAMPOLINA PACCI, D.; TAKEUTI VAZ RODRIGUES, C. Inteiros de Gauss. Campinas: UNICAMP - Universidade Estadual de Campinas, 2013. Disponível em: https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/DC_M2_FM_2013.pdf. Acesso em: 09 de abril de 2021.

COSTA, Icoracy Coutinho da. *Inteiros de Gauss:* uma abordagem elementar. Manaus: Universidade Federal do Amazonas, 2016. Disponível em: https://tede.ufam.edu.br/handle/tede/5074. Acesso em 31 de outubro de 2021.

DU SAUTOY, Marcus. *A música dos números primos:* a história de um problema não resolvido na matemática. Tradução: Diego Alfaro. Rio de Janeiro: Jorge Zahar Ed., 2007.

GETHNER, E.; WAGON, S. & WICK, B. A Stroll Through the Gaussian Primes. The American Mathematical Monthlly, vol. 105, p. 327-337, 1998.

MORETTO PISSINI, Mariana., ALMEIDA MAIOCHI, Marina de. Inteiros de Gauss. Campinas: UNICAMP – Universidade Estadual de Campinas, 2013. Disponível em: https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/MM_M2_FM_2013.pdf. Acesso em: 18 de julho de 2021.

SIMON SCHAFASCHEK, Gabriel. Uma introdução ao estudo dos números algébricos. Florianópolis: UFSC – Universidade Federal de Santa Catarina, 2016. Disponível em: https://www.escavador.com/sobre/560614278/gabriel-simon-schafaschek. Acesso em: 12 de setembro de 2021.