RELIMAT
Revista Eletrônica do Curso de Licenciatura em Matemática

Uni-FACEF
Centro Universitário Municipal de Franca

OS NÚMEROS PRIMOS:

uma análise no campo dos complexos

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

Letícia Faleiros Chaves Rodrigues
Mestre em Matemática Universitária e Docente do Uni-FACEF
leticia@facef.br

RESUMO

O trabalho tem como tema uma análise a respeito dos números primos quando sua definição é ampliada para o conjunto dos complexos, que foi escolhido considerando a trajetória histórica de estudos matemáticos sobre o assunto, como por exemplo a Hipótese de Riemann, que é considerada como o problema não resolvido mais importante e cuja a resolução, além de ter consequências consideráveis para a ciência, oferta uma recompensa de um milhão de dólares americanos para aquele que conseguir solucioná-la. Tem-se como principal objetivo, analisar uma seleção de primos complexos e comparar seus comportamentos ao serem dispostos no plano, a fim de buscar possíveis padrões relacionados aos seus distanciamentos adjacentes. Assim, foram escolhidos autores que tratam da obra de renomados matemáticos que possuem contribuições significativas sobre o tema, como Churchill (1975), Endler (1986) e Santos (2020), além de pesquisadores da história da Matemática, como Boyer (1996), Du Sautoy (2004) e Viana (2022). Inicialmente fez-se breve abordagem histórica, com a finalidade de apresentar os estudiosos de épocas diferentes que já se dedicavam à busca de compreender os números primos. Na sequência, trata-se dos conceitos principais de Teoria dos Números Algébricos e de Inteiros de Gauss. Por fim, foram selecionados e mapeados alguns números primos complexos que tiveram sua disposição e comportamento analisados.

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

ABSTRACT

The work has as theme an analysis about prime numbers when its definition is extended to the set of complexes, which was chosen considering the historical trajectory of mathematical studies on the subject, such as the Riemann Hypothesis, which is considered the most important unsolved problem and whose resolution, besides having considerable consequences for science, offers a reward of one million U.S. dollars for those who can solve it. The main objective is to analyze a selection of complex primes and compare their behavior when arranged in the plane, in order to search for possible patterns related to their adjacent distances. Thus, authors were chosen who deal with the work of renowned mathematicians who have significant contributions on the subject, such as Churchill (1975), Endler (1986) and Santos (2020), as well as researchers in the history of mathematics, such as Boyer (1996), Du Sautoy (2004) and Viana (2022). Initially, a brief historical approach was made, in order to present the scholars from different times who were already dedicated to the search of understanding prime numbers. In the sequence, the main concepts of Algebraic Number Theory and Gauss' Integers were addressed. Finally, it was selected and mapped some complex prime numbers that had their disposition and behavior analyzed.

Keywords: Primes. Riemann Hypothesis. Gauss integers. Gauss primes. Complex primes.

1 INTRODUÇÃO

Este Trabalho de Conclusão de Curso tem como temática os números primos complexos, um tópico dentro de Teoria dos Números Algébricos, estudado pela Matemática Pura. O objetivo principal é mapear no plano complexo, conhecido também como Plano de Argand-Gauss, uma seleção de números primos complexos, analisando as distâncias entre seus adjacentes. Os objetivos específicos são mostrar a evolução dos estudos acerca dos números primos ao longo dos anos e apresentar conceitos importantes de Teoria dos Números Algébricos, dando destaque ao conjunto chamado Inteiros de Gauss.

A pesquisa se faz pertinente, uma vez que atualmente, com o avanço e praticidade que a tecnologia proporciona para a humanidade, existe uma grande preocupação com criptografia e proteção de dados, cuja base operacional está pautada na existência dos números primos. Assim, há um interesse geral em se compreender a natureza desses números específicos, e, para os matemáticos, uma necessidade histórica de desvendar o comportamento misterioso dessa classe natural de números.

No segundo capítulo, faz-se uma abordagem da trajetória histórica dos estudos matemáticos a respeito do assunto, desde os primórdios, com as primeiras descobertas, até as contribuições de maiores relevâncias, feitas nos últimos séculos.

No terceiro capítulo, apresenta-se alguns princípios, definições, proposições e teoremas considerados básicos pela Teoria dos Números, mais especificamente pelo ramo Elementar, mas que são de extrema importância para a compreensão de como foi estabelecido o conjunto numérico conhecido como Inteiros de Gauss e, posteriormente, os números primos complexos.

No quarto capítulo, trata-se da definição e de algumas propriedades específicas do conjunto dos Inteiros de Gauss, como a unidade, a norma, o Lema de Gauss e o Lema de Euclides, além de definir e esclarecer como podemos identificar os números primos de Gauss, pertencentes ao conjunto dos números complexos.

No último capítulo, realiza-se a seleção, mapeamento e análise da disposição de certos números primos de Gauss, no plano complexo, também conhecido como Plano de Argand-Gauss. Para esta etapa, foi utilizado o programa *RStudio* aplicando-se a linguagem de programação *R Language*, para a seleção dos

números, composição de gráficos e cálculos das distâncias os quais são apresentados e analisados.

Por fim, as considerações finais abordam as conclusões obtidas através do desenvolvimento deste trabalho, bem como possibilidades e sugestões para continuidade da pesquisa futuramente, em busca de melhorar os resultados aqui apresentados. As referências de pesquisa são apresentadas, conforme previsto pelas normas da ABNT.

2 OS NÚMEROS PRIMOS ATRAVÉS DOS TEMPOS

Os matemáticos têm sido atraídos pelo estudo dos números primos nos últimos séculos. Um dos motivos que levou o tema a atingir um destaque maior é a Hipótese de Riemann. Apresentada pela primeira vez em 1859, foi elaborada pelo matemático alemão Bernhard Riemann (1826 – 1866). Atualmente, é considerada por grande parte dos matemáticos como um dos problemas não resolvidos mais importantes da história.

> 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, p. 64-65)

Assim como vários outros matemáticos de sua época, Riemann estava interessado em compreender a natureza dos números primos. De maneira extremamente simplificada em comparação com sua magnitude, pode-se descrever sua hipótese como uma fórmula capaz de identificar todos os números primos existentes.

> Em 1859, Bernhard Riemann escreveu uma certa fórmula ζ(x), chamada função zeta. Ela já aparecera em trabalhos de Euler de 1740, mas Riemann estendeu a definição para os números x complexos, e mostrou que essa função nos diz muita coisa sobre os números primos. (VIANA, 2022, p. 1)

Uma peculiaridade a respeito da Hipótese de Riemann está na sua nomenclatura, pois, os demais problemas matemáticos que ainda não foram provados, mas também não foram refutados, convencionalmente recebem nome de conjecturas. Já o proposto por Riemann, é chamado de hipótese. Isto se deve ao fato de que diversos trabalhos, não somente na área de Matemática, mas também na Física e na Computação, foram desenvolvidos considerando que o trabalho de Riemann seja verdadeiro, mesmo que ainda não haja prova.

Inclusive, todos os trabalhos que não foram refutados e fazem uso da Hipótese de Riemann em seu desenvolvimento, dependem exclusivamente da prova para que sejam validados. Assim, a comprovação de que o proposto pelo matemático alemão há quase duzentos anos está certo, não só transformará a fórmula emteorema, como também vai garantir que os trabalhos que fizeram seu uso com a fé deque um dia a hipótese seja provada, sejam validados.

> Riemann sabia que existem muitos outros zeros [...]. Não sendo capaz de provar, aceitou esse fato como hipótese, deduzindo vários resultados a partir dele. Muitos matemáticos fizeram o mesmo desde então, resultando em dúzias de teoremas "provisórios", cuja validade depende de que alguém prove a hipótese. (VIANA, 2022, p. 1)

No entanto, não se deve cometer o equívoco de atribuir a descoberta da importância dos números primos a Riemann, uma vez que se tem conhecimento histórico de que os estudos matemáticos acerca do assunto, percorreram uma longa trajetória, iniciada centenas de anos antes de Cristo, com os gregos e com Euclides (século III a.C.). Destaca-se a seguir, alguns dos momentos e das descobertas principais a respeito, de suma importância para a compreensão da continuidade deste trabalho.

Desde os primórdios, já se compreendia e estudava a classificação dos números de acordo com as propriedades que eles apresentam diante da natureza. Inicialmente, os números inteiros foram classificados da seguinte forma: primos e compostos.

No princípio, os gregos tiveram a preocupação em garantir que não surgiria nenhum número pária, ou seja, um número que não fosse primo ou composto. A forma de provar, foi uma estratégia que posteriormente seria utilizada em várias outras provas matemáticas: supõe-se a existência de algo que se pretende provar que não existe e demonstra-se de fato porque ele não existe.

> Nosso estratagema inicial é um pouco ardiloso: supomos a existência das coisas que não queremos que existam e terminamos provando que elas não existem. Essa estratégia de pensar o impensável se tornou, para os gregos, uma ferramenta poderosa na construção de provas. Ela se baseia no fato lógico de que qualquer afirmação deve ser ou verdadeira ou falsa. Se supusermos que uma assertiva é falsa e chegarmos a uma contradição, poderemos inferir que nosso pressuposto estava errado e deduzir que a afirmação deveria ser, no fim das contas, verdadeira. (DU SAUTOY, 2004, p. 119)

Para o desenvolvimento desta estratégia, os gregos escolhiam um número como candidato a pária e, partindo do pressuposto de que todos os seus antecessores haviam sido verificados como primos ou compostos, concluía-se que o candidato não poderia ser um número pária.

Porém, o raciocínio era válido apenas para o valor escolhido e a intenção era garantir sua veracidade para todo e qualquer número existente. Então, os matemáticos da Grécia Antiga foram além, encontrando uma maneira de comprovar a inexistência de qualquer número pária:

> Os gregos compreenderam como poderiam transformar esse exemplo particular em um argumento mais geral, que pudesse ser aplicado a todos os números. É curioso notar que seu argumento se inicia fazendo-nos imaginar que *existem* números párias – aqueles que não são primos nem podem ser expressos pela multiplicação de primos. Se esses párias existem, então, ao caminharmos pela sequência de todos os números, em algum momento encontraremos o primeiro deles. (DU SAUTOY, 2004, p. 117-118)

Os gregos conseguiram um grande feito ao generalizar a ideia de que um número específico não é um pária, para a comprovação de que qualquer número existente, pode ser apenas primo ou composto. Posteriormente, esta prova foi nomeada como Teorema Fundamental da Aritmética. No capítulo seguinte, apresentaremos seu enunciado e demonstração.

Depois, o próximo grande avanço no assunto, foi com o matemático egípcio Euclides (século III a.C.). 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. De acordo com Du Sautoy (2004, p.120-121):

> A parte central dos Elementos de Euclides lida com as propriedades dos números; nela se encontra o que talvez seja o primeiro momento brilhante de raciocínio matemático. Na proposição 20, Euclides explica uma verdade simples, porém fundamental, sobre os números primos: há um número infinito deles.

Fazendo um comparativo com o estudo de Química, a tabela periódica de elementos químicos proposta por Mendeleiev (1834 – 1907), em 1869, conta atualmente com 118 elementos diferentes, de acordo com Novais (2022). Todamatéria é formada a partir destes. O que Euclides nos garante com sua prova, é que não há uma “tabela periódica” de números primos, responsáveis pela formação de todos os demais números, uma vez que existem infinitos números primos. Retomaremos este teorema na continuidade do trabalho.

A respeito de construir uma listagem de números primos, o matemático Eratóstenes de Cirene (século I a.C.), fez uma grande contribuição. Ele desenvolveu um algoritmo para, em um intervalo sequencial de números, filtrar quais são os primos. Este dispositivo é conhecido como Crivo de Eratóstenes, e foi fundamental para facilitar a identificação de números primos até determinado intervalo, na época em que não havia cálculos computacionais e o desenvolvimento matemático era realizado manualmente através de escrita.

> […] Com esse processo sistemático ele produziu tabelas de primos. Mais tarde, o procedimento passou a ser chamado de crivo de Erastótenes. Cada novo primo gerava um "crivo" que Erastótenes utilizava para eliminar os números não primos. O tamanho do crivo se alterava em cada etapa, mas ao atingir o número 1.000, somente os números primos resistiam a todos os crivos. (DU SAUTOY, 2004, p. 80-81)

Pelos milhares de anos seguintes à descoberta de Euclides, a Matemática foi evoluindo em diversas frentes, como Aritmética, Geometria, Álgebra e Cálculo. Mas ainda assim, a curiosidade sobre as características dos números em relação à sua natureza, prevaleceu. Durante muito tempo, inclusive, até os dias de hoje, as perguntas mais importantes sobre os números primos são: como saber qual será o próximo? De que maneira eles se comportam?

Diversos são os matemáticos que, ao pensar e tentar encontrar uma resposta para essas questões, fizeram outras descobertas e avanços correlacionados que, embora não respondam à pergunta principal, expandiram cada vez mais os conhecimentos matemáticos em direção ao objetivo principal. Ainda, temos os casos em que, ao buscar respostas para outras perguntas matemáticas, alguns chegaram em resultados que também contribuem para o estudo de números primos, principalmente com desenvolvimentos em funções, conjunto dos números complexos e Teoria dos Números Algébricos.

A partir do século XV, os maiores avanços matemáticos estavam centrados na Europa pré-guerra, principalmente na Alemanha, com grande destaque para a capital, Berlim, e para a cidade de Göttingen. Cita-se a seguir, alguns dos principais matemáticos, inclusive contemporâneos, que apresentaram contribuições, tanto diretas como paralelas, ao estudo dos números primos. A escolha deles foi realizada com base na relevância para o fomento dos estudos necessários ao desenvolvimento deste trabalho acadêmico.

Os italianos Scipione del Ferro (1465 – 1526), Niccolò Tartaglia (1500 – 1557), Girolamo Cardano (1501 – 1576), Lodovico Ferrari (1522 – 1565) e Rafael Bombelli (1526 – 1572), responsáveis por feitos como a resolução da equação cúbica, extensão da solução para a equação quártica e introdução dos números negativos e imaginários.

Os franceses Marin Mersenne (1588 – 1648) e Pierre de Fermat (1601 – 1655), contemporâneos que se correspondiam acerca de seus estudos. O primeiro é conhecido pelos seus estudos direcionados a encontrar uma fórmula para calcular

os números primos, denominada *Primos de Mersenne*. O segundo, além de contribuições significativas para a Física, elaborou teoremas que envolviam números primos, destacando-se o problema matemático que perdurou por mais tempo sem resolução na história, o *Último Teorema de Fermat*.

O também francês, René Descartes (1596 – 1650) que, juntamente com os suíços, Leonhard Euler (1707 – 1783) e Jean-Robert Argand (1768 – 1822) e o alemão Carl Friedrich Gauss (1777 – 1855), fizeram significativas contribuições para a estruturação matemática do conjunto dos números complexos e suas propriedades.

Resumidamente, a trajetória de estudos que estabeleceram esses novos números, teve início com o engajamento dos italianos em resolver a equação cúbica, mas sua evolução demandou mais algumas centenas de anos, além da junção de ideias de vários matemáticos.

A princípio, o italiano Cardano faleceu sem conseguir entender o paradoxo do caso irredutível, cuja reprodução é: quando

$$\left(\frac{p}{3}\right)^3 > \left(\frac{q}{2}\right)^2$$

a equação $x^3 = px + q$ tem três raízes reais, mas para aplicar o método de resolução, há a necessidade de lidar com raízes quadradas de números negativos.

Depois, Rafael Bombelli, em 1572 com a publicação de *L'algebra*, discorreu a respeito do papel desse novo tipo de número, mas sua natureza continuou misteriosa. O próximo avanço foi feito por Descartes, ao apelidar tais números de imaginários.

Então, o suíço Euler foi o responsável por usar a letra i para representar $\sqrt{-1}$ e Gauss chamou de complexos os números da forma a + bi. A aceitação do novo conjunto numérico foi consolidada quando Argand propôs sua representação como vetores no plano cartesiano, conhecido para os complexos como Plano de Argand-Gauss.

Por fim, antes de chegar a Bernhard Riemann (1826 – 1866), é relevante ressaltar que Gauss foi seu professor na Universidade de Göttingen, além de que, fez uma importante contribuição ao estudo dos números primos, uma fórmula capaz de determinar, em um dado intervalo sequencial, quantos seriam os primos.

> O grande avanço de Gauss foi fazer uma pergunta diferente. Em vez de tentar prever a localização precisa do próximo primo, ele buscou ao menos descobrir quantos primos haveria entre os primeiros 100 números, os primeiros 1.000 e assim por diante. (DU SAUTOY, 2004, p. 152)

Assim, quando Riemann chegou à universidade, além de ter Gauss, um dos maiores matemáticos da história, como professor, teve acesso aos estudos mais recentes da época, o que permitiu que desenvolvesse sua hipótese, na tentativa de unir os números complexos a um método que permitisse identificar quais são os primos e como eles se comportam, para que se descubra o posterior com base no conhecimento de seu antecessor.

> Posteriormente, ficaria claro que Euler tinha em mãos uma equação que romperia o impasse dos primos, mas seriam necessários outros cem anos, e outra grande mente, para demonstrar o que Euler não percebera. Essa mente pertencia a Bernhard Riemann. Entretanto, Gauss foi o responsável por inspirar a nova perspectiva de Riemann, introduzindo outro de seus clássicos passos laterais. (DU SAUTOY, 2004, p. 146-147)

Atualmente, cento e sessenta e três anos depois da formulação da Hipótese de Riemann, sabe-se que a importância de compreender os númerosprimos, deve ser vista em duas perspectivas diferentes: a sua relevância para a aplicação prática em diferentes áreas científicas, que proporcionam facilitadores aos seres humanos, e sua significância para os matemáticos. Para o segundo grupo, consiste em entender a base de toda a Matemática, os números.

> “Essa é uma pergunta que aparece muito na matemática pura”, disse a EXAME Augusto Teixeira, pesquisador do Instituto de Matemática Pura e Aplicada (IMPA). “Existem muitas áreas cujas descobertas às vezes não têm uma aplicação imediata, mas que continuam na ativa na esperança de que tudo se torne útil um dia.” Foi assim que começou com esses algarismos quando as pesquisas em torno deles foram iniciadas. (VIANA, 2019, p. 1)

Agora, quando se pensa em aplicação de números primos, a principal utilização está em criptografia e segurança de dados, tema cada vez mais recorrente na atualidade e indispensável para a continuidade dos avanços tecnológicos pelos quais a sociedade tem passado. De acordo com Viana (2022, p. 1):

> Por isso, esse problema aparece em todas as listagens de problemas matemáticos, desde a famosa lista de Hilbert no Congresso Internacional de Matemáticos de 1900, até os 7 problemas do Milênio, distinguidos pelo Instituto Clay com prêmios de US$ 1 milhão. Hilbert disse: “Se eu despertasse depois de ter dormido durante mil anos, a minha primeira pergunta seria: a hipótese de Riemann foi provada?”

Com um breve conhecimento a respeito da trajetória dos números primos no decorrer da história, veremos a seguir alguns teoremas e demonstrações que compõem o estudo de Teoria dos Números, fundamentais para a compreensão deste trabalho, já que serão exploradas as definições e propriedades dos números primos, ultrapassando o domínio para o conjunto dos complexos para análise.

3 CONCEITOS INTRODUTÓRIOS DE TEORIA DOS NÚMEROS

A Matemática é a ciência que estuda, por método dedutivo, objetos abstratos (números, figuras, funções) e as relações existentes entre eles. Com o passar dos séculos, a amplitude de descobertas e conhecimentos matemáticos, assim como os tópicos a serem investigados cientificamente, tornou-se cada vez maior, havendo a necessidade de ramificar e dividir as áreas de estudos matemáticos.

Dentre a vastidão de ramos está a Teoria dos Números, cujos algoritmos e demonstrações de seus princípios, leis e teoremas se fazem necessários para a compreensão dos capítulos seguintes. A Teoria dos Números tem seu objetivo bem definido e foi dividida em três ramos para estudo. De acordo com Santos (2020, prefácio) “o estudo das propriedades dos números inteiros positivos é o objetivo central da Teoria dos Números. São três os principais ramos em que se divide a Teoria dos Números: Teoria Elementar, Teoria Analítica e Teoria Algébrica”.

Os conceitos e demonstrações apresentados na sequência, são abordados pela Teoria Elementar e, apesar de serem considerados básicos, foram de extrema importância para a prova de diversos teoremas, evidenciando sua relevância nos estudos matemáticos.

3.1 PRINCÍPIO DA INDUÇÃO FINITA

O Princípio da Indução Finita é uma ferramenta indispensável para a demonstração de diversos teoremas. Para realizarmos a sua demonstração, o Princípio da Boa Ordem deve ser assumido como um postulado, uma vez que será a hipótese. A seguir, a definição do Princípio da Boa Ordem e uma das duas formas possíveis de se definir o Princípio da Indução Finita.

3.1.1 Princípio da Boa Ordem (PBO)

Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.

3.1.2 Primeira forma do Princípio de Indução Finita

Seja B um subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades

(i) $1 \in \mathrm{B}$

(ii) $k + 1 \in \mathrm{B}$

então B contém todos os inteiros positivos.

Deseja-se provar que se B é um subconjunto dos inteiros positivos, possuindo as propriedades (i) e (ii), então B, necessariamente, contém todos os inteiros positivos. A prova é por contradição.

Seja A o conjunto dos inteiros positivos não contidos em B. Pelo PBO, A possui um menor elemento e este é maior do que 1 pois $1 \in \mathrm{B}$. Seja a_0 este elemento. É claro que $a_0 - 1$ pertence a B e como B satisfaz (ii) então o sucessor de $a_0 - 1$, que é a_0, também deve pertencer a B. Esta contradição nos leva a concluir que A tem que ser vazio, o que conclui a demonstração.

3.2 DIVISIBILIDADE

Para demonstrarmos o Algoritmo da Divisão, escrito por Euclides em sua obra “Elementos”, por volta de 300 a.C., faz-se necessário a compreensão da definição, das proposições e do teorema que fundamentam a divisibilidade, além do Teorema de Eudoxius que “[...] costuma ser erroneamente atribuído a Arquimedes e chamado “Princípio de Arquimedes”.” de acordo com Santos (2020, p. 4). Vejamos a definição, as proposições e o teorema acerca de divisibilidade.

Definição 1: Se a e b são inteiros, diz-se que a divide b, denotando pôr a|b, se existir um inteiro c tal que b = ac. Se a não divide b escreve-se a∤b.

Proposição 1:

(i) Se a, b e c são inteiros, a|b e b|c, então a|c.

(ii) Se a, b, c, m e n são inteiros, c|a e c|b então c|(ma + nb).

Teorema 1 (Divisibilidade): a divisão tem as seguintes propriedades:

(i) n|n

(ii) d|n ⇒ ad|na

(iii) ad|an e a ≠ 0 ⇒ d|n

(iv) 1|n

(v) n|0

(vi) d|n e n ≠ 0 ⇒ |d| ≤ |n|

(vii) d|n e n|d ⇒ |d| = |n|

(viii) d|n e d ≠ 0 ⇒ (n/d)|n.

Teorema 2 (Eudoxius): dados a e b inteiros com b ≠ 0 então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e b ≠ 0 existe um inteiro q tal que, para b > 0,

$$qb \leq a < (q+1)b$$

e para b < 0,

$$qb \leq a \leq (q-1)b.$$

3.3 ALGORITMO DA DIVISÃO

Agora, tendo conhecimentos a respeito de divisibilidade, pode-se abordar o algoritmo da divisão.

Teorema 3: Dados dois inteiros a e b, b > 0, existe um único número par de inteiros q e r tais que

$$a = qb + r, \quad com\ 0 \leq r < b \quad (r = 0 \Leftrightarrow b|a)$$

(q é chamado de quociente e r de resto da divisão de a por b).

Demonstração: Pelo Teorema de Eudoxius, como b > 0, existe q satisfazendo:

$$qb \leq a < (q+1)b$$

o que implica

$$0 \leq a - qb \quad e \quad a - qb < b.$$

Desta forma, se definirmos r = a – qb, teremos, garantida, a existência de q e r. A fim de mostrarmos a unicidade, vamos supor a existência de outro par q_1 e r_1 verificando:

$$a = q_1 b + r_1 \quad com \quad 0 \leq r_1 < b.$$

Disto temos

$$(qb + r) - (q_1 b + r_1) = 0 \Rightarrow b(q - q_1) = r_1 - r,$$

o que implica

$$b|(r_1 - r).$$

Mas como

$$r_1 < b \text{ e } r < b,$$

Temos

$$|r_1 - r| < b$$

e, portanto, como $b|(r_1 - r)$ devemos ter $r_1 - r = 0$ o que implica $r = r_1$.

Logo

$$q_1 b = qb \Rightarrow q_1 = q,$$

uma vez que b ≠ 0.

3.3.1 Divisão Euclidiana

Teorema 4: Sejam $r_0 = a \; e \; r_1 = b$ inteiros não-negativos com b ≠ de 0. Se o algoritmo da divisão for aplicado sucessivamente para se obter

$$r_j = q_{j+1} r_{j+1} + r_{j+2}, 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0,1,2, \ldots, n-1 \; e \; r_{n+1} = 0 \; então \; (a,b) = r_n$, o último resto não-nulo.

Demonstração: Inicialmente, aplicaremos o teorema do algoritmo da divisão para dividir $r_0 = a$ por $r_1 = b$ obtendo $r_0 = q_1 r_1 + r_2$. Em seguida, dividimos r_1 por r_2 obtendo $r_1 = q_2 r_2 + r_3$ e assim, sucessivamente até a obtenção do resto $r_{n+1} = 0$.

Como, a cada passo o resto é sempre menor do que o anterior, e estamos lidando com números inteiros positivos, é claro que após um número finito de aplicações do teorema do algoritmo da divisão, teremos resto nulo.

Temos, pois, a seguinte sequência de equações:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 \quad 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \quad 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4 \quad 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0
\end{aligned}$$

3.4 CONGRUÊNCIA

A congruência é um tópico de Teoria dos Números desenvolvido por Gauss e publicado em sua obra de 1801 *Disquisitiones Arithmeticae*. Inclusive, a notação proposta por ele é a mesma utilizada até os dias de hoje.

Apresentaremos a seguir, três definições, três proposições e seis teoremas, indispensáveis para sua compreensão e posterior aplicação.

Definição 2: Se a e b são inteiros, dizemos que a é congruente a b módulo m (m > 0) se m|(a – b). Denotamos isto por a ≡ b (mod m). Se m ∤ (a – b) dizemos que a é incongruente a b módulo m e denotamos a ≢ b (mod m).

Definição 3: Se h e k são dois inteiros com h ≡ k (mod m), dizemos que k é um resíduo de h módulo m.

Definição 4: O conjunto dos inteiros $\{r_1, r_2, \dots, r_s\}$ é um sistema completo de resíduos módulo m se

(1) $r_i \not\equiv r_j (mod\ m)\ para\ i \neq j$

(2) Para todo inteiro n existe um r_i tal que $n \equiv r_i (mod\ m)$.

Proposição 2: Se a e b são inteiros, temos que $a \equiv b (mod\ m)$ se, e somente se, existir um inteiro k tal que $a \equiv b + km$.

Proposição 3: Se a, b, m e d são inteiros, m > 0, as seguintes sentenças são verdadeiras:

1. $a \equiv a (mod\ m)$
2. Se $a \equiv b (mod\ m)$, então $b \equiv a (mod\ m)$
3. Se $a \equiv b (mod\ m)$ e $b \equiv d (mod\ m)$, então $a \equiv d (mod\ m)$.

Proposição 4: Se a, b, k e m são inteiros com k > 0 e $a \equiv b (mod\ m)$, então $a^k \equiv b^k (mod\ m)$.

Teorema 5: Se a, b, c e m são inteiros, tais que $a \equiv b (mod\ m)$, então

1. $a + c \equiv b + c (mod\ m)$
2. $a - c \equiv b - c (mod\ m)$
3. $ac \equiv bc (mod\ m)$

Teorema 6: Se a, b, c, d e m são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então

1. $a + c \equiv b + d (mod\ m)$
2. $a - c \equiv b - d (mod\ m)$

3. $ac \equiv bd(mod\ m)$

Teorema 7: Se a, b, c e m são inteiros e $ac \equiv bc(mod\ m)$, então $a \equiv b(mod\ m/d)$ onde d = (c, m).

Teorema 8: Se k inteiros $r_1, r_2, \dots, r_k$ formam um sistema completo de resíduos módulo m então k = m.

Teorema 9: Se $r_1, r_2, \dots, r_m$ é um sistema completo de resíduos módulo m e a e b são inteiros com (a, m) = 1, então

$$ar_1 + b, ar_2 + b, \dots, ar_m + b$$

também é um sistema completo de resíduos módulo m.

Teorema 10: Se $a \equiv b\ (mod\ m_1), a \equiv b(mod\ m_2), \dots, a \equiv b(mod\ m_k)$ onde $a, b, m_1, m_2, \dots, m_k$ são inteiros com m_i positivos, i = 1, 2, ..., k, então

$$a \equiv b(mod[m_1, m_2, \dots, m_k])$$

onde $[m_1, m_2, \dots, m_k]$ é o mínimo múltiplo comum de $m_1, m_2, \dots, m_k$.

3.5 NÚMEROS PRIMOS

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

No capítulo anterior, citamos o fato de que os gregos provaram que um número é primo ou o produto de primos. É possível reproduzir o raciocínio empregado da seguinte maneira: a princípio considera-se o caso do número 612, o candidato a pária. Supõe-se que todos os números anteriores a 612 já foram verificados e são primos ou compostos. Propõe-se então, mostrar que 612 não é um número primo, expressando-o por meio de uma multiplicação entre fatores primos, como 4 x 153.

Nesta etapa, há o conhecimento de que 4 e 153 são números compostos, pois já foi verificado que os números menores que 612 atendem aclassificação da natureza dos números estabelecida. Escreve-se 4 como 2 x 2 e 153 como 3 x 3 x 17. Assim, o número 612 pode ser transcrito como 2 x 2 x 3 x 3 x 17. Aoassociar as informações conhecidas com as obtidas, conclui-se que 612 pode ser

expresso através da multiplicação entre fatores primos, o que o classifica como número composto, ou seja, não é um número pária.

Porém, o raciocínio apresentado é válido apenas para o número 612, e a intenção da prova é garantir a generalização de sua veracidade para todo e qualquer número existente. Os gregos foram além, encontrando uma maneira de comprovar a inexistência de qualquer número pária, através do raciocínio, segundo Du Sautoy (2004, p. 118), a seguir:

> Vamos chamá-lo de N (que é às vezes chamado de criminoso mínimo). Como esse número hipotético N não é primo, temos de ser capazes de expressá-lo pela multiplicação de dois números menores, A e B. Afinal, se isso não fosse possível, N seria primo. Já que A e B são menores que N, nossa escolha de N implica que A e B podem ser expressos como produtos de primos. Portanto, se multiplicarmos todos os primos que formam A e todos os primos que formam B, obteremos o número original, N. Neste momento, demonstramos que N pode ser expresso pela multiplicação de números primos, o que contradiz nossa escolha original de N. Portanto, nossa suposição inicial de que existem números párias não é defensável. Assim, todos os números devem ser primos ou gerados pela multiplicação de primos.

O procedimento acima, recebeu o nome de Teorema Fundamental da Aritmética, com uma definição bem elaborada, assim como apresentado por Santos (2020, p. 9) “Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos”.

Também no capítulo anterior, apresentamos a importância do feito de Euclides ao garantir que existem infinitos números primos. Tal descoberta recebeu o nome de Teorema de Euclides.

Definição 5: a sequência dos números primos é infinita.

Demonstração: Vamos supor que a sequência dos primos seja finita. Seja pois $p_1, p_2, \dots, p_n$ a lista de todos os primos. Consideramos o número

$$R = p_1.p_2 \dots p_n + 1.$$

É claro que R não é divisível por nenhum dos p_i de nossa lista e que R é maior do que qualquer p_i. Mas pelo Teorema Fundamental da Aritmética, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence à nossa lista. Portanto a sequência dos números primos não pode ser finita.

3.5.1 Crivo de Eratóstenes

Ao discorrer sobre os principais momentos históricos da Matemática a respeito do estudo dos números primos, no capítulo 2 deste trabalho, abordamos a

questão de elaborar listas de números primos a partir de um método sistemático, desenvolvido por Eratóstenes de Cirene, chamado de Crivo de Eratóstenes, assim como nos diz Boyer (1996, p. 110) "tendo dado contribuições a vários domínios do conhecimento, Eratóstenes é bem conhecido dos matemáticos pelo "crivo de Eratóstenes", um método sistemático para isolar os números primos".

O Crivo de Eratóstenes é uma importante aplicação prática, que foi desenvolvida de acordo com o seguinte teorema:

Teorema 11: Se n não é primo, então n possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{n}$.

Demonstração: Sendo n composto então $n = n_1.n_2$ onde

$$1 < n_1 < n \quad , \; 1 < n_2 < n$$

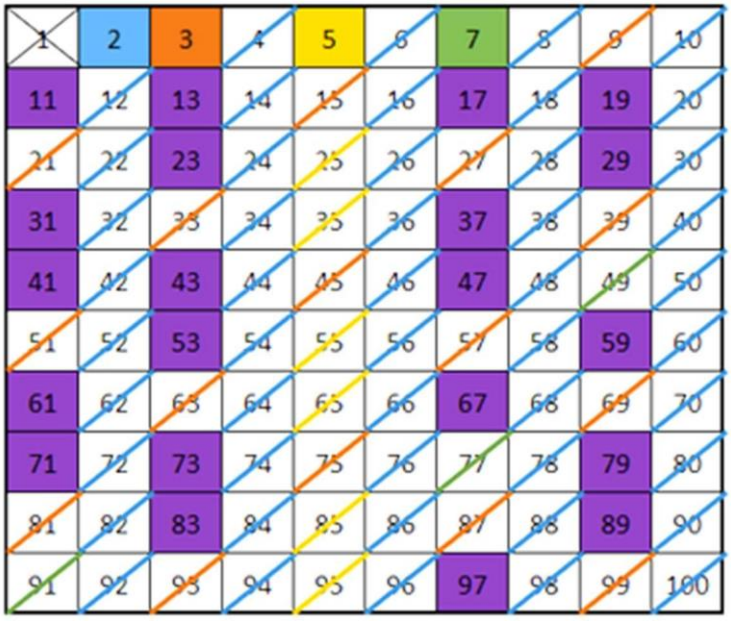
Sem perda de generalidade vamos supor $n_1 \leq n_2$. Logo n_1 tem que ser $\leq \sqrt{n}$ pois, caso contrário, teríamos $n = n_1.\, n_2 > \sqrt{n}.\, \sqrt{n} = n$ o que é absurdo. Assim, pelo Teorema Fundamental da Aritmética, n_1 possui algum fator primo p, este deve ser $\leq \sqrt{n}$. Como p, sendo um fator primo de n_1 é também um fator de n, a demonstração está completa.

A partir desse teorema, é possível concluir que, para testar se um número é primo, basta testar a divisibilidade apenas pelos primos $\leq \sqrt{n}$, o que nos leva ao Crivo de Eratóstenes que, segundo Boyer (1996, p. 110), tem seu funcionamento da seguinte forma:

> Com todos os números naturais dispostos em ordem, simplesmente são cancelados os números de dois em dois seguindo o dois, de três em três (na sequência de partida) seguindo o três, de cinco em cinco seguindo o cinco, e continua-se assim a cancelar cada *n*-ésimo número seguindo o número *n.* Os números restantes, de dois em diante, serão, é claro, primos.

Vejamos a seguir, uma representação visual de como realizar os procedimentos para a organização do crivo:

Figura 1 – Crivo de Eratóstenes



Fonte: OLIVEIRA, 2020, on-line.

Como podemos observar na imagem, o número 1, por convenção, não é primo. A partir do 2, faz-se o procedimento de eliminar todos os seus múltiplos. Depois, o mesmo processo é feito com o 3, que é o próximo número válido na sequência. Assim sucessivamente até que, neste caso específico da numeração de 1 a 100, após aplicar o método com o 7, restam apenas os primeiros 25 números primos conhecidos.

As primeiras listagens de primos conhecidas, foram formuladas com o uso do Crivo de Eratóstenes, em um período em que os matemáticos sequer imaginavam que seria possível realizar cálculos computacionais. A história relata que o interesse de Gauss pelos números primos foi aguçado justamente por uma dessas listas, que estava na contracapa de um livro de logaritmos.

> Na contracapa do livro que Gauss ganhara havia sido publicada uma tabela de números primos. A presença dos primos e logaritmos no mesmo livro era curiosa, pois Gauss percebeu, após cálculos extensos, que esses dois tópicos aparentemente desconexos pareciam estar relacionados. (DU SAUTOY, 2004, p. 148)

E graças à inspiração que uma lista de números primos em um livro de logaritmos despertou no jovem alemão, na época com 15 anos, é que seus estudos evoluíram muito além de qualquer perspectiva de seus professores, gerando contribuições fundamentais para a compreensão não só dos números primos, como também de diversos outros tópicos matemáticos desenvolvidos por ele, tornando-o assim, um dos maiores e mais importantes contribuintes da história da Matemática.

Inclusive, o assunto do próximo capítulo deste trabalho é justamente sobre um tópico matemático desenvolvido por Gauss e que se faz de extrema importância para chegarmos ao objetivo de analisar a distribuição gráfica de números primos complexos.

4 OS INTEIROS DE GAUSS

Durante o período entre 1808 e 1825, o matemático alemão Carl Friedrich Gauss, estava tentando desvendar algumas propriedades dos números primos, através de relações com as reciprocidades cúbicas e quadráticas. Percebeu então, 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.

Em homenagem a Gauss, esses complexos foram chamados de números inteiros de Gauss ou números inteiros gaussianos. A forma como foram aplicados, em conjunto com a possibilidade de transportar grande parte da teoria de Euclides sobre as propriedades dos números inteiros para a nova aplicação, foram essenciais para desencadear o vasto campo matemático conhecido como Teoria dos Números Algébricos.

Para definir os números Inteiros de Gauss, deve-se dizer que 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

$$Z_{[i]} = \{a + bi \ / \ a, b \in \mathbb{Z} \ e \ i^2 = -1\}.$$

Na Teoria dos Números Algébricos há uma importante classificação dos números em dois grupos, algébricos e transcendentes. Para que seja considerado algébrico, deve atender à definição de inteiro gaussiano, ou seja, 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) $i \Rightarrow x^2 + 1 = 0;$

(ii) $\sqrt{2} \Rightarrow x^2 - 2 = 0$

Quando um número não atende à condição necessária para ser um inteiro algébrico, ele é classificado como número transcendente (PACCI; 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:

(i) o número de Euler $e \cong 2{,}71828182845$

(ii) o número $\pi \cong 3{,}14159265359$

Os números inteiros de Gauss possuem algumas propriedades e particularidades de suma importância para o desenvolvimento do conceito de número primo complexo (COSTA, 2016). A princípio, define-se o que são estes inteiros gaussianos especiais e, depois, apresenta-se os principais conhecimentos necessários para a compreensão.

No campo dos inteiros de Gauss, pode-se fazer uma generalização da definição dos números primos, da seguinte forma (GETHNER et al., 1998):

(i) Se $a, b \neq 0$, então $a + bi$ 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;

(ii) Um inteiro gaussiano da forma a ou ai, com a pertencendo ao conjunto dos números inteiros, é um Primo de Gauss se, e somente se, a é um número primo e $a \equiv 3(mod\ 4)$

Apresentaremos a seguir, as seguintes propriedades dos inteiros de Gauss: Norma, Unidade, Divisão Euclidiana, Lema de Gauss, Lema de Euclides e Fatoração Única.

4.1 NORMA

A Norma é uma função definida com domínio nos inteiros gaussianos, utilizada para realizar comparações entre eles. Seu pape é muito importante, uma vez que as desigualdades são fundamentais no estudo das propriedades aritméticas e algébricas dos inteiros (PACCI; RODRIGUES, 2013).

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.

4.2 UNIDADE

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.

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

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

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) = a²+b² = 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 $unidade \Leftrightarrow N(x) = 1$.

4.3 DIVISÃO EUCLIDIANA

Tratando agora da Divisão Euclidiana, aplicada aos Inteiros de Gauss, precisamos ter o conhecimento inicial do conceito de divisibilidade, visto anteriormente, que nada mais é que:

$$a, b \in Z_{[i]}, a|b \; se \; \exists c \in Z_{[i]} \; tal \; que \; b = ac$$

Partindo deste ponto, temos 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

$$|m - \frac{xz + yw}{z^2 + w^2}|, |n - \frac{yz - xw}{z^2 + w^2}| \leq \frac{1}{2}$$

e ainda, considerando que $q = (m + ni)$ teremos:

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

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

4.4 LEMA DE GAUSS

O Lema de Gauss é um importante resultado acerca de números relativamente primos. Apresentaremos sua definição, porém, visto que para realizar a demonstração, faz-se necessário outros conceitos de Teoria dos Números que não foram abordados deste trabalho, a mesma não será feita.

Dados $a, b \text{ e } c \in \mathbb{Z}$. Se a|bc e (a, b) = 1, então a|c.

Além disso, se $a, b \, e \, c \in \mathbb{Z}$, com b e c não nulos, temos que

$$b|a \, e \, c|a \Leftrightarrow \frac{bc}{(b,c)}|a.$$

4.5 LEMA DE EUCLIDES

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 e o Lema de Gauss, é possível realizar a demonstração.

Para a = 0 e b = 0, o resultado é imediato. Agora, vamos provar para a ≠ 0 e b ≠ 0. Suponha que p∤a, então, (p, a) = 1. Como, por hipótese, p|ab, segue, pelo Lema de Gauss, que p|b.

Como resultado segue que, se $p, p_1, \ldots, p_n$ são primos e $p|p_1 \ldots p_n$, então $p = \pm p_i$ para algum $1 \leq i \leq n$.

4.6 FATORAÇÃO ÚNICA

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.

4.7 NÚMEROS PRIMOS COMPLEXOS

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 que serão abordados a seguir.

Na primeira situação, se p é par, só podemos ter p = 2 e, como π = a + bi, então

$$a^2 + b^2 = 2 \Leftrightarrow \pi = \pm 1 \pm i$$

obtendo assim, os quatro primeiros números primos de Gauss, sendo 1+i, 1-i, -1+i e -1-i.

No segundo caso, 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

$$\pi = c + di, \text{com c e d} \in \mathbb{Z} \text{ e } 1 < \mathrm{N}(\pi) < \mathrm{p}^2.$$

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.

Por fim, 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

$$x^2 \equiv (1 \times 2 \times \ldots \times \frac{(p-1)}{2}) \times (1 \times 2 \times \ldots \times \frac{(p-1)}{2}) \equiv$$

$$\equiv (1 \times 2 \times \ldots \times \frac{(p-1)}{2}) \times (\frac{(p+1)}{2} \times \ldots \times (p-2) \times (p-1)) \equiv$$

$$\equiv 1 \times (p-1)! \equiv -1(mód. p).$$

Logo,

$$p|x^2 + 1 = (x + i)(x - i).$$

Como □ é um primo de Gauss que divide p, então □ □ ℤ, □|x + i ou □|x - i □ □|1, o que é um absurdo.

Portanto □ □ $Z_{[i]}$ tal que p = □□.

Seja □ = a + bi e □ = c + di, com a, b, c, d □ ℤ .

Como p é primo em ℤ, então mdc(a;b) = mdc(c;d) = 1.

Temos p = (a + bi)(c + di) = ac – bd + (bc + ad)i.

Como p □ ℤ, então bc = –ad □ (a = c e b = – d) ou (a = –c e b = d) □ □ = □ □.

Como p > 0, então □ =□ □ N(□) = p, logo □ é primo (e □ e seu conjugado são os únicos primos de Gauss que dividem p).

Com a compreensão das possibilidades para que um número inteiro de Gauss seja considerado um número primo complexo, passaremos agora ao mapeamento de alguns destes primos, no plano cartesiano, a fim de buscar uma correlação entre suas distâncias e verificar se há algum padrão.

5 MAPEAMENTO DOS PRIMOS COMPLEXOS

O desenvolvimento deste capítulo do trabalho ocorreu em dois momentos distintos. No primeiro, foram escolhidos quais números primos de Gauss seriam dispostos no plano complexo. No segundo, realizamos os cálculos de distância entre cada primo selecionado e seu adjacente, com a finalidade de verificar possíveis padrões entre os dados obtidos.

5.1 MAPEAMENTO NO PLANO DE ARGAND-GAUSS

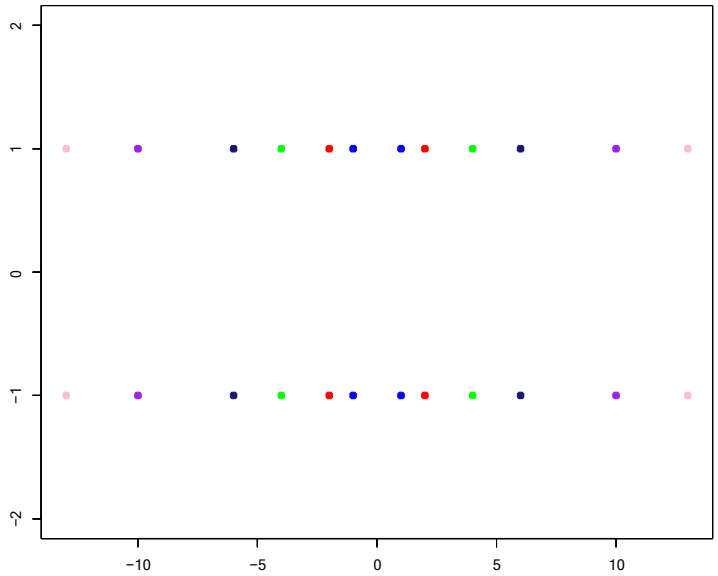
É importante recordar que, sendo os números primos complexos pertencentes ao conjunto dos inteiros de Gauss, apresentam sempre a forma $x = a + bi$. Ao dispormos no Plano de Argand-Gauss, o eixo horizontal representa a parte real e o eixo vertical a parte imaginária.

A fim de mapear os números primos de Gauss no plano complexo, primeiramente realizamos a seleção de alguns destes, pelo seguinte método: considere o número $x = a + bi$, onde $a \in \mathbb{Z}$ e $b = \pm 1$. Logo, temos os seguintes números primos de Gauss:

$$a^2 + b^2 = 2 \Longrightarrow \{(-1,-1);(-1,1);(1,-1);(1,1)\}$$
$$a^2 + b^2 = 5 \Longrightarrow \{(-2,-1);(-2,1);(2,-1);(2,1)\}$$
$$a^2 + b^2 = 17 \Longrightarrow \{(-3,-1);(-3,1);(3,-1);(3,1)\}$$
$$a^2 + b^2 = 37 \Longrightarrow \{(-4,-1);(-4,1);(4,-1);(4,1)\}$$
$$a^2 + b^2 = 101 \Longrightarrow \{(-10,-1);(-10,1);(10,-1);(10,1)\}$$
$$a^2 + b^2 = 197 \Longrightarrow \{(-13,-1);(-13,1);(13,-1);(13,1)\}$$
$$\vdots$$

Em seguida, realizamos a disposição no plano, conforme a figura:

Gráfico 1 - Disposição dos primos complexos onde $b = \pm 1$

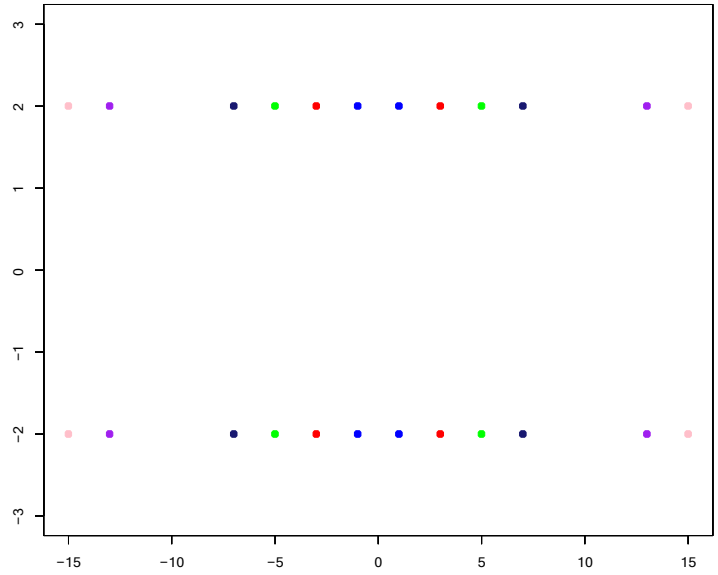


Fonte: elaborado pela autora.

Realizando o mesmo processo anterior, porém, considerando $b = \pm 2$, temos

$$a^2 + b^2 = 5 \Longrightarrow \{(-1,-2);(-1,2);(1,-2);(1,2)\}$$
$$a^2 + b^2 = 13 \Longrightarrow \{(-3,-2);(-3,2);(3,-2);(3,2)\}$$
$$a^2 + b^2 = 29 \Longrightarrow \{(-5,-2);(-5,2);(5,-2);(5,2)\}$$
$$a^2 + b^2 = 53 \Longrightarrow \{(-7,-2);(-7,2);(7,-2);(7,2)\}$$
$$a^2 + b^2 = 173 \Longrightarrow \{(-13,-1);(-13,1);(13,-1);(13,1)\}$$
$$a^2 + b^2 = 229 \Longrightarrow \{(-15,-1);(-15,1);(15,-1);(15,1)\}$$
$$\vdots$$

Gráfico 2 - Disposição dos primos complexos onde $b = \pm 2$

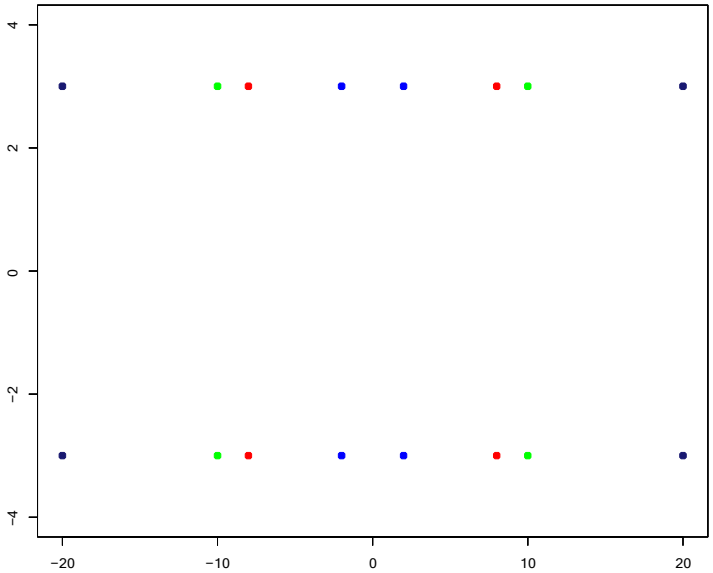


Fonte: elaborado pela autora.

Analogamente, considerando $b = \pm 3$, temos:

$$a^2 + b^2 = 13 \Longrightarrow \{(-2,-3);(-2,3);(2,-3);(2,3)\}$$
$$a^2 + b^2 = 73 \Longrightarrow \{(-8,-3);(-8,3);(8,-3);(8,3)\}$$
$$a^2 + b^2 = 109 \Longrightarrow \{(-10,-3);(-10,3);(10,-3);(10,3)\}$$
$$a^2 + b^2 = 409 \Longrightarrow \{(-20,-3);(-20,3);(20,-3);(20,3)\}$$
$$\vdots$$

Gráfico 3 - Disposição dos primos complexos onde $b = \pm 3$

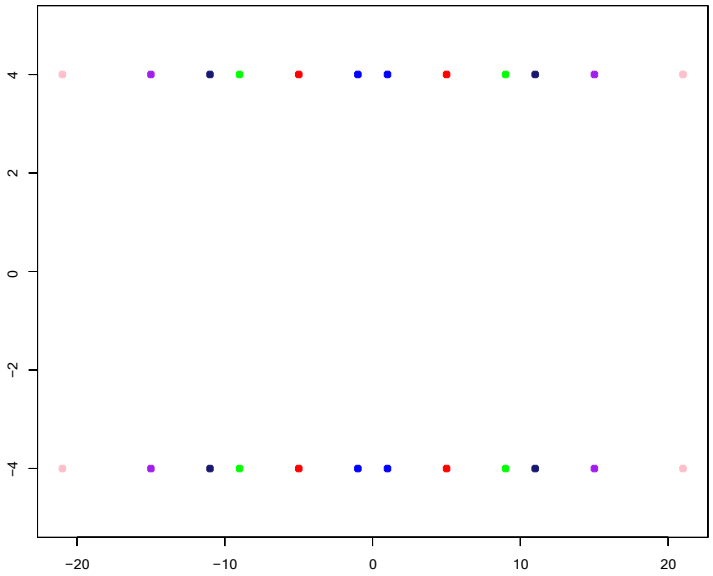


Fonte: elaborado pela autora.

Por fim, considerando $b = \pm 4$, temos:

$$a^2 + b^2 = 17 \Longrightarrow \{(-1,-4);(-1,4);(1,-4);(1,4)\}$$
$$a^2 + b^2 = 41 \Longrightarrow \{(-5,-4);(-5,4);(5,-4);(5,4)\}$$
$$a^2 + b^2 = 97 \Longrightarrow \{(-9,-4);(-9,4);(9,-4);(9,4)\}$$
$$a^2 + b^2 = 137 \Longrightarrow \{(-11,-4);(-11,4);(11,-4);(11,4)\}$$
$$a^2 + b^2 = 241 \Longrightarrow \{(-15,-4);(-15,4);(15,-4);(15,4)\}$$
$$a^2 + b^2 = 457 \Longrightarrow \{(-21,-4);(-21,4);(21,-4);(21,4)\}$$
$$\vdots$$

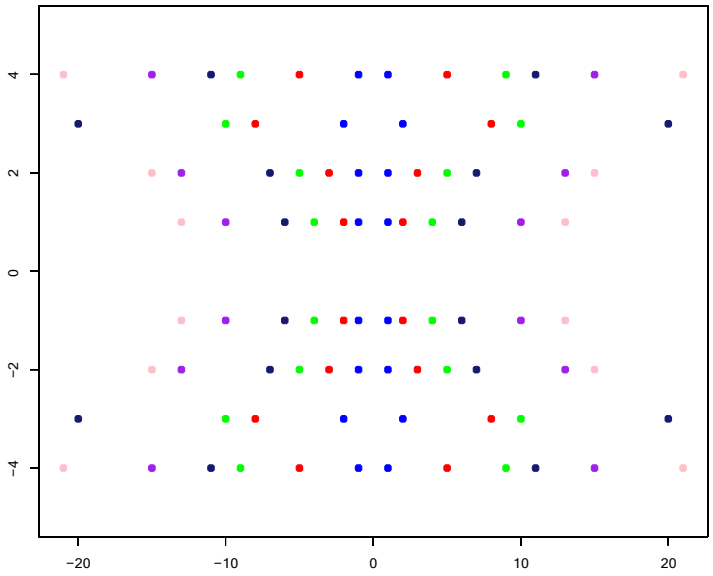
Gráfico 4 - Disposição dos primos complexos onde $b = \pm 4$



Fonte: elaborado pela autora.

Em seguida, será apresentado um único gráfico com todos os pontos gerados anteriormente, considerando os valores de $b \in \{\pm 1, \pm 2, \pm 3, \pm 4\}$.

Gráfico 5 - Disposição de todos os primos complexos gerados



Fonte: elaborado pela autora.

5.2 DISTÂNCIAS

Após mapear os números primos de Gauss no plano complexo, foram analisadas as distâncias *dp* entre um destes primos e o mais próximo primo adjacente.

Por exemplo, ao considerar $b = 1$, temos as seguintes coordenadas do número $x = a + bi$,

$$\{(1,1); (2,1); (4,1); (6,1); (10,1); (13,1); (16,1); (20,1); (24,1); (26,1); \cdots\}$$

Cuja a distância entre cada um destes números respectivamente, gera a sequência

$$\{1,2,2,4,3,3,4,4,2,10,4,14,2,10,8,10,6,4, \ldots\}$$

De maneira análoga, sendo $b = 2$, temos

$$\{(1,2); (3,2); (5,2); (7,2); (13,2); (15,2); (17,2); (27,2); (33,2); \cdots\}$$

Cuja a distância entre cada um destes números respectivamente, gera a sequência

$$\{2,2,2,6,2,2,10,6,2,2,10,6,2,2,8,2,10,8 \ldots\}$$

Para $b = 3$, temos

$$\{(2,3); (8,3); (10,3); (20,3); (32,3); (38,3); (40,3); (52,3); (58,3); \cdots\}$$

Cuja a distância é,

$$\{6,2,10,12,6,2,12,6,4,8,12,6,10, \cdots\}$$

Para $b = 4$, temos

$$\{(1,4); (5,4); (9,4); (11,4); (15,4); (21,4); (25,4); (29,4); (31,4); \cdots\}$$

Cuja a distância é,

$$\{4,4,2,4,6,4,4,2,10,8,2,4,10,10,4,2,8,2,4,4, \cdots\}$$

Quando analisamos as distâncias geradas entre os primos de Gauss adjacentes, é possível identificar o aparecimento de alguns padrões entre elas, inclusive, certos padrões que já foram verificados por diversos matemáticos ao analisarem os números primos convencionais, nos mostrando assim, que propriedades aplicáveis aos dois conjuntos podem implicar em comportamentos semelhantes, aparentemente.

A primeira verificação realizada foi de que, a distância entre dois primos complexos consecutivos será:

(i) um resultado ímpar em uma única situação, quando temos 1+i e 2+i, que gera distância 1. Similarmente, no conjunto dos números inteiros, a distância entre dois primos adjacentes só é ímpar quando temos 2 e 3.

(ii) um resultado par em todas as situações, com exceção à mencionada no item (i). Esta ocorrência é devido ao fato de que,

assim como entre os primos convencionais, quaisquer dois consecutivos maiores que 3 terem diferença par.

Outro padrão verificado, que também acontece no conjunto dos inteiros é que, conforme aumentamos a quantidade de números primos analisada, as distâncias apresentam a possibilidade de uma variação maior. Se observarmos as sequências de distâncias, dos casos 1, 2 e 4, podemos constatar que para obtermos um resultado de 10, precisamos verificar pelo menos cinco primos de Gauss consecutivos.

Por fim, compreendemos que, embora ao olhar os gráficos, seja possível visualizar que há uma simetria padronizada entre os pontos localizados, para estabelecermos mais relações entre a posição dos primos complexos selecionados, seriam necessários estudos mais avançados do tópico, além do uso de melhores técnicas de programação para validação das informações.

6 CONSIDERAÇÕES FINAIS

Ao chegar no final deste trabalho, mudanças significativas tanto em nível de conhecimento como em perspectivas aconteceram. Primeiramente, foi possível desenvolver um estudo mais aprofundado acerca da trajetória histórica dos números primos na Matemática, através dos séculos. Um dos aprendizados mais importantes, inclusive, fica explícito ao refletirmos sobre quantos avanços relevantes foram feitos por matemáticos que, a princípio tinham objetivos diferentes dos quais atingiram.

Em relação à motivação para a escrita deste, evidencia-se ainda mais o fato de que a Matemática é uma ciência sem fronteiras ou limites, onde se tem muitas descobertas brilhantes em diversas áreas a serem exploradas, com questionamentos a serem respondidos e hipóteses a serem provadas. E, ainda, por mais que se resolvam os problemas ainda não solucionados, sempre haverá espaço para outras perguntas e novas ideias.

Por fim, destacamos a possibilidade que ficou em aberto para, futuramente, dar sequência no estudo aqui iniciado, uma vez que os esforços empregados geraram resultados que a princípio, não trazem clareza a respeito da correlação entre o comportamento dos números primos no conjunto dos inteiros com os primos de Gauss no campo dos complexos e que, para melhorar a análise seja necessário maior entendimento de Teoria dos Números Algébricos, juntamente com recursos tecnológicos facilitadores de cálculos.

REFERÊNCIAS

BOYER, Carl B. *História da matemática.* Revisão: Uta C. Merzbach. Tradução: Elza F. Gomide. 2. ed. São Paulo: Edgard Blücher, 1996.

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.

CHURCHILL, Ruel Vance. *Variáveis complexas e suas aplicações.* Tradução: Tadao Yoshioka. São Paulo: McGraw-Hill do Brasil e Editora da Universidade de São Paulo, 1975.

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 17 de outubro de 2022.

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., 2004.

ENDLER, Otto. *Teoria dos Números Algébricos.* Rio de Janeiro: Instituto de Matemática Pura e Aplicada – IMPA, 1986.

EVES, Howard. *Introdução à história da matemática*. Tradução: Hygino H. Domingues. Campinas, SP: Editora da UNICAMP, 2004.

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.

NOVAIS, Stéfano Araújo. *Tabela Periódica*; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/quimica/tabela-periodica.htm. Acesso em 23 deoutubro de 2022.

OLIVEIRA, Victória. *Números primos e compostos: história, definição e relações*. Descomplica. Disponível em: https://descomplica.com.br/artigo/numeros-primos-e-compostos-historia-definicao-e-relacoes/VWC/. Acesso em 14 de outubro de 2022.

ROSA NETO, Ernesto. *Números complexos.* São Paulo: PAED – Pesquisa e Assessoria em Educação, 1980.

SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números.* 3.ed. Rio de Janeiro: IMPA, 2020.

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.

VIANA, Marcelo. *A pergunta secular de US$ 1 milhão.* Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/colunas/marceloviana/2022/02/a-pergunta-secular-de-us-1-milhao.shtml?origin=folha. Acesso em: 18 de setembro de 2022.