PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1021

Generalização do Mapa Logístico como estratégia de ensino de Sistemas Dinâmicos

Cássio Kiechaloski Correia de Mello André Fabiano Steklain Lisbôa

Resumo

Neste trabalho apresentamos diferentes alternativas ao Mapa Logístico para o estudo de Sistemas Dinâmicos unidimensionais. Entre as alternativas estão o Mapa Logístico Generalizado, o Mapa Trigonométrico e o Mapa Tenda. Propomos a possibilidade de explorar os mapas utilizando ferramentas computacionais acessíveis e gratuitas e mostramos que este estudo pode ser introduzido com limitações para alunos do Ensino Médio como complemento ao estudo de progressões numéricas. Os exemplos abordados permitem identificar características comuns e diferenças no comportamento dos sistemas com relação à presença de caos.

Palavras-chave: Sistemas Dinâmicos; Mapa Logístico; Expoente de Lyapunov; Ensino Médio

Abstract

In this work, we present different alternatives to the Logistic Map to study one-dimensional Dynamic Systems. The other options are the Generalized Logistic Map, the Trigonometric Map, and the Tent Map. We propose the possibility of exploring maps using accessible and free computational tools and show that this study can be introduced with limitations for high school students as a complement to the study of numerical progressions. The examples discussed allow us to identify common characteristics and differences in the behavior of systems regarding the presence of chaos.

Keywords: Dynamical Systems; Logistic Map; Lyapunov Exponent; High School

1. Introdução

O desenvolvimento da Teoria do Caos deveu-se principalmente à introdução do computador. Como explica Bentley [2], em 1961 Lorenz modelava um sistema de previsão climática usando um computador. Na impossibilidade de reiniciar a simulação com as mesmas condições iniciais, ele utilizava números ligeiramente diferentes, e os resultados obtidos eram completamente distintos. O efeito descoberto por Lorenz é hoje conhecido como *Efeito Borboleta*, pois, em suas palavras, "uma borboleta batendo asas no Brasil pode produzir um tornado no Texas". Esse efeito reflete uma das principais características de um sistema caótico, que é a alta sensibilidade às condições iniciais.

Apesar de atualmente o termo "caos" fazer parte do vocabulário popular, os conceitos matemáticos envolvidos ainda não são dominados pela maioria. Nesse sentido, cabe um esforço no sentido de adaptar a apresentação dos conceitos para que os estudantes do ensino médio possam compreendê-los a um nível que vai além da mera curiosidade, e, a partir disso, possam ser encaminhados para estudos mais avançados.

Para trabalhar nesta adaptação contamos com dois ingredientes fundamentais. O primeiro é o fato de sistemas simples apresentarem caos. Apesar de as aplicações rotineiras concentrarem-se em sistemas baseados em equações diferenciais (sistemas contínuos), é possível detectar a presença de caos em sistemas baseados em relações de recorrência (sistemas discretos). Isso permite que os estudantes do ensino médio possam compreender plenamente os sistemas em que estão trabalhando, além de encontrarem interseção com conteúdos tradicionalmente ministrados, tais como progressões numéricas.

O outro ingrediente é o desenvolvimento e popularização dos computadores. Nos dias de hoje é possível a todas as escolas contarem com um laboratório de informática a um baixo custo. Além disso existem diversas plataformas gratuitas, incluindo Planilhas Eletrônicas (*Google Sheets*), Sistemas de Geometria Algébrica (*Geogebra*) [10] e Sistemas de Computação Algébrica e Simbólica (*wxMaxima*) [9]. Tais sistemas permitem trabalhar conceitos matemáticos avançados permitindo cálculos rápidos e visualização de imagens de forma interativa, o que não seria possível de outra maneira.

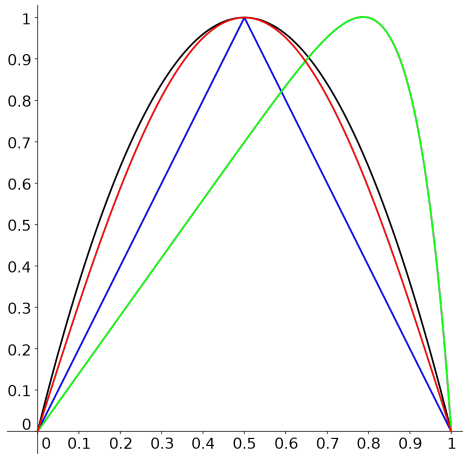


Figura 1: Funções investigadas neste artigo. Em preto, o Mapa Logístico. Em verde, o Mapa Logístico Generalizado com $\mu = 10$. Em vermelho, o Mapa Trigonométrico. Em azul, o Mapa Tenda.

Neste trabalho investigaremos a possibilidade de utilizar modelos que vão além do Mapa Logístico, que é um exemplo canônico normalmente utilizados na introdução à Teoria do Caos. Os modelos trabalhados estão ilustrados na Figura 1. Esses modelos são baseados na ideia central do Mapa Logístico, e preservam sua simplicidade, permitindo explorar a generalidade dos conceitos trabalhados. A ideia é utilizar o computador para fazer explorações numéricas que permitirão traçar paralelos e diferenças entre os diferentes modelos, para assim explorar quais propriedades são fundamentais em um sistema caótico. Neste trabalho não descreveremos os detalhes para a utilização das ferramentas computacionais, apenas mencionaremos quais podem ser utilizadas para cada caso. Para um roteiro mais detalhado da utilização de cada ferramenta, o leitor interessado pode consultar a dissertação de mestrado relacionada [3].

2. Mapa Logístico e Ferramentas Computacionais

O exemplo mais comum apresentado no estudo do caos é o Mapa Logístico, que possui raízes no estudo da dinâmica populacional. Diferentemente do Modelo Malthusiano, que cresce indefinidamente, o Mapa Logístico possui um limitador que pode ser explicado pelo fato de os recursos naturais serem finitos. Este sistema foi proposto inicialmente por Pierre François Verhulst e desenvolvido posteriormente por Robert May. Aqui reproduziremos em termos gerais a dedução dada por Villate [4]. Sendo P_n o número que

representa a população no instante n, introduzimos uma constante a referente à taxa de nascimentos e uma constante b referente à taxa de mortalidade em n. Nesse caso a população em um instante posterior $n+1$ é dada por

$$P_{n+1} = P_n + aP_n - bP_n^2. \tag{1}$$

Por esta expressão fica clara a impossibilidade de termos $a \leq -1$, o que implicaria $P_{n+1} \leq 0$, e portanto na extinção imediata da população. O fator b aparece multiplicado pelo quadrado de P_n, pois, de acordo com Cipolli [5], como "os recursos são limitados, haverá uma competição por eles, que é proporcional ao número de encontros entre os membros da espécie". Esse número de encontros é estimado como P_n^2. Rearranjando a Equação 1 de forma a isolar o fator comum P_n, temos:

$$P_{n+1} = (a+1)P_n\left(1 - \frac{bP_n}{a+1}\right). \tag{2}$$

Definindo a quantidade $r = a + 1$ e fazendo a troca de variáveis

$$x_n = \frac{b}{r}P_n, \tag{3}$$

obtemos a conhecida expressão do Mapa Logístico,

$$x_{n+1} = r \cdot x_n(1 - x_n). \tag{4}$$

Note que o Mapa Logístico possui uma única constante r que caracteriza cada sistema, e será a quantidade que definirá se o sistema é caótico ou não, como veremos posteriormente. O Mapa Logístico é uma fórmula de recorrência que permite obter a quantidade x_{n+1} a partir da quantidade x_n através da fórmula $x_{n+1} = f(x_n)$, sendo $f(x) = r \cdot x(1-x)$. Dessa forma precisamos conhecer apenas o valor inicial x_0 para obter todos os valores x_n. As sequências de valores $\{x_n\}$ são chamadas *órbitas* do sistema. Note que f é uma função quadrática com raízes em 0 e 1 e valor máximo em $x_{max} = 1/2$ dado por $f(x_{max}) = r/4$. Isso significa que restringindo r ao intervalo $(0, 4]$ se os valores iniciais são tais que $0 \leq x_0 \leq 1$, então todos os valores da órbita permanecerão no intervalo $[0, 1]$. Nesse caso diz-se que a órbita é limitada. Para analisar as diferentes órbitas geradas pela recorrência é interessante usar planilhas eletrônicas, pois dada uma célula é possível escrever uma fórmula que depende da célula anterior e usar o recurso de arrastar para obter os demais termos. Com este recurso é possível gerar rapidamente tantos valores quantos forem necessários e as órbitas podem ser rapidamente geradas e comparadas. Um exercício interessante é começar com diferentes condições iniciais e observar o comportamento das órbitas geradas para um mesmo valor de r.

As órbitas podem se comportar de diversas maneiras. Em alguns casos podemos ter $f(x_n) = x_n$ implicando que $x_{n+1} = x_n$. Tais pontos são chamados *pontos fixos*. No caso do Mapa Logístico a expressão $f(p) = p$ fornece $p = 0$ e $p = 1 - 1/r$, que são os únicos pontos fixos do Mapa Logístico, sendo que o último ocorre somente se $r > 1$. Nesse caso simples os pontos fixos podem ser obtidos, analiticamente, através da resolução da equação. Porém, em outros casos os pontos fixos podem ser estimados através de métodos numéricos ou, graficamente, analisando-se a interseção entre o gráfico de f e a reta $y = x$. Para essa tarefa é possível usar comandos do *wxMaxima* que fornecem soluções numéricas de uma equação ou o *Geogebra* para encontrar, graficamente, as interseções entre as curvas que fornecem os pontos fixos. O método gráfico está ilustrado na Figura 2 para o Mapa Logístico Generalizado, que será apresentado mais adiante.

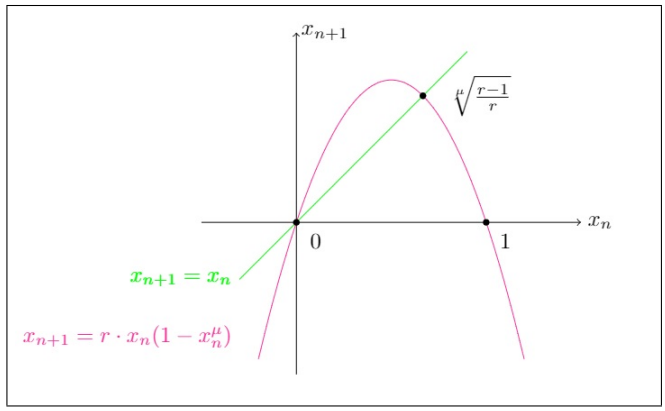


Figura 2: Pontos fixos do Mapa $x_{n+1} = rx_n(1 - x_n^{\mu})$. Note que os pontos correspondem à interseção entre o gráfico da função f e da reta $y = x$.

É interessante avaliar o que ocorre na vizinhança desses pontos, isto é, o que acontece com os termos seguintes a um determinado elemento que está próximo a um ponto fixo. Dentre as possibilidades, dois tipos de comportamento são destacados. A primeira possibilidade é que os valores seguintes fiquem cada vez mais próximos ao valor do ponto fixo. Nesse caso o ponto fixo é chamado *atrator*. A segunda possibilidade é que os valores seguintes afastem-se do valor do ponto fixo. Em tal caso, o ponto fixo é chamado *repulsor*. O Teorema do Ponto Fixo [7] permite estabelecer quando um ponto fixo é atrator ou repulsor a partir da análise do módulo da derivada calculada no ponto fixo. Em particular o ponto fixo é atrator se $|f'(p)| < 1$ e repulsor se $|f'(p)| > 1$. No caso do Mapa Logístico, o ponto fixo $p = 0$ é atrator para $r < 1$ e repulsor para $r > 1$, e o ponto $1 - 1/r$ é atrator para r no intervalo $(1, 3)$ e repulsor para os demais casos. A dinâmica dos pontos fixos pode ser visualizada do diagrama *cobweb* (teia de aranha), que mostra a evolução dos pontos (x_n, x_{n+1}). A Figura 3 gerada através do *wxMaxima* ilustra como a visualização das órbitas pode ser melhorada usando este tipo de diagrama. Nesse caso usamos o Mapa Logístico com $r = 3{,}2$, sendo que à esquerda apresentamos a maneira com a qual uma sequência normalmente seria apresentada na forma do gráfico de uma função de n, e à direita a mesma órbita em um diagrama *cobweb*. Nesse caso tanto o ponto $p = 0$ quanto $p = 1 - 1/r = 0{,}6875$ são repulsores. Nesse diagrama o valor inicial é $x_0 = 0,001$. Os valores x_n que começam próximos de 0 rapidamente são repelidos e ficam próximos de $0{,}6875$. Como esse ponto também é repulsor, os valores x_n gradualmente começam a se afastar desse ponto também. O diagrama *cobweb* é um instrumento útil para analisar a dinâmica dos pontos fixos sem a necessidade de cálculos analíticos.

A dinâmica entre os dois pontos fixos influencia profundamente no comportamento das sequências. Para $0 < r < 1$, por exemplo, o fato de 0 ser o único ponto fixo atrator faz com que todas as órbitas acabem eventualmente tendendo a 0, o que pode ser interpretado como a extinção da população. Para $1 < r < 3$ o ponto 0 é repulsor e o ponto $1 - 1/r$ é atrator, e todas as órbitas tentem ao último. No entanto, para $r > 3$ os dois pontos são repulsores. Nesse caso as órbitas apresentam um comportamento não trivial.

Para entender tal comportamento vamos definir o conceito de órbita periódica. Uma determinada órbita é dita *periódica* de período n se temos $x_{k+m} = f_m(x_k) = x_k$ para algum m. Isso significa que a cada m iterações o mesmo ponto é obtido. O menor inteiro positivo n em que ocorre a órbita repete-se é denominado *período* da órbita. Para obter tais pontos analiticamente é necessário aplicar n vezes a relação de recorrência e resolver a equação obtida, de maneira análoga ao efetuado para o ponto fixo. No entanto, resolver essas equações não acrescenta nada à discussão, que pode se basear no estudo do comportamento das órbitas

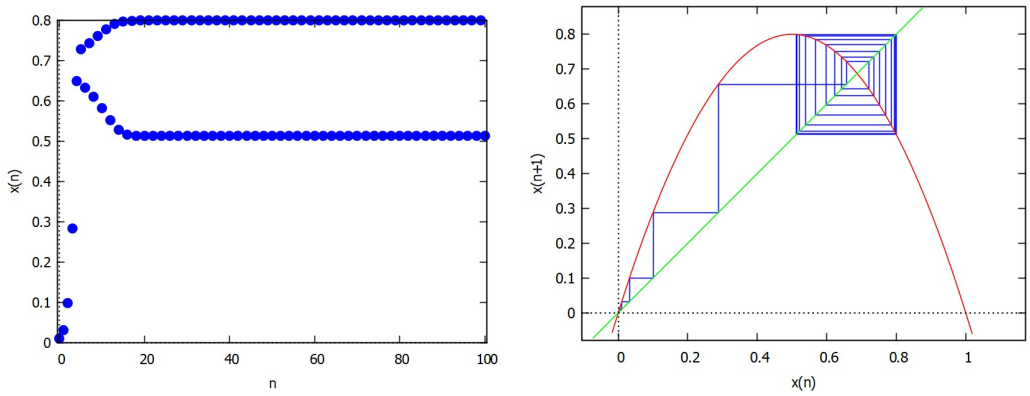


Figura 3: À esquerda, o gráfico da evolução do Mapa Logístico, com $r = 3{,}2$ e $x_0 = 0{,}001$. À direita, diagrama *cobweb* para a mesma configuração.

obtidas para cada parâmetro r.

Para $r > 3$ as órbitas primeiramente oscilando entre dois valores distintos (pontos periódicos de período 2). Conforme aumenta r, os períodos começam a duplicar, até o sistema finalmente apresentar um comportamento completamente caótico, sem tender a nenhum valor. O comportamento caótico é caracterizado por não apresentar nenhuma característica periódica e pela sensibilidade às condições iniciais. No painel superior da Figura 4 apresentamos uma órbita típica para $r = 4$. Note que não existe nenhum padrão desenhado no diagrama *cobweb*. No painel inferior da Figura 4 mostramos duas órbitas do sistema em função do número de iterações n. Apesar de as condições iniciais $x_0 = 0,2$ e $0,200001$ serem bastante próximas, as órbitas são completamente diferentes, divergindo uma da outra nas primeiras iterações. Isso faz com que seja impossível prever o comportamento do sistema caso não se saiba exatamente a condição inicial aplicada. Qualquer incerteza faz com que o comportamento da órbita seja completamente imprevisível.

A melhor maneira de observar esse comportamento é usar um diagrama de bifurcações, que consiste em fazer o gráfico do número de valores limite em função do parâmetro em questão. Tal diagrama pode ser obtido usando o *wxMaxima* e pode ser observado na Figura 5.

A principal característica de um sistema caótico é apresentar uma elevada sensibilidade às condições iniciais nos casos em que as órbitas são limitadas. No caso em que as órbitas não são limitadas, é possível que condições iniciais se afastem rapidamente mesmo na ausência de caos. É importante observar que nos casos não caóticos os valores limite apresentados no diagrama de bifurcações não dependem das condições iniciais, pois eventualmente as órbitas tendem ao mesmo comportamento. No caso caótico, no entanto, duas órbitas que iniciam com condições iniciais próximas rapidamente se afastam uma da outra, apresentando comportamentos distintos. Esse comportamento pode ser atestado com o uso de planilhas eletrônicas, e pode ser medido através dos expoentes de Lyapunov. O expoente de Lyapunov serve para indicar se a separação entre duas órbitas com condições iniciais distintas (porém próximas) é exponencial. A fórmula é dada por

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|. \tag{5}$$

O indicador λ é usado para caracterizar as órbitas. Em particular, se $\lambda > 0$ a separação entre órbitas vizinhas é exponencial e a órbita é caótica. Apesar de a fórmula ser de difícil compreensão para um aluno do Ensino Médio, ela pode ser facilmente implementada numericamente, seja através do *wxMaxima* ou através de

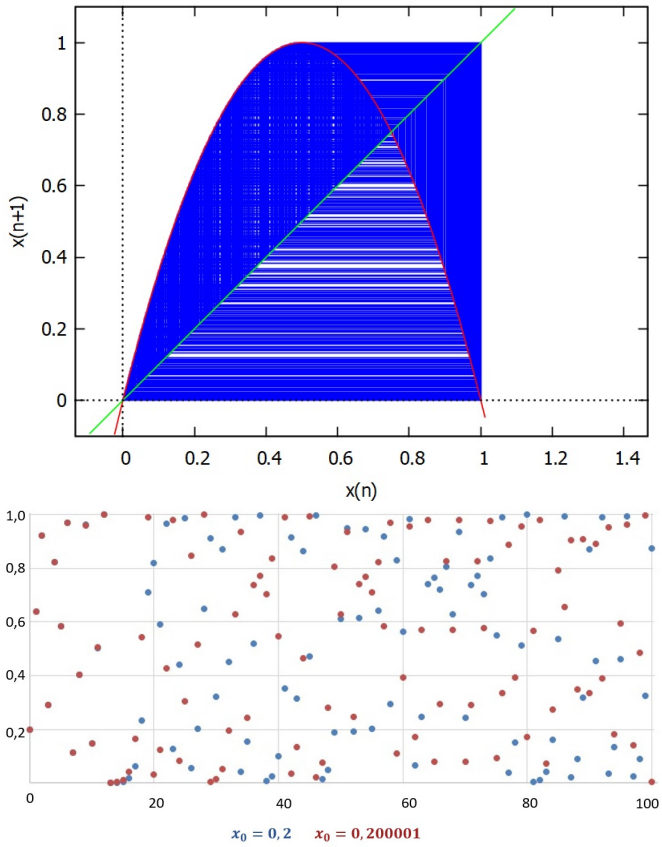


Figura 4: Acima: órbita do Mapa Logístico com $r = 4$ no diagrama *cobweb*. Abaixo: órbitas do Mapa Logístico com $r = 4$ para $x_0 = 0,2$ e $0,200001$. Note que apesar de as condições iniciais serem próximas, as órbitas divergem uma da outra nas primeiras iterações.

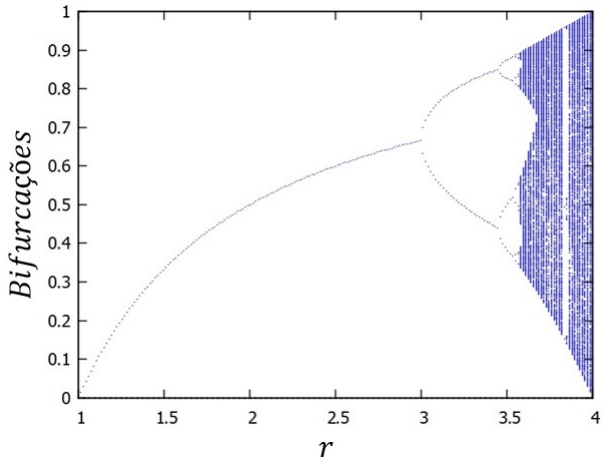


Figura 5: Diagrama de Bifurcações do Mapa Logístico.

planilhas eletrônicas. É possível observar que para valores acima de $r = 3,57$ é possível observar órbitas caóticas. Na Figura 6 é possível observar expoentes de Lyapunov obtidos para as mesmas condições iniciais e diferentes valores de r.

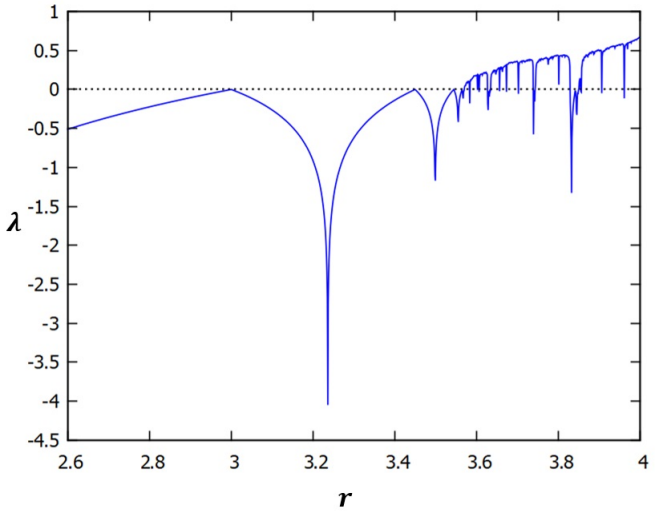


Figura 6: Expoentes de Lyapunov para o Mapa Logístico.

O Mapa Logístico é um exemplo simples e por isso faz parte do cânone do estudo dos sistemas dinâmicos e Teoria do Caos. No entanto, é possível propor outros sistemas para estudar as mesmas propriedades. Mesmo que um tratamento analítico de tais sistemas seja mais complexo ou mesmo impossível, a utilização de ferramentas computacionais permite a exploração numérica e a consequente caracterização das órbitas de diferentes sistemas dinâmicos.

3. Mapa Logístico Generalizado

O Mapa Logístico pode ser generalizado acrescentando ao elemento x_n do fator $(1 - x_n)$ um expoente μ, resultando no mapa

$$x_{n+1} = r \cdot x_n(1 - x_n^{\mu}). \tag{6}$$

Quando $\mu = 1$ recupera-se o Mapa Logístico original. A princípio μ pode ser qualquer número real, mas para assegurar que as órbitas estejam sempre limitadas ao intervalo $[0, 1]$ vamos considerar $\mu > 0$. Nesse caso temos que o máximo absoluto da função $f(x) = r \cdot x(1 - x^{\mu})$ no intervalo fechado $[0, 1]$ ocorre em

$$x_{max} = \left(\frac{1}{1+\mu}\right)^{1/\mu}. \tag{7}$$

Tal valor representa uma diferença com relação ao Mapa Logístico original, que era simétrico com relação ao ponto $1/2$. Usando esse valor encontramos que o máximo valor da função f está em

$$f(x_{max}) = r \cdot \frac{\mu}{1+\mu}\left(\frac{1}{1+\mu}\right)^{1/\mu}. \tag{8}$$

É possível verificar que o lado direito da Equação 8 varia entre 0 e r, de acordo com o valor de μ. Para que as órbitas fiquem limitadas ao intervalo $[0, 1]$ devemos ter $f(x_{max}) \leq 1$, de forma que a condição sobre r

agora é dada para cada μ através da inequação

$$r \leq \frac{(1+\mu)^{\frac{\mu+1}{\mu}}}{\mu}. \tag{9}$$

Para $\mu = 1$ recuperamos a condição $r \leq 4$, esperada para o Mapa Logístico original.

Os pontos fixos são obtidos novamente através da equação $f(p) = p$, ou seja,

$$rp(1 - p^{\mu}) = p. \tag{10}$$

Mais uma vez $p = 0$ é uma solução trivial. Quando $r > 1$ adicionalmente obtemos a solução

$$p = \left(1 - \frac{1}{r}\right)^{1/\mu}. \tag{11}$$

Podemos determinar quais as condições para as quais os pontos fixos serão atratores através do Teorema do Ponto Fixo. A derivada de $f(x) = r \cdot x(1 - x^{\mu})$ é dada por $f'(x) = r - r \cdot (\mu + 1)x^{\mu}$. Para $p = 0$ temos mais uma vez $f'(p) = r$ e o comportamento é o mesmo do que ocorre no Mapa Logístico original. Para $p = \sqrt[\mu]{\frac{r-1}{r}}$ temos

$$f'(p) = \mu(1 - r) + 1. \tag{12}$$

A análise dessa derivada permite concluir que esse ponto fixo é atrator quando r pertence ao intervalo $\left(1, \frac{\mu+2}{\mu}\right)$ e repulsor se nos outros casos.

Como exemplo vamos utilizar $\mu = 10$, de forma que $x_{n+1} = rx_n(1 - x_n^{10})$. Em tal caso o ponto fixo será atrator quando $r \in (1, 1{,}2)$. Para ilustrar uma órbita simples vamos usar $r = 1{,}2$ e $x_0 = 0{,}2$. É possível observar que a órbita oscila entre dois valores. Outra maneira de visualizar as soluções é através no diagrama *cobweb* apresentado na Figura 7.

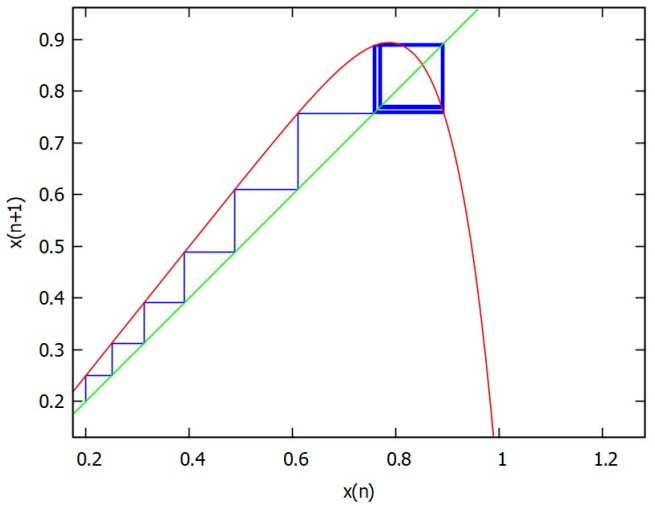


Figura 7: Órbita de $x = 0{,}2$ para o Mapa Logístico Generalizado com $\mu = 10$, $0 \leq n \leq 100$.

É importante observar que o surgimento de outros valores limite (bifurcações) ocorre para valores menores de r se comparado ao Mapa Logístico original. Assim como o intervalo $\left(1, \frac{\mu+2}{\mu}\right)$ torna-se mais curto à medida que o valor de μ aumenta, o mesmo ocorre com intervalos entre todas as outras bifurcações, uma vez que a razão δ entre os tamanhos de intervalos consecutivos permanece constante. Quando $r = 1{,}389$ já é possível observar um comportamento caótico. Esse fato é confirmado pelo cálculo do Expoente de Lyapunov, que resulta em $\lambda = 1{,}12$. Na Figura 8 apresentamos o diagrama de bifurcações. É possível perceber que o comportamento é bastante similar ao do Mapa Logístico original, porém, como antecipado, a região caótica é alcançada para valores menores de r. A mesma análise pode ser feita através dos expoentes de Lyapunov dados na Figura 9.

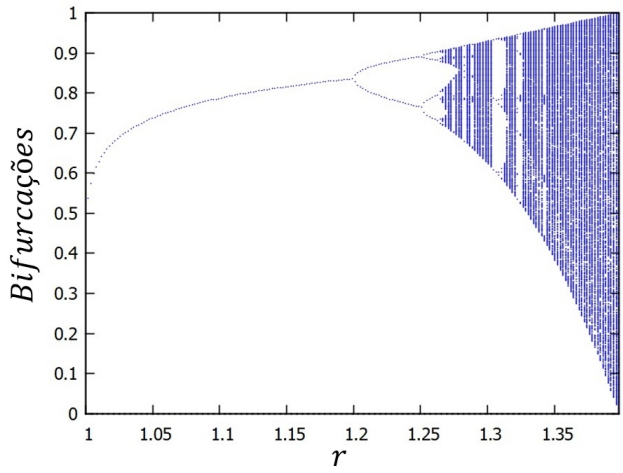


Figura 8: Diagrama de Bifurcações - $x_{n+1} = rx_n(1 - x_n^{10})$, $1 \leq r \leq \frac{11}{10}\sqrt[10]{11}$

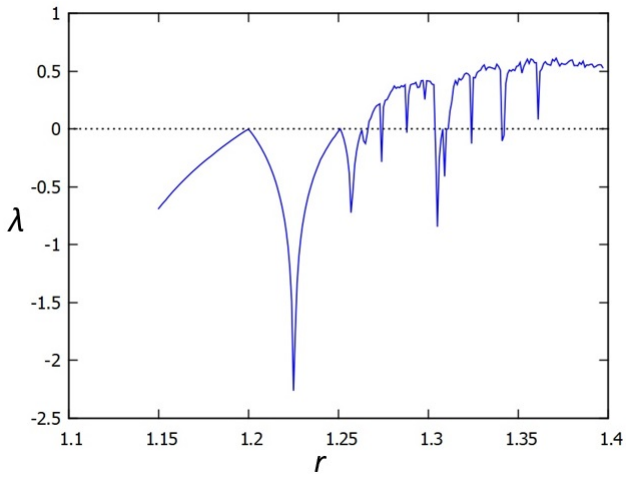


Figura 9: Expoentes de Lyapunov para o Mapa Logístico Generalizado com $\mu = 10$.

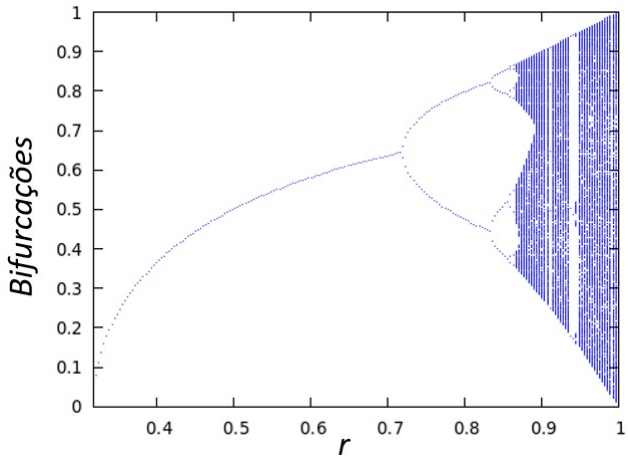


Figura 10: Diagrama de bifurcações para o Mapa Trigonométrico.

4. O Mapa Trigonométrico

O Mapa Logístico generalizado apresenta poucas diferenças se comparado ao modelo original. Ambos os casos podem ser estudados analiticamente no que se refere ao cálculo dos pontos fixos e sua estabilidade. Vamos ilustrar um exemplo em que os métodos numéricos são a única maneira de explorar o problema. Vamos considerar o mapa

$$x_{n+1} = r \cdot \text{sen}\,(\pi x_n)\,. \tag{13}$$

A função $f(x) = \text{sen}(\pi x)$ possui zeros em 0 e 1 como no caso logístico. Para que os valores x_n fiquem restritos ao intervalo $[0, 1]$ a condição sobre r é dada por

$$0 < r \leq 1. \tag{14}$$

Ao tentar se obter os pontos fixos obtemos a equação

$$r \cdot \text{sen}\,(\pi p) = p. \tag{15}$$

Mais uma vez temos que $p = 0$ é um ponto fixo. No entanto, uma vez que a equação obtida é transcendental, não é possível obter outras soluções de forma analítica. Nesse caso a equação pode ser resolvida numericamente ou através do método da interseção entre os gráficos para cada valor de r. Pode-se mostrar que nesse caso a condição para a existência do segundo ponto fixo é $r > 1/\pi$.

Vamos usar como exemplo o caso $r = 0{,}75$. Usando um método numérico qualquer podemos encontrar uma aproximação para o ponto fixo não trivial, o que fornece $p \approx 0{,}66$. Usando a derivada $f'(x) = \pi r\cos(\pi x)$ encontramos $|f'(0)| = 2{,}36$ e $|f'(0{,}659)| = 1{,}13$, de forma que ambos são pontos fixos repulsores. Neste caso novamente a órbita oscila entre dois pontos limite. O diagrama de bifurcações da Figura 10 mostra o comportamento do mapa conforme variamos o parâmetro r. Note que para $r = 1$ o comportamento é completamente caótico. Apesar de a função utilizada não ser um polinômio, note que a estrutura do diagrama de bifurcações segue o mesmo padrão do Mapa Logístico. Esse comportamento também fica evidente analisando os expoentes de Lyapunov dados na Figura 11.

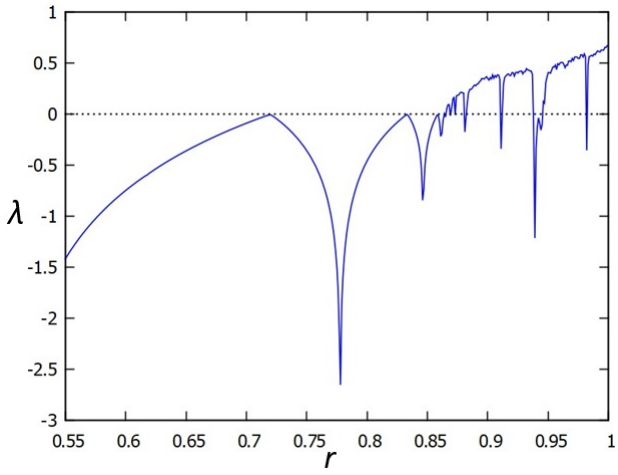


Figura 11: Expoentes de Lyapunov para o Mapa Trigonométrico.

5. O Mapa Tenda

O Mapa Tenda é um caso interessante, uma vez que o mapa não é uma função suave em todo o domínio, apresentando uma descontinuidade na derivada. O Mapa Tenda é dado por

$$x_{n+1} = r \cdot \left(1 - 2\left|x_n - \frac{1}{2}\right|\right). \tag{16}$$

Neste caso, a função $f(x) = r \cdot \left(1 - 2\left|x - 1/2\right|\right)$ possui zeros em 0 e 1 e máximo em $x_{max} = 1/2$, correspondente ao valor $f(x_{max}) = r$. Para manter as órbitas restritas ao intervalo $[0, 1]$, portanto, o parâmetro r precisa mais uma vez ser dado de forma que

$$0 < r \leq 1. \tag{17}$$

Os pontos fixos desse mapa podem ser mais uma vez ser obtidos resolvendo-se analiticamente a equação

$$r \cdot \left(1 - 2\left|p - \frac{1}{2}\right|\right) = p. \tag{18}$$

Resolvendo-se essa equação obtemos, para $r < 1/2$, apenas o ponto fixo atrator $p = 0$, de forma que todas as órbitas tendem a tal ponto. Para $r > 1/2$, além de $p = 0$, encontramos adicionalmente o ponto fixo $p = 2r/(1 + 2r)$, ambos repulsores. Para $r = 1/2$ temos uma situação singular em que todos os pontos pertencentes ao intervalo $[0, 1/2]$ são pontos fixos, mas que não possuem natureza definida. Não iremos tratar esse último caso, pois foge ao escopo do trabalho.

Na Figura 12 mostramos um exemplo de órbita para o Mapa Tenda para $r = 1$ e $x_0 = 0,2$. O Mapa Tenda é sempre caótico se $r > 1/2$. De fato, é fácil demonstrar que o seu Expoente de Lyapunov é $\lambda = \ln 2r$, sendo, portanto, sempre positivo para $r > 1/2$. Uma outra maneira de visualizar esta característica é através do diagrama de bifurcações, dado na Figura 13. Note que neste caso padrão é bastante diferente dos casos anteriores. Esse comportamento deve-se ao fato de que o Mapa Tenda, apesar de utilizar uma função mesmo de contínua, não é suave em todo o domínio, apresentando uma descontinuidade na derivada em $x = 1/2$.

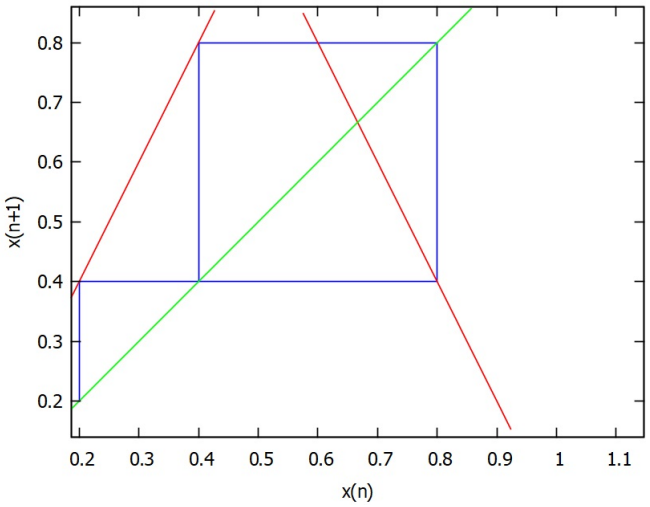


Figura 12: Exemplo de órbita no Mapa Tenda com $\mathrm{r} = 1$ e $\mathrm{x}_0 = 0,2$.

De fato, o padrão do diagrama de bifurcações dos demais mapas depende da suavidade das funções que fornecem as recorrências.

Outro fato interessante sobre o Mapa Tenda surge ao se utilizar planilhas para estudar as suas órbitas para $\mathrm{r} = 1$. Nesse caso o mapa é caótico e as órbitas passam eventualmente por todos os pontos do intervalo $[0, 1]$. Ao ficarem muito próximos de $1/2$, no entanto, o arredondamento da máquina faz com que o número seja considerado exatamente $1/2$, fazendo com que ele seja mapeado em 1 e depois em 0, sendo esse último um ponto fixo. Isto dá a impressão de que 0 é um ponto atrator e que o sistema não é caótico em tal caso. É importante nesses casos que a análise não seja superficial por envolver mapas mais complexos, ou pode-se chegar a conclusões enganosas.

6. Aplicação em Sala de Aula

Em sala de aula é possível começar com a principal aplicação do Modelo Logístico, isto é, analisando uma dinâmica populacional que atinge um limite segundo o modelo de Verhulst. O objetivo é identificar populações com fatores de equilíbrio, populações oscilantes ou comportamento caótico. Inicialmente, vamos retomar as limitações do modelo exponencial. Para tal, devemos propor uma reflexão sobre as consequências do crescimento ilimitado malthusiano, o qual provocaria a extinção da espécie pelo esgotamento dos recursos de sobrevivência devido à superpopulação. Em seguida, apresentamos o Mapa Logístico aos estudantes. É importante explicar que, neste modelo, a população deve ser sempre representada por um valor no intervalo $(0, 1)$, sendo 1 o limite da população que a levará à extinção devido ao esgotamento dos recursos de sobrevivência. É também relevante refletir juntamente com os estudantes o efeito do fator $(1 - \mathrm{x_n})$, que diferencia o Mapa Logístico do modelo Malthusiano na contenção do tamanho da população. Essa atividade pode ser integrada de maneira transversal com outros componentes, como Biologia e Geografia. Algumas questões podem ser exploradas a partir dos resultados encontrados. A contribuição de outras áreas com dados pertinentes à pesquisa será enriquecedora para o trabalho.

O estudo numérico pode envolver um dos recursos computacionais apresentados, ou mesmo uma combinação dos três. Os estudantes são então orientados a explorar os diferentes fatores de crescimento e o seu impacto na dinâmica populacional. Além disso, o professor pode explorar diferentes conceitos, como os pontos fixos,

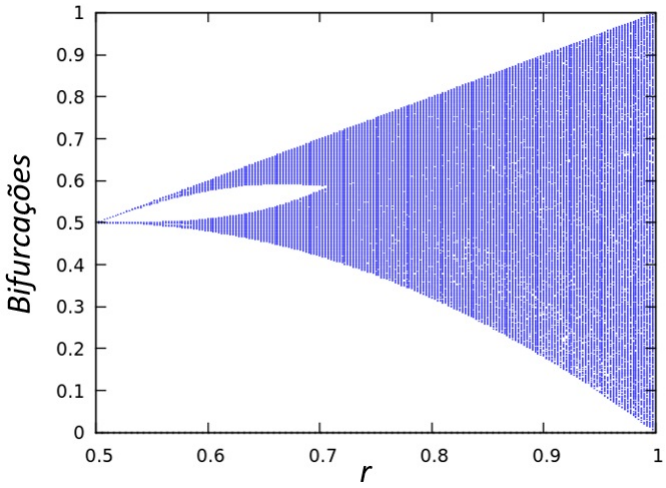


Figura 13: Diagrama de bifurcações para o Mapa Tenda.

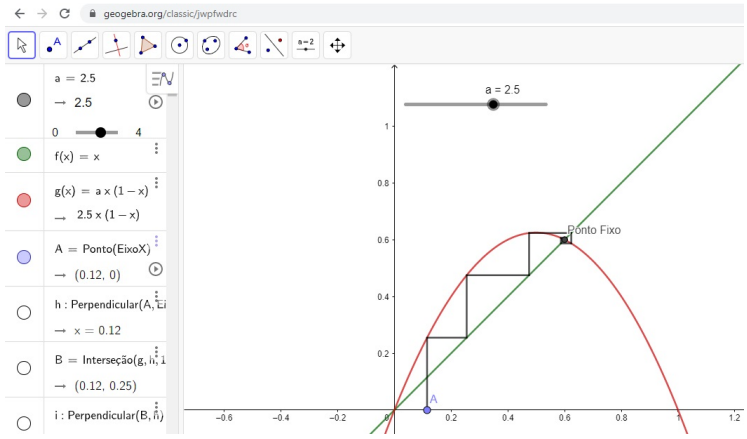


Figura 14: Exemplo de limite da população usando diagrama de bifurcações.

que podem ser obtidos analiticamente e analisados numericamente. Na Figura 14 é apresentado um exemplo do estudo da órbita do mapa $x_{n+1} = r \cdot x_n \cdot (1 - x_n)$ com o uso do *Geogebra*. No arquivo em questão, sugerimos os controles deslizantes para permitir aos estudantes a variação dos valores de r e do valor inicial da população, de maneira que observem o diagrama *cobweb* em diferentes condições. Além disso, o uso de ferramentas visuais auxilia na melhor compreensão dos estudantes. Boaler [11] defende que "é muito importante que os estudantes engajem-se no pensamento visual sobre matemática, pois isso dá acesso à compreensão e ao uso de diferentes rotas cerebrais". Por fim, os estudantes podem identificar a presença de caos para algumas dinâmicas populacionais, e como detectar o caos usando, por exemplo, os expoentes de Lyapunov.

Uma vez que os estudantes têm domínio das ferramentas usadas na análise do Mapa Logístico, os outros modelos podem ser apresentados. É importante ilustrar neste ponto a utilidade das ferramentas numéricos, como no caso da identificação e caracterização dos pontos fixos, que nem sempre podem ser encontrados analiticamente. A presença de caos nesses sistemas podem ser igualmente exploradas através dos métodos numéricos, em suas semelhanças e diferenças.

7. Conclusões

A exploração de diferentes mapas permite concluir que o surgimento do comportamento caótico não é uma particularidade do Mapa Logístico. De fato, mapas com características semelhantes às do Mapa Logístico, apresentam comportamentos semelhantes se explorarmos o diagrama de bifurcações. As órbitas dos Mapa Logístico Generalizado e Mapa Trigonométrico apresentam um comportamento similar à do Mapa Logístico, possuindo órbitas periódicas ou caóticas, dependendo do parâmetro utilizado. O Mapa Tenda, por outro lado, possui comportamento caótico independentemente do parâmetro utilizado. É interessante notar a relação entre a suavidade da curva e a estrutura das órbitas geradas.

Apesar de ser um tema de aparente complexidade, apresentamos neste artigo uma proposta envolvendo conceitos que podem ser trabalhados computacionalmente com os estudantes. Muitos desses conceitos envolvem a noção do limite de sequências, que é introduzida ao se estudar Progressões Geométricas infinitas. Neste caso, o conteúdo pode ser ampliado usando-se outras sequências, como as que foram apresentadas aqui. Com o uso combinado de ferramentas como planilhas, Sistemas de Computação Algébrica e Simbólica e Sistemas de Geometria Dinâmica é possível trabalhar conceitos que são utilizados em diversas pesquisas de ponta.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (Capes) – Código de Financiamento 001. Agradecemos à Profa. Dra. Nara Bobko e ao Prof. Dr. Lucas Pedroso por suas contribuições ao trabalho desenvolvido. Agradecemos também ao revisor anônimo por suas observações que elevaram a qualidade deste artigo.

Referências

[1] Crilly, T. *50 ideias de Matemática que você precisa conhecer*. São Paulo: Planeta, 2017.

[2] Bentley, P., *O Livro dos Números - Uma história ilustrada da matemática*. Rio de Janeiro: Jorge Zahar, 2009.

[3] Mello, C. K. C. *Sistemas Dinâmicos e Caos - Análise de Mapas Discretos e Possibilidades de Aplicação no Ensino Médio*, Universidade Tecnológica Federal do Paraná, 2021.

[4] Villate, J. E. *Introdução aos sistemas dinâmicos - uma abordagem prática com Máxima*. Porto: Universidade do Porto, 2007.

[5] Cipolli, V. G. *Sistemas dinâmicos discretos - análise de estabilidade*, Universidade Estadual Paulista, 2012.

[6] Anton H. *Cálculo - um novo horizonte*, Porto Alegre: Bookman, 2000.

[7] Alligood, K., Sauer, T., Yorke, J. *Chaos - an introduction to Dynamical Systems*, New York: Springer, 1996.

[8] Feigenbaum, M. J. *Quantitative universality for a class of nonlinear transformations*, J Stat. Phys. 19, 25–52, 1978.

[9] Maxima *Maxima, a Computer Algebra System* Versão 18.02.0, 2018. Disponível em https://maxima.sourceforge.io/.

[10] Hohenwarter, M. *et al.*, *GeoGebra* Versão 5.0.507.0, 2018. Disponível em http://www.geogebra.org.

[11] Boaler, J., *Mentalidades Matemáticas - estimulando o potencial dos estudantes por meio da matemática criativa, das mensagens inspiradoras e do ensino inovador*, Porto Alegre: Penso, 2018.

Cássio Kiechaloski Correia de Mello
Universidade Tecnológica Federal do Paraná
<cassio_mello@hotmail.com>

André Fabiano Steklain Lisbôa
Universidade Tecnológica Federal do Paraná
<steklain@utfpr.edu.br>

Recebido: 14/10/2021
Publicado: 28/06/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1022

Uma prova geométrica do Problema da Basileia

Darlan Ferreira de Oliveira Joãonito de Jesus Santos

Resumo

O presente artigo tem como objetivo apresentar, através de conceitos da geometria plana, uma forma para calcular a soma dos inversos dos quadrados dos números naturais. Esse problema ficou conhecido na literatura como Problema da Basileia e foi mostrado por Euler, usando técnicas do cálculo diferencial, que tal soma vale $\pi^2/6$.

Palavras-chave: Problema da Basileia; Teorema Inverso de Pitágoras; Geometria plana.

Abstract

This article aims to present, through concepts of plane geometry, a way to calculate the sum of the inverses of the squares of natural numbers. This problem is known in the literature as the Basel Problem and it was shown by Euler, using differential calculus techniques, that such a sum is worth $\pi^2/6$.

Keywords: Basel Problem; Inverse Theorem of Pythagoras; plane geometry.

1. Introdução

Basileia é uma cidade localizada na zona noroeste da Suíça, próxima às fronteiras do país com França e Alemanha, onde, em 15 de abril de 1707, nasceu um de seus filhos mais ilustres, Leonhard Paul Euler.

O talento de Euler para a Matemática logo foi descoberto pelo matemático Johann Bernoulli, que o incentivou a matricular-se no curso de Matemática da Universidade de Basileia, onde concluiu em 1726 seu doutorado com uma tese sobre a propagação do som.

A obra de Euler consta de pelo menos 530 trabalhos publicados em vida e uma série de manuscritos deixados após sua morte. Foi em 1735 que Euler ganhou fama internacional após resolver um famoso problema em teoria dos números, proposto pela primeira vez por Pietro Mengoli, de achar o valor exato da soma

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\cdots,$$

mostrando que a série converge para o valor $\dfrac{\pi^2}{6}$ Este fato que surpreendeu a todos, pois a resposta trazia relação com uma das constantes mais importantes da História da Matemática. Muitos matemáticos importantes da época debruçaram-se sobre esse problema, dentre eles Jacques Bernoulli,

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

mas não obtiveram sucesso. Por fim, o problema ficou conhecido como o Problema de Basileia, em homenagem à cidade natal de Euler.

A proposta deste trabalho é estudar, a partir de uma abordagem geométrica, o Problema da Basileia, evidenciando a aplicação de vários conceitos da geometria plana estudados no ensino básico.

2. Convergência da soma

O Problema da Basileia consiste em encontrar a soma dos inversos dos quadrados dos números naturais,

$$\sum_{n\in\mathbb{N}} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} + \cdots . \tag{1}$$

A primeira pergunta que deve ser feita quando se estuda o Problema da Basileia é se, de fato, a soma envolvida no problema converge para algum número real. Para ver que a soma no Problema da Basileia é finita, considere para cada número natural n a seguinte desigualdade:

$$(n-1)n < n^2 < n(n+1).$$

Para cada número natural n maior do que 1, vale a desigualdade

$$\frac{1}{(n+1)n} < \frac{1}{n^2} < \frac{1}{n(n-1)}$$

, que pode ser reescrita como

$$\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2} < \frac{1}{n-1} - \frac{1}{n}.$$

Como essa última desigualdade vale para todo natural n maior do que 1, temos

$$\begin{aligned}
\frac{1}{2} - \frac{1}{3} &< \frac{1}{2^2} < 1 - \frac{1}{2},\\
\frac{1}{3} - \frac{1}{4} &< \frac{1}{3^2} < \frac{1}{2} - \frac{1}{3},\\
\frac{1}{4} - \frac{1}{5} &< \frac{1}{4^2} < \frac{1}{3} - \frac{1}{4},\\
&\vdots\\
\frac{1}{n} - \frac{1}{n+1} &< \frac{1}{n^2} < \frac{1}{n-1} - \frac{1}{n}.
\end{aligned}$$

Somando, membro a membro estas desigualdades, obtemos

$$\frac{1}{2} - \frac{1}{n+1} < \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 1 - \frac{1}{n}.$$

Acrescentando 1 a todos os membros, obtemos

$$\frac{3}{2} - \frac{1}{n+1} < 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}.$$

Nesse momento, o leitor familiarizado com o conceito de limite deve concluir que quanto maior o valor de n os termos $\frac{1}{n+1}$ e $\frac{1}{n}$ se tornam mais próximos de zero, de modo a concluir que o valor da soma no Problema da Basileia fica compreendido entre 3/2 e 2.

Mais detalhes sobre a prova original de Euler podem ser encontrados nos trabalhos [1, 2, 3, 4, 5].

3. Sequência de circunferências encaixadas

No que segue, a sequência de circunferências encaixadas tangentes num ponto O

$$\Gamma_1, \Gamma_2, \Gamma_3, \cdots, \Gamma_n, \cdots$$

centradas em $O_1, O_2, O_3, \cdots, O_n, \cdots$, respectivamente, satisfazem as seguintes propriedades:

P1. Γ_n é tangente interior à Γ_{n+1} no ponto O;

P2. O diâmetro de Γ_{n+1} é o dobro do diâmetro de Γ_n.

Sendo d_n o diâmetro da circunferência Γ_n, segue das propriedades P1 e P2 que os centros $O_1, O_2, O_3, \cdots, O_n, \cdots$ estão alinhados, e $d_n = \overline{OO_{n+1}} = 2^{n-1}d_1$. A Figura 1 ilustra as quatro primeiras circunferências encaixadas tangentes em O.

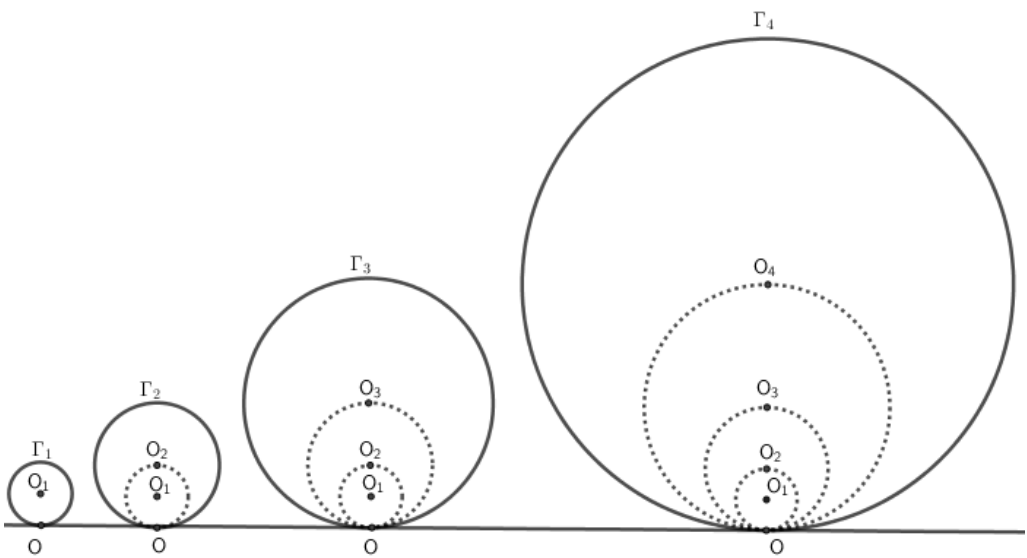


Figura 1: Circunferências encaixadas tangentes em O

A construção dessa sequência de circunferências encaixadas será usada para auxiliar no cálculo do inverso do quadrado da medida do diâmetro da circunferência Γ_1.

4. Pontos singulares

Considere a sequência de circunferências encaixadas $\Gamma_1, \Gamma_2, \Gamma_3, \cdots, \Gamma_n, \cdots$ tangentes num ponto O. Nesta seção será descrita a construção de 2^{i-1} pontos $O_{i1}, O_{i2}, \cdots, O_{i(2^{i-1})}$ sobre a circunferência Γ_i, os quais serão denominados **pontos singulares de** Γ_i.

Inicialmente, considere a circunferência Γ_1 tangente interior no ponto O à circunferência Γ_2, conforme ilustra a Figura 2.

Definição 1. O ponto singular sobre Γ_1 é dado por $O_{11} = O_2$.

Definição 2. Os dois pontos singulares sobre Γ_2 são obtidos pela interseção da reta tangente à Γ_1 no ponto O_2 com a circunferência Γ_2 e são denotados por O_{21} e O_{22}. Veja Figura 3.

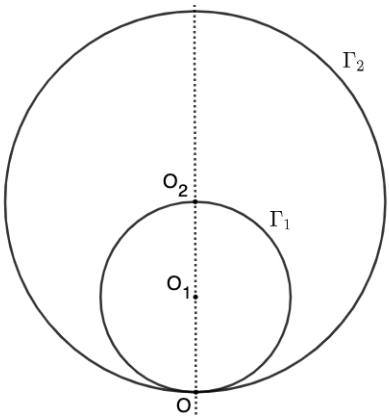


Figura 2: Ponto singular O_{11} sobre Γ_1

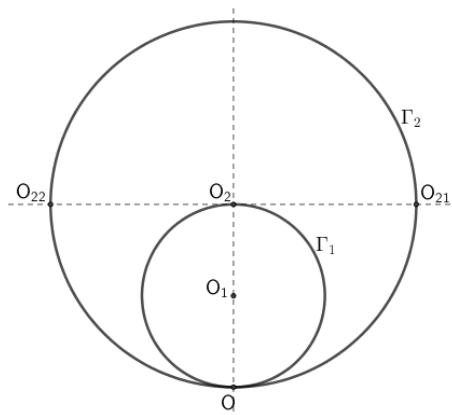


Figura 3: Pontos singulares O_{21} e O_{22} sobre Γ_2

Seguindo, considere, agora, a circunferência Γ_2 tangente interior no ponto O à circunferência Γ_3.

Definição 3. Os quatro pontos singulares sobre Γ_3 são obtidos pelas interseções das retas secantes à Γ_2 pelos pares de pontos (O_3, O_{21}) e (O_3, O_{22}) com a circunferência Γ_3, e são denotados, respectivamente, por O_{31}, O_{33} e O_{32}, O_{34}. Veja Figura 4.

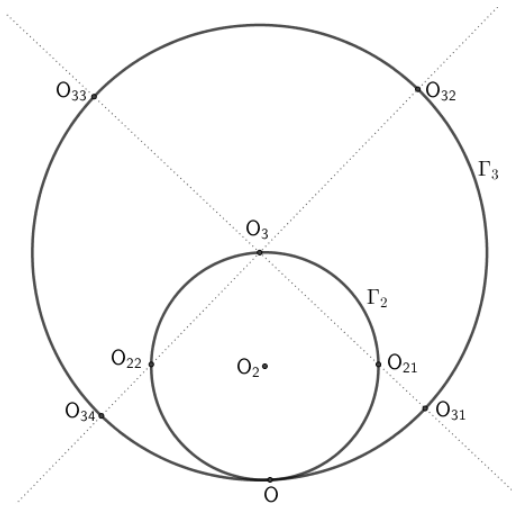


Figura 4: Pontos singulares O_{31}, O_{32}, O_{33} e O_{34} sobre Γ_3

Mais geralmente temos a seguinte definição:

Definição 4. Os 2^{i-1} pontos singulares sobre Γ_i são obtidos pelas interseções das retas secantes à Γ_{i-1} pelos pares de pontos $(O_i, O_{(i-1)k})$ com a circunferência Γ_i e são denotados, respectivamente, para cada $1 \leq k \leq 2^{i-2}$, por O_{ik} e $O_{i(k+2^{i-2})}$.

Definição 5. Os pontos singulares sobre Γ_n determinados pela interseção da reta secante que passa pelo centro de Γ_n e um ponto singular de Γ_{n-1} são chamados pontos singulares conjugados de Γ_n.

4.1. Propriedades envolvendo pontos singulares

Para os pontos singulares de uma circunferência Γ_n valem as seguintes propriedades:

Propriedade 1. O ângulo central $P\widehat{O}_nQ$, onde P e Q são pontos singulares consecutivos da circunferência encaixada Γ_n, mede $\dfrac{\pi}{2^{n-2}}$, para todo $n \geq 2$.

Demonstração. Para $n = 2$ temos apenas dois pontos singulares O_{21} e O_{22} onde o segmento $O_{21}O_{22}$ é o diâmetro de Γ_2. Assim o ângulo central $O_{21}\widehat{O}_2O_{22}$ mede π e a afirmação é verdadeira para $n = 2$. Suponha que o ângulo central $P\widehat{O}_nQ$ da circunferência encaixada Γ_n mede, para um certo natural n, $\dfrac{\pi}{2^{n-2}}$ para quaisquer P e Q consecutivos sobre Γ_n. Para mostrar que essa relação vale para o natural $n+1$ são tomados dois pontos consecutivos P' e Q' sobre Γ_{n+1}. Sendo P o ponto de interseção da reta que passa por O_{n+1} e P' com Γ_n e Q o ponto de interseção da reta que passa por O_{n+1}, e Q' com Γ_n, vamos considerar dois casos:

Caso 1. O_{n+1} não pertence ao menor arco sobre Γ_n determinado por P e Q. Veja Figura 5.

Segue do Teorema do ângulo inscrito que

$$\begin{aligned} P'\widehat{O}_{n+1}Q' &= P\widehat{O}_{n+1}Q \\ &= \frac{1}{2}P\widehat{O}_nQ \\ &= \frac{1}{2}\left(\frac{\pi}{2^{n-2}}\right) \\ &= \frac{\pi}{2^{n-1}} \end{aligned}$$

Caso 2. O_{n+1} pertence ao menor arco sobre Γ_n determinado por P e Q. Veja Figura 6.

Segue do Teorema do ângulo inscrito que

$$\begin{aligned} P'\widehat{O}_{n+1}Q' &= \pi - P\widehat{O}_{n+1}Q \\ &= \pi - \frac{1}{2}\Big(\text{arco determinado por P e Q que não contém } O_{n+1}\Big) \\ &= \pi - \frac{1}{2}\Big(2\pi - P\widehat{O}_nQ\Big) \\ &= \frac{\pi}{2^{n-1}} \end{aligned}$$

Segue do Princípio de indução finita que a propriedade é válida para todo número natural n.

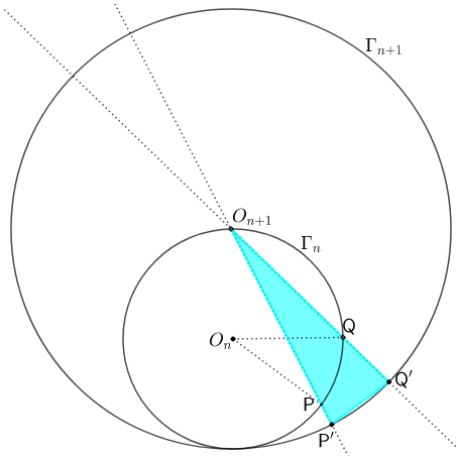


Figura 5: Ângulo central $P'\widehat{O}_{n+1}Q'$ de Γ_{n+1}

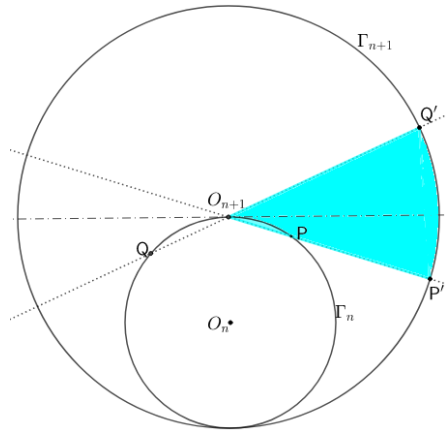


Figura 6: Ângulo central $P'\widehat{O}_{n+1}Q'$ de Γ_{n+1}

Propriedade 2. Os arcos determinados por pontos singulares consecutivos de uma circunferência Γ_n têm comprimentos medindo πd_1, para todo $n \geq 2$, onde d_1 é o diâmetro de Γ_1.

Demonstração. Sejam P e Q dois pontos singulares consecutivos sobre a circunferência Γ_n, e α o arco determinado por P e Q. O comprimento C do arco α é dado por αr_n, onde r_n é o raio da circunferência Γ_n. Segue da Propriedade 1 que

$$\begin{aligned} C &= \alpha \frac{d_n}{2} \\ &= P\widehat{O}_n Q \frac{2^{n-1} d_1}{2} \\ &= \frac{\pi}{2^{n-2}} 2^{n-2} d_1 \\ &= \pi d_1. \end{aligned}$$

5. Triângulos singulares inscritos

Dados dois pontos singulares conjugados O_{ik} e $O_{i(k+2^{i-2})}$ em Γ_i a eles associamos o **triângulo singular** $OO_{ik}O_{i(k+2^{i-2})}$ inscrito em Γ_i, o qual denotamos por Δ_{ik} para cada natural k, com $1 \leq k \leq 2^{i-2}$.

Propriedade 3. O triângulo singular Δ_{ik} é retângulo em O, e o segmento $OO_{(i-1)k}$ é a altura em relação ao lado oposto ao vértice O. Veja Figura 7.

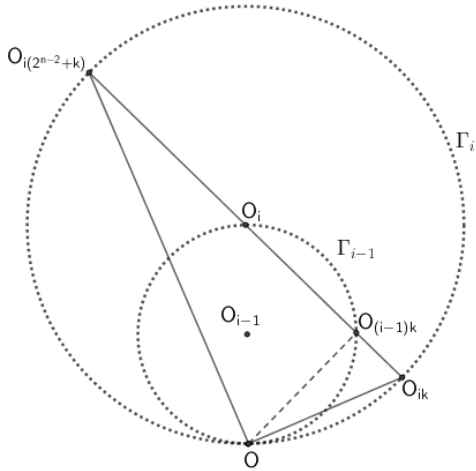


Figura 7: Triângulo singular Δ_{ik} inscrito em Γ_i

Demonstração. Basta notar que os vértices O, no triângulo $OO_{ik}O_{i(2^{i-2}+k)}$, e $O_{(i-1)k}$, no triângulo $OO_{(i-1)k}O_i$, são opostos, respectivamente, aos lados que são diâmetros das circunferências Γ_i e Γ_{i-1} nos quais esses triângulos estão inscritos. Então, pelo Teorema do ângulo inscrito, segue que os ângulos $O_{i(2^{i-2}+k)}\widehat{O}O_{ik}$ e $O\widehat{O}_{(i-1)k}O_i$ são retos.

No que segue, faremos uso do seguinte resultado cuja demonstração decorre diretamente do Teorema de Pitágoras.

Teorema 1 (Teorema Inverso de Pitágoras)**.** *Em todo triângulo retângulo, o quadrado do inverso da altura relativa à hipotenusa é igual à soma dos inversos dos quadrados dos catetos, ou seja,*

$$\frac{1}{h^2} = \frac{1}{b^2} + \frac{1}{c^2}.$$

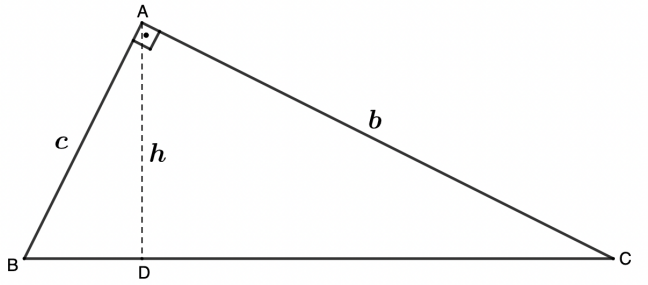


Figura 8: Teorema Inverso de Pitágoras

6. Inverso do quadrado do diâmetro de Γ_1

Nesta seção mostraremos como escrever o inverso do quadrado do diâmetro de Γ_1 em função dos comprimentos das cordas OO_{nk} de uma circunferência Γ_n, para $1 \leq k \leq 2^{n-1}$.

Observe, inicialmente, que

$$\frac{1}{d_1^2} = \frac{1}{\overline{OO_2}^2} = \frac{1}{\overline{OO_{11}}^2}. \tag{2}$$

Como o segmento OO_{11} é altura do triângulo singular $OO_{21}O_{22}$, como ilustra a Figura 9, segue do Teorema 1 que

$$\frac{1}{d_1^2} = \frac{1}{\overline{OO_{11}}^2} = \frac{1}{\overline{OO_{21}}^2} + \frac{1}{\overline{OO_{22}}^2}. \tag{3}$$

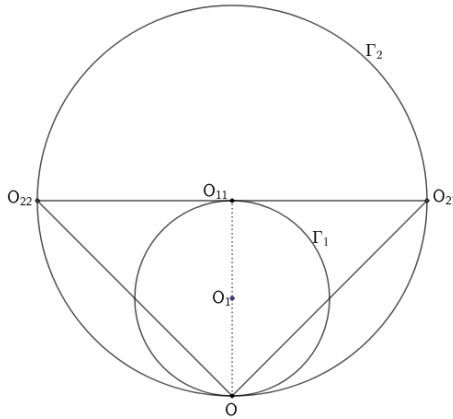


Figura 9: Triângulo singular $OO_{21}O_{22}$

Segue da Propriedade 3 que os segmentos OO_{21} e OO_{22} são alturas, respectivamente, dos triângulos singulares $OO_{31}O_{33}$ e $OO_{32}O_{34}$ donde, novamente, pelo Teorema 1 obtemos de (3) que

$$\frac{1}{d_1^2} = \frac{1}{\overline{OO_{31}}^2} + \frac{1}{\overline{OO_{33}}^2} + \frac{1}{\overline{OO_{32}}^2} + \frac{1}{\overline{OO_{34}}^2}. \tag{4}$$

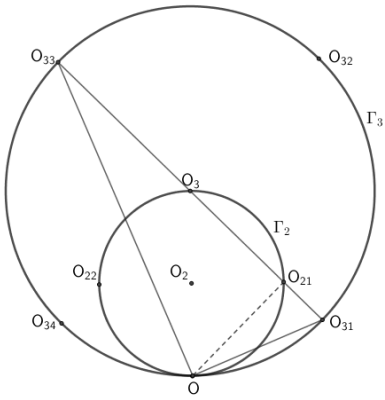


Figura 10: Triângulo singular $OO_{31}O_{33}$

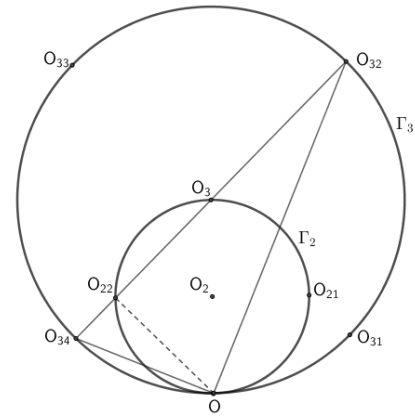


Figura 11: Triângulo singular $OO_{32}O_{34}$

De forma mais geral, as identidades obtidas em (2), (3) e (4) sugerem a seguinte igualdade envolvendo os comprimentos das cordas OO_{ni} de uma circunferência Γ_n para $1 \leq i \leq 2^{n-1}$

$$\frac{1}{d_1^2} = \sum_{i=1}^{2^{n-1}} \frac{1}{\overline{OO_{ni}}^2}. \tag{5}$$

Na verdade, essa igualdade mantém-se verdadeira para todo número natural n, e é o conteúdo da proposição a seguir:

Proposição 1.

$$\frac{1}{d_1^2} = \sum_{i=1}^{2^{n-1}} \frac{1}{\overline{OO_{ni}}^2} \quad \textit{para todo número natural } n. \tag{6}$$

Demonstração. Segue das igualdades (2), (3) e (4) a validade da afirmação para os três primeiros números naturais. Suponha a validade de (6) para um número natural n qualquer. Para a soma envolvendo as cordas $OO_{(n+1)i}$, com $1 \leq i \leq 2^n$, da circunferência Γ_{n+1} temos

$$\sum_{i=1}^{2^n} \frac{1}{\overline{OO_{(n+1)i}}^2} = \sum_{i=1}^{2^{n-1}} \left(\frac{1}{\overline{OO_{(n+1)i}}^2} + \frac{1}{\overline{OO_{(n+1)(i+2^{n-1})}}^2} \right) \tag{7}$$

Como os pontos $O_{(n+1)i}$ e $O_{(n+1)(i+2^{n-1})}$ são singulares conjugados, segue da Propriedade 3 que o segmento OO_{ni} é altura do triângulo retângulo $OO_{(n+1)i}O_{(n+1)(i+2^{n-1})}$. Do Teorema 1 obtemos

$$\frac{1}{\overline{OO_{(n+1)i}}^2} + \frac{1}{\overline{OO_{(n+1)(i+2^{n-1})}}^2} = \frac{1}{\overline{OO_{ni}}^2}. \tag{8}$$

Combinando (6), (7) e (8) obtemos

$$\sum_{i=1}^{2^n} \frac{1}{\overline{OO_{(n+1)i}}^2} = \frac{1}{d_1^2}$$

onde (6) é válida para o natural $n+1$. Segue do Princípio de Indução Finita que (6) é valida para todo número natural n.

Observação 1. Finalizamos esta seção destacando que a partir da simetria existente entre os pontos singulares de uma circunferência Γ_n em relação à reta que contém os centros das circunferências valem as seguintes igualdades para os comprimentos das cordas $OO_{n1}, OO_{n2}, \cdots, OO_{n2^{n-1}}$ da circunferência Γ_n:

$$\begin{aligned}
\overline{OO_{n1}} &= \overline{OO_{n(2^{n-1})}}\\
\overline{OO_{n2}} &= \overline{OO_{n(2^{n-1}-1)}}\\
\overline{OO_{n3}} &= \overline{OO_{n(2^{n-1}-2)}}\\
&\vdots\\
\overline{OO_{n2^{n-2}}} &= \overline{OO_{n(2^{n-2}+1)}}
\end{aligned}$$

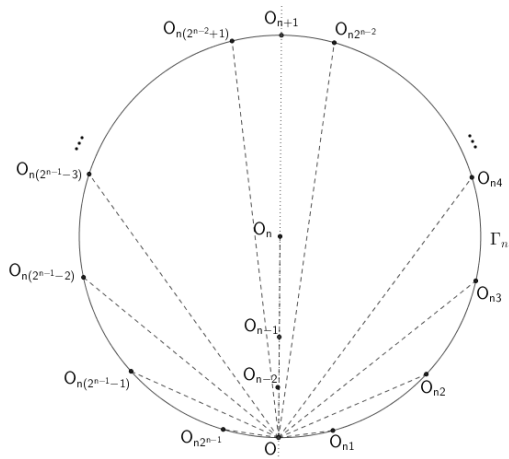


Figura 12: Cordas em Γ_n

Segue dessa observação que a igualdade (6) pode ser reescrita como

$$\frac{1}{d_1^2} = 2\sum_{i=1}^{2^{n-2}} \frac{1}{\overline{OO_{ni}}^2}. \tag{9}$$

7. Estimando o comprimento das cordas OO_{ni} da circunferência Γ_n.

Segue da Propriedade 1 que o ângulo central $O_{n2^{n-1}}\widehat{O_n}O_{n1}$ vale $\frac{\pi}{2^{n-2}}$. Como $\overline{OO_{n1}} = \overline{OO_{n(2^{n-1})}}$, o ângulo central $O\widehat{O}_nO_{n1} = O\widehat{O}_nO_{n(2^{n-1})} = \frac{\pi}{2^{n-1}}$. Consequentemente, os ângulos centrais

$$O\widehat{O}_nO_{n1}, O\widehat{O}_nO_{n2}, \cdots, O\widehat{O}_nO_{nk}, \cdots, O\widehat{O}_nO_{n2^{n-2}}$$

medem, respectivamente,

$$\frac{\pi}{2^{n-1}}, \frac{3\pi}{2^{n-1}}, \cdots, \frac{\pi}{2^{n-1}} + \frac{(k-1)\pi}{2^{n-2}}, \cdots, \pi - \frac{\pi}{2^{n-1}},$$

veja Figura 13. Além disso, lembremos o argumento para calcular o comprimento de uma corda em função de seu ângulo central. Na ilustração da Figura 14, temos uma circunferência de raio r centrada em O, e os pontos A e B sobre ela definem uma corda AB de comprimento c com ângulo central α e um arco de comprimento s. Temos

$$\operatorname{sen}\beta = \frac{c}{2r} \quad \text{e} \quad s = \alpha r$$

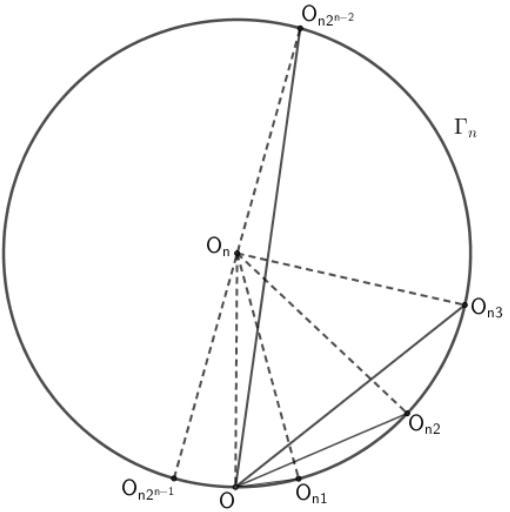


Figura 13: Cordas $OO_{n1}, OO_{n2}, \cdots, OO_{n2^{n-2}}$

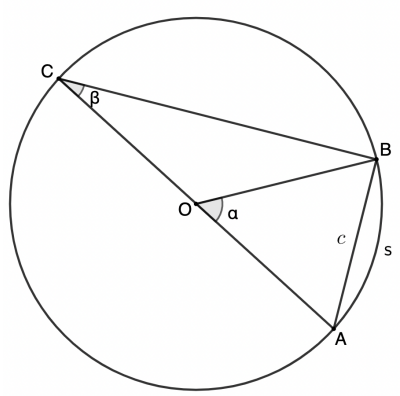


Figura 14: Corda c em função do arco s

e daí segue que

$$\begin{aligned} c &= 2r \operatorname{sen} \beta \\ &= \frac{2s}{\alpha} \operatorname{sen} \frac{\alpha}{2} \\ &= s \frac{\operatorname{sen} \frac{\alpha}{2}}{\frac{\alpha}{2}}. \end{aligned}$$

Para a corda OO_{nk}, que tem ângulo central $O\widehat{O}_nO_{nk} = \frac{(2k-1)\pi}{2^{n-1}}$, a igualdade anterior fornece-nos

$$\begin{aligned} \overline{OO_{nk}} &= s \frac{\operatorname{sen} \frac{\alpha}{2}}{\frac{\alpha}{2}} \\ &= \frac{(2k-1)\pi}{2^{n-1}} r_n \frac{\operatorname{sen} \frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}} \\ &= \frac{(2k-1)\pi}{2^{n-1}} \frac{d_n}{2} \frac{\operatorname{sen} \frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}} \\ &= \frac{(2k-1)\pi}{2^{n-1}} 2^{n-2} d_1 \frac{\operatorname{sen} \frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}} \\ &= \frac{(2k-1)\pi}{2} d_1 \frac{\operatorname{sen} \frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}} \end{aligned}$$

Substituindo essa última igualdade em (9), obtemos

$$\frac{1}{d_1^2} = 2\sum_{k=1}^{2^{n-2}} \frac{1}{\overline{OO_{nk}}^2} = 2\sum_{k=1}^{2^{n-2}} \left(\frac{1}{\frac{(2k-1)\pi}{2} d_1 \frac{\operatorname{sen}\frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}}} \right)^2. \tag{10}$$

Simplificando a igualdade (10), chegamos a

$$\frac{\pi^2}{8} = \sum_{k=1}^{2^{n-2}} \left(\frac{1}{(2k-1)\frac{\operatorname{sen}\frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}}} \right)^2 \tag{11}$$

que vale para todo número natural n. Para concluir, vamos mostrar que

$$\frac{\pi^2}{8} = \lim_{n\to\infty} \sum_{k=1}^{2^{n-2}} \left(\frac{1}{(2k-1)\frac{\operatorname{sen}\frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}}} \right)^2 = \sum_{k=1}^{\infty} \frac{1}{(2k-1)^2}. \tag{12}$$

Para isso, considere a seguinte família de números reais $\{a_{k,n}\}_{k,n\in\mathbb{N}}$ dada por:

$$a_{k,n} = \begin{cases} \dfrac{1}{(2k-1)\frac{\operatorname{sen}\frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}}}, & \text{se } k \le 2^{n-2} \\ 0, & \text{se } k > 2^{n-2} \end{cases}$$

Para qualquer número natural k fixado, segue do limite trigonométrico fundamental que

$$\lim_{n\to\infty} \frac{1}{(2k-1)\frac{\operatorname{sen}\frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}}} = \frac{1}{2k-1}.$$

Para qualquer número natural m fixado, temos

$$\lim_{n\to\infty} \sum_{k=1}^{m} a_{k,n}^2 = \sum_{k=1}^{m} \lim_{n\to\infty} a_{k,n}^2 = \sum_{k=1}^{m} \frac{1}{(2k-1)^2}$$

de onde, fazendo m tender ao infinito, obtemos

$$\lim_{n\to\infty} \sum_{k=1}^{\infty} a_{k,n}^2 = \sum_{k=1}^{\infty} \frac{1}{(2k-1)^2}.$$

Note que, para cada $n \in \mathbb{N}$, o somatório $\sum_{k=1}^{\infty} a_{k,n}^2$ tem apenas as 2^{n-2} primeiras parcelas não nulas, isto é,

$$\sum_{k=1}^{\infty} a_{k,n}^2 = \sum_{k=1}^{2^{n-2}} a_{k,n}^2.$$

Assim,

$$\sum_{k=1}^{\infty}\frac{1}{(2k-1)^2}=\lim_{n\to\infty}\sum_{k=1}^{\infty}a_{k,n}^2=\lim_{n\to\infty}\sum_{k=1}^{2^{n-2}}a_{k,n}^2=\lim_{n\to\infty}\sum_{k=1}^{2^{n-2}}\left(\frac{1}{(2k-1)\frac{\operatorname{sen}\frac{(2k-1)\pi}{2^n}}{\frac{(2k-1)\pi}{2^n}}}\right)^2=\frac{\pi^2}{8}$$

e segue a validade da igualdade (12). Obtemos daí a seguinte proposição:

Proposição 2.

$$\frac{\pi^2}{8}=\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots.$$

Finalmente, para ver que a soma em (1) converge para $\frac{\pi^2}{6}$, usamos a Proposição 2 combinada com o seguinte argumento:

$$\begin{aligned}\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\cdots&=\left(\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots\right)+\left(\frac{1}{2^2}+\frac{1}{4^2}+\frac{1}{6^2}+\frac{1}{8^2}+\cdots\right)\\&=\frac{\pi^2}{8}+\frac{1}{4}\left(\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots\right).\end{aligned}$$

Segue daí que

$$\frac{3}{4}\left(\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots\right)=\frac{\pi^2}{8}$$

, e, por fim, obtemos

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=\frac{\pi^2}{6}.$$

8. Considerações Finais

"A Geometria faz com que possamos adquirir o hábito de raciocinar, e esse hábito pode ser empregado, então, na pesquisa da verdade e ajudar-nos na vida".
(Jacques Bernoulli)

A ideia deste trabalho é apresentar uma demonstração do Problema de Basileia, como ficara conhecida a soma dos inversos dos quadrados dos números naturais, utilizando elementos da Geometria Plana, mas, também, mostrar a importância dos conceitos geométricos na construção do conhecimento matemático, sobretudo no ensino básico.

Esse problema caracterizou-se com grande complexidade, sobretudo, nos séculos XVII e XVIII, quando estudiosos como Gottfried Wilhelm Leibniz (1646-1716), John Wallis (1616-1703) e os matemáticos da família Bernoulli debruçaram-se sobre ele.

Revisando a literatura, percebemos que as resoluções são datadas a partir de 1735, quando Euler encontrou a primeira solução e, quase sempre, fazem uso apenas de conceitos algébricos nas demonstrações.

Sabendo do papel fundamental exercido pela geometria na aprendizagem da Matemática, sobretudo, nas escolas de educação básica e, também, por não encontrar um material escrito evidenciando os conceitos para a prova geométrica do Problema da Basileia, decidimos escrever, ao nosso ver, aquelas que seriam as ideias geométricas necessárias para uma boa compreensão do citado problema.

Agradecimentos

Os autores agradecem à Universidade Estadual de Feira de Santana, à Capes e à SBM pelo apoio financeiro e promoção do Profmat, ao professor Marcos Petrúcio Cavalcante pelas sugestões, ao revisor deste artigo pelas valiosas sugestões de correções e a todos que contribuíram direta ou indiretamente para a realização deste trabalho.

Referências

[1] GAYO, Jairo e WILHELM, Roy. "O problema que tornou Euler Famoso". *Ciência e Natura*, Santa Maria. Vol. 37 Ed. Especial Profmat, 2015, p. 342-355.

[2] HRANKOWSKY, Adam. *Euler's Solution to the Basel Problem*. MathAdam. 2020. Disponível em: <https://medium.com/mathadam/eulers-solution-to-the-basel-problem-77698f08996f>. Acesso em: 17 mai. 2021.

[3] MOURA, Wilbertt José de Oliveira. *O problema da Basileia*. 2013. 51 f. Dissertação (Mestrado Profissional em Matemática), Universidade Federal do Piauí, 2013.

[4] SANDERSON, Grant. *Why is pi here? And why is it squared? A geometric answer to the Basel problem*. 3Blue1Brown. 2018. Disponível em: <https://www.3blue1brown.com/lessons/basel-problem>. Acesso em 03 mar. 2021.

[5] SANDIFER, Ed. *How Euler Did It: Estimating the Basel Problem*. MAA Online. 2003. Disponível em: < http://eulerarchive.maa.org/hedi/HEDI-2003-12.pdf >. Acesso em: 10 mai. 2021.

Darlan Ferreira de Oliveira
Universidade Estadual de Feira de Santana,
Departamento de Ciências Exatas,
Feira de Santana, BA, 44036-900, Brasil.
<dfoliveira@uefs.br>

Joãonito de Jesus Santos
Colégio Municipal Eraldo Tinoco,
Brejões, BA, 45325-000, Brasil
<prof.joao27@gmail.com>

Recebido: 17/08/2021
Publicado: 04/07/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1023

Uma proposta para o cálculo de áreas de polígonos utilizando o GeoGebra

Glaucia Maria Bressan Patricia Spati Elenice Weber Stiegelmeier

Resumo

O presente trabalho tem como objetivo abordar a possibilidade de utilização do *software* Geogebra como ferramenta de ensino no estudo de área de polígonos e analisar o aprendizado de alunos do 3° ano do Ensino Médio. A metodologia de pesquisa utilizada foi a pesquisa de natureza qualitativa, onde utilizou-se da pesquisa-ação colaborativa considerando uma experiência em sala de aula. Os estudos foram baseados na aplicação de atividades práticas aos alunos do 3° ano do Ensino Médio, considerando o contexto do uso das tecnologias como ferramentas de ensino. Nesse processo, apresentam-se aspectos relevantes sobre o estudo de matrizes para o cálculo da área de polígonos. A partir das informações registradas, constatou-se que o uso desse tipo de *software* de matemática dinâmica contribui para uma melhor interação dos alunos, consequentemente, despertando o interesse pelos conteúdos abordados resultando em uma maior aprendizagem.

Palavras-chave: Geometria Analítica; Área de Polígonos; Tecnologia Digital; Ensino de Matemática

Abstract

The goal of this work is to address the use of Geogebra software as a teaching tool in the study of polygon area and analyze the learning of students from 3rd year high school. The research methodology used was a qualitative research, which used collaborative action research considering an experience in the classroom. The studies were based on the application of practical activities to 3rd year high school students considering the context of the use of technologies as teaching tools. In this process, relevant aspects about the study of matrices for the calculation of the polygon areas are presented. From the registered information it was found that the use of this kind of dynamic mathematics software contributes to a better interaction of students, consequently, arousing interest in the content covered, resulting in greater learning.

Keywords: Analytical Geometry; Polygon areas; Digital Technology; Math teaching

1. Introdução

O ensino de Matemática vem passando por diversas transformações ao longo das décadas. A Matemática vem deixando de ser considerada uma ciência de formalização de estruturas, de teorização, de sistematização e de raciocínio lógico formal, e passando a ser mais dinâmica na construção do conhecimento matemático, a partir da inclusão de situações concretas vivenciadas pelo aluno, suas experiências, expectativas e questionamentos diários. D'Ambrosio afirma que os movimentos

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

começaram a dar maior ênfase a uma aprendizagem mais participativa, com uma percepção da importância das atividades para os alunos [7]. Diante dessa perspectiva, o PCNEM – Parâmetros Curriculares Nacionais do Ensino Médio [5] e os PCN - Parâmetros Curriculares Nacionais [6] retomam e reafirmam o discurso da LDB - Lei de Diretrizes e Bases da Educação Nacional (LDB 9394/96) [4], de que o ensino da Matemática deve contribuir para que os alunos desenvolvam habilidades relacionadas à representação, compreensão, comunicação, investigação e, também, à contextualização sociocultural.

Recentemente, testes de rendimentos aplicados aos alunos pelos Governos, tanto Estadual quanto Federal, tais como a Prova Brasil e o SAEB (Sistema de Avaliação do Ensino Brasileiro), entre tantos outros, indicam um baixo desempenho e rendimento na área de Matemática, que tem sido apontada como a disciplina que mais contribui, significativamente, na elevação das taxas de retenção. Pode-se ressaltar novamente a LDB (Lei nº 9.394/96) [4], a qual afirma que o ensino médio tem como finalidades centrais tanto a consolidação e o aprofundamento dos conhecimentos adquiridos durante o nível fundamental, quanto o intuito de garantir a continuidade de estudos, seja ele voltado à preparação para o trabalho ou para o exercício da cidadania, a formação ética, o desenvolvimento da autonomia intelectual e/ou a compreensão dos processos produtivos.

No que concerne ao processo de ensino-aprendizagem de álgebra, pode-se inferir que esse caracteriza-se pela utilização de regras que, de um modo geral, vêm se apresentando completamente desvinculadas da realidade dos alunos. Como afirma [18], o ensino-aprendizagem de matrizes é um ensino voltado para a transmissão de regras, descontextualizado da realidade e da própria Matemática, em descompasso com os avanços tecnológicos e com os estudos já realizados pela Psicologia Educacional.

As crianças e os jovens usam as tecnologias digitais com frequência, utilizando dispositivos para acesso à internet. Visto que diferentes usos já estão incorporados na vida de muitos estudantes, é necessário incluir ferramentas tecnológicas para viabilizar práticas pedagógicas com aplicativos, *softwares*, buscadores, redes sociais, com a finalidade educacional, para além do uso social [20]. As tecnologias podem não só representar um conjunto de ferramentas auxiliares para o trabalho do professor e dos alunos, como podem abrir novas oportunidades de aprendizagem.

Pode-se identificar a docência para o século XXI no professor que é capaz de integrar várias mídias em suas práticas docentes, além das habilidades e dos saberes específicos da sua área [20]. Dessa forma, cabe à educação estabelecer diálogos com as práticas culturais dos adolescentes e jovens, qualificar crítica e eticamente os usos que eles fazem das tecnologias na direção de uma participação social mais efetiva [20, 21].

Considerando as competências específicas de Matemática segundo a Base Nacional Comum Curricular (BNCC), a tecnologia está explicitamente presente nas competências 5 e 6.

,

> *Competência 5. Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados [2].*
> *Competência 6. Enfrentar situações-problema em múltiplos contextos, incluindo-se situações imaginadas, não diretamente relacionadas com o aspecto prático-utilitário, expressar suas respostas e sintetizar conclusões, utilizando diferentes registros e linguagens (gráficos, tabelas, esquemas, além de texto escrito na língua materna e outras linguagens para descrever algoritmos, como fluxogramas, e dados)* [2].

O uso das Tecnologias da Informação e Comunicação (TIC) deve ser visto como uma oportunidade de aperfeiçoar a aprendizagem dos alunos, embasada em uma discussão crítica, muito além da incursão de novos recursos didáticos. No atual contexto social, com acesso à informação e à comunicação, toda instituição é conduzida a inlcuir o uso da tecnologia no ensino, tornando capaz de adaptar-se à sociedade [23].

Integrar a tecnologia ao ambiente educacional requer planejamento e organização, tendo que ser voltada para o processo de aprendizagem do aluno e as demandas que cada escola possui. Por isso, a modernização da educação deve ser feita com cuidado, para que a tecnologia seja uma ferramenta de auxílio e não de dispersão do aluno. O uso de tecnologias digitais no ensino pode ter grande contribuição no aprendizado dos alunos. Quando aliada ao processo educacional e com planejamento, a utilização de tecnologias oferece uma enorme gama de opções a serem exploradas tanto dentro como fora da sala de aula [22, 23].

O objetivo deste trabalho é abordar a possibilidade de utilização do *software* GeoGebra [12] como ferramenta de ensino para o cálculo de áreas de polígonos, quando são conhecidas as coordenadas de seus vértices, por meio de Determinantes. As atividadas propostas foram aplicadas em alunos do 3° ano do Ensino Médio, considerando o contexto do uso das tecnologias digitais como ferramentas de ensino.

2. Revisão da Literatura

A educação tecnológica básica hoje é uma das diretrizes que a LDBEN estabelece para orientar o currículo do Ensino Médio. A lei associa a "compreensão dos fundamentos científicos dos processos produtivos [4]" ao relacionamento entre teoria e prática em cada disciplina do currículo. E, ainda, tem o sentido de preparar os alunos para viver e conviver em um mundo no qual a tecnologia está cada vez mais presente, no qual a tarja magnética, o celular, o código de barras e outros tantos recursos digitais se incorporam velozmente à vida das pessoas, qualquer que seja sua condição socioeconômica.

Os trabalhos [11, 14] apresentam uma análise nos periódicos disponibilizados nas Plataformas na internet com o objetivo de investigar como conceitos matemáticos são ensinados aos alunos. Mais especificamente, [14] faz um estudo das Metodologias Ativas no ensino da Álgebra Linear. Os resultados apresentados demonstram que as metodologias ativas contribuem para a aproximação entre os estudantes e o professor durante as aulas, o que facilita a mediação desse durante o processo de ensino-aprendizagem nessa disciplina. O autor ressalta que a aplicabilidade das aulas diferenciadas ganhou importantes discussões, pois possibilita compreender as potencialidades das metodologias ativas de ensino, assim como a transformação das práticas educacionais no ambiente escolar.

As Diretrizes Curriculares Nacional de Educação para o Ensino Médio (DCNE- EM) indicam a importância do uso das tecnologias em sala de aula, afirmando que o projeto político-pedagógico das unidades escolares que ofertam o Ensino Médio deve considerar a utilização de diferentes mídias como processo de dinamização dos ambientes de aprendizagem e construção de novos saberes [3].

Assim, a utilização das Tecnologias Digitais na sala de aula tem se tornado fundamental no processo de ensino. A necessidade de mudanças no ensino encontra-se na BNCC, que afirma que, em decorrência do avanço e da multiplicação das tecnologias de informação e comunicação, os estudantes estão dinamicamente inseridos nessa cultura. Os jovens têm se engajado cada vez mais como protagonistas da cultura digital, envolvendo-se diretamente em novas formas de interação multimidiática e multimodal e de atuação social em rede [2]. Na BNCC, o foco está no reconhecimento

das potencialidades das tecnologias digitais para a realização de atividades relacionadas a todas as áreas do conhecimento que permite aos estudantes usar diversas ferramentas de *software* e aplicativos para compreender e produzir conteúdos em diversas mídias, simular fenômenos e processos das diferentes áreas do conhecimento, e elaborar e explorar diversos registros de representação matemática [2].

Buscando novos meios para o ensino da Matemática, [22] utilizou o *software* GeoGebra para o estudo de Geometria Analítica. Os resultados mostram que a inclusão das tecnologias digitais na aula de Matemática pode se tornar um grande diferencial para a realização de um processo de ensino e aprendizagem mais significativo e prazeroso, e que a utilização do *software* pode contribuir para o ensino e aprendizagem de Geometria da Analítica.

Para auxiliar os professores da Educação Básica, [1] utiliza do *software* GeoGebra no ensino de matrizes e algumas de suas aplicações, especialmente das matrizes circulantes e de sua importância do ponto de vista computacional, aos alunos do Ensino Médio para que estabeleçam relações entre os conteúdos da sala de aula com o mundo real, podendo, assim, o desinteresse pela Matemática ser minimizado.

Pensando na importância do estudo de matrizes no cotidiano e nas dificuldades apontadas por [22] no ensino da matemática, [19] utiliza o *software* GeoGebra como estratégia para o ensino de vetores, matrizes, projeções ortogonais e o método de mínimos quadrados. O GeoGebra é utilizado para ilustrar graficamente as soluções e realizar cálculos complexos de forma simples, contribuindo para a aprendizagem dos estudantes e fazendo com que novos professores adotem o *software* como ferramenta para aprimorar suas práticas pedagógicas. Neste sentido, também com o objetivo de aprofundar a formação do profissional da matemática na Educação Básica, [17] utiliza o *software* GeoGebra para o ensino matrizes e determinantes, e assim assimilar a teoria e a prática com o uso da tecnologia, contribuindo muito, devido à possibilidade de visualização e manipulação das construções geométricas.

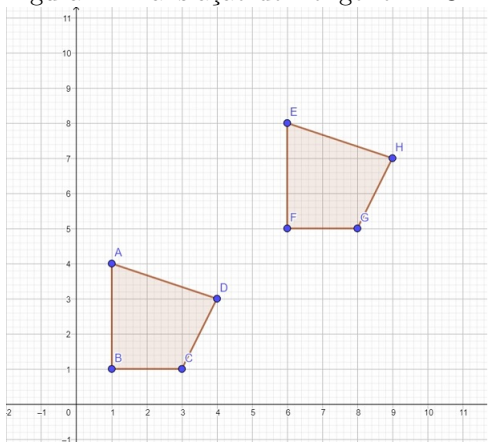
Dessa forma, a inserção das tecnologias digitais na sala de aula pode favorecer o entendimento das propriedades nas aulas de Matemática, pois o uso das mesmas faz com que um novo mundo abra-se ao educando. O aluno pode compreender melhor a construção do conhecimento e, com isso, produzir significado ao que lhe está sendo apresentado. E, assim, fazendo a junção dos conteúdos matemáticos com as tecnologias, pode-se conseguir que os alunos tenham menores dificuldades no aprendizado. Em todos os trabalhos aqui apresentados, observa-se a necessidade de buscar novos métodos de ensino, diferente do tradicional, onde o aluno constrói seu conhecimento com aulas mais dinâmicas, fazendo com que desenvolvam sua criatividade e colaboração. Nesse sentido, a tecnologia abre espaço para que os estudantes possam viver novas experiências matemáticas.

3. Uso do GeoGebra no Cálculo de Áreas

Esta seção apresenta a utilização do GeoGebra para o cálculo de áreas de polígonos utilizando conceitos de matrizes e determinantes. A versão utilizada neste trabalho é o *GeoGebra Classic* para a modalidade *Desktop*, com sistema operacional *Windows*. Como fonte de consulta para os conceitos de Geometria Analítica utilizados nessa seção, indica-se [8].

Considerando os polígonos ABCD e EFGH, congruentes, representados na Figura 1, constroem-se as matrizes M e N, representadas a seguir, ambas 4x2, utilizando as coordenadas dos vértices do polígono.

Figura 1: Translação do Polígono ABCD.



Fonte: Elaborada pelas autoras.

$$M = \begin{bmatrix} 1 & 4 \\ 1 & 1 \\ 3 & 1 \\ 4 & 3 \end{bmatrix} \qquad N = \begin{bmatrix} 6 & 8 \\ 6 & 5 \\ 8 & 5 \\ 9 & 7 \end{bmatrix}$$

O polígono EFGH foi obtido a partir de duas movimentações de ABCD, sendo uma na horizontal e outra na vertical (veja Figura 1). Efetuando-se a operação N – M, como a seguir, obtém-se a matriz m1, também 4x2, tal que a primeira coluna é composta pelo número 5, e a segunda coluna pelo número 4, o que significa que o polígono ABCD precisa deslocar 5 unidades para a direita e 4 unidades para cima para coincidir com o polígono EFGH, representado na Figura 1.

$$N = \begin{bmatrix} 6 & 8 \\ 6 & 5 \\ 8 & 5 \\ 9 & 7 \end{bmatrix} - M = \begin{bmatrix} 1 & 4 \\ 1 & 1 \\ 3 & 1 \\ 4 & 3 \end{bmatrix} = m1 = \begin{bmatrix} 5 & 4 \\ 5 & 4 \\ 5 & 4 \\ 5 & 4 \end{bmatrix}.$$

Efetuando-se a operação M – N, como a seguir, obtém-se a matriz m2, também 4x2, sendo que o número –5 está na primeira coluna e –4 na segunda coluna, ou seja, o polígono EFGH precisa deslocar 5 unidades para a esquerda e 4 unidades para baixo, para coincidir com o polígono ABCD.

$$M = \begin{bmatrix} 1 & 4 \\ 1 & 1 \\ 3 & 1 \\ 4 & 3 \end{bmatrix} - N = \begin{bmatrix} 6 & 8 \\ 6 & 5 \\ 8 & 5 \\ 9 & 7 \end{bmatrix} = m2 = \begin{bmatrix} -5 & -4 \\ -5 & -4 \\ -5 & -4 \\ -5 & -4 \end{bmatrix}.$$

Um método para a obtenção de áreas de polígonos representados no plano cartesiano, quando são conhecidas as coordenadas de seus vértices, pode ser dado pelo cálculo de determinantes. Se as coordenadas dos vértices de um triângulo representado no plano cartesiano são conhecidas, é possível calcular sua área por intermédio da composição e/ou decomposição de polígonos auxiliares. Nesse

processo, é realizada uma série de multiplicações entre resultados de subtrações entre abscissas e entre ordenadas dos pontos A, B e C, além da divisão por 2. As etapas desse cálculo podem ser resumidas em um determinante de ordem 3, formado pelas coordenadas desses pontos, obedecendo à formatação da equação (1).

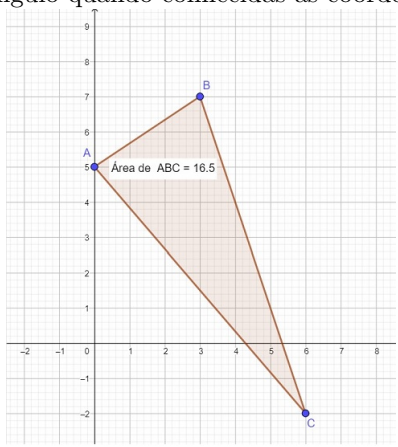
$$\begin{vmatrix} x_A & y_A & 1 \\ x_B & y_B & 1 \\ x_C & y_C & 1 \end{vmatrix}. \tag{1}$$

Considerando o caso do triângulo de vértices com coordenadas A$(0, 5)$, B$(3, 7)$ e C$(6, -2)$, tem-se (2).

$$\text{Área}_{(ABC)} = \text{metade do valor absoluto de} \begin{vmatrix} 0 & 5 & 1 \\ 3 & 7 & 1 \\ 6 & -2 & 1 \end{vmatrix}. \tag{2}$$

O resultado está ilustrado na Figura 2.

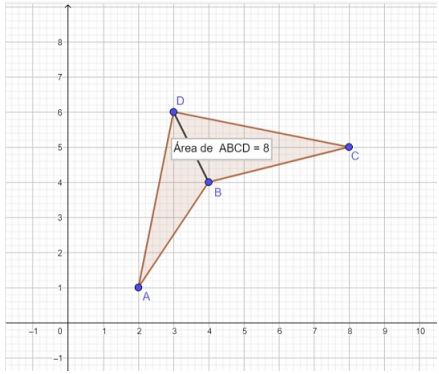
Figura 2: Área do triângulo quando conhecidas as coordenadas de seus vértices.



Fonte: Elaborada pelas autoras.

A área de um polígono representado no plano cartesiano pode ser calculada a partir das coordenadas de cada vértice, baseando-se no princípio de que um polígono pode ser dividido em vários triângulos, como ilustra a Figura 3.

Figura 3: Área de um polígono quando conhecidas as coordenadas de seus vértices.



Fonte: Elaborada pelas autoras.

O quadrilátero é dividido em dois triângulos, ABD e BCD. A área do quadrilátero ABCD será a soma das áreas dos triângulos ABD e BCD.

$$\text{Área}_{(\text{ABCD})} = \text{Área}_{(\text{ABD})} + \text{Área}_{(\text{BCD})}$$

Como a área do triângulo é

$$\text{Área} = \frac{1}{2}\left|\text{determinante[matriz]}\right|$$

tem-se que a área do polígono ABCD será dada por (3).

$$\text{Área} = \frac{1}{2}\left|\text{determinante[M]}\right| + \frac{1}{2}\left|\text{determinante[N]}\right| \tag{3}$$

4. Procedimentos Metodológicos

As atividades aqui propostas foram aplicadas no segundo semestre de 2019, a 55 alunos do 3º ano do Ensino Médio, sendo 26 do 3º ano A e 29 do 3º ano B da Escola Estadual Professor José Leite Pinheiro, da cidade de Cerqueira César, estado de São Paulo.

A abordagem metodológica utilizada nessa pesquisa enquadra-se no tipo qualitativa. A escolha dessa abordagem deve-se à busca pela observação e compreensão das ações, fatos e resultados de forma mais abrangente, evidenciando as ações dos sujeitos investigados [15].

A segunda autora dessa proposta é a professora regente destas turmas. Dessa forma, na pesquisa-ação colaborativa, muito comum em situações que envolvem a dinâmica escolar, os conhecimentos produzidos a partir da interação professor-alunos são fontes para o trabalho investigativo e oportunizam reflexões pedagógicas para um melhor fazer docente [9].

Primeiramente, foi aplicada uma avaliação diagnóstica, com o objetivo de investigar os conhecimentos adquiridos pelos alunos sobre o tema e sobre a utilização de recursos computacionais durante sua vida estudantil. Em seguida, uma aula teórica sobre os conceitos de matrizes e determinantes foi ministrada, para apresentação do conteúdo. Nas aulas seguintes, foram realizadas as atividades propostas, descritas na Seção 3, utilizando o GeoGebra no laboratório de informática.

Ao final das atividades, a segunda avaliação diagnóstica foi aplicada, a fim de verificar a receptividade das atividades propostas, além de verificar se o uso do GeoGebra influenciou positivamente no processo de ensino e aprendizagem dos conteúdos abordados. Essa análise diagnóstica qualitativa colabora para a elaboração de um planejamento adequado, como forma de minimizar as dificuldades, ampliar a contextualização do uso de tecnologias no ensino de matemática, aproximando-a da realidade dos estudantes, na busca por um ensino inovador, que priorize o uso de tecnologias e que obtenha, como resultado final, a consolidação dos conteúdos abordados.

5. Resultados e Discussão

Nesta seção, são apresentadas as porcentagens das respostas obtidas pelos alunos nas avaliações diagnósticas e a percepção dos autores quanto à aplicação das atividades, aplicadas aos alunos do 3º ano do Ensino Médio, conforme descrito anteriormente.

5.1. Resultado da Avaliação Diagnóstica 1

O objetivo desta avaliação é conhecer a relação dos alunos com a disciplina de Matemática e investigar os conhecimentos prévios dos estudantes relacionados aos recursos computacionais na escola e como esses recursos foram utilizados. O primeiro questionário é composto por 7 questões, apresentadas a seguir, cujas respostas possíveis eram "sim" ou "não," com espaço para escrever justificativas.

Questão 1: Você tem dificuldade na aprendizagem dos conteúdos de Matemática? A maioria dos alunos, 37 dos 55 estudantes pesquisados, afirmou encontrar alguma dificuldade na aprendizagem de conceitos matemáticos, representando 67% do total.

Questão 2: Você sabe o que é matriz?

Grande parte dos estudantes, 68%, assinalou a opção "não", dizendo que não apresenta domínio dos conceitos de matrizes. Vale ressaltar que os alunos participantes da pesquisa já haviam estudado os conceitos abordados. Dentre os alunos pesquisados, 38 deles alegam que já estudaram os conceitos de matrizes, porém não lembram.

Questão 3: Você sabe calcular a área de triângulos?

Como resposta a essa questão, é possível observar que 39 alunos apresentam domínio dos conceitos de área de triângulos, ou seja, 70% assinalaram a opção "sim", porém, precisam utilizar a fórmula (metade do produto entre base e altura).

Questão 4: Você sabe calcular a área de polígonos?

Um total de 31 alunos, representando 56%, assinalou que não tem conhecimento do cálculo da área de polígonos. Até então, os alunos não haviam utilizado a ideia de dividir o polígono em triângulos e calcular a área separadamente, já que esse conceito é conhecido por eles.

Questão 5: Você já utilizou determinantes para calcular a área de polígonos?

Um total de 90% dos alunos desconhecia a técnica de utilizar determinantes para o cálculo de área de polígonos quando conhecidos seus vértices, e embora já estudado, os estudantes que participaram da pesquisa não tinham se apropriado, de modo significativo, dos conceitos de determinantes.

Questão 6: Você acredita que o uso do computador pode ajudá-lo(a) a aprender Matemática?

Ao serem questionados sobre a utilização de recursos computacionais nas aulas de matemática, 51 alunos, ou seja, 94%, afirmam que a utilização de uma ferramenta computacional pode facilitar o processo de ensino e aprendizagem da matemática.

Algumas justificativas para essa resposta merecem destaque: "Pois a internet já é costume para a nova geração, então usá-la a favor dos estudos seria bom"; "A internet possui muitas informações que podem ajudar e facilitar o aprendizado dos alunos"; "Muito, pois através do computador conseguimos obter mais informações"; "Com o computador é possível utilizar programas que auxiliam no aprendizado de matemática"; "Acho que a tecnologia pode auxiliar e muito nos estudos e a aula fica mais dinâmica"; "O jovem se sente atraído pela tecnologia, ficando bem mais fácil aprender com o uso do recurso".

Questão 7: Você conhece ou já utilizou o software *GeoGebra?*

Verificou-se que a ferramenta computacional GeoGebra não era de domínio dos alunos, pois 86% assinalaram a opção "não", mas afirmaram que, por meio da visualização e construção do objeto de estudo, há uma melhor compreensão de conceitos matemáticos.

A partir das análises dos resultados da primeira avaliação diagnóstica, verificou-se que a maioria dos alunos mostrou não ter conhecimento sobre os conceitos de matrizes e sobre o cálculo da área de polígonos, embora já tivessesm estudado determinantes. Por outro lado, os alunos mostraram-se dispostos a utilizar ferramentas computacionais como o GeoGebra na aula de Matemática, ressaltando que pode auxiliar no processo de ensino e aprendizagem de conteúdos matemáticos.

5.2. Atividade 1 - Aplicação de conceitos de Matrizes no Ensino Médio

Após a aplicação da avaliação diagnóstica, foram apresentadas aos alunos as definições formais de matrizes e suas operações. Em seguida, os alunos realizaram algumas atividades utilizando os conceitos de matrizes, assim como suas operações de adição, subtração e multiplicação, cujas habilidades [20] são: "*Utilizar elementos de matrizes para organizar e justificar a resolução de situações-problema baseadas em contextos do cotidiano*", "*Relacionar representações geométricas a comandos na linguagem matemática*" e "*Utilizar a notação matricial para representar figuras planas.*" Foram utilizadas aproximadamente 4 aulas de 50 minutos para a realização dessa atividade.

5.3. Atividade 2 - Aplicação dos conceitos de matrizes com o uso do GeoGebra

Após a aplicação da Atividade 1, os alunos foram levados ao laboratório de informática para execução da Atividade 2 com a utilização do *software* GeoGebra. Primeiramente foi apresentado o *software*, destacando suas principais ferramentas e funções e posteriormente, foram desenvolvidas atividades de modo a facilitar a compreensão dos princípios básicos de funcionamento do *software* no ensino de matrizes. O laboratório de informática possuía somente 10 computadores em funcionamento. Diante disso, os alunos formaram grupos para a realização da atividade. Foram utilizadas 2 aulas para a apresentação do GeoGebra e 4 aulas para a realização da Atividade 2.

No início da atividade, os alunos demonstraram muitas dúvidas quanto à execução dos comandos, mas, com o tempo, mostraram-se mais interessados na utilização do programa e passaram dicas uns para os outros, demonstrando-se muito entusiasmados com a atividade.

Na realização dessa atividade, foi possível observar que a introdução da ferramenta computacional despertou o interesse dos alunos pelo seu uso e a colaboração no aprendizado dos demais colegas.

5.4. Atividade 3 - Aplicação de área de polígonos usando determinantes

A aplicação da Atividade 3 também foi executada no laboratório de informática com a utilização do GeoGebra. Os alunos realizaram a construção de triângulos calculando assim suas áreas. As áreas dos triângulos representados no plano cartesiano puderam ser calculadas a partir das coordenadas de cada vértice, via determinante de uma matriz quadrada de ordem 3 e logo após compararam os resultados obtidos através da ferramenta "Área" do GeoGebra. Os alunos concluíram que a área do triângulo é a metade do módulo do determinante de uma matriz quadrada de ordem 3. O cálculo da área de polígonos de 4 lados ou mais foi facilmente realizado, visto que um polígono pode ser dividido em vários triângulos. Foram utilizadas aproximadamente 4 aulas para a realização dessa atividade.

A partir dessa análise, concluiu-se que, para obter um ensino de matemática eficiente, faz-se necessário que o docente traga para a aula ferramentas inovadoras que despertem a curiosidade dos alunos e promovam a relação entre conteúdos estudados, como o uso de determinantes para o cálculo de área de polígonos. De acordo com [10], o uso do GeoGebra vem cada vez mais ganhando espaço quando se trata de uma melhoria no ensino-aprendizagem.

5.5. Resultado da Avaliação Diagnóstica 2

Após o término da Atividade 3 foi aplicada a segunda avaliação, para verificar a repercussão da execução das atividades propostas. Os resultados são apresentados a seguir.

Questão 1:Como você classificaria a aula utilizando o GeoGebra que você participou?

Inicialmente foi solicitado que os alunos classificassem as atividades realizadas como "Muito Bom", "Bom", "Regular" ou "Ruim", onde 31 alunos, 59% classificaram como "Muito Bom" e 24 alunos, 41% classificaram como "Bom," o que mostra que a proposta foi bem aceita.

Questão 2:O GeoGebra despertou seu interesse pelo assunto estudado?

Um total de 48 alunos, que representam 86%, responderam que, utilizando recursos computacionais como o GeoGebra, os conteúdos são mais fáceis de assimilar, sendo assim o interesse pelo assunto estudado. O restante, 14%, respondeu que despertou o interesse "parcialmente". Algumas justificativas merecem ser destacadas: "No começo achei difícil, mas é engenhoso e prático e eu posso dizer que realmente aprendi algo novo"; "Despertou meu interesse pela praticidade e consegui aprender o conteúdo"; "Uma aula diferenciada é muito mais legal de se aprender"; "Toda aula diferenciada é boa e facilita muito despertando o interesse dos alunos"; "É uma atividade dinâmica onde podemos pôr em prática nossos aprendizados".

Questão 3:Você acredita que a utilização do GeoGebra como recurso complementar às aulas tradicionais de Matemática tornaria o conteúdo mais atrativo/compreensível?

A resposta a essa pergunta foi unânime, todos responderam que sim. Algumas justificativas apontadas pelos alunos: "Sim, pela facilidade para calcular a área e o determinante"; "Sim, pois saímos da rotina e cada vez fazemos algo novo e diferente"; "Sim, a aula foge do convencional e passa a

ser mais interessante"; "Sim, aprendi várias coisas novas"; "Ajuda muito nas atividades e fica mais fácil de aprender"; "A facilidade dos cálculos, aprendi a fazer matriz no GeoGebra".

Por meio das respostas obtidas com os alunos do 3º ano do Ensino Médio, constatou-se que o uso do Geogebra despertou o interesse da maioria dos alunos pelo conteúdo estudado e todos afirmaram que o uso do *software* facilita a compreensão do conteúdo abordado, além de proporcionar o contato com uma nova ferramenta computacional. Esse resultado está de acordo com [13], que afirmam que o ensino não deve ser praticado apenas na forma tradicional, mas também utilizando outras metodologias, como é o caso do uso do GeoGebra, proposto neste trabalho, apresentando o conteúdo de uma forma mais dinâmica e favorecendo a apropriação dos conhecimentos.

A partir das justificativas apontadas pelos alunos, é possível concluir que a utilização do *software* GeoGebra como ferramenta de ensino contribui para uma melhor interação dos alunos e, consequentemente, na aprendizagem. De acordo com [10], o uso do GeoGebra traz bons resultados e motiva os alunos a estudarem um pouco mais, por deixar alguns conteúdos mais intuitivos. Dessa forma, as tecnologias podem ser aliadas ao processo de ensino e aprendizagem.

6. Considerações Finais

O presente trabalho abordou o uso do *software* Geogebra como ferramenta de ensino para o cálculo de área de polígonos. As atividades propostas foram aplicadas a alunos de uma turma de 3° ano do Ensino Médio, buscando-se valorizar o processo de ensino e aprendizagem através da utilização desse *software* de matemática dinâmica. Dessa forma, o ensino de matemática passa a assumir uma ação ativa diante do conhecimento, uma vez que não se limita somente aos aspectos puramente abstratos e formais, mas incorpora os aspectos criativos da própria Matemática; permitindo um maior protagonismo dos estudantes.

São apresentados, principalmente, aplicações que contribuem para o entendimento das operações de matrizes, como a soma, subtração e produto, o cálculo de determinante de uma matriz quadrada de ordem 3 e o cálculo de área de polígonos por meio de determinantes, pois associando matrizes à geometria, aproveitam-se recursos visuais no processo de ensino e aprendizagem.

Diante do exposto, é possível estabelecer algumas considerações importantes em relação ao objeto de estudo pesquisado e ao grupo de alunos que foram sujeitos de pesquisa. Observa-se que a ferramenta tecnológica representa um importante recurso para a sala de aula, quando inserids nas aulas de forma planejada, para que não se disperse, objetivando o processo de aprendizagem do aluno e as demandas da escola.

É importante destacar que os alunos participantes da pesquisa já haviam estudado de forma teórica os conceitos abordados; entretanto, durante a aplicação da primeira atividade, foi observado que a maioria dos alunos não apresentava domínio dos conceitos. Tal situação foi constatada também com os demais conceitos abordados nas atividades. A utilização da ferramenta computacional GeoGebra também não era de domínio dos alunos, sendo necessária a apresentação das principais janelas do *software* antes do início da atividade.

Durante a aplicação das atividades, os alunos foram orientados e suas dúvidas esclarecidas. Dessa forma, todos conseguiram resolver as atividades propostas, e foi possível observar que os alunos mantiveram-se motivados, entusiasmados e comprometidos em aprender a resolver as situações propostas e a verificar, por meio da construção das respostas no *software* GeoGebra, o que representava tal imagem ou resultado, assim interpretando e refletindo cada resposta. Vale ressaltar que os alunos familiarizaram-se rapidamente com os comandos do *software* GeoGebra, e, quanto

aos recursos próprios do computador, nenhum aluno demonstrou ter dificuldade com a nova ferramenta. Dessa forma, o objetivo do trabalho, de abordar a possibilidade de utilização do Geogebra como ferramenta de ensino no estudo de área de polígonos, foi atingido.

Os resultados obtidos nesse trabalho mostraram-se satisfatórios, uma vez que, ao serem desenvolvidas as atividades das situações-problema sobre área de polígonos com os alunos, demostrou-se que a utilização das tecnologias digitais fazem com que os estudantes passem a se relacionar melhor com matemática, tornando-os mais independentes e agentes do seu próprio aprendizado.

As atividades aqui propostas estão longe de esgotar as possibilidades de abordagem do assunto, porém tornam possível o conhecimento de matrizes como estruturas de representação dessa importante ferramenta de uso computacional, possibilitando um aumento do interesse pela matemática e, consequentemente, auxiliam no ensino de Matemática. Trata-se, pois, de atividades fundamentais, e a utilização do *software* GeoGebra corrobora para um ensino dinâmico e temporal. E, ainda, vale destacar que, no Ensino Médio, a incorporação de tecnologias, devido a sua importância, está no próprio nome de área "Matemática e suas Tecnologias [16]".

É importante ressaltar que, segundo a nova BNCC, o conteúdo de Matrizes foi recentemente retirado do currículo paulista do Ensino Médio. No entanto, o conteúdo de matrizes é utilizado de forma implícita para resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, cálculo de áreas de figuras geométricas, usando técnicas algébricas e gráficas com o apoio de tecnologias digitais, como apresentado no presente trabalho. Vale destacar que no Referencial Curricular para o Ensino Médio do Paraná [16] os conteúdos de Matrizes e determinantes são citados na unidade temática de Números e Álgebra. Tais conteúdos, além da inclusão do uso de tecnologias digitais em sala de aula, ainda constam na BNCC.

Portanto, para que o ensino de matemática seja eficiente, fica evidente a necessidade de escolas preparadas, que possam oferecer uma educação de qualidade, com espaços físicos e materiais adequados ao seu desenvolvimento. Além disso, torna-se primordial que o docente passe a fazer uso das tecnologias da informação em suas aulas, pois são grandes os desafios enfrentados no ensino, e desenvolver práticas pedagógicas eficientes faz-se necessário neste novo cenário educacional.

Referências

[1] ARRUDA FILHO, E. P. *As elegantes matrizes circulantes*, 2019. 54p. Dissertação de Mestrado Profissional em Matemática em Rede Nacional - Universidade Federal de São João Del Rei, São João Del Rei, 2019.

[2] BRASIL, Ministério da Educação. *Base Nacional Comum Curricular*. Brasília: MEC, 2018.

[3] BRASIL, Ministério da Educação. *Diretrizes Curriculares Nacionais para o Ensino Médio 4/5/2011 - Projetos Políticos Pedagógicos/Cap. VIII*. Brasília: MEC, 2011.

[4] BRASIL. Ministério de Educação e Cultura. *LDB - Lei nº 9394/96, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da Educação Nacional*. Brasília: MEC, 1996.

[5] BRASIL, Ministério da Educação. Secretaria de Educação Média e Tecnológica. *Parâmetros Curriculares Nacionais*: ensino médio: ciências da natureza, matemática e suas tecnologias. Brasília: MEC, 1999.

[6] BRASIL, Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais*: introdução aos PCNs. Secretaria de Educação Fundamental. Brasília: MEC, 1997.

[7] D'AMBROSIO, U. *Educação Matemática*: da teoria à prática. 2ª ed. Campinas, SP, Papirus (Coleção Perspectivas em Educação Matemática), 1997.

[8] DELGADO, J.; FRENSEL, K.; CRISSAFF, L. *Geometria analítica* - Coleção Profmat. Rio de Janeiro: Sociedade Brasileira de Matemática, 2013.

[9] ESTEBAN, M. P. S. *Pesquisa qualitativa em educação*: fundamentos e tradições. Porto Alegre: AMGH, 2010.

[10] FEITOSA, M. C.; AQUINO, A. A.; SOUSA, B. F.; LAVOR, O. P. "O uso do GeoGebra mobile como ferramenta auxiliar no ensino de funções inversas e logarítmicas". *Remat: Revista Eletrônica da Matemática*, v.6 n°2, p.e2003, 2020.

[11] FONDA, C. R. S.; SILVA, M. J. F. "Um panorama das pesquisas a respeito de área de triângulos". *Revista de Produção Discente em Educação Matemática*, São Paulo, v.8, n°1, p. 37-53, 2019.

[12] GEOGEBRA. *Estudo de Matrizes e Sistemas Lineares com GeoGebra*. Disponível em <https://www.geogebra.org/m/haar5brw>. Acesso em: 27 jun. 2021.

[13] LOPES,T.B.;SANTOS,L.G.dos. O uso do GeoGebra como ferramenta auxiliar para estudo da reta tangente a um gráfico. *RENOTE:Revista Novas Tecnologias na Educação*, v.14, n°2, 2016.

[14] MORAES, E. A. *Metodologias ativas no ensino da Álgebra Linear*: um estado de arte, 2020. 58p. Dissertação de Mestrado Profissional em Matemática em Rede Nacional - Universidade Federal do Amazonas, Manaus, 2020.

[15] OLIVEIRA, M. M. *Como fazer pesquisa qualitativa*. 4ª ed. Petrópolis: Vozes, 2012.

[16] PARANÁ. *Referencial Curricular para o Ensino Médio do Paraná*. Secretaria de Educação e do Esporte do Estado do Paraná, 2021

[17] REIS, M. A. L. *A utilização do GeoGebra no ensino das Transformações Lineares*, 2020. 63p. Dissertação de Mestrado Profissional em Matemática em Rede Nacional - Universidade Federal do Amazonas, Manaus, 2020.

[18] SANCHES, M. H. F. *Efeitos de uma estratégia diferenciada dos conceitos de matrizes*, 2002. 138p. Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Educação, Campinas, 2002.

[19] SANTANA, F. T.; MACEDO, I. M. A.; MARCONE, M. H. F.; SANTANA, F. L. "Inovação no processo de ensino e aprendizagem de álgebra linear usando o software geogebra". *Brazilian Journal of Development*, Curitiba, v. 5, n° 9, p. 15095-15105, 2019.

[20] SÃO PAULO. Secretaria de Estado da Educação. *Diretriz Curricular de Tecnologia e Inovação*. São Paulo SEE, 2019.

[21] SÃO PAULO. *Currículo Paulista*. Secretaria da Educação do Estado de São Paulo, 2019.

[22] SILVA, Ana Paula. *A utilização do software GeoGebra no ensino de Geometria*: uma experiência em uma turma do 3º ano do Ensino Médio, 2019. 86p. Dissertação de Mestrado Profissional em Matemática em Rede Nacional - Universidade Federal de São João del Rei, São João del Rei, 2019.

[23] Todescat, M.; Santos, N. *Universidade e a EAD na Sociedade do Conhecimento: Contemporaneidade Organizacional. In*: 4º Seminário Nacional ABED de Educação a Distância "Apoio ao aluno para o sucesso a aprendizagem", Brasília – DF, 2006.

Glaucia Maria Bressan
Universidade Tecnológica Federal do Paraná
Departamento Acadêmico de Matemática
<glauciabressan@utfpr.edu.br>

Patricia Spati
Universidade Tecnológica Federal do Paraná
Departamento Acadêmico de Matemática
<patispati@gmail.com>

Elenice Weber Stiegelmeier
Universidade Tecnológica Federal do Paraná
Departamento Acadêmico de Matemática
<elenicew@utfpr.edu.br>

Recebido: 29/09/2021
Publicado: 12/07/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1024

Ensino não presencial de Cálculo 3: relato de experiência

Marcus V. Lima Humberto L. Talpo Luiz Hartmann

Resumo

Este trabalho apresenta uma experiência vivenciada em disciplinas de cálculo integral em várias variáveis, ministrada conjuntamente por três docentes, na modalidade de ensino não presencial emergencial, consequência da pandemia de Covid-19. Foram duas ofertas, uma no segundo semestre de 2020 e outra no primeiro semestre de 2021, para aproximadamente 360 estudantes dos cursos do Centro de Ciências Exatas e Tecnologia da Universidade Federal de São Carlos. A estratégia de ensino foi baseada em metodologias ativas, que colocam o estudante como protagonista da sua própria aprendizagem, principalmente na sala de aula invertida (ou *flipped classroom*). A sala de aula invertida é caracterizada, de acordo com Valente [6], como uma modalidade *e-learning*, na qual o aluno deve estudar o conteúdo e receber instruções *online*, antes de frequentar a aula presencial, que passa a ser o local para trabalhar os conteúdos já estudados, realizando as atividades práticas como resolução de problemas, desenvolvimento de projetos, discussão em grupo, etc. Dado o regime não presencial emergencial, algumas adaptações nessa metodologia ativa foram necessárias, ainda assim vimos uma ótima oportunidade de aplicá-la. Neste relato são apresentadas a maneira como a disciplina foi ministrada, os resultados e a avaliação de todo o processo de ensino-aprendizagem.

Palavras-chave: ensino não presencial emergencial; metodologias ativas; sala de aula invertida.

Abstract

We present an experience in emergency remote teaching on integral calculus of several variables, taught jointly by three professors, in the emergency non-face-to-face teaching modality, as a result of the COVID-19 pandemic. There were two offers, one in the second semester of 2020 and another in the first semester of 2021, for approximately 360 students from *Centro de Ciências Exatas e Tecnologia* of Federal University of São Carlos. The teaching strategy was based on active methodologies, which place the student as a protagonist of their own learning, mainly the flipped classroom. The flipped classroom is characterized, according to Valente [6], a e-learning modality, in which the student must study the content and receive online instructions, before attending the class, which becomes the place to work on the contents already studied, carrying out practical activities such as problem solving, project development, group discussion, etc. Given the emergency remote teaching, some adaptations to this active methodology were necessary, yet we saw a great opportunity to apply it. This report presents the way in which the discipline was taught, the results and the evaluation of the entire teaching-learning process.

Keywords: emergency remote teaching; active learning; flipped classroom.

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

1. Introdução

Devido à pandemia de Covid-19, a Universidade Federal de São Carlos (UFSCar) suspendeu suas atividades acadêmicas presenciais a partir de 16 de março de 2020 [3]. Após a suspensão, a universidade passou a discutir como retomar as atividades, ainda que de forma emergencial, em regime não presencial, de modo a minimizar os impactos da tão repentina mudança.

Dentre os principais desafios, destacavam-se os de prover equipamentos e acesso aos estudantes em situação de vulnerabilidade social, oferecer formação mínima aos docentes para atuarem no ensino não presencial emergencial e garantir que a retomada das atividades ocorresse de maneira a assegurar a qualidade do processo de ensino-aprendizagem.

Nesse contexto, foi instituído um período acadêmico suplementar de maio a julho de 2020 [4], em que foram ofertadas atividades acadêmicas por meios digitais, em caráter excepcional e temporário, dentre as quais várias Atividades Curriculares de Integração Ensino, Pesquisa e Extensão (Aciepe), sendo a primeira experiência em ensino não presencial para muitos docentes e para praticamente todos os estudantes que participaram desse período suplementar que, até então, só tinham a experiência do ensino presencial.

A retomada das disciplinas regulares dos cursos de graduação no formato de Ensino Não Presencial Emergencial (Enpe), normatizada pelas resoluções do Conselho de Graduação [5], ocorreu a partir de 31 de agosto de 2020 com três calendários diferentes, flexibilizando períodos e horários, denominado Enpe 1. A partir de 22 de fevereiro de 2021 iniciou-se um novo período, no mesmo formato anterior, denominado Enpe 2. É importante destacar a postura da UFSCar frente à oferta das disciplinas, flexibilizando não somente os períodos, como também a forma de oferta, com docentes desenvolvendo as disciplinas individualmente ou em grupos, além de duas possibilidades de ambientes virtuais de aprendizagem: as plataformas Moodle-UFSCar e *Google Classroom*.

Ainda no período acadêmico suplementar, os mesmos docentes que participam deste relato ofertaram conjuntamente uma Aciepe, sobre equações de diferenças e modelagem discreta, com auxílio das metodologias ativas. Na ocasião, além da sala de aula invertida, utilizamos também aprendizagem por pares (*Peer Instruction*) – metodologia que preconiza a abordagem de uma determinada temática combinando intervenções e monitoramento do professor, compartilhamento de conhecimentos por parte dos alunos, além de enfatizar o debate e aprendizagem baseada em projetos (*Project Based Learning*). O projeto consistia da modelagem discreta de um problema e sua solução, mesmo que qualitativa e com recursos computacionais. Alguns problemas foram apresentados, mas os estudantes foram incentivados a buscar outros problemas de interesse particular ou da sua área de formação. O desenvolvimento do projeto deu-se ao longo da atividade, promovendo a interdisciplinaridade e o desenvolvimento de competências transversais, sob orientação dos professores. Como a atividade aconteceu no formato não presencial, foram necessárias algumas adaptações nessas metodologias, como por exemplo a interação entre os alunos e entre alunos e professores acontecendo através do *chat* do ambiente virtual ou através de videochamadas.

A experiência nessa atividade foi positiva e motivou-nos a continuar com a utilização das metodologias ativas, ainda que adaptadas, nas disciplinas regulares desse novo formato não presencial emergencial. A experiência que vamos relatar agora foi desenvolvida conjuntamente pelos autores, nas disciplinas de Cálculo 3 (Enpe 1 e Enpe 2) e Cálculo Diferencial e Integral 3 (Enpe 1), com um total de 180 estudantes matriculados no Enpe 1 e 189 estudantes matriculados no Enpe 2, e tem como objetivo apontar as potencialidades, apresentar o planejamento, a execução, alguns dos problemas enfrentados e a percepção dos alunos em relação à metodologia desenvolvida nas referidas disciplinas.

2. Estruturação da disciplina para a modalidade não presencial

As disciplinas de Cálculo 3 e Cálculo Diferencial e Integral 3 na UFSCar são disciplinas de terceiro ou quarto período, com carga horária de 60 horas, dos cursos de graduação em engenharias, física, química, estatística e computação. A ementa de ambas, resumidamente, é composta por integrais duplas, triplas e aplicações, integrais de linha, de superfície e aplicações. Por essa razão, as referências "à disciplina" serão feitas como se fosse uma única. Além disso, a estrutura descrita abaixo foi mantida nas duas ofertas, Enpe 1 e Enpe 2.

O desenvolvimento da disciplina no Enpe foi feito em dezesseis semanas, mesma duração do ensino presencial, em que são ministradas quatro aulas (duas aulas duplas) por semana, na intenção de manter a estrutura da disciplina próxima do habitual, reduzindo os impactos dessa mudança, uma vez que tal período emergencial exigiu muitas adaptações tanto para os docentes quanto para os estudantes para além da vida acadêmica. Redução de impactos, porém,, de uma maneira que não fosse apenas uma transposição do ensino presencial para o não presencial, mas sim uma adaptação para esse novo regime.

Com a experiência positiva desenvolvidada na Aciepe, continuamos com a utilização da sala de aula invertida, caracterizada em [1, 6], como uma forma de *e-learning*, em que os conteúdos e as instruções são estudados de maneira *on-line* (por meio de vídeos curtos e textos indicados) antes da aula presencial, seguida de atividades mais práticas como discussão e resolução de exercícios e problemas, individualmente ou em grupos, na aula presencial. Em resumo, temos a seguinte estrutura na sala de aula invertida:

- **Antes da aula -** O professor disponibiliza os materiais relativos ao tema, tomando cuidado tanto com a qualidade do disponibilizado para estudo, quanto com a quantidade, de modo que seja possível ao aluno cumprir os estudos ou efetuar as tarefas em tempo hábil até a aula presencial.
- **Durante a aula -** Na aula presencial o professor trabalha as dificuldades dos alunos, ao invés de fazer apresentações sobre o conteúdo selecionado, como ocorre na aula tradicional. É possível fazer uma breve apresentação do material, intercalada com questões para discussão dos conceitos. Durante a aula, o professor desenvolve as atividades programadas para a sala de aula, aprofundando a aprendizagem dos alunos, tendo como base o assunto inicialmente estudado por eles anteriormente. O objetivo é estimular a capacidade de análise, síntese, o desenvolvimento do pensamento crítico e a capacidade de resolução de problemas.
- **Depois da aula -** O professor organiza atividades para que o estudante revise e tenha a oportunidade de ampliar os conhecimentos adquiridos nas duas etapas anteriores. Ele deve promover atividades de avaliação formativa, e o estudante começa a tratar o material disponibilizado pelo professor para a próxima aula presencial, repetindo-se assim o ciclo para cada aula ao longo do período letivo.

No Enpe foi necessária uma adaptação nessa estrutura, pois como não ocorreram encontros presenciais, e a normativa da UFSCar [5] determina a não obrigatoriedade de participação dos estudantes nos encontros síncronos realizados em ambiente virtual, a estratégia adotada foi estabelecer um canal de comunicação através do mural do ambiente virtual onde eram postadas as dúvidas, que eram respondidas no próprio mural e também levadas para os encontros síncronos. A interação através do mural ajudava na preparação das atividades a serem desenvolvidas durante o encontro síncrono.

O ambiente virtual utilizado para a disciplina foi o *Google Classroom*, disponível na G-Suíte da UFSCar. Apesar de possuir menos recursos em comparação com a plataforma Moodle-UFSCar, a escolha desse ambiente deu-se pela sua simplicidade de uso, por atender às nossas necessidades (básicas) de um ambiente virtual e por ser de fácil adaptação para os docentes e para os estudantes, principalmente por dispositivos móveis como celular e *tablet*.

Sabendo que a adoção da estratégia de ensino da sala de aula invertida (adaptada) exigiria dos estudantes uma postura mais ativa, maior regularidade e organização em seus estudos, os conteúdos da disciplina foram programados por semanas, e tal programação era divulgada semanalmente, com o objetivo de criar uma rotina de estudos. Nessa programação constavam todas as atividades que seriam realizadas, prazos e horários de entrega das mesmas, textos e vídeos sobre o tema a ser desenvolvido na semana e que seria discutido no encontro síncrono. A carga horária semanal (estimada) que deveria ser dedicada à disciplina foi entre 5h e 6h30min. Mais precisamente, as atividades semanais, bem como o tempo estimado de dedicação a cada um deles, estão listados abaixo:

- Indicação do texto para estudos individuais. Tempo estimado 1h30min a 2h;
- Disponibilização de vídeo(s) curto(s) (entre 10 e 20 minutos cada) sobre o conteúdo indicado no texto. Tempo estimado 30min;
- Indicação de listas (mínimas) de exercícios. Tempo estimado 1h a 1h30min;
- Disponibilização de atividades de frequência. Tempo estimado 30min;
- Realização de um encontro síncrono para discussão do conteúdo da semana. Tempo estimado 1h30min a 2h;

O tempo de interação no mural da disciplina bem como os horários de atendimento da monitoria, de dois períodos de uma hora, não foram contabilizados nas atividades semanais. Vale a pena observar que a carga horária nos encontros síncronos foi estimada em, praticamente, metade da carga horária semanal da disciplina, que é de 4 aulas por semana. Essa decisão foi tomada para não sobrecarregar os estudantes, uma vez que boa parte das atividades deveriam ser executadas antes do encontro síncrono.

Por julgar essencial que os estudantes tivessem um livro-texto, e como a UFSCar não dispunha de assinatura de biblioteca digital no início do Enpe 1, o passo inicial foi buscar um texto, de livre acesso, que pudesse ser disponibilizado aos estudantes. O texto adotado foi [2]. Para o Enpe 2, apesar da assinatura de uma biblioteca virtual pela UFSCar, o livro-texto continuou o mesmo adotado no Enpe 1. O motivo foi que a utilização *online* dos textos da biblioteca virtual depende de uma boa conexão com a internet, além de um bom equipamento (celular, *tablet* ou computador) para acessar o texto virtual, enquanto o texto escolhido poderia ser utilizado *offline*.

Com relação aos vídeos, apesar de existirem videoaulas disponíveis na internet de várias instituições consagradas de ensino, os vídeos disponibilizados no ambiente virtual foram gravados pelos próprios docentes. Essa decisão basou-se em dois fatores principais: manter uma identidade na disciplina, em termos de linguagem, abordagem e contexto em geral, e os vídeos foram elaborados como um apoio ao livro-texto, com o objetivo de guiar a leitura, destacando os conceitos centrais, questionando hipóteses, demonstrando resultados em situações particulares e com questões para serem respondidas após o estudo do texto. A duração dos vídeos variava entre 10min e 20min,

ao passo que algumas videoaulas chegam a 1h30min, destoando da proposta adotada. Foram disponibilizados no máximo dois vídeos por semana.

As listas de exercícios disponibilizadas foram elaboradas pelos professores, com algumas indicações de exercícios do próprio livro-texto. Os exercícios buscavam relacionar o essencial dos tópicos da semana, com no máximo 10 exercícios. O monitor da disciplina auxiliava os estudantes na resolução e também disponibilizava os gabaritos, que continham a resolução completa das questões.

O acompanhamento dos estudantes era realizado, além da interação no mural, através das atividades de frequência disponibilizadas no ambiente virtual da disciplina. Tais atividades consistiam de questionários *on-line* (formulário *Google*) e/ou exercícios para serem entregues, escritos de próprio punho, digitalizados. Em cada semana, o conteúdo das atividades de frequência estava relacionado com o conteúdo desenvolvido na mesma, com entrega até as sextas-feiras às 23:59h. Após a entrega das atividades de frequência, quando necessário, eram enviados comentários particulares através do próprio ambiente virtual acerca da resolução, dando retorno ao estudante de possíveis erros cometidos. Quando ocorria alguma atividade avaliativa durante a semana, essa era contabilizada também como frequência, diminuindo a carga de atividades do estudante naquela semana.

Dentro da metodologia da sala de aula invertida, os encontros síncronos faziam o papel da aula presencial e cumpriram a importante tarefa de estabelecer uma rotina nos estudos, além de promover uma oportunidade de interagir sincronamente com os estudantes. Nesses encontros, eram apresentados exemplos e discutidas dúvidas do texto, dos vídeos e das listas de exercícios, além de uma compilação das interações no mural da disciplina. Participavam simultaneamente os três professores, cada um usando uma parte do tempo, conferindo uma boa dinâmica aos encontros, segundo relatos dos próprios estudantes. Os encontros não foram gravados pelas seguintes razões: estimular o estudante a se preparar para o encontro síncrono, estabelecendo uma rotina de horários e organização de estudos e evitar a disponibilização de novos materiais ao longo da semana, gerando acúmulo de material. No entanto, os exemplos e anotações apresentados durante o encontro síncrono eram sempre disponibilizados no ambiente virtual da disciplina após os encontros. A presença dos estudantes era sempre incentivada, apesar de não ser obrigatória. No Enpe 1, na primeira metade da disciplina houve presença em cada encontro síncrono de mais de 80% dos estudantes. Esse número caiu para cerca de 60%, em média, até o final da disciplina. No Enpe 2, na primeira metade da disciplina a presença foi em torno de 60% dos estudantes inscritos, caindo para aproximadamente 30% na parte final. Um fator que pode ter contribuído para a queda na participação, relatado por alguns estudantes, foi o acúmulo de atividades das diversas disciplinas no final do período.

O processo de avaliação nesse período não presencial emergencial foi desafiador, tendo em vista que o estudante sequer era obrigado a participar de atividades síncronas, mesmo avaliativas. Optamos por utilizar vários elementos distintos na avaliação e na composição da nota final. Os estudantes foram avaliados individualmente por meio de atividades avaliativas síncronas, assíncronas e participação na disciplina e também em grupo, por meio do trabalho final, composto de texto escrito e vídeo. Abaixo descrevemos com mais detalhes cada um destes elementos:

- **Avaliações síncronas -** No Enpe 1, foram aplicadas 4 avaliações síncronas e, para efeito de cálculo da média final, foram utilizadas as 3 maiores notas. No Enpe 2, foram aplicadas 3 avaliações síncronas e todas as notas obtidas entraram no cálculo da média final. Houve dois formatos dessas avaliações: prova de correção automática (elaborada no formulário *Google*, composta de itens que variavam entre múltipla escolha, caixa de seleção, grade de seleção e verdadeiro ou falso) e prova mista (uma parte de correção automática e uma parte envolvendo uma questão

dissertativa que deveria ser resolvida de próprio punho e enviada em arquivo digitalizado). O tempo disponibilizado para a realização da parte de correção automática foi de 40 ou 50 minutos, e para a realização da parte dissertativa foi de 30 minutos. As avaliações foram realizadas nos horários reservados para a disciplina. Não foi exercido nenhum tipo de controle sobre o aluno, como solicitição de câmera durante a realização da avaliação ou algo neste sentido. As únicas exigências foram que a entrega deveria ser pelo ambiente virtual respeitando o tempo determinado. Esse elemento avaliativo compunha 30% da nota final.

- **Avaliações assíncronas -** No Enpe 1 foram aplicadas 5 avaliações assíncronas e, para efeito de cálculo da média final, foram utilizadas as 4 maiores notas. No Enpe 2, foram aplicadas 4 avaliações assíncronas e todas as notas entraram no cálculo da média final. Houve dois formatos dessas avaliações: prova de correção automática (elaborada no formulário *Google*, composta de itens que variavam entre múltipla escolha, caixa de seleção, grade de seleção e verdadeiro ou falso) e dissertativa, com questões que deveriam ser resolvidas de próprio punho e enviadas em arquivo digitalizado. Em algumas avaliações foram utilizados os dois formatos. Essas avaliações eram disponibilizadas no período da manhã com entrega até as 23:59h do mesmo dia por meio do ambiente virtual. E Sempre realizadas nos dias em que havia horário reservado para aula da disciplina, dimensionada para que fosse resolvida em até duas horas. Este elemento avaliativo compunha 20% da nota final.

- **Participação na disciplina -** Composta por duas partes:

  – Participação no mural - A principal razão para adotar a participação no mural como parte da nota final foi estimular o ambiente de cooperação e interação entre os estudantes. Como participação foram consideradas postagens com perguntas/dúvidas de exercícios e da teoria, postagens respondendo a essas dúvidas (mediadas pelos professores), postagens envolvendo compartilhamento de material (*links* para vídeos e/ou material escrito) sobre tópicos da disciplina. Postagens como "concordo", "também tenho essa dúvida", por exemplo, não foram contabilizadas como participação no mural.

  – Avaliação estrutural da disciplina - Composta de duas etapas, uma na metade do período e outra no final, teve como objetivo coletar impressões, sugestões e críticas através de um questionário (elaborada no formulário *Google*) com questões relativas ao formato adotado no andamento da disciplina. Os detalhes e resultados dessa avaliação serão tratados na próxima seção.

  Esse elemento avaliativo compunha 20% da nota final.

- **Trabalho final -** Com o objetivo de aplicar os conteúdos da disciplina na resolução de problemas, foi proposto o desenvolvimento do trabalho a partir da primeira metade do período. Foram apresentados alguns exemplos típicos de problemas, mas os estudantes tinham liberdade para escolher em que trabalhar. O trabalho final foi composto por:

  – texto contendo motivação da escolha do tema, explicação, resolução e análise do trabalho escolhido, podendo ser um aprofundamento teórico em algum tema relativo à disciplina, aplicação dos conceitos, resolução de problemas ou modelo na área específica de formação do estudante.

  – vídeo com duração entre 8 e 10 minutos contendo exposição oral do trabalho escrito através de *slides*, destacando interesse, formulação do problema, resolução e quais e como foram aplicados os conteúdos da disciplina.

No Enpe 1, o trabalho final poderia ser desenvolvido individualmente ou em grupo de até 6 estudantes de uma mesma turma, já no Enpe 2, apenas em grupo de 3 a 6 estudantes de uma mesma turma. No Enpe 1, os estudantes fizeram ainda uma apresentação para a turma em um encontro síncrono pelo *Google Meet*. Devido às críticas e sugestões recebidas na avaliação estrutural da disciplina no Enpe 1, afirmando ter sido pouco proveitoso assistir às apresentações dos grupos, especialmente em final de período letivo, a apresentação dos grupos foi suprimida no Enpe 2. Tal elemento avaliativo compunha 30% da nota final.

3. Resultados

Como resultados das duas ofertas em Enpe, são apresentados alguns dados coletados nos questionários de avaliação estrutural da disciplina. Essa avaliação foi realizada em duas etapas, a primeira na oitava semana letiva e a segunda na última semana letiva, e teve como objetivo coletar impressões, sugestões e críticas dos estudantes com o formato adotado na condução da disciplina. Para os docentes, a primeira avaliação funcionou como indicação de "correções de rota" do planejamento e execução até a primeira metade do período letivo. Entre as mudanças implementadas por sugestões colhidas na primeira avaliação estrutural, houve aumento da duração da avaliação síncrona (Enpe 1, adotada também no Enpe 2), foram gravados vídeos contendo explicação e resolução de exemplos simples para ilustrar a teoria (Enpe 2), e foi criado um grupo no *Google Chat* para estimular a interação entre os estudantes (Enpe 2), como forma alternativa de participação no mural, facilitando, por exemplo, a postagem de imagens.

No Enpe 1, dentre os estudantes matriculados nas diversas turmas, 151 responderam o segundo questionário de avaliação estrutural da disciplina. Desses, 99 (65,6%) estavam cursando a disciplina pela primeira vez e 52 (34,4%) já a haviam cursado, no ensino presencial. No Enpe 2, dentre os matriculados, 187 responderam ao segundo questionário de avaliação da disciplina em que 163 (87,2%) estavam cursando a disciplina pela primeira vez e 24 (12,8%) já haviam cursado a disciplina anteriormente.

Em relação à estratégia de ensino adotada, o estudo prévio do conteúdo (antes do encontro síncrono) era essencial. A percepção dos estudantes quanto à sua preparação para os encontros síncronos é apresentada na Tabela 1 abaixo.

Antes de cada encontro síncrono, com que frequência		**baixa**	**média**	**alta**
Enpe 1	Estudei o texto	23 (15,2%)	78 (51,7%)	50 (33,1%)
	Assisti ao vídeo sobre o texto	12 (8,0%)	50 (33,1%)	89 (58,9%)
	Discuti o conteúdo com um colega	55 (36,4%)	52 (34,5%)	44 (29,1%)
Enpe 2	Estudei o texto	28 (15,0%)	92 (49,2%)	67 (35,8%)
	Assisti ao vídeo sobre o texto	13 (7,0%)	64 (34,2%)	110 (58,8%)
	Discuti o conteúdo com um colega	72 (38,5%)	64 (34,2%)	51 (27,3%)

Tabela 1: Percepção dos estudantes quanto ao estudo prévio dos diversos materiais para os encontros síncronos

Pelos dados apresentados, nas duas ofertas a percepção foi bem similar. Nota-se uma preferência pelo vídeo explicativo em comparação com o texto escrito. A baixa interação com os colegas pode ser consequência do período de isolamento.

Na Tabela 2, estão apresentados, na percepção dos estudantes, a importância do material previamente disponibilizado e indicado, como preparação para os encontros síncronos.

Em relação aos encontros síncronos (estudantes)		pouco importante	indiferente	muito importante
Enpe 1	Assistir previamente o vídeo	17 (11,3%)	21 (13,9%)	113 (74,8%)
	Estudar previamente o texto	19 (12,6%)	16 (10,6%)	116 (76,8%)
	Resolver previamente os exemplos	28 (18,5%)	27 (17,9%)	96 (63,6%)
Enpe 2	Assistir previamente o vídeo	22 (11,8%)	27 (14,4%)	138 (73,8%)
	Estudar previamente o texto	18 (9,6%)	27 (14,4%)	142 (76,0%)
	Resolver previamente os exemplos	49 (26,2%)	41 (21,9%)	97 (51,9%)

Tabela 2: Percepção dos estudantes quanto à importância dos materiais disponibilizados previamente para um melhor aproveitamento nos encontros síncronos

Pelos dados da Tabela 2, observa-se a grande importância, na percepção dos estudantes, do preparo para o encontro síncrono, um indicativo de que a metodologia da sala de aula invertida (adaptada) teve respaldo dos estudantes nas duas ofertas.

Em relação às duas principais atividades desenvolvidas nos encontros síncronos, a Tabelas 3 apresenta, na percepção dos estudantes, a importância de cada uma delas.

Em relação aos encontros síncronos (professores)		pouco importante	indiferente	muito importante
Enpe 1	Resolução de exemplos	1 (0,6%)	3 (2,0%)	147 (97,4%)
	Discussão de dúvidas	20 (13,3%)	18 (11,9%)	113 (74,8%)
Enpe 2	Resolução de exemplos	0 (0,0%)	7 (3,8%)	180 (96,2%)
	Discussão de dúvidas	19 (10,2%)	29 (15,5%)	139 (74,3%)

Tabela 3: Percepção dos estudantes quanto à importância das atividades desenvolvidas nos encontros síncronos no processo de aprendizagem

Nos dados da Tabela 3, observa-se a grande importância que os estudantes dão para os encontros síncronos. Tal importância pode ser devido à interação "em tempo real"em que as dúvidas tanto da parte teórica como dos exercícios eram discutidas e esclarecidas.

A Tabela 4 abaixo apresenta, na percepção dos estudantes, a contribuição dos diversos materiais disponibilizados ao longo do semestre, bem como do trabalho final, para o seu aprendizado nas disciplinas.

Como avalia para o seu aprendizado a contribuição do		baixa	média	alta
Enpe 1	Texto escrito	43 (28,5%)	60 (39,7%)	48 (31,8%)
	Vídeo sobre o texto	12 (8,0%)	50 (33,1%)	89 (58,9%)
	Listas de exercícios	5 (3,3%)	45 (29,8%)	101 (66,9%)
	Gabaritos das listas de exercícios	4 (2,7%)	26 (17,2%)	121 (80,1%)
	Encontro síncrono	23 (15,2%)	63 (41,7%)	65 (43,1%)
	Trabalho final	46 (30,5%)	64 (42,4%)	41 (27,1%)
Enpe 2	Texto escrito	33 (17,7%)	61 (32,6%)	93 (49,7%)
	Vídeo sobre o texto	14 (7,5%)	69 (36,9%)	104 (55,6%)
	Listas de exercícios	12 (6,4%)	71 (38,0%)	104 (55,6%)
	Gabaritos das listas de exercícios	7 (3,8%)	47 (25,1%)	133 (71,1%)
	Encontro síncrono	29 (15,5%)	71 (38,0%)	87 (46,5%)
	Trabalho final	32 (17,1%)	83 (44,4%)	72 (38,5%)

Tabela 4: Percepção dos estudantes quanto à importância dos materiais e atividades no processo de aprendizagem

Na Tabela 4 é possível notar que há muita similaridade nas percepções do Enpe 1 e Enpe 2. Em ambos, as maiores contribuições são dadas, por ordem de importância, para os gabaritos das listas de exercícios e as listas de exercícios. As listas com gabarito (que tinham toda a resolução dos exercícios e não apenas os resultados) eram de exercícios adicionais que complementavam as listas do livro-texto. A maior importância dada a elas pode estar relacionada à insegurança na redação da resolução dos exercícios pelos estudantes.

A Tabela 5, abaixo, apresenta o número de horas de estudo, por semana, que os estudantes dedicaram às atividades da disciplina no formato ENPE, nas duas ofertas.

Oferta	**3,5 a 4,5 horas**	**4,5 a 5,5 horas**	**5,5 a 6,5 horas**	**6,5 ou mais horas**
Enpe 1	17%	29,6%	22%	31,4%
Enpe 2	30,8%	35,1%	21,1%	13%

Tabela 5: Horas de estudos semanais reservadas pelos estudantes para a disciplina

Na Tabela 5, do Enpe 1 para o Enpe 2 observa-se uma "inversão"nas horas de estudo dedicadas à disciplina. Enquanto no Enpe 1 a recomendação para o estudante inscrever-se em até 4 disciplinas foi seguida pela maioria dos estudantes, no Enpe 2 isso não se repetiu. Com inscrição em um maior número de disciplinas, o número de horas de estudo para cada uma delas diminuiu. Outro fator que pode ter contribuído para a dedicação em número de horas ter diminuído é que no Enpe 2 os estudantes já teriam se adaptado ao novo formato não presencial.

A Tabela 6, abaixo, apresenta os índices de aprovação, média das notas finais (de todos os estudantes) e a satisfação dos estudantes com a disciplina no formato Enpe, nas duas ofertas.

Oferta	**Aprovados**	**Média das notas finais**	**não gostei**	**indiferente**	**gostei**
Enpe 1	92,89%	6,99 (desvio padrão de 1,56)	5,3%	13,9%	80,8%
Enpe 2	95,85%	7,42 (desvio padrão de 0,78)	2,1%	22,5%	75,4%

Tabela 6: Notas finais e percepção dos estudantes com relação à satisfação no desenvolvimento da disciplina

4. Discussão e Conclusão

Ofertar uma disciplina de graduação na modalidade não presencial e trabalhando em um grupo de professores foi tanto motivador quanto desafiador, principalmente pela falta de experiência com tal modelo de ensino. Para essa tarefa, o entrosamento e afinidade foram essenciais para que o trabalho docente em grupo se desenvolvesse bem. A abordagem dos tópicos, indicação de listas de exercícios, elaboração das atividades de frequência, elaboração das avaliações e definição dos critérios de correção foram discutidas e decididas em comum acordo entre os professores. Além das questões diretamente relacionadas ao planejamento e execução da disciplina, o convívio (mesmo que virtual), em que assuntos relacionados ao cotidiano da universidade eram compartilhados e discutidos, foram de grande importância durante o período de isolamento social. Vale ressaltar também que o trabalho em equipe permitiu resolver facilmente algumas situações, por exemplo, no caso de problemas de conexão durante um encontro síncrono ou mesmo a necessidade de afastamento de um docente por um certo período.

Com relação à estratégia adotada, a combinação de um livro-texto com vídeos explicativos da teoria e resolução de exercícios compõe um ótimo subsídio para os estudantes, permitindo uma otimização do tempo em sala de aula, explorando relações entre os conceitos estudados. O livro-texto traz em detalhes o conteúdo, mas não explora tanto as motivações e as experimentações que podem ser realizadas e também não realiza o "passo-a-passo" da resolução de alguns exemplos. A complementação disso com um vídeo ou com um encontro síncrono auxilia o aprendizado dos estudantes, desde que o livro-texto tenha realmente sido utilizado por eles. Vários estudantes relataram preferência por "videoaulas", alegando ser mais prático que o estudo prévio, mas nada subsutitui um texto escrito: é como ler um livro e assistir a um filme sobre o livro; são experiências completamente diferentes! A gravação dos vídeos só foi possível devido ao trabalho em equipe. A divisão das tarefas semanais entre os três docentes permitiu que a gravação e a edição dos vídeos, que demandam um tempo considerável, fosse realizada sem prejuízo de outras atividades como a preparação para o encontro síncrono, mediação das postagens no mural de cada turma, verificação do envio de atividades de frequência e administração do ambiente virtual, todas tarefas que não são típicas do ensino presencial e que exigem disponibilidade e dedicação por parte dos docentes. Outro ponto muito importante foi o estabelecimento de uma rotina para o desenvolvimento da disciplina, através do planejamento e descrição das atividades, divulgados a cada semana e cumpridos sem modificações, garantindo previsibilidade e maior organização.

Em relação ao percentual de aprovação, os índices foram bem mais altos do que a média histórica (em torno de 60%) observada entre 2005 e 2019, na mesma disciplina no formato presencial. Apesar disso, não há evidências de que o processo de ensino-aprendizagem tenha sido mais eficiente. Dentre os vários aspectos que podem, de alguma forma, ter contribuído para os índices de aprovação atingidos estão: o caráter mais direcionado das unidades didáticas; a divisão por tópicos bem mais delineada, com duas atividades de frequência semanais que versavam sobre o conteúdo estudado na semana; um número maior de atividades avaliativas com uma quantidade menor de conteúdo sendo avaliada em cada uma delas. Além disso, no ensino não presencial, a maior parte das atividades avaliativas foram de itens de correção automática, em que a argumentação do estudante não era avaliada, sendo essa a principal diferença entre as avaliações do ensino presencial, em que a maior parte, se não a totalidade, dos itens das avaliações, eram dissertativas.

Ainda em relação às avaliações, os itens dissertativos foram aplicados principalmente nas avaliações assíncronas. No Enpe 1, a questão dissertativa na avaliação síncrona (do tipo mista) foi motivo de grande estresse dos estudantes (relatos obtidos na primeira avaliação estrutural da disciplina), devido à grande preocupação com o tempo para resolução, digitalização e envio. Observando as notas de todas as turmas, a média na parte de correção automática foi 28% mais alta do que a média das notas na questão dissertativa. Tendo em vista essa diferença expressiva nas notas, além do relato dos estudantes, a opção foi utilizar itens dissertativos nas avaliações assíncronas (total ou parcialmente) e itens de correção automática nas avaliações síncronas. No Enpe 2, as notas da parte de correção automática foram cerca de 10% mais altas do que as da parte dissertativa (considerando as médias de todas as turmas em avaliação do tipo mista, em avaliação assíncrona, sobre o mesmo conteúdo).

O caráter emergencial da modalidade Enpe permitiu várias experiências diferentes e foi um grande impulsionador de mudanças nas nossas práticas docentes; dentre elas, trabalho em um grupo de professores, adoção de novas estratégias de ensino (como o uso de metodologias ativas), utilização de ambientes virtuais de aprendizagem como instrumento de avaliação, e utilização de novas ferramentas de ensino-aprendizagem (como gravação de vídeos). Um grande desafio trazido por essa experiência foi o processo de avaliação dos estudantes. Esse foi o ponto mais discutido, pensado e

modificado ao longo do Enpe, tendo em vista a realização das avaliações em um ambiente virtual (não controlado), diferindo do ensino presencial e do EaD.

Como proposta futura pretendemos aplicar a estratégia de ensino apresentada neste relato no ensino presencial, utilizando a parte virtual como material de apoio ao estudante, ou mesmo no ensino "híbrido", com parte do desenvolvimento virtual e parte presencial. Alguns pontos que destacamos desta experiência e que podem contribuir são: ministrar disciplinas básicas em um grupo de professores em que todos participam conjuntamente do início ao final da disciplina, usar um ambiente virtual de aprendizagem como apoio ao ensino presencial em que fica disponibilizado o planejamento semanal das atividades a serem desenvolvidas (tópicos a serem discutidos, listas de exercícios selecionados, atividades em ambiente virtual com correção automática para aferir o estudo da semana), gravar pequenos vídeos com resolução comentada de exemplos e/ou dúvidas de teoria e exercícios postados no ambiente virtual, realizar um questionário de avaliação *on-line* da disciplina durante o período letivo para fazer pequenas (ou grandes!) correções de rota (isso foi de grande importância no Enpe). Para finalizar, o objetivo deste relato não é comparar modelos de ensino (Enpe *versus* presencial) quanto a eficiência dos processos de ensino-aprendizagem, tampouco quanto aos índices de aprovação, mas sim contribuir com sugestões para o aperfeiçoamento contínuo da prática docente.

Referências

[1] BISHOP, J. L.; VERLEGER, M. A. *The Flipped Classroom: A Survey of the Research*. In: ASEE ANNUAL CONFERENCE & EXPOSITION, Atlanta, 2013. Disponível em: <https://peer.asee.org/22585>. Último acesso em: 07/07/2021.

[2] MATOS, M. P; SILVA, A. de A. e. *Cálculo de Várias Variáveis*: UFPB-CCEN. Disponível em: <http://www.mpmatos.com.br/Calculo3/Texto_Parte%20II.pdf>. Último acesso em: 07/07/2021.

[3] UFSCar. Resolução CoG nº 319 - Suspensão dos Calendários Acadêmicos e administrativos - COVID-19. Disponível em: <http://www.prograd.ufscar.br/conselho-de-graduacao-1/resolucoes-cog>. Último acesso em: 07/07/2021.

[4] UFSCar. Resolução CoG nº 320 - Criação de Calendário Suplementar - COVID-19. Disponível em: <http://www.prograd.ufscar.br/conselho-de-graduacao-1/resolucoes-cog>. Último acesso em: 07/07/2021.

[5] UFSCar. Resolução CoG nº 332 e nº 371 - Normativas específicas para os períodos de Ensino Não Presencial Emergencial-ENPE. Disponível em: <http://www.prograd.ufscar.br/conselho-de-graduacao-1/resolucoes-cog>. Último acesso em: 07/07/2021.

[6] VALENTE, J.A. "Blended learning e as mudanças no ensino superior: a proposta da sala de aula invertida". *Educar em Revista*, Curitiba, Brasil, Edição Especial n. 4, p. 79-97, 2014.

Marcus V. Lima
Academia da Força Aérea
<marcus@ufscar.br;marcusmval@fab.mil.br>

Humberto L. Talpo
Universidade Federal de São Carlos
<htalpo@ufscar.br>

Luiz Hartmann
Universidade Federal de São Carlos
<luizhartmann@ufscar.br>

Recebido: 13/04/2022
Publicado: 12/07/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1025

Equações diofantinas lineares e não lineares: uma abordagem por meio de questões de Olimpíadas de Matemática

Érick C. A. do Nascimento [1] Thiago Yukio Tanaka [2] Barbara Costa da Silva[3]

Resumo

Neste trabalho, apresentaremos métodos e técnicas de solução para equações diofantinas lineares e não lineares por meio de questões de Olimpíadas de Matemática. No tratamento das equações lineares, exploraremos a teoria de divisibilidade nos números inteiros, o conceito de máximo divisor comum (MDC) e, então, apresentaremos um resultado, provando, assim, a existência de soluções. No caso não linear, exploraremos técnicas para determinados casos, uma vez que, para equações diofantinas não lineares, não há um método geral de solução. Apresentaremos quatro casos de resolução baseados em aritmética dos inteiros, fatorações, desigualdades e parametrizações. Esperamos que este trabalho sirva como fonte de estudo e pesquisa aos discentes e docentes interessados em Olimpíadas de Matemática.

Palavras-chave: Equações Diofantinas; Olimpíadas de Matemática; Número de Frobenius.

Abstract

In this work, we will present methods and solution techniques for Linear and Nonlinear Diophantine Equations through Mathematical Olympiad questions. In the treatment of linear equations, we will explore the theory of divisibility in whole numbers, the concept of greatest common divisor (GCD) and, then, we will present a result, thus proving the existence of solutions. In the nonlinear case, we will explore techniques for certain cases, since, for nonlinear Diophantine Equations, there is no general solution method. We will present four cases solving based on integer arithmetic, factorizations, inequalities and parameterizations. We hope that this work will serve as a source of study and research for students and teachers interested in Mathematics Olympiads.

Keywords: Diophantine Equations; Mathematics Olympiads; Frobenius Number.

1. Introdução

Em diversos problemas matemáticos, estamos interessados em encontrar soluções inteiras para alguma equação, como o problema *Frobenius*, as *Equações de Pell* ou o problema das famosas

[1]Discente do Departamento de Matemática da UFRPE
[2]Docente do Departamento de Matemática da UFRPE
[3]Docente do Departamento de Matemática da UFRPE

Ternas Pitagóricas de números naturais. Equações que permitem que suas variáveis admitam apenas números inteiros como solução são chamadas de *Equações Diofantinas*.

Esse nome é devido ao matemático, Diofante de Alexandria, o primeiro a investigar sobre como encontrar soluções inteiras (ou racionais) positivas, em problemas que possuem mais variáveis que equações. Os problemas estudados por ele, em geral, eram os indeterminados (que admitem infinitas soluções). Sua obra mais famosa, "Aritmética", é composta por 13 livros, dos quais acreditava-se que apenas 6 haviam sobrevivido ao tempo. No entanto, recentemente, alguns historiadores julgam ter encontrado outros quatro livros de sua obra, traduzidos em árabe [13]. Nessa obra, Diofante propõe a resolução de dezenas de problemas, de diversas naturezas, como equações polinomiais de primeiro, segundo e terceiro graus, e resolução de problemas envolvendo medidas de lado racionais para triângulos retângulos. Inclusive, em seu segundo livro, o problema mais famoso é o de número 8, pois, segundo [14], foi na margem de uma cópia que pertencia a Fermat que ele escreveu, ao lado do problema 8, uma observação que ficou mundialmente conhecida como o "Último Teorema de Fermat".

Figura 1: Diofante de Alexandria. Fonte: [3].

Sabemos pouco da vida de Diofante, sendo incertos o período em que viveu e sua idade. Em [14], há relatos de que ele, supostamente, teria vivido após 150 d.C. e antes de 364 d.C.. Além disso, sobre a sua idade: "De acordo com a memória de um resolvedor de problemas, o único detalhe sobre a vida de Diofante que restou foi um enigma, que dizem ter sido gravado na lápide de seu túmulo." (SINGH, 2014).

O texto que supostamente carrega esse enigma é dado por:

> Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois, por um doze avos, ele cobriu seu rosto com a barba. A luz do casamento iluminou-o após a sétima parte e cinco anos depois do casamento Ele concedeu-lhe um filho. Ah! criança tardia e má, depois de viver metade da vida de seu pai, o destino frio a levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos, Diofante terminou sua vida.

Sendo x o valor de sua idade, o problema pode ser representado pela equação

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x,$$

o que concluímos que Diofante teria vivido 84 anos.

As Olimpíadas Matemáticas costumam chamar a atenção de muitas escolas e universidades, pois além de incentivarem o estudo da Matemática nas diversas idades, são capazes de revelar e dar holofotes a diversos talentos. No Brasil, Olimpíadas de Matemática ganharam força em 1979, com a criação da Olimpíada Brasileira de Matemática (OBM), que, com o passar dos anos, passou por diversas mudanças, como a divisão por séries e a implementação do nível universitário, até que em 2017, a OBM integrou-se à Olimpíada Brasileira de Matemática das Escolas Públicas (Obmep).

Desde de 1979, o Brasil tem sido representado por uma equipe olímpica na Olimpíada Internacional de Matemática (*International Mathematical Olympiad, IMO*), com um total de 41 participações, obtendo 11 medalhas de ouro, 50 de prata, 81 de bronze e 33 menções honrosas. Destaca-se, dentre os premiados, o medalhista de ouro, Arthur Ávila, primeiro brasileiro a obter uma medalha *Fields*.

As Olimpíadas Matemáticas abordam diversos temas, como Álgebra, Teoria dos Números, Combinatória e Geometria, promovendo assim o estudo de teorias e técnicas para a resolução dos problemas propostos. Neste trabalho, daremos foco a um tema que relaciona Álgebra e Teoria dos Números: equações diofantinas. Mais especificamente, destacaremos métodos de resolução de questões olímpicas relacionadas como o tema.

Há diversos trabalhos que trazem resultados envolvendo equações diofantinas com fins educacionais. Por exemplo, [3] elabora uma sequência didática que serve como material de apoio para o estudo das equações diofantinas lineares e aborda o caso das não lineares por meio do método da descida infinita de Fermat. Já [4] trata de equações diofantinas lineares de n variáveis, suas soluções e suas aplicações na resolução de problemas relacionados a números inteiros. Em [12], são propostas atividades que envolvem equações diofantinas próprias para serem aplicadas em uma sala de aula no Ensino Médio. Semelhante ao nosso trabalho, na revista do Professor de Matemática Online (PMO), há dois artigos que abordam temas olímpicos. Em [5], a autora desenvolve a solução para diversos problemas olímpicos de Matemática, nos temas de Aritmética dos Inteiros e Teoria dos Números. Já em [6], os autores abordam sobre dois importantes resultados da Geometria que são os Teoremas de Ceva e o de Menelaus, assim como suas diversas aplicações.

Este trabalho traz uma abordagem inovadora para a discussão do tema das Equações Diofantinas, por meio da análise e resolução de questões olímpicas nacionais e internacionais. Reunimos uma série de resultados significativos, tanto para o caso linear, quanto para o caso não linear, e destacamos a aplicação dessas ferramentas na solução dos problemas propostos.

Este trabalho foi dividido de maneira quase independente, deixando o(a) leitor(a) livre para ler na ordem que preferir, pois cada seção aborda um método específico de resolução de equações que independe dos demais. Apesar disso, sugerimos que o(a) leitor(a), que não tem muita familiaridade com a aritmética, comece pela Seção 2, pois nela realizamos uma abordagem teórica dos principais conceitos e resultados utilizados no decorrer do trabalho. Na Seção 3, descrevemos os principais resultados envolvidos na busca de soluções das equações diofantinas lineares presentes em diversos problemas olímpicos. Na Seção 4, tratamos dos casos que são mais recorrentes em Olimpíadas de Matemática envolvendo equações diofantinas não lineares, especificamente, abordamos quatro métodos de soluções envolvendo técnicas de fatoração, desigualdades, parametrizações e aritmética modular. Por fim, na Seção 5, fazemos a conclusão do trabalho.

2. Um pouco sobre Aritmética dos Inteiros

Exibiremos e demonstraremos alguns conceitos e resultados que serão importantes ao decorrer deste artigo: divisibilidade, máximo divisor comum e congruência modular. A aplicação destes resultados é destacada a partir de soluções de problemas do banco de questões da Obmep.

Definição 1 (Divisibilidade)**.** Dados dois números inteiros a e b com $a \neq 0$, diz-se que a divide b, e denota-se $a \mid b$, quando existe um inteiro c tal que $ac = b$. Nesse caso, também podemos dizer que b é um múltiplo de a. Se a não divide b, então não existe c inteiro tal que $ac = b$. Quando isso acontece, denotamos por $a \nmid b$.

Proposição 1. *Sejam a, b e c números inteiros. Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Como $a \mid b$ existe $q_1 \in \mathbb{Z}$ tal que $b = aq_1$, do mesmo modo, como $b \mid c$ existe $q_2 \in \mathbb{Z}$ tal que $c = bq_2$. Assim, temos que $c = (aq_1)q_2$, concluindo que $a \mid c$.

□

Teorema 1 (Divisão Euclidiana)**.** *Sejam a e b números inteiros, com $0 \neq b$. Existem dois únicos inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$.*

Demonstração. Temos dois casos a considerar: quando $b > 0$ e $b < 0$. É fácil perceber que a deve estar entre dois múltiplos consecutivos de b.

Para $b < 0$, tome $q \in \mathbb{Z}$ tal que

$$qb \leq a < (q-1)b \quad \Rightarrow \quad qb \leq a < qb - b \quad \Rightarrow \quad 0 \leq a - qb < -b.$$

Então, considerando $r = a - qb$, garantimos a existência de q e r satisfazendo as condições do teorema.

Para provar a unicidade, tome q' e r' tais que $a = bq' + r'$, com $0 \leq r' < |b|$. Daí, utilizando as duas expressões para a, temos que $(bq + r) - (bq' + r') = 0$ o que implica que $r - r' = b(q' - q)$. Isso nos diz que $b \mid r - r'$, mas como $r < |b|$ e $r' < |b|$ temos que $|r - r'| < |b|$. Logo, a única possibilidade é termos $r - r' = 0$, logo $r' = r$ e $b(q' - q) = 0$, e como $b \neq 0$ concluímos que $q' = q$, provando assim a unicidade.

Para $b > 0$, basta considerar $qb \leq a < (q+1)b$ e seguir de forma análoga.

□

Observação 1. Nas condições do teorema acima, q e r são respectivamente o quociente e o resto da divisão de a por b.

A proposição que provaremos a seguir vai nos ajudar a concluir o resultado do Exemplo 1.

Proposição 2. *Sejam a, b e c inteiros tais que $a \mid b$ e $a \mid c$, então $a \mid bx + cy$, para quaisquer $x, y \in \mathbb{Z}$.*

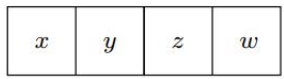
Demonstração. Como $a \mid b$ e $a \mid c$, temos que $b = aq_1$ e $c = aq_2$. Dessa forma, para quaisquer $x, y \in \mathbb{Z}$, temos que

$$bx + cy = (aq_1)x + (aq_2)y = a(q_1x + q_2y),$$

como $q_1x + q_2x \in \mathbb{Z}$, então $a \mid bx + cy$. □

A seguir, é explorado um problema do banco de questões da Obmep 2013 cuja solução que envolve uma equação Diofantina e aplica os resultados apresentados.

Exemplo 1 (Banco de questões OBMEP, 2013, Nível 3, Problema 21, [9])**.** Os números x, y, z e w na figura são números inteiros todos diferentes entre si, maiores do que 1, e foram colocados nas casas abaixo de modo que cada número (a partir do y) é divisor do número na casa da esquerda.



Descubra todas as soluções possíveis para x, y, z e w, sabendo que a soma deles é 329.

Solução. Pelas relações apresentadas no enunciado, vemos que

$$1 < w < z < y < x < 329.$$

Além disso, como $w \mid z$ e $z \mid y$, pela Proposição 1 temos que $w \mid y$, e como $y \mid x$ também concluímos que $w \mid x$, ou seja, w é divisor de todos os números das casas. Dessa forma, pela Proposição 2, w é divisor da soma dos números das casas, isto é, é divisor de 329. Agora, note que 329 pode ser fatorado como a multiplicação de dois primos da seguinte forma: $329 = 7 \cdot 47$, daí concluímos que $w = 7$ ou $w = 47$. Vamos olhar os dois casos.

Caso w = 47. Nesse caso, temos que $x + y + z = 2 \cdot 3 \cdot 47$. Aplicando o mesmo argumento utilizado para w, teremos $z \mid x$ e $z \mid y$, daí z divide $2 \cdot 3 \cdot 47 = 2 \cdot 47 + 2 \cdot 47 + 2 \cdot 47$. Como $z < y < x$, temos que z deve ser menor do que $2 \cdot 47$. Mas z não pode ser igual a $w = 47$ e também não pode ser menor, logo não existe solução quando $w = 47$.

Caso w = 7. Aqui, temos $x + y + z = 322$. Daí, com os mesmos argumentos, sabemos que z divide $322 = 2 \cdot 7 \cdot 23$. Como $w \mid z$ temos que as únicas possibilidades para w são $7 \cdot 2$ e $7 \cdot 23$, mas , como $z < y < x$, para satisfazer a soma devemos ter $z < 7 \cdot 23$, concluindo que $z = 7 \cdot 2$. Substituindo o valor encontrado para z e sabendo que $y \mid x$, vemos que y divide $x + y = 308$, que pode ser fatorado tal como $308 = 2 \cdot 2 \cdot 7 \cdot 11$. Como $14 = z < y$, os valores possíveis para y são $2 \cdot 2 \cdot 7$ e $2 \cdot 7 \cdot 11$. Já que queremos que $x + y = 308$ com $y < x$, temos que $y = 2 \cdot 2 \cdot 7$. E finalmente concluímos que $x = 329 - 7 - 14 - 28 = 280$. Portanto, $w = 7, z = 7 \cdot 2, y = 7 \cdot 2 \cdot 2$ e $x = 7 \cdot 4 \cdot 10$. ■

Definição 2 (Máximo Divisor Comum)**.** Sejam a e b dois inteiros não simultaneamente nulos, diz-se que o inteiro positivo d é o máximo divisor comum de a e b, e denotamos por $d = mdc(a, b)$, se d satisfaz as seguintes condições:

(i) d é um divisor comum de a e b, ou seja, $d \mid a$ e $d \mid b$;

(ii) d é divisível por todo divisor comum de a e b, isto é, se c é divisor comum de a e b, então $c \mid d$.

Teorema 2. *Seja d o máximo divisor comum de a e b. Então existem m e n inteiros, tais que $d = ma + nb$.*

Demonstração. Considere o conjunto

$$A = \{xa + yb; x, y \in \mathbb{Z}\}$$

de todas as combinações lineares de a e b. Claramente, A é não vazio e contém números positivos, negativos e o zero. Dessa forma, podemos escolher m e n tais que $c = ma + nb$ seja o menor inteiro positivo que pertence ao conjunto A.

Note que $c \mid a$ e $c \mid b$. De fato, suponha que $c \nmid a$, pela divisão euclidiana, existem q e r tais que $a = qc + r$, com $0 \leq r < c$. Note que se $0 < r < c$ teríamos

$$r = a - qc \quad \Rightarrow \quad r = a - q(ma + nb) \quad \Rightarrow \quad r = (1 - qm)a - qnb,$$

o que nos diz que r é uma combinação linear de a e b e então pertence a A. O que é uma contradição, pois $0 < r < c$ e tomamos c como o menor número positivo em A. Logo $r = 0$ e, consequentemente, $c \mid a$. De forma análoga, $c \mid b$. Como $d = mdc(a, b)$, vale então que $c \mid d$.

Além disso, existem q_1 e q_2 tais que $a = q_1 d$ e $b = q_2 d$, e então

$$c = ma + nb \quad \Rightarrow \quad c = mq_1 d + nq_2 d \quad \Rightarrow \quad c = d(mq_1 + nq_2),$$

ou seja, $d \mid c$.

Portanto, como $c \mid d$ e $d \mid c$, e sendo ambos positivos, concluímos que $d = c = ma + nb$.

□

Lema 1 (Lema de Euclides)**.** *Sejam a, b e n inteiros não nulos, com $a \leq na < b$, então existe $mdc(a, b)$ e $mdc(a, b) = mdc(a, b\text{-}na)$.*

Demonstração. Seja $d = mdc(a, b - na)$, como $d \mid a$, $d \mid b - na$ e $b = b - na + na$, a Proposição 2 garante-nos que $d \mid b$. Logo, d é divisor comum de a e b. Tome c, outro divisor comum de a e b, ou seja, $c \mid a$ e $c \mid b$, mas isso implica que $c \mid b - na$, assim $c \mid d$, pois $d = mdc(a, b - na)$. Note que acabamos de provar que $d = mdc(a, b)$. Portanto, $mdc(a, b)$ existe e é igual ao $mdc(a, b - na)$.

□

Exemplo 2 (OBM, 2011, 2ª Fase, Nível 2, Problema 3, [8])**.** Quantos são os pares ordenados (a, b), com a e b inteiros positivos, tais que

$$a + b + mdc(a, b) = 33?$$

Solução: Considere $d = mdc(a, b)$, daí podemos reescrever a equação da seguinte forma:

$$\frac{a}{d} + \frac{b}{d} + 1 = \frac{33}{d}.$$

Como $d \mid a$ e $d \mid b$, temos que o lado esquerdo da equação acima é uma soma de números inteiros, logo, o lado direito deve ser um número inteiro, o que nos diz que d divide 33. Além disso, pelo Lema 1, vale que

$$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = mdc\left(\frac{a}{d}, \frac{33}{d} - 1\right) = mdc\left(\frac{b}{d}, \frac{33}{d} - 1\right) = 1.$$

Portanto, se fixarmos d, basta encontrarmos pares de inteiros positivos (x, y) com $mdc\left(x, \frac{33}{d} - 1\right) = 1$ com $x + y = \frac{33}{d} - 1$, pois daí também vamos obter $mdc\left(y, \frac{33}{d} - 1\right) = 1$ e que $(a, b) = (dx, dy)$ também é solução. Agora, como $d \mid 33$, vemos que d só pode admitir um dos quatro valores: $1, 3, 11$ e 33. Vejamos os casos:

Caso 1. Para $d = 1$ temos que $x + y = 32$, daí podemos ter 16 soluções, pois basta escolher x ímpar.

Caso 2. Para $d = 3$ temos que $x + y = 10$, teremos 4 possibilidades, pois x deve ser um número menor do que 10 que não pode ser par e nem múltiplo de 5.

Caso 3. Para $d = 11$ temos que $x + y = 2$, logo vamos ter apenas uma solução para x.

Caso 4. Para $d = 33$, não teremos solução, pois nesse caso $x + y = 0$, mas x e y são inteiros positivos.

Assim, concluímos que existem 21 pares de soluções. ■

Exemplo 3 (OBM, 2012, 1ª Fase, Nível 3, Problema 5, [8])**.** Em 2012, foi realizada a edição 34 da OBM, e $mdc(2012, 34) = 2$. Supondo que a OBM sempre será realizada todo ano, qual é o maior valor possível para o MDC do ano e da edição da OBM realizado no ano?

Solução: Se estivermos na edição de número x da OBM, estaremos no ano $1978 + x$. Dessa forma, estamos procurando o valor máximo para $mdc(x, 1978 + x)$. Note que, pelo Lema 1, $mdc(x, 1978 + x) = mdc(x, 1978 + x - x) = mdc(x, 1978)$, portanto o maior valor possível para esse MDC é 1978, que é obtido quando tomamos $x = 1978$. ■

Definição 3. Sejam $a, b, p \in \mathbb{Z}$. Dizemos que a é congruente a b módulo p se $p \mid (a - b)$, ou seja, se a e b deixam o mesmo resto na divisão por p. Nesse caso, denotamos tal congruência por

$$a \equiv b \mod p.$$

Enunciaremos, agora, algumas propriedades de congruência, porém não as provaremos devido à grande quantidade de itens; elas podem ser encontradas em [7].

Proposição 3. *Sejam a, b, c, d, m e n números inteiros, com $m, n > 1$, então:*

1. *Se $a \equiv b \mod n$ e $b \equiv c \mod n$, então $a \equiv c \mod n$;*
2. *Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então $a \cdot c \equiv b \cdot d \mod n$ e $a + c \equiv b + d \mod n$;*
3. *Se $a \equiv b \mod n$, então $a^k \equiv b^k \mod n$, para todo $k \in \mathbb{N}$;*
4. *Se $a \equiv b \mod n$ e $m \mid n$, então $a \equiv b \mod m$;*
5. *Se $a \equiv b \mod n$, então $mdc(a, n) = mdc(b, n)$;*
6. *Se $a + c \equiv b + c \mod n$, então $a \equiv b \mod n$;*
7. *Se $a \equiv b \mod m \cdot n$, então $a \equiv b \mod m$ e $a \equiv b \mod n$;*
8. *Se $a \equiv b \mod m$ e $a \equiv b \mod n$, com $mdc(m, n) = 1$, então $a \equiv b \mod m \cdot n$.*

As propriedades de congruência modular são fortes ferramentas para a resolução de questões olímpicas relacionadas, principalmente, para encontrar restos de uma divisão. Mais adiante, vamos utilizar essas ideias como um método de resolução de equações diofantinas não lineares.

Exemplo 4 (Caderno de Exercícios, Portal da Obmep, Aritmética Modular, Exercício 17, [11])**.** Qual o resto de $36^{36} + 41^{41}$ na divisão por 77?

Solução: Perceba que os números do problema obedecem à seguinte relação: $36 + 41 = 77$. Dessa forma,

$$\begin{aligned} -36 &\equiv 41 \mod 77 \\ (-36)^{41} &\equiv 41^{41} \mod 77 \\ 36^{36} + (-36)^{41} &\equiv 36^{36} + 41^{41} \mod 77 \\ 36^{36}\left(1 - 36^5\right) &\equiv 36^{36} + 41^{41} \mod 77. \end{aligned}$$

Então, basta encontrarmos o resto da divisão de $1 - 36^5$ por 77. Como $36 = 7 \cdot 5 + 1$, temos que $36 \equiv 1 \mod 7$, daí $36^5 \equiv 1 \mod 7$. Além disso, é fácil ver que $36 \equiv 3 \mod 11$ e como $3^5 = 243 = 11 \cdot 22 + 1$, podemos concluir que $36^5 \equiv 3^5 \equiv 1 \mod 11$. Uma vez que $mdc(7, 11) = 1$ e ambos dividem $36^5 - 1$, conclui-se que 77 divide $36^5 - 1$. Portanto, $36^{36} + 41^{41}$ deixa resto 0 na divisão por 77. ■

3. Equações Diofantinas Lineares

Agora com as ferramentas em mãos, iremos nos concentrar em resolver problemas de equações diofantinas lineares que são equações do tipo $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, onde os a_i, com $i = 1, \ldots, n$ são inteiros não simultaneamente nulos e b um inteiro conhecido. Já os símbolos $x_1, \ldots, x_n$ representam as incógnitas da equação, e estamos interessados em encontrar apenas soluções inteiras para a equação. Por conveniência, enunciaremos apenas os resultados para o caso em duas variáveis, mas que podem ser facilmente generalizados para o caso de n variáveis, ver [3].

Teorema 3. *A equação Diofantina $ax + by = c$, com $a \neq 0$ ou $b \neq 0$, terá solução inteira se, e somente se, $d = mdc(a, b)$ divide c.*

Demonstração. Seja (x_0, y_0) uma solução particular e $d = mdc(a, b)$, então temos $a = dk_1$, $b = dk_2$ e $ax_0 + by_0 = c$, o que implica que $dk_1x_0 + dk_2y_0 = c$, ou seja, $d(k_1x_0 + k_2y_0) = c$, portanto $d \mid c$. Reciprocamente, suponha que $d = mdc(a, b)$ e $d \mid c$. Como $d \mid c$, temos $c = dt$. Como $d = mdc(a, b)$ pelo Teorema 2 existem $m, n \in \mathbb{Z}$ tais que $am + bn = d$, multiplicando a igualdade por t, obtemos $amt + bnt = dt = c$. Portanto (mt, nt) é uma solução para a equação em questão.

□

Observação 2. Note que, sempre que o $mdc(a, b)$ divide c podemos simplificar a equação $ax+by = c$ por uma do tipo $a'x + b'y = c'$ onde $a' = a/mdc(a, b)$, $b' = b/mdc(a, b)$ e $c' = c/mdc(a, b)$. Dessa forma a' e b' são primos entre si, o que significa que $mdc(a', b') = 1$. Portanto, sempre que uma equação diofantina admite soluções inteiras, podemos obter uma equação equivalente cujos coeficientes são primos entre si, daí segue o resultado:

Proposição 4. *Seja (x_0, y_0) uma solução particular da equação $ax + by = c$, onde $mdc(a, b) = 1$. Então todas as soluções inteiras (x, y) da equação são da seguinte forma: $x = x_0 - bt$, $y = y_0 + at$ e $t \in \mathbb{Z}$.*

Demonstração: Seja (x_0, y_0) uma solução particular conhecida, então $ax_0+by_0 = c$. Se (x, y) é outra solução qualquer, temos $ax + by = c$. Assim, $ax_0 + by_0 = ax + by$, ou seja, $a(x_0 - x) = b(y - y_0)$, o que implica que $a \mid b(y - y_0)$, mas como $mdc(a, b) = 1$ temos, $a \mid y - y_0$, assim $at = y - y_0$. Substituindo, temos $a(x_0 - x) = bat$, obtendo $bt = x_0 - x$. Portanto, $x = x_0 - bt, \quad y = y_0 + at, \quad t \in \mathbb{Z}$. Note que x e y, como definidos acima, são soluções, pois

$$ax + by = a(x_0 - bt) + b(y_0 + at) = ax_0 + by_0 = c.$$

□

Exemplo 5 (Obmep, 2008, 1ª Fase, Nível 2, Problema 13, [9])**.** Os 535 alunos e os professores de uma escola fizeram um passeio de ônibus. Os ônibus, com capacidade para 46 passageiros cada, ficaram lotados. Em cada ônibus havia um ou dois professores. Em quantos ônibus havia dois professores?

Solução: Sendo x o número de ônibus com 1 professor e y o número de ônibus com 2 professores. Note que nos ônibus com 1 professor há 45 alunos e nos ônibus com 2 professores há 44 alunos, pois todos os 46 lugares dos ônibus estão lotados. Assim, obtemos a equação $45x + 44y = 535$, onde queremos encontrar uma solução (x, y) de números naturais. Como $mdc(45, 44) = 1$ e $1 \mid 535$ a equação possui solução, e notando que $45 \cdot 1 + 44 \cdot (-1) = 1$ isso implica que $45 \cdot 535 + 44 \cdot (-535) = 535$. Logo, uma solução particular para a equação é $x_0 = 535$ e $y_0 = -535$. Pela Proposição 4, temos que a solução geral é

$$x = 535 - 44t \quad \text{e} \quad y = -535 + 45t, \ t \in \mathbb{Z}.$$

Como queremos que a solução (x, y) seja um par de números naturais, devemos ter $535 - 44t > 0$ e $-535 + 45t > 0$. Resolvendo essas desigualdades, encontramos o único inteiro $t = 12$ e, consequentemente, a única solução natural é o par $x = 7$ e $y = 5$. Portanto, havia 5 ônibus com 2 professores.

■

Note que uma equação diofantina linear de duas variáveis da forma $ax + by = c$ também pode ser vista como a reta $y = \dfrac{c - ax}{b}$ e, desde que $mdc(a, b)$ divida c, as soluções que estamos procurando para essa equação que modela o problema em tela são os pontos dessa reta cujas coordenadas são, ambas, números inteiros. Durante a solução do Exemplo 5, trabalhamos com a equação $45x + 44y = 535$, e sua reta correspondente é representada a seguir:

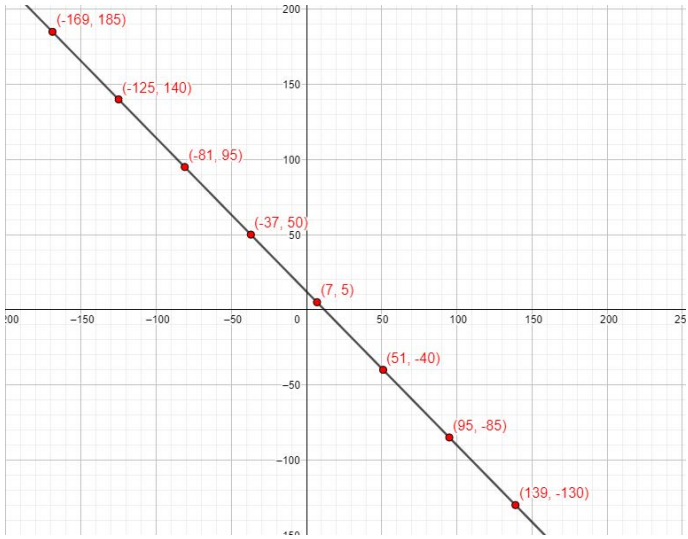


Figura 2: Reta - Exemplo 6. Fonte: Autores.

Os pontos destacados na reta são algumas das infinitas soluções para a equação $45x + 44y = 535$, cujas coordenadas são ambas inteiras. Note que a única solução em inteiros positivos é de fato $x = 7$ e $y = 5$. ■

O exemplo a seguir, apesar de não pertencer a nenhuma olimpíada, é importante pois determina quais dos inteiros positivos podem ser expressos como uma combinação linear positiva de dois inteiros positivos a e b com $mdc(a, b) = 1$. Tal resultado pode ser útil para resolver problemas como o do Exemplo 5.

Exemplo 6 (O Número de Frobenius)**.** Dados a e b inteiros positivos tais que $mdc(a, b) = 1$. Determine o maior inteiro positivo $g = g(a, b)$ tal que todo $d > g$ pode ser expresso como uma combinação linear positiva de a e b, isto é, existem $x, y \in \mathbb{Z}^+$ tais que $ax + by = d$.

Solução: Este é o famoso problema do Número de Frobenius em duas variáveis, e, nesse caso, temos que $g(a, b) = ab - a - b$. De fato, como $mdc(a, b) = 1$ podemos representar qualquer número inteiro positivo p como $p = xa + yb; x, y \in \mathbb{Z}$. Além disso, pela Proposição 4, existem diversas maneiras de representar p desde que $x = x_0 - bt$ e $y = y_0 + at$ onde (x_0, y_0) é uma solução particular e $t \in \mathbb{Z}$. Contudo, note que essa representação torna-se única, quando estamos procurando por $0 \leq x < b$, e nesse caso, p é representável se $y \geq 0$, e o contrário, se $y < 0$. Então, o maior número que não pode ser expresso é quando $x = b - 1$ e $y = -1$, portanto,

$$g(a, b) = (b - 1)a + (-1)b = ab - a - b.$$

■

Este resultado estende-se para n variáveis, e o caso mais geral pode ser encontrado em [1].

4. Traçando Estratégias para Equações Diofantinas Não Lineares

Diferente de problemas de equações diofantinas lineares, os casos não lineares não possuem um método de solução, sendo necessário uma análise específica para cada caso. A grande maioria das

questões de Olimpíadas de Matemática sobre equações diofantinas acaba trazendo em si equações não lineares. Ainda assim, veremos, nesta seção, que mesmo não tendo um formato unificado de solução, há estratégias que podem ser empregadas, dependendo do tipo de solução que envolve o problema (por exemplo: provar que há infinitas soluções ou que não há solução). Apresentaremos quatro técnicas (fatorações, desigualdades, parametrizações e aritmética modular) para o caso não linear.

4.1. Método das Fatorações

A busca por soluções naturais ou inteiras para equações diofantinas, muitas vezes, recai em manipulações algébricas de equações ou sistemas de equações, de modo que essas possam ser simplificadas até que possamos obter conclusões parciais ou mesmo finais. Quando procuramos por soluções que podem ser solúveis por meio de radicais (ou seja, que podem ser resolvidas por meio de operações algébricas ou raízes), as fatorações por meio dos produtos notáveis consistem em fortes ferramentas para essas simplificações, de maneira a deixar explícito informações como divisibilidade ou termos em comum que podem ser simplificados. Nosso primeiro problema recai no uso de um produto notável comum em competições, mas menos usualmente conhecido e utilizado.

Exemplo 7 (POTI, 2012, Teoria dos Números, Nível 2, Aula 1, Problema 38, [10])**.** Encontre todos os pares de inteiros (x, y) tais que $1 + 1996x + 1998y = xy$.

Solução: Reorganizando a identidade, obtemos

$$xy - 1996x - 1998y = 1. \tag{1}$$

A expressão no lado esquerdo de (1) sugere o seguinte produto: dados $x, y, a, b \in \mathbb{R}$, é possível mostrar que

$$(x - a)(y - b) = xy - bx - ay + ab.$$

Perceba que para corresponder ao produto, ainda falta o termo ab, que nesse caso será $1996 \cdot 1998$. Somando $1996 \cdot 1998$ em ambos os lados de (1) ficaremos com

$$(x - 1998)(y - 1996) = 1996 \cdot 1998 + 1. \tag{2}$$

Relembremos do produto notável $a^2 - b^2 = (a + b)(a - b)$, e perceba agora que o lado direito de (2), o produto $1996 \cdot 1998$ pode ser reescrito, pois $1996 = (1997 - 1)$ e $1998 = (1997 + 1)$, donde

$$1996 \cdot 1998 + 1 = (1997 - 1)(1997 + 1) + 1 = (1997^2 - 1) + 1 = 1997^2. \tag{3}$$

Combinando (2) e (3), concluímos que

$$(x - 1998)(y - 1996) = 1997^2.$$

Chegando aqui, precisamos descobrir os divisores de 1997. Como $45^2 = 2025$, então testando os divisores primos menores do que 45, descobrimos que o número 1997 não é divisível por nenhum deles, portanto 1997 é um número primo. Assim, os divisores de 1997^2 são ± 1, ± 1997 e $\pm 1997^2$, de modo que

$$1997^2 = (\pm 1)(\pm 1997^2) = (\pm 1997)(\pm 1997) = (\pm 1997^2)(\pm 1).$$

Portanto, as possibilidades são

$$\begin{cases} x-1998=\pm 1, \\ y-1996=\pm 1997^2, \end{cases} \quad \text{ou} \quad \begin{cases} x-1998=\pm 1997, \\ y-1996=\pm 1997, \end{cases} \quad \text{ou} \quad \begin{cases} x-1998=\pm 1997^2, \\ y-1996=\pm 1. \end{cases}$$

Perceba que o sistema é simples de ser solucionado, bastando somar 1998 e 1996 em ambos os lados da equação para x e y respectivamente. Obtemos, assim, as soluções

$$(x,y) \in \{(1998 \pm 1, 1996 \pm 1997^2), (1998 \pm 1997, 1996 \pm 1997), (1998 \pm 1997^2, 1996 \pm 1)\}.$$

■

Exemplo 8 (OBM, 2006, 3ª Fase, Nível 1, Primeiro Dia, Problema 3, [8])**.** Encontre todos os pares ordenados (x,y) de inteiros tais que

$$x^3 - y^3 = 3(x^2 - y^2). \tag{4}$$

Solução. Primeiramente, é fácil notar que, para $x = y$, obtemos uma identidade verdadeira em (4). Isso nos diz que os pares da forma (n,n) com $n \in \mathbb{Z}$ são soluções. Daqui em diante, consideramos $x \neq y$. Dados $a, b \in \mathbb{R}$, é possível mostrar que

$$a^3 - b^3 = (a-b)(a^2+ab+b^2) \quad \text{e} \quad a^2 - b^2 = (a+b)(a-b).$$

Perceba que a equação (4) pode ser reescrita como

$$(x-y)(x^2+xy+y^2) = 3(x+y)(x-y).$$

Como $x \neq y$, podemos simplificar os termos $x-y$ e ficamos com

$$x^2 + xy + y^2 = 3x + 3y,$$

que é equivalente à seguinte equação quadrática na variável x,

$$x^2 + (y-3)x + y^2 - 3y = 0. \tag{5}$$

Para que a equação acima tenha solução real, devemos impor a condição que o descriminante Δ deve ser não negativo. Como

$$\Delta = (y-3)^2 - 4(y^2-3y) = (y-3)^2 - 4y(y-3) = (y-3)[(y-3)-4y] = (y-3)(-3y-3) = -3(y-3)(y+1).$$

Forçando a condição $\Delta \geq 0$, obtemos

$$-3(y-3)(y+1) \geq 0 \quad \Leftrightarrow \quad (y-3)(y+1) \leq 0.$$

Fazendo um estudo do sinal para a função $p(y) = (y-3)(y+1)$, percebemos que ela é não positiva para $-1 \leq y \leq 1$. Uma vez que y é inteiro, então temos as seguintes possibilidades $y \in \{-1, 0, 1, 2, 3\}$. Para cada valor de y assumido, substituiremos esse valor na equação (5) e encontraremos as soluções inteiras para x.

Caso 1. $y = -1$**.** A equação (5) assume o seguinte formato

$$x^2 - 4x + 4 = 0 \quad \Rightarrow \quad (x-2)^2 = 0 \quad \Rightarrow \quad x = 2,$$

portanto, obtemos a solução $(-1, 2)$.

Caso 2. $y = 0$**.** A equação (5) assume o seguinte formato

$$x^2 - 3x = 0 \quad \Rightarrow \quad x(x-3) = 0 \quad \Rightarrow \quad x = 0 \text{ ou } x = 3,$$

e as soluções são $(0, 0)$ e $(3, 0)$.

Caso 3. $y = 1$**.** A equação (5) assume o seguinte formato

$$x^2 + 2x - 2 = 0,$$

que não tem solução inteira, pois o discriminante nesse caso é igual a 12.

Caso 4. $y = 2$**.** A equação (5) assume o seguinte formato

$$x^2 - x - 2 = 0 \quad \Rightarrow \quad (x+1)(x-2) = 0 \quad \Rightarrow \quad x = -1 \text{ ou } x = 2.$$

As soluções desse caso são $(-1, 2)$ e $(2, 2)$.

Caso 5. $y = 3$**.** Finalmente, a equação (5) assume o seguinte formato

$$x^2 = 0 \quad \Rightarrow \quad x = 0,$$

e a última solução é $(0, 3)$. Dessa forma, todas as soluções de (4) são

$$\{(-1, 2), (2, -1), (3, 0), (0, 3)\} \cup \{(n, n)/n \in \mathbb{Z}\}.$$

■

4.2. Método das Desigualdades

Outra possibilidade de manipulação consiste no desenvolvimento de desigualdades, de maneira a encaixar as possibilidade em intervalos. Desse modo, como as soluções são inteiras, a quantidade de possibilidades é limitada, fazendo com que o resultado possa ser obtido por meio do esgotamento dos casos possíveis.

Exemplo 9 (Olimpíada de Matemática Romena, [2])**.** Encontre todos os números inteiros positivos x, y, z tais que

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}. \tag{6}$$

Solução: Como a expressão em (6) é simétrica nas variáveis x, y e z, uma vez que encontramos uma solução (a, b, c) de (6) então qualquer permutação ainda é uma solução. Observe agora que se qualquer uma das variáveis for 1, já não há mais solução, uma vez que $\frac{3}{5} < 1$. Assim, para mapear as soluções, vamos supor

$$2 \leq x \leq y \leq z, \tag{7}$$

de modo que qualquer outra solução é obtida por permutação das soluções que encontraremos. Da desigualdade (7), concluímos que

$$\frac{1}{z} \leq \frac{1}{y} \leq \frac{1}{x}, \tag{8}$$

logo,

$$\frac{3}{5} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \leq \frac{3}{x}, \tag{9}$$

donde, $x \leq 5$. Limitamos assim as possibilidades de x ao intervalo $[2, 5]$. Olharemos, agora, cada caso para esgotar as possibilidades:

Caso 1. $x = 2$**.** Nessa situação a equação (6) torna-se

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{10}. \tag{10}$$

Observando a expressão acima, concluímos que tanto y quanto z devem ser maiores do que 10. Mais ainda, prosseguindo como em (8) e (9) obtemos

$$\frac{1}{10} \leq \frac{2}{y} \quad \Rightarrow \quad y \leq 20.$$

Portanto, $11 \leq y \leq 20$. Multiplicando (10) por $10yz$, e organizando, obtemos

$$yz - 10y - 10z = 0 \quad \Rightarrow \quad yz - 10y - 10z + 100 = 100 \quad \Rightarrow \quad (y-10)(z-10) = 100,$$

e isolando z obtemos

$$z = 10 + \frac{100}{y-10}, \tag{11}$$

de modo que 100 precisa ser divisível por $y - 10$ para que z seja inteiro. As únicas possibilidades são $y \in \{11, 12, 14, 15, 20\}$ e, pondo esses valores em (11), obtemos as soluções inteiras $(2, 11, 110)$, $(2, 12, 60)$, $(2, 14, 35)$, $(2, 15, 30)$ e $(2, 20, 20)$.

Para os demais casos, o raciocínio é análogo, considerando y no intervalo pertinente, e considerando as diversas possibilidades inteiras para z.

Caso 2. $x = 3$**.** Obtemos $\frac{1}{y} + \frac{1}{z} = \frac{4}{15}$, o que nos dá

$$\frac{4}{15} \leq \frac{2}{y} \quad \Rightarrow \quad y \leq \frac{15}{2},$$

portanto, $y \in [3, 7]$. Perceba que

$$z = \frac{15y}{4y - 15},$$

e, novamente substituindo os valores de y, encontramos as seguintes soluções de triplas inteiras $(3, 4, 60)$, $(3, 5, 15)$ e $(3, 6, 10)$.

A partir daqui, usaremos as mesmas ideias dos casos 1 e 2, dessa maneira, omitiremos os detalhes.

Caso 3. $x = 4$**.** A equação (6) reduz-se a $\frac{1}{y} + \frac{1}{z} = \frac{7}{20}$, o que nos dá $y \in [4, 5]$, e a única solução é $(4, 4, 10)$.

Caso 4. $x = 5$**.** Por fim, ficamos com $\frac{1}{y} + \frac{1}{z} = \frac{2}{5}$, e $y = z = 5$ é a única solução; portanto obtemos $(5, 5, 5)$.

Considerando $x < y < z$, obtemos como soluções $(x, y, z) \in \{(2, 11, 110), (2, 12, 60), (2, 14, 35), (2, 15, 30), (2, 20, 20), (3, 4, 60), (3, 5, 15), (3, 6, 10), (4, 4, 10), (5, 5, 5)\}$. Cabe observar que, como (6) é simétrica em relação às variáveis x, y, z, então todas as permutações das ternas ordenadas indicadas compõem o conjunto solução de (6). ■

Exemplo 10 (Olimpíada de Matemática da Rússia, 1997, Rodada Final, 10ª Série, Primeiro Dia, Problema 1, [2])**.** Encontre todas as soluções inteiras da equação

$$(x^2 - y^2)^2 = 1 + 16y. \tag{12}$$

Solução. O formato de (12) sugere-nos imediatamente fatorações diversas utilizando produtos notáveis, todas sem grandes conclusões. Por outro lado, olhando sob a perspectiva do método das desigualdades, rapidamente vemos que o lado direito de (12), por ser o quadrado de um número, deve ser positivo ou nulo, assim, olhando para o lado direito de (12), devemos ter $y \geq 0$, obtemos, assim, a primeira desigualdade para y. Mais ainda, temos que $1 + 16y \geq 1$. Podemos então reescrever a seguinte desigualdade envolvendo (12),

$$(x^2 - y^2)^2 \geq 1 \quad \Rightarrow \quad x^2 - y^2 \geq 1 \quad \text{ou} \quad x^2 - y^2 \leq -1,$$

donde

$$x^2 \geq y^2 + 1 \quad \text{ou} \quad x^2 \leq y^2 - 1.$$

Como x e y são inteiros, dizer que $x^2 \geq y^2 + 1$, implica que $|x|$ é pelo menos uma unidade maior do que $|y|$, dessa maneira $|x| > |y| + 1$. Pensando de forma análoga, dizer que $x^2 \leq y^2 - 1$, implica que $|x|$ é pelo menos uma unidade menor do que $|y|$, donde $|x| \leq |y| - 1$. Elevando ao quadrado as duas desigualdades, ficaremos com

$$|x|^2 \geq (|y| + 1)^2 \quad \Rightarrow \quad |x|^2 \geq |y|^2 + 2|y| + 1 \quad \Rightarrow \quad |x|^2 - |y|^2 \geq 2|y| + 1, \tag{13}$$

e

$$|x|^2 \leq (|y| - 1)^2 \quad \Rightarrow \quad |x|^2 \leq |y|^2 - 2|y| + 1 \quad \Rightarrow \quad |y|^2 - |x|^2 \geq 2|y| - 1. \tag{14}$$

Elevando as últimas expressões do lado direito de (13) ou de (14), obtemos a seguinte desigualdade

$$(2y - 1)^2 \leq \left(|x|^2 - |y|^2\right)^2. \tag{15}$$

Combinando (15) com (12), obtemos

$$(2y - 1)^2 \leq 1 + 16y \quad \Rightarrow \quad 4y^2 - 4y + 1 \leq 1 + 16y \quad \Rightarrow \quad 4y^2 - 20y \leq 0 \quad \Rightarrow \quad 0 \leq y \leq 5. \tag{16}$$

Agora basta esgotar os casos.

Caso 1. $y = 0$ A equação (12) assume o seguinte formato

$$x^4 = 1 \quad \Rightarrow \quad x = -1 \text{ ou } x = 1,$$

obtemos portanto as soluções $(-1, 0)$ e $(1, 0)$.

Caso 2. $y = 1$ Nesse caso, teremos

$$(x^2 - 1)^2 = 17,$$

e portanto, x não será inteiro.

Caso 3. $y = 2$ Aqui, a equação (12) fica

$$(x^2 - 4)^2 = 33,$$

e, novamente, não temos soluções inteiras para x.

Caso 4. $y = 3$ Teremos

$$(x^2 - 9)^2 = 49 \quad \Rightarrow \quad x^2 - 9 = \pm 7,$$

portanto

$$x^2 = 2 \quad \text{ou} \quad x^2 = 16,$$

logo, as soluções são $(-4, 3)$ e $(4, 3)$.

Caso 5. $y = 4$ Aqui, a equação (12) fica

$$(x^2 - 16)^2 = 65,$$

e novamente não temos soluções inteiras para x.

Caso 6. $y = 5$ No último caso teremos

$$(x^2 - 25)^2 = 81 \quad \Rightarrow \quad x^2 - 25 = \pm 9,$$

portanto

$$x^2 = 16 \quad \text{ou} \quad x^2 = 34,$$

cujas soluções inteiras são $x = -4$ e $x = 4$. Assim, as soluções são $(-4, 5)$ e $(4, 5)$.

Obtemos as soluções $\{(-1, 0), (1, 0), (-4, 3), (4, 3), (-4, 5), (4, 5)\}$ que podem ser vistas, geometricamente, com a seguinte figura

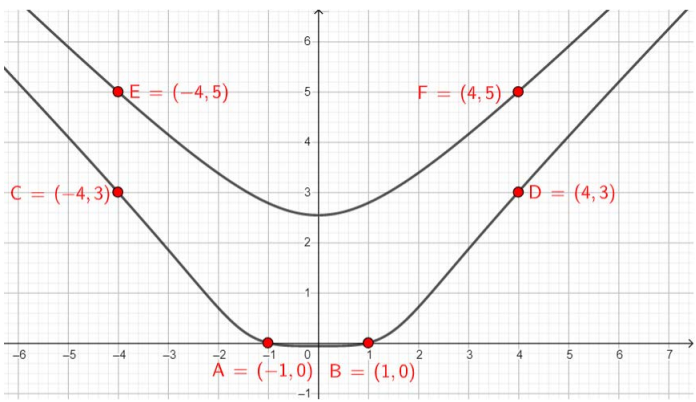


Figura 3: Pontos com coordenadas inteiras da curva implícita $(x^2 - y^2) = 1 + 16y$. Fonte: Autores.

■

4.3. Método da Parametrização

Veremos agora que há casos em que a equação diofantinas pode ser representada da seguinte maneira

$$f(x_1, x_2, ..., x_{n-1}, x_n) = 0,$$

e, nessa situação, as soluções podem ser escritas como equações paramétricas da forma

$$x_i = g_i(k_1, k_2, ..., k_{l-1}, k_l),\ i = 1, 2, ..., n-1, n,$$

com $g_i : \mathbb{Z}^n \to \mathbb{Z}$ são funções e $k_j \in \mathbb{Z}$, $j = 1, ..., l$. O tratamento desses casos, em geral, ocorre quando não há uma maneira explícita de encontrar todas as soluções, em particular, o método que explicitaremos garante-nos a existência de infinitas soluções para esses problemas.

Exemplo 11 (Torneio das Cidades, [2])**.** Prove que existem infinitas triplas de inteiros (x, y, z) tais que

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2. \tag{17}$$

Solução: Perceba, inicialmente, que o enunciado não nos pede para explicitar exatamente quais são essas soluções; mais ainda, por serem infinitas, certamente estamos em um caso de parametrização de soluções. Para darmos o primeiro passo, colocaremos alguma das variáveis em função de outra(s), de maneira que consigamos reduzir a quantidade de termos iniciais. Perceba que se $z = -y$, então

$$y^3 + z^3 = 0 \quad \text{e} \quad y^2 + z^2 = 2y^2. \tag{18}$$

Pondo (18) em (17), obtemos

$$x^3 = x^2 + 2y^2. \tag{19}$$

Novamente, para simplificar a expressão (19) acima, podemos considerar $y = kx$, com $k \in \mathbb{Z}$, e obtemos

$$x^3 = x^2 + 2(kx)^2 \quad \Rightarrow \quad x^3 = x^2(1 + 2k^2) \quad \Rightarrow \quad x = 0 \text{ ou } x = 2k^2 + 1. \tag{20}$$

O caso $x = 0$ torna-se trivial e pode ser desconsiderado. Portanto, triplas da forma $(x, y, z) = (g_1(k), g_2(k), g_3(k)) = (2k^2 + 1, 2k^3 + k, -2k^3 - k)$, com $k \in \mathbb{Z}$, satisfazem a equação. ■

Finalizaremos o método da parametrização com o clássico problema das ternas pitagóricas.

Mas antes vamos considerar o seguinte lema:

Lema 2. *Seja (x, y, z) uma Terna Pitagórica primitiva, isto é, $x^2 + y^2 = z^2$ com $x, y, z \in \mathbb{Z}$ primos entre si. Então x e y têm paridades distintas e z é ímpar.*

Demonstração. Primeiramente, note que não podemos ter x e y, ambos pares, já que, por hipótese, eles são primos entre si. Agora, sem perda de generalidade, podemos supor que y é ímpar. Assim, existe k_1 inteiro tal que $y = 2k_1 + 1$, logo

$$y^2 = 4k_1^2 + 4k_1 + 1 \equiv 1 \bmod 4.$$

Note que dado um inteiro par qualquer $p = 2k$, temos que

$$p^2 = 4k^2 \equiv 0 \bmod 4,$$

dessa forma, vemos que todo quadrado perfeito nos inteiros é congruente a 0 ou 1 módulo 4. Logo, x não pode ser ímpar, pois caso o fosse existiria k_2 inteiro tal que $x^2 = 4k_2^2 + 4k_2 + 1$, e, então, $z^2 = x^2 + y^2 \equiv 2 \bmod 4$, o que não pode ocorrer. Portanto x é par e, consequentemente, z é ímpar.

□

Exemplo 12 (Ternas Pitagóricas)**.** Encontre todas as soluções de inteiros positivos (x, y, z) tais que

$$x^2 + y^2 = z^2. \tag{21}$$

Solução. Certamente esse problema tem infinitas soluções. Note que $(3, 4, 5)$ é uma terna solução de (21), pois $3^2+4^2 = 9+16 = 25 = 5^2$. Dessa maneira, também serão soluções as ternas $(3k, 4k, 5k)$ com $k \in \mathbb{Z}$. A questão aqui não é apenas mostrar que (21) tem infinitas soluções, mas sim encontrar todas as soluções, o que torna este problema um pouco mais refinado.

Procedendo como no problema anterior, perceba que se $y = k_1 x$, onde k_1 é um inteiro, então o lado esquerdo de (21) torna-se mais simples, e ficamos com

$$x^2 + k_1^2 x^2 = z^2 \quad \Rightarrow \quad z^2 = x^2(k_1^2 + 1) \quad \Rightarrow \quad z = x\sqrt{k_1^2 + 1}.$$

Apesar de conseguirmos expressar y e z em função de x, o que permitiria uma parametrização da solução bastando tomar $x = k_2$, ainda devemos nos preocupar em explicitar valores de k_1 de maneira que $k_1^2 + 1$ seja um quadrado perfeito. Seguiremos, então, outra estratégia. Pelo Lema 2 podemos tomar y e z ímpares: além disso, $y \leq z$. Perceba que podemos reescrever (21) da seguinte maneira:

$$x^2 = z^2 - y^2 = (z + y)(z - y). \tag{22}$$

Como y e z são ímpares, $z + y$ e $z - y$ são pares. Sendo $mdc(y, z) = 1$, pelo Lema 1, temos que $mdc(y + z, z) = mdc(y + z - z, z) = 1$. Além disso, como $y + z$ é par, vale que $mdc(2z, z + y) = 2$ e novamente pelo Lema 1, notando que $z \geq y$, temos $mdc(2z, z + y) = mdc(2z - (z + y), z + y) = mdc(z - y, z + y) = 2$, e daí $mdc\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$. Por (22) temos que $(z-y)(z+y)$ é um quadrado perfeito, e $\frac{z-y}{2}$ e $\frac{z+y}{2}$ são primos entre si; daí, pelo Teorema Fundamental da Aritmética, concluímos que $\frac{z-y}{2}$ e $\frac{z+y}{2}$ são quadrados perfeitos. Considere $k_1, k_2 \in \mathbb{N}$ tais que

$$\frac{z+y}{2} = k_1^2 \quad \text{e} \quad \frac{z-y}{2} = k_2^2, \quad \text{com} \quad mdc(k_1, k_2) = 1. \tag{23}$$

Comparando (23) com (22) temos que $x = 2k_1k_2$. E, finalmente, isolando z e y em (23) concluímos que todas as soluções de (21) de inteiros positivos são da forma $(x, y, z) = (g_1(k_1, k_2), g_2(k_1, k_2), g_3(k_1, k_2)) = \left(2k_1k_2, k_1^2 - k_2^2, k_1^2 + k_2^2\right)$, em que $k_1 > k_2$ são inteiros positivos. ■

4.4. Utilizando Aritmética Modular

A aritmética modular é uma forte ferramenta quando tratamos de casos específicos, em particular, por permitirem simplificações. É possível, com as relações de congruência modular, verificar a existência de soluções de uma equação, sem precisar de fato resolvê-la. Por exemplo, se estamos trabalhando com quadrados perfeitos, uma boa ideia é usar congruência módulo 3, módulo 4 ou módulo 8, pois todo quadrado perfeito é congruente a 0 ou 1 módulo 3 ou módulo 4, e é congruente a 0, 1 ou 4 módulo 8; nos casos de cubos perfeitos a estratégia é usar congruência módulo 7, pois todo cubo perfeito é congruente a 0, 1 ou 6 módulo 7.

Exemplo 13 (Olímpia Matemática Húngara, [2])**.** Mostre que a equação

$$(x+1)^2 + (x+2)^2 + \ldots + (x+99)^2 = y^z \tag{24}$$

não possui solução com x, y, z inteiros tais que $z > 1$.

Solução. Já sabemos, nesse ponto, que fatorações podem ser ferramentas para obtenção da solução ou simplificação de cálculos. Dados $a, b \in \mathbb{R}$, temos que $(a+b)^2 = a^2 + 2ab + b^2$.

Além disso, destacamos as fórmulas fechadas para a soma dos n primeiros números naturais e soma dos quadrados dos n primeiros inteiros positivos.

$$\sum_{i=1}^{n} i = 1 + 2 + \ldots + (n-1) + n = \frac{n(n+1)}{2}, \tag{25}$$

e

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \ldots + (n-1)^2 + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{26}$$

Salientamos que tais fórmulas podem ser rapidamente provadas pelo Princípio de Indução Finita. Este resultado pode ser encontrado em [2] ou [10]. Por meio destes resultados, perceba que

$$\begin{aligned}
y^z &= (x+1)^2 + (x+2)^2 + \ldots + (x+98)^2 + (x+99)^2 \\
&= (x^2 + 2x + 1) + (x^2 + 2\cdot 2x + 2^2) + \ldots + (x^2 + 2\cdot 98x + 98^2) + (x^2 + 2\cdot 99x + 99^2) \\
&= (x^2 + 2x + 1) + (x^2 + 2x\cdot 2 + 2^2) + \ldots + (x^2 + 2x\cdot 98 + 98^2) + (x^2 + 2x\cdot 99 + 99^2) \\
&= 99x^2 + 2x(1 + 2 + \ldots + 98 + 99) + (1 + 2^2 + \ldots + 98^2 + 99^2) \\
&= 99x^2 + 2x(1 + 2 + \ldots + 98 + 99) + (1 + 2^2 + \ldots + 98^2 + 99^2) \\
&= 99x^2 + 2x\frac{99\cdot 100}{2} + \frac{99\cdot 100\cdot 199}{6} = 99x^2 + 99\cdot 100x + 33\cdot 50\cdot 199 \\
&= 33(3x^2 + 300x + 50\cdot 199) = 3\cdot 11(3x^2 + 300x + 50\cdot 199).
\end{aligned}$$

Como x, y, z são inteiros, então y^z é uma potência inteira de y. Como 3 divide y^z, então devemos ter $3|y$, o que implica $3^2|y^2$. Mas note que $z \geq 2$, portanto $3^2|y^z$. Mas isso é falso, pois $3x^2 + 300x + 50\cdot 199$ não é divisível por 3, uma vez que $3|3x^2 + 300x$, mas $3 \nmid 50\cdot 199$. Provamos assim que não existem inteiros x, y, z com $z > 1$ satisfazendo (24). ■

Um resultado comumente utilizado em simplificações em cálculos de congruência modular é o seguinte

Teorema 4 (Pequeno Teorema de Fermat)**.** *Dados $a, p \in \mathbb{Z}$ com p primo, têm-se que $a^p \equiv a \bmod p$. Em particular, se $mdc(a,p) = 1$, então $a^{p-1} \equiv 1 \bmod p$.*

Demonstração. Ver [7].

Em posse desse resultado, considere.

Exemplo 14 (OBM, 2009, 3ª Fase, Nível 2, Problema 3, [8])**.** Prove que não existem inteiros positivos x e y tais que $x^3 + y^3 = 2^{2009}$.

Solução. Pelos comentários no início da questão, como estamos trabalhando com termos elevados ao cubo, optaremos por trabalhar com congruência módulo 7. Sabemos que para todo número inteiro x, temos que x^3 só pode ser congruente a 0, 1 ou 6 módulo 7, e o mesmo ocorre com y^3. Assim, fazendo uma combinação dessas possibilidades, temos que $x^3 + y^3$ deve ser congruente a 0, 1, 2, 5 ou 6 módulo 7. Mas pelo Pequeno Teorema de Fermat, $2^7 \equiv 2 \mod 7$ ou $2^6 \equiv 1 \mod 7$, donde

$$2^{2009} \equiv 2^{6\cdot 334+5} = (2^6)^{334} \cdot 2^5 \equiv (1)^{334} \cdot 2^5 \equiv 32 \equiv 4 \mod 7.$$

Isso prova que não existem x e y inteiros positivos tais que $x^3 + y^3 = 2^{2009}$. ■

5. Conclusão

Neste trabalho, são discutidos alguns resultados e técnicas de soluções envolvendo equações diofantinas lineares e não lineares. Em relação às lineares, fizemos uma revisão de conceitos importantes como divisão euclidiana, máximo divisor comum e congruência modular, a fim de encontrarmos soluções para equações com duas variáveis. Por outro lado, fizemos o tratamento do caso não linear por meio de quatro abordagens bem específicas, divididas por métodos que utilizam fatorações; desigualdades; parametrizações e aritmética modular. Pudemos observar que o método das fatorações é uma ferramenta muito útil nas simplificações das expressões algébricas contidas nos problemas. O método das desigualdades é eficiente, quando conseguimos determinar um intervalo em que a(s) variável(is) estão limitada(s), de maneira que podemos esgotar os casos ao estudar todas as possibilidades. Já o método das parametrizações é utilizado na busca por soluções de equações com infinitas soluções. E, por fim, o método que utiliza aritmética modular está muito presente nas questões que lidam com restos de divisões ou para determinar a existência de solução em alguns problemas, por meio de resultados sobre congruência módulo já conhecidos.

Referências

[1] ALFONSÍN, Jorge L. Ramírez *et al.* The diophantine Frobenius problem. Oxford University Press on Demand, 2005.

[2] ANDREESCU, Titu *et al.* An introduction to Diophantine equations: a problem-based approach. New York: Birkhäuser, 2010.

[3] ANJOS, A. A. Equações Diofantinas: Sequência Didática e o Método da Descida Infinita de Fermat. Mestrado Profissional em Rede Nacional - Centro de Ciências e Tecnologia, Universidade Federal do Ceará, Fortaleza, 2015.

[4] CAMPOS, Giseli Duardo Maciano. Equações diofantinas lineares. 70 f. Dissertação Profmat (Mestrado Profissional em Matemática) - Universidade Federal de Mato Grosso, Cuiabá, 2013.

[5] CHAVES, A. P. A. Álgebra e teoria dos números para olimpíadas. *Professor de Matemática Online (PMO)*, v. 7, nº 1, p. 66-76, 2019.

[6] DOS SANTOS, Jhonata Avelar et al.Explorando os teoremas de Menelaus e Ceva em questoes de olimpıadas de matemática. *Professor de Matemática Online (PMO)*, v. 9, n° 3, 2021.

[7] NETO, Altino da Silva. Convite às Equações Diofantinas: uma abordagem para a educação básica. Dissertação Profmat (Mestrado Profissional em Matemática) — Universidade Federal de Roraima, Boa Vista, 2016. Disponível em ⟨https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?cpf=

57831246215&d=20210421133048&h=52cfdaf6160ca690145f62a1c045fad6649ec641⟩. Acesso em 11 Mar. de 2021.

[8] Olimpíada Brasileira de Matemática. Disponível em: ⟨https://www.obm.org.br/⟩. Acesso em 11 Mar. de 2021.

[9] Olimpíada Brasileira de Matemática das Escolas Públicas. Disponível em: ⟨http://www.obmep.org.br⟩. Acesso em 11 Mar. de 2021.

[10] Polos Olímpicos de Treinamento Intensivo. Disponível em: ⟨https://poti.impa.br/⟩. Acesso em 21 Fev. de 2021.

[11] Portal da Obmep - Aritmética dos Restos - Caderno de Exercícios - Aritmética Modular. Disponível em: ⟨https://cdnportaldaobmep.impa.br/portaldaobmep/uploads/material/5oeoy5b8w0gso.pdf⟩. Acesso em 11 Mar. de 2021.

[12] RIBEIRO, Rildo. *Equações diofantinas: uma abordagem para o ensino médio*. Dissertação PROFMAT (Mestrado Profissional em Matemática) — Universidade de Brasília, Brasília, 2014.

[13] SERRÃO, Marcelo Miranda; BRANDEMBERG, João Cláudio. *Utilizando problemas da história antiga da Matemática como estratégia para o ensino de equações no 9º ano da escola básica*. X Seminário Nacional de História da Matemática. Campinas - São Paulo, 2013.

[14] SINGH, Simon. *O último teorema de Fermat: A história do enigma que confundiu as mais brilhantes mentes do mundo durante 358 anos*. Editora Best Seller, 2014.

Érick C. A. do Nascimento
Universidade Federal Rural de Pernambuco
Departamento de Matemática (DM-UFRPE)
Recife/PE
<erick.alves@ufrpe.br>

Thiago Yukio Tanaka
Universidade Federal Rural de Pernambuco
Departamento de Matemática (DM-UFRPE)
Recife/PE
<thiago.tanaka@ufrpe.br>

Barbara Costa da Silva
Universidade Federal Rural de Pernambuco
Departamento de Matemática (DM-UFRPE)
Recife/PE
<barbara.costasilva@ufrpe.br>

Recebido: 10/09/2021
Publicado: 13/07/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo1026

Triplos pitagóricos e as interações entre álgebra, geometria e aritmética

Rubens Vilhena Fonseca Ana Paula Sales Brito Gabriel Dias de Pinho
Yuri Albino Marigliani Richard Campos Vilhena Fonseca

Resumo

Neste artigo, apresentamos quatro teoremas, não muito presentes nos livros didáticos, e que geralmente não estão inclusos nos currículos da Escola Básica, com o objetivo de que o leitor perceba a interação entre as diferentes áreas da Matemática mais comuns aos estudantes, a saber: Aritmética, Álgebra, Geometria e Trigonometria. Espera-se que as provas desses teoremas, além de ilustrar a conexão entre essas áreas, destacadas neste artigo, mostrem a necessidade de essas áreas interagirem entre os vários tipos de pensamentos matemáticos. Acreditamos que o professor, ao considerar o entrelaçamento desses tópicos, tende a refletir e elaborar tipos de atividades que ampliem o que é apresentado em sala de aula. Por meio de nossas pesquisas bibliográficas, foi possível observar suas implicações didáticas, correlações com a Base Nacional Comum Curricular e algumas teorias educacionais envolvidas que, devido ao nosso objetivo, não serão objetos de discussão, mas estão implícitas neste texto.

Palavras-chave: álgebra; geometria; trigonometria; teoria dos números

Abstract

In this article, we present four theorems, not very present in textbooks, and which are generally not included in the Basic School curricula, with the objective that the reader perceives the interaction between the different areas of Mathematics most common to students, namely Arithmetic, Algebra, Geometry and Trigonometry. It is hoped that the proofs of these theorems, in addition to illustrating the connection between these areas, highlighted in this article, show the need for these areas to interact between the various types of mathematical thinking. We believe that the teacher, when considering the intertwining of these topics, tends to reflect and elaborate types of activities that expand what is presented in the classroom. Through our bibliographic research, it was possible to observe its didactic implications, correlations with the National Curricular Common Base and some educational theories involved that, due to our objective, will not be objects of discussion, but are implicit in this text.

Keywords: algebra; geometry; trigonometry; number theory

1. Introdução

Nossa motivação ao escrever este artigo deu-se pela percepção, como professores de Matemática, de que os conteúdos matemáticos passam por inúmeras modificações no decorrer do tempo [10].

O que se pode apresentar nos livros didáticos é uma versão sem os dramas humanos de erros, frustrações e acertos que levaram à evolução daqueles conteúdos, além da omissão, por uma questão de necessidade, de muitos resultados paralelos importantes que foram obtidos no estudo de um problema em particular. Sendo nosso objetivo que o leitor perceba a interação entre diferentes áreas da matemática, destacamos o Teorema de Pitágoras e os Triplos Pitagóricos, por serem tópicos de estudos na Teoria dos Números que sempre rendem resultados surpreendentes e podem nos auxiliar na elaboração de uma didática eficiente para o ensino. Em particular, centramos neste artigo as conexões entre a Aritmética, Álgebra e Geometria.

Primeiramente, definimos o que são triplos e triângulos pitagóricos. O Teorema 1 apresenta a forma geral de como obtê-los. Nesse contexto, é feita uma sugestão que conduza à discussão do Teorema Fundamental da Aritmética para alunos da Escola Básica. Em seguida, discutimos a fórmula de Heron.

A partir desses resultados, na terceira seção, consideramos a instauração de um desafio a ser proposto em sala de aula, e a trigonometria apresenta-se como o ramo da Matemática ideal para fazer a interação necessária com outros ramos. Para isso, apresentamos os conceitos de inraio e incírculo num triângulo pitagórico para obtermos resultados como os Teoremas 2 e 3, que se constituem como prova de que as conexões entre Geometria, Álgebra e Aritmética são possíveis.

Afirma-se que, certa vez, Carl Friedrich Gauss (1777-1855) disse: "A Matemática é a Rainha das ciências e a Teoria dos Números (Aritmética) é a Rainha da Matemática" [4, p. 435]. David M. Burton (1930-2016), que foi professor emérito de Matemática da University of New Hampshire, escreveu: "Para aqueles que, como Gauss, consideram a Teoria dos Números a 'Rainha da Matemática', a Lei de Reciprocidade Quadrática é uma das joias em sua coroa" [2, p. 167]. Neste artigo, nosso interesse é apresentar outros assuntos relacionados à Teoria dos Números que auxiliem no ensino e aprendizagem de Matemática na Educação Básica.

2. Teorema de Pitágoras e os triplos pitagóricos

O Teorema de Pitágoras é apresentado aos alunos do Ensino Fundamental. Para o aprendizado desse conteúdo, é exigida dos alunos a habilidade, descrita na Base Nacional Comum Curricular (BNCC) [3], de resolver e de elaborar problemas de aplicação desse teorema [3, p. 271], postulando que a soma dos quadrados dos catetos a e b de um triângulo retângulo é igual ao quadrado da hipotenusa c. Em símbolos (Figura 1):

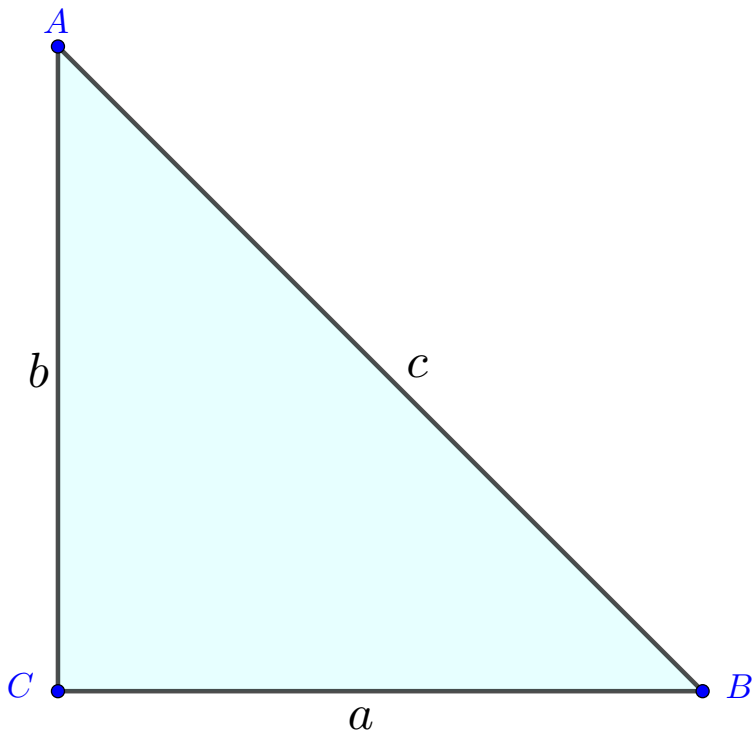


Figura 1: Para o triângulo retângulo de catetos a, b e hipotenusa c, vale a relação $a^2 + b^2 = c^2$.

Uma vez que estamos interessados em promover um encontro entre a Álgebra, Geometria e a Aritmética (Teoria dos Números), iremos nos concentrar principalmente nos triângulos pitagóricos, que são triângulos retângulos cujos lados (a, b, c) são números inteiros positivos (naturais), chamados de triplos pitagóricos [9], cujo estudo começou muito antes da época de Pitágoras. Existem tabuinhas babilônicas que contêm lista desses triplos, incluindo alguns bem grandes, indicando que os babilônios provavelmente tinham um método sistemático para produzi-las [15]. Ainda mais surpreendente é o fato de que os babilônios podem ter usado suas listas de triplos pitagóricos como tabelas trigonométricas primitivas [16]. Os triplos pitagóricos também eram usados no antigo Egito [7].

Estudos arqueológicos demonstraram que os babilônios e egípcios tinham razões práticas para estudar os triplos pitagóricos. Essas razões ainda existem? Provavelmente não. No entanto, há pelo menos uma boa razão para estudar os triplos pitagóricos na Escola Básica, e é a mesma pela qual vale a pena estudar a arte de Rembrandt e a música de Beethoven. Há beleza e complexidade nas maneiras como os números interagem entre si, assim como há beleza e complexidade na composição de uma pintura ou sinfonia. Para apreciar essa beleza, é preciso estar disposto a despender uma certa quantidade de energia mental, porque o resultado na formação de quem está na escola para sua vida futura vale bem o esforço. Assim, neste artigo, as situações apresentadas procuram motivar o leitor a apreciar algumas verdadeiramente belas, refletir como acontece a interação entre diversas manifestações, como é o caso aqui da Aritmética, Álgebra e Geometria, e, principalmente,

incentivar um processo de ensino e aprendizagem que considere conexões entre essas áreas da Matemática.

Uma das belezas da Aritmética é que ela usa muitas vezes suas ferramentas mais básicas, como a fatoração, paritismo, fator comum e divisibilidade, para nos provar grandes resultados. Uma vez que não nos prenderemos necessariamente a uma apresentação matemática abstrata ou axiomática, usaremos alguns conceitos da Teoria dos Números sem o rigor de um texto matemático sobre o assunto.

Vamos começar com uma pergunta típica em Teoria dos Números: existem infinitos triplos pitagóricos, ou seja, triplos de números naturais (a, b, c) satisfazendo a equação $a^2 + b^2 = c^2$? Esse questionamento é de fato positivo, por uma razão não muito difícil. Para mostrar que é assim, basta tomarmos um triplo pitagórico (a, b, c) e multiplicar por algum outro número k: obteremos um novo triplo pitagórico (ka, kb, kc). Isso é verdade porque,

$$(ka)^2 + (kb)^2 = k^2(a^2 + b^2) = k^2c^2 = (kc)^2$$

Esses novos triplos pitagóricos não serão o foco deste artigo. Nossa atenção será em triplos pitagóricos sem fatores comuns, os chamados triplos pitagóricos primitivos.

Definição 1. Um triplo pitagórico primitivo (TPP) é um triplo de números naturais (a, b, c), tal que a, b e c não têm fatores comuns, ou seja, MDC(a, b, c) = 1, e satisfaz $a^2 + b^2 = c^2$.

Além dos dois triplos pitagóricos primitivos mais comuns $(3, 4, 5)$ e $(5, 12, 13)$, incluímos uma pequena lista com outros na Tabela 1

a	**b**	**c**
7	24	25
8	15	17
9	40	41
11	60	61
12	35	37

Tabela 1: Triplos pitágoricos.

Algumas questões podem ser observadas na Tabela 1. Por exemplo, o fato de que quando a é par, b é ímpar e vice-versa, isto é, a e b têm paritismo diferentes. Algo que pode ser conjecturado é que c é sempre ímpar. São questões interessantes para analisar mesmo em turmas do Ensino Fundamental, uma vez que não é difícil provar que essas conjecturas estão corretas. E o que é interessante é que, no meio da argumentação da prova, há outros fatos que precisam ser verificados, o que poderá enriquecer o debate em sala de aula.

Nesse sentido, no que segue, vamos explorar tal conjectura. Primeiro, se a e b fossem pares, então c também seria par. Isso significa que a, b e c teriam um fator comum múltiplo 2, portanto, o triplo pitagórico não seria primitivo. Em seguida, suponha que a e b fossem ímpares, o que implicaria que c teria que ser par. Isso diria que existem números naturais s, u e v tais que

$$a = 2s + 1, \quad b = 2u + 1, \quad c = 2v.$$

Podemos substituí-los na equação $a^2 + b^2 = c^2$, para obter

$$(2s + 1)^2 + (2u + 1)^2 = (2v)^2,$$

$$4s^2 + 4s + 4u^2 + 4u + 2 = 4v^2.$$

Dividindo por 2,

$$2s^2 + 2s + 2u^2 + 2u + 1 = 2v^2.$$

Essa última equação diz que um número ímpar é igual a um número par, o que é impossível; então a e b não podem ser ímpares. Como acabamos de verificar que eles não podem ter a mesma paridade, então é verdade que um é par e o outro é ímpar, isso significa ter paridade diferente. Logo, pela equação $a^2 + b^2 = c^2$ temos que c é ímpar.

Sempre podemos trocar o paritismo de a e b numa demonstração conforme nossa argumentação, sem com isso perder a generalização. Nosso problema agora é encontrar todas as soluções em naturais para a equação

$$a^2 + b^2 = c^2$$

com a par (ou ímpar), b ímpar (ou par) e a, b, c sem fatores comuns.

Nossa primeira observação é que se (a, b, c) é um triplo pitagórico primitivo, então podemos fatorar

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

Observe pela Tabela 2 que sempre que consideramos a como ímpar e b como par, parece que $(c-b)$ e $(c + b)$ são sempre quadrados:

a	b	c	$a^2 = c^2 - b^2$	(c - b)(c + b)
3	4	5	$3^2 = 5^2 - 4^2$	1 . 9
5	12	13	$5^2 = 13^2 - 12^2$	1 . 25
7	24	25	$7^2 = 25^2 - 24^2$	1 . 49
15	8	17	$15^2 = 17^2 - 8^2$	9 . 25

Tabela 2: Triplos pitagóricos primitivos e fatorações.

Logo, precisamos provar que (c - b)(c + b) são quadrados. Outro fato que tende a ser aparente, observando a Tabela 2 acima, é que (c - b)(c + b) parecem não ter fatores comuns. Vamos provar agora essa última afirmação.

Suponha que d seja um fator comum de (c - b)(c + b); ou seja, d divide (c - b) e (c + b). Então d também divide

$$(c - b) + (c + b) = 2c \text{ e } (c + b) - (c - b) = 2b.$$

Assim, d divide 2b e 2c. Mas b e c não têm fatores comuns porque estamos assumindo que (a, b, c) é um triplo pitagórico primitivo. Portanto, d deve ser igual a 1 ou 2. Mas d também divide $(c - b)(c + b) = a^2$, e a pode ser ímpar, então d teria que ser sempre 1, para evitar contradições.

Em outras palavras, o único número que divide sempre (c - b) e (c + b) é 1, então (c - b) e (c + b) não têm fatores comuns.

Agora sabemos que (c - b) e (c + b) são inteiros positivos sem fatores comuns. O seu produto é um quadrado, pois $(c-b)(c+b) = a^2$. A única maneira disso acontecer é se (c - b) e (c + b) forem, eles próprios, quadrados.

Assumindo agora, sem perda de generalidade, que a é par e que b é ímpar, vamos escrever $a = 2t$ e colocar isso na equação $a^2 + b^2 = c^2$, obtendo,

$$(2t)^2 + b^2 = c^2.$$

e assim

$$(2t)^2 = c^2 - b^2 = (c+b)(c-b),$$

que podemos reescrever como

$$t^2 = \frac{(c+b)}{2} \cdot \frac{(c-b)}{2} \tag{1}$$

Note que como b e c são ambos ímpares, sua soma e diferença são ambas pares; consequentemente, cada um dos fatores na equação (1) é um inteiro, e esses inteiros são relativamente primos. Caso tivessem um fator comum, então a soma $\frac{(c+b)}{2} + \frac{(c-b)}{2} = c$ e a diferença $\frac{(c+b)}{2} - \frac{(c-b)}{2} = b$. E em vista da equação $a^2 + b^2 = c^2$, esse fator comum também seria compartilhado por a, ao contrário da suposição de que (a, b, c) é primitivo.

Agora, uma vez que o lado esquerdo da equação anterior é um quadrado perfeito, o mesmo ocorre com o lado direito, e os dois fatores do lado direito são relativamente primos. Os primos na fatoração de $(c-b)$ serão distintos dos primos na fatoração de $(c+b)$. Essas fatorações em primos devem incluir em cada fator um número igual de vezes; ou seja, cada um dos fatores do lado direito é em si um quadrado perfeito. Então vamos escrever duas equações

$$\frac{c+b}{2} = m^2, \frac{c-b}{2} = n^2 \tag{2}$$

onde m e n são relativamente primos, e $m > n$. Adicionando e subtraindo equações às duas equações acima, obtemos $c = m^2 + n^2$ e $b = m^2 - n^2$; e como b e c são ímpares, qualquer uma dessas últimas equações mostram que m e n têm paritismo diferentes. Finalmente, substituindo as equações (2) na equação (1), ficamos com $t^2 = m^2n^2$, a partir do qual $t = mn$ e, portanto, $a = 2mn$.

Assim, podemos afirmar, obviamente não com tanto rigor quanto necessário, que temos uma prova para o seguinte teorema [19, 11]:

Teorema 1. *Para um triângulo pitagórico com catetos a, b e hipotenusa c, qualquer triplo pitagórico primitivo pode ser escrito como*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Onde m e n são dois inteiros positivos quaisquer, $m > n$, m *e* n *são relativamente primos e com paridades diferentes.*

Nosso comentário a respeito do "rigor" vem do fato de termos assumido que existe uma única decomposição em fatores primos para cada número natural. De modo nenhum essa é uma afirmação óbvia. Uma sugestão de como apresentar uma ideia desse assunto a nível de escola básica, poderia ser como segue.

Pedir para os alunos considerarem em uma realidade, com uma outra aritmética, onde os únicos números que são conhecidos são os números pares. Então, neste mundo, os únicos números que existem são

$$\rho = \{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, ...\}.$$

Observe que nessa realidade podemos adicionar, subtrair e multiplicar números como de costume, já que a soma, a diferença e o produto de números pares são novamente números pares. Também podemos falar sobre divisibilidade. Podemos dizer que um número m divide um número n se houver um número k com n = mk. Mas lembre-se que estamos agora nessa nova realidade, então a palavra "número" significa um número que pertence a ρ. Por exemplo, 6 divide 12, uma vez que $12 = 6 \times 2$; mas 6 não divide 18, uma vez que não há um número k em ρ satisfazendo 18 = 6k.

Podem-se definir números primos nessa nova situação. Diremos que um número p é primo se não for divisível por qualquer número em ρ. Observe que, nessa realidade, um número não é divisível por si mesmo. Assim, temos alguns primos:

$$2, 6, 10, 14, 18, 22, 26, 30.$$

Em nossa aritmética, prova-se que se um número primo divide um produto ab, então ele divide a ou divide b [17, p. 109]. Agora voltemos à nova situação em que colocamos os alunos e consideremos o primo 6 e os números r = 10es = 18. O número 6 divide r.s = 180, uma vez que $180 = 10 \times 18$; mas 6 não divide nem o 10 nem o 18. Então, uma verdade em nossa aritmética, não é verdade nessa nova aritmética.

Consideremos agora o fato de que cada número pode ser fatorado como um produto de primos exatamente de uma maneira, a menos da ordem dos fatores. Uma atividade pode consistir nos alunos mostrarem que nessa aritmética cada número pode ser escrito como um produto de primos. Mas consideremos as seguintes fatorações:

$$180 = 6 \times 30 = 10 \times 18.$$

Os alunos poder ver que todos os números 6, 30, 10 e 18 são primos. Isso significa que 180 pode ser escrito como um produto de primos de duas maneiras diferentes. Os alunos podem verificar se há mais maneiras de escrevê-lo como um produto de primos. Situações como essa, permitem que o professor inicie um debate matemático, mesmo que o rigor e as demonstrações ainda não sejam possíveis.

Trabalhar com Números Primos já é ter acesso a uma gema com complexidade, preciosidade e beleza muito especiais. A seguir, vamos apresentar outro fato em que a Álgebra e a Geometria estão conectadas.

2.1. A fórmula de Heron

A partir da conhecida fórmula para o cálculo da área do triângulo, é possível deduzir algebricamente uma fórmula que nos fornece a área de um triângulo, a partir dos seus elementos mais básicos,

a medida de seus lados. Essa fórmula é atribuída a Heron (ou Herão) de Alexandria (10 d.C.-80 d.C.), e garante-nos que, em um triângulo qualquer, a área é dada por $A = \sqrt{(s(s-a)(s-b)(s-c))}$, sendo a, b, c as medidas dos lados e $s = \frac{(a+b+c)}{2}$ o semiperímetro do triângulo ilustrado na Figura 2.

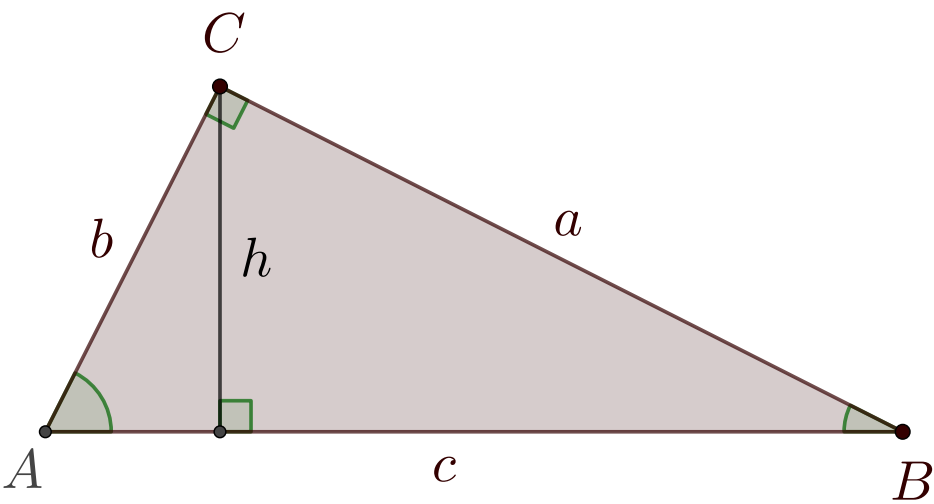


Figura 2: Triângulo de lados a, b, c e altura h.

Assim, para os propósitos da nossa demonstração,

$$2s = a + b + c, \qquad 2(s-a) = -a + b + c,$$
$$2(s-b) = a - b + c, \qquad 2(s-c) = a + b - c.$$

Há pelo menos um lado do triângulo dado, cuja altura está "dentro" do triângulo. Por conveniência, seja esse lado o de medida c. Informamos que não fará nenhuma diferença: tal escolha apenas dá um referencial para nossa argumentação [14].

Nossa tarefa é expressar h em termos de a, b e c, substituí-lo em $A = \frac{1}{2}ch$ (Figura 3).

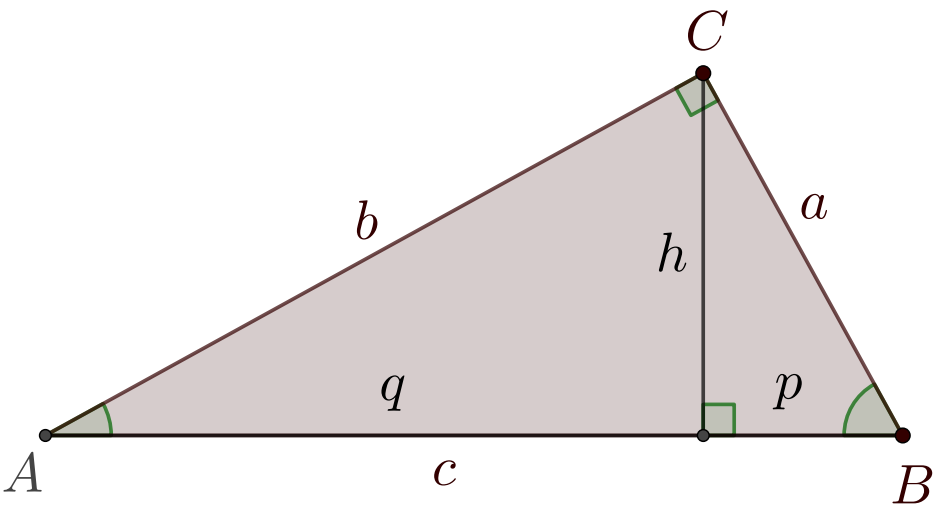


Figura 3: Triângulos retângulos de lados a, p, h e b, q, h.

Seja $p + q = c$ como indicado. Então,

$$h^2 + p^2 = a^2 \text{ e } h^2 + q^2 = b^2$$

Uma vez que $q = c - p$, então $q^2 = (c - p)^2 \iff q^2 = c^2 - 2cp + p^2$. Adicionando h^2 a ambos os lados da igualdade, temos $h^2 + q^2 = h^2 + p^2 - 2cp + c^2$.

Agora, substituindo, nessa equação, os valores correspondentes, temos $b^2 = a^2 - 2cp + c^2$, e resolvendo em p, obtemos

$$p = \frac{a^2 + c^2 - b^2}{2c}$$

Uma vez que $h^2 = a^2 - p^2 = (a + p)(a - p)$, teremos:

$$h^2 = \left[a + \frac{(a^2 + c^2 - b^2)}{2c}\right]\left[a - \frac{(a^2 + c^2 - b^2)}{2c}\right]$$

$$= \frac{(2ac + a^2 + c^2 - b^2)(2ac - a^2 - c^2 - b^2)}{4c^2}$$

$$= \frac{(a + c)^2 - b^2)(b^2 - (a - c)^2)}{4c^2}$$

$$= \frac{(a + b + c)(a + c - b)(b + a - c)(b - a + c)}{(4c^2)}$$

$$= \frac{(a+b+c)(-a+b+c)(a-b+c)(a+b-c)}{4c^2}$$

$$= \frac{(2s.2(s-a).2(s-b).2(s-c))}{(4c^2)}.$$

Logo,

$$h^2 = \frac{4s(s-a)(s-b)(s-c)}{c^2}$$

$$h = \frac{2\sqrt{s(s-a)(s-b)(s-c)}}{c}.$$

E uma vez que

$$A = \frac{1}{2}ch,$$

então,

$$A = \frac{1}{2}c\left(\frac{2\sqrt{s(s-a)(s-b)(s-c)}}{c}\right),$$

e

$$A = \sqrt{s(s-a)(s-b)(s-c)}.$$

Na seção a seguir, apresentaremos mais algumas conexões entre Álgebra, Geometria e Aritmética.

3. Interações matemáticas e a sala de aula

Na Teoria dos Números, há importantes fatos sobre os triângulos pitagóricos, como o inraio e o incírculo [2, p. 248]. Ao apresentar uma prova, em nível elementar, de que o inraio de um triângulo pitagórico é um número inteiro, pode-se refletir de que forma os assuntos que têm relação com o conjunto dos números inteiros estão distribuídos ao longo da Educação Básica, considerando um planejamento que envolva uma geometria com números inteiros.

Ao se estudar os triângulos pitagóricos na Escola Básica, é dada uma grande atenção aos lados do triângulo. Mas o que pode ser dito sobre os ângulos de um triângulo pitagórico? O professor desse nível de ensino pode surpreender e motivar seus alunos ao mostrar que o estudo do incírculo leva a um resultado fundamental sobre esses ângulos, e que o incírculo dá um significado geométrico simples para os fatores que ocorrem no radical na fórmula de Heron.

Desafiar os alunos a encontrar triângulos não retângulos com lados inteiros e inraios inteiros seria uma excelente atividade envolvendo grupos de alunos e o uso da calculadora. Uma possibilidade é começar com quaisquer dois triângulos pitagóricos e, em seguida, criar um triângulo a partir de ampliações e uniões dos dois originais.

A seguir, apresentamos o que consideramos acima e concluímos com mais um fato que pode ser interessante para os alunos da Escola Básica: como dois triângulos pitagóricos estão relacionados pelo incentro.

a	b	c	r
3	4	5	1
5	12	13	2
7	24	25	3
9	40	41	4

Tabela 3: Medidas dos inraios.

3.1. O inraio do incírculo

O incírculo de um triângulo é um círculo inscrito neste triângulo. A Figura 4 ilustra o incírculo de um triângulo pitagórico e o seu raio (inraio). O centro I do incírculo (incentro) é o ponto de encontro das bissetrizes dos ângulos do triângulo. Neste artigo, discutimos vários fatos incomuns sobre triângulos pitagóricos relacionados a propriedades do inraio

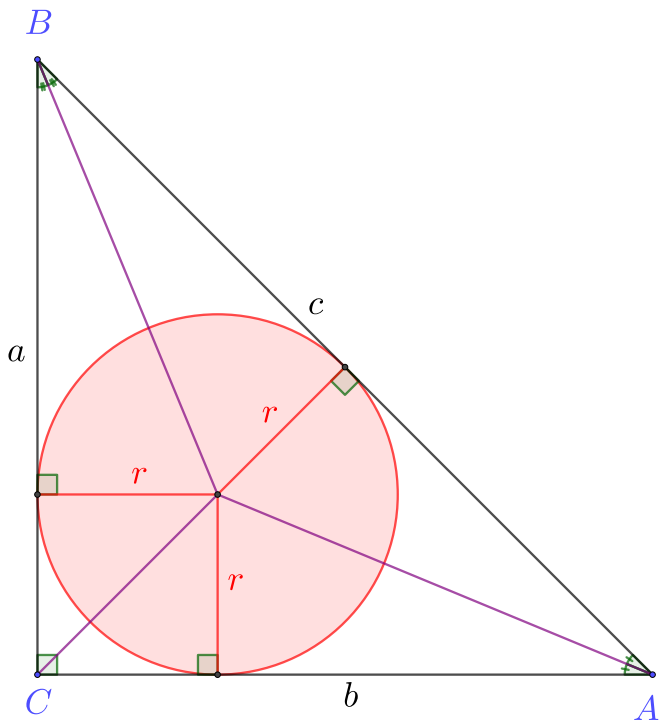


Figura 4: Incírculo em um triângulo retângulo.

O inraio r, do incírculo de um triângulo pitagórico, é um número inteiro [5, p. 11]. Por exemplo, o inraio do triângulo (3, 4, 5) é igual a 1 e o inraio do triângulo $(5, 12, 13)$ é igual a 2 e outros valores são mostrados na Tabela 3. Agora, iremos apresentar uma prova a nível elementar, de que o inraio em um triângulo pitagórico é um número inteiro. Começamos com um teorema sobre

o inraio do incírculo em qualquer triângulo [1].

Teorema 2. *Sejam* a, b *e* c *os lados de um triângulo. Seja* A, *a área do triângulo e* $s = \frac{(a+b+c)}{2}$ *é o semiperímetro. Então, o inraio* r *do incírculo (Figura 5) é dado por*

$$r = \frac{A}{s} \quad e \quad r = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}}$$

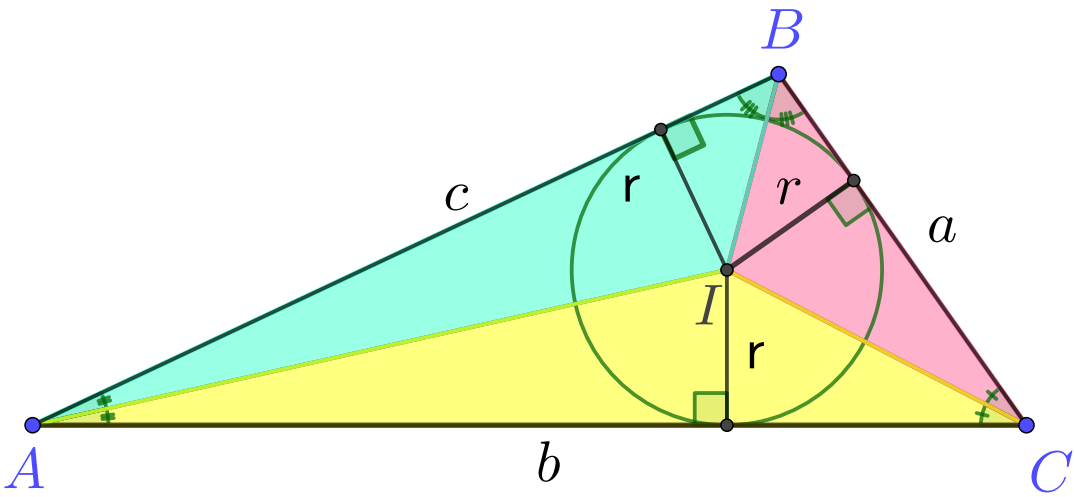


Figura 5: Inraio do incírculo em qualquer triângulo.

Demonstração. A área A do triângulo ABC é igual à soma das áreas dos três triângulos interiores AIB, AIC e BIC formado pelas bissetrizes internas. Esta soma é

$$A = \frac{1}{2}ra + \frac{1}{2}rb + \frac{1}{2}rc = \frac{1}{2}r(a+b+c) = rs$$

Logo, $r = \frac{A}{s}$.

De acordo com a fórmula de Heron, $A = \sqrt{s(s-a)(s-b)(s-c)}$. Então,

$$\sqrt{s(s-a)(s-b)(s-c)} = rs$$

$$r^2s^2 = s(s-a)(s-b)(s-c)$$

Assim, $r = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}}$, o que conclui a prova

□

A seguir, queremos determinar o inraio em um triângulo pitagórico. Apresentamos duas demonstrações acessíveis e que podem servir para incentivar provas e demonstrações na Escola Básica [14].

Teorema 3. *Seja ABC um triângulo pitagórico com catetos a, b e hipotenusa c e o incírculo com incentro I neste triângulo. Então, o inraior é um inteiro dado por* $r = n(m-n)$.

Demonstração. Sejar o inraio do incírculo no triângulo pitagórico ABC como na Figura 6.

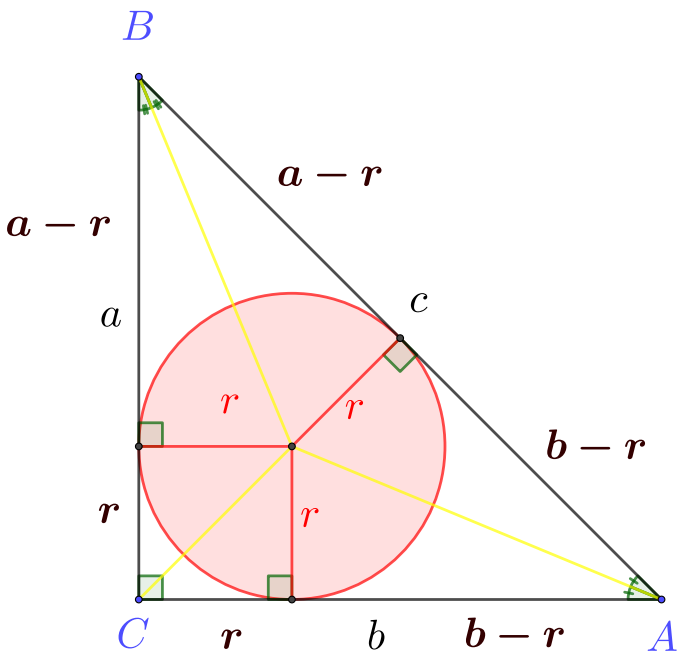


Figura 6: Triângulo pitagórico com catetos a, b e hipotenusa c e o incírculo com incentro I.

Assim,

$$c = (a-r) + (b-r) = a + b - 2r \iff r = \frac{a+b-c}{2}$$

Como o triângulo é pitagórico,

$$r = \frac{(m^2 - n^2 + 2mn - m^2 - n^2)}{2} = \frac{(2mn - 2n^2)}{2} = n(m-n).$$

Logo,r é um inteiro dado por $r = n(m-n)$. □

Demonstração. Na Figura 7, A área A do triângulo ABC é igual à soma das áreas dos três triângulos interiores AIB, AIC e BIC formado pelas bissetrizes internas.

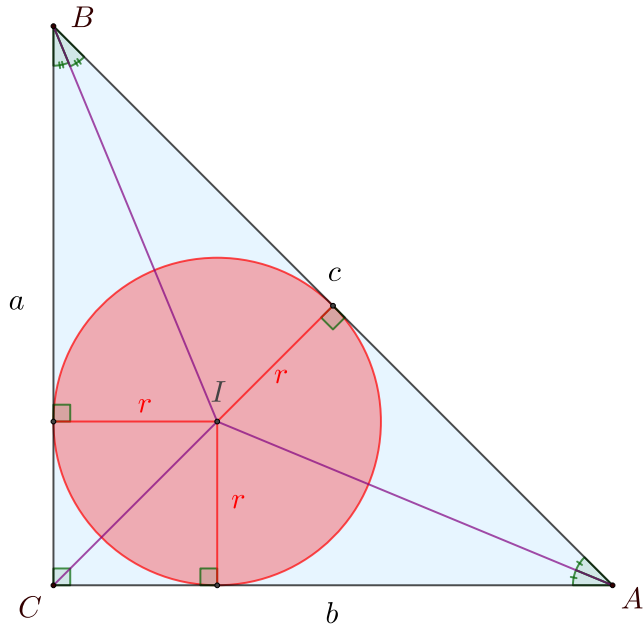


Figura 7: Três triângulos interiores AIB, AIC e BIC.

Então, A = Área AIB+ Área AIC+ ÁreaBIC.

$$\frac{1}{2}ab = \frac{1}{2}rc + \frac{1}{2}ra + \frac{1}{2}rb$$

e,

$$r = \frac{ab}{a+b+c} = \frac{(m^2-n^2)2mn}{(m^2-n^2+2mn+m^2+n^2)} = \frac{[2mn(m-n)(m+n)]}{[2m(m+n)]} = n(m-n)$$

Logo, r é um inteiro dado por $r = n(m-n)$. □

A seguir, uma interação entre Aritmética, Álgebra e Trigonometria. Depois de analisar nossos apontamentos, pretendemos que a apresentação evidencie a validade a interação para a educação do pensamento matemático nas escolas, e a trigonometria é o ramo da Matemática que permite essa interação.

3.2. Conexão com a trigonometria

Nesta subseção, mostraremos que os ângulos formados pelas bissetrizes dos triângulos pitagóricos satisfazem algumas relações interessantes. A Figura 8 ilustra os detalhes de vários segmentos no triângulo pitagórico relacionados ao incentro [13]. As medidas desses segmentos podem ser deduzidas através dos casos de semelhança de triângulos e com o fato de o inraio ser $r = n(m-n)$.

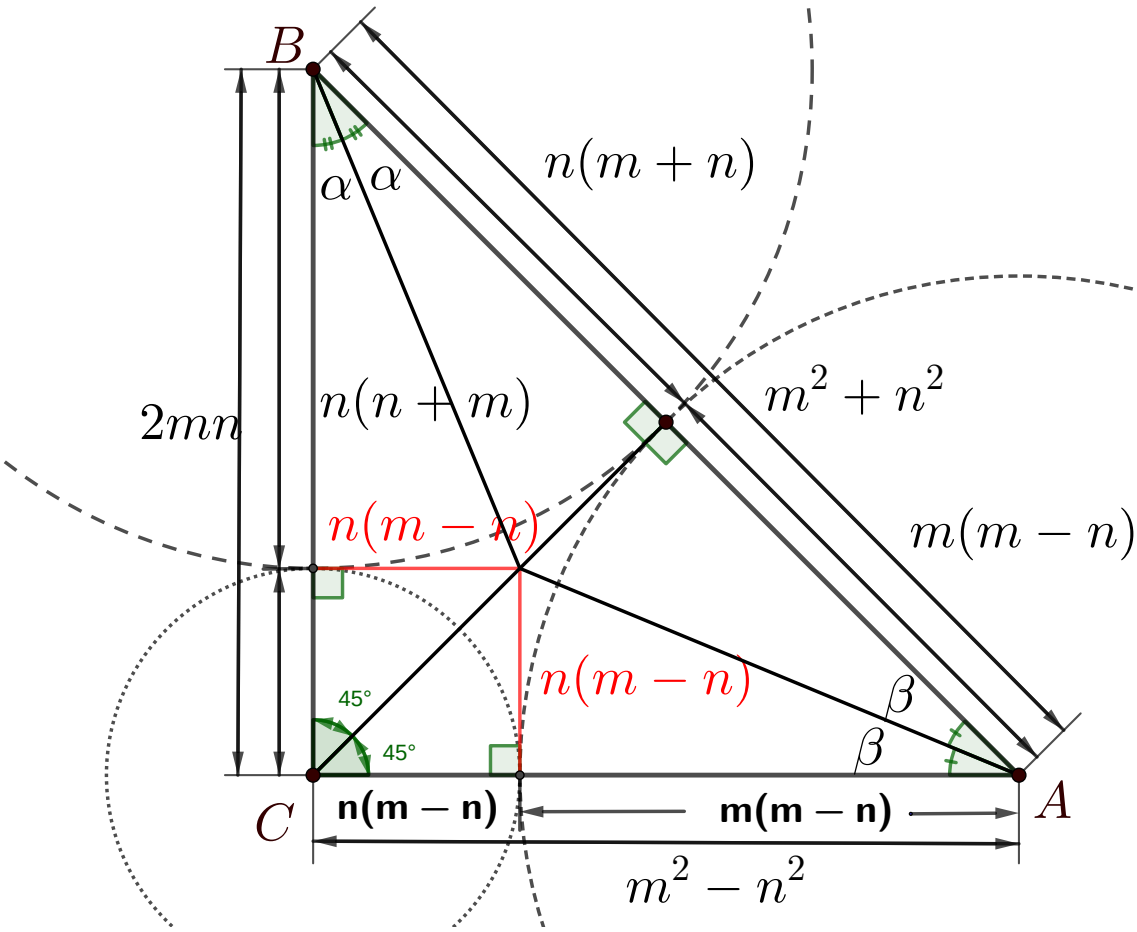


Figura 8: Bissetrizes do triângulo pitagórico.

Do triângulo pitagórico de lados $a = m^2 - n^2$, $b=2mn$ e $c = m^2 + n^2$, obtemos as seguintes relações trigonométricas:

$$\operatorname{tg} 2\alpha = \frac{m^2 - n^2}{2mn} \iff 2\alpha = \operatorname{tg}^{-1}\left(\frac{m^2 - n^2}{2mm}\right)$$

e

$$\operatorname{tg} 2\beta = \frac{2mn}{m^2 - n^2} \iff 2\beta = \operatorname{tg}^{-1}\left(\frac{2mn}{m^2 - n^2}\right)$$

temos

$$\operatorname{tg} \alpha = \frac{m - n}{m + n} \iff \alpha = \operatorname{tg}^{-1}\left(\frac{m - n}{m + n}\right)$$

e

$$\operatorname{tg} \beta = \frac{n}{m} \iff \beta = \operatorname{tg}^{-1}\left(\frac{n}{m}\right)$$

Notemos que os arco-tangentes dos ângulos 2α e 2β são funções racionais quadráticas de m e n, enquanto os arco-tangentes correspondentes às metades α e β são expressões racionais lineares

mais simples. Em particular, a relação entre os triplos pitagóricos e essas expressões fornece de imediato o seguinte teorema:

Teorema 4. *Seja* $\frac{n}{m}$ *qualquer número racional positivo tal que* $\frac{n}{m} < 1$. *Existe um triângulo pitagórico com um ângulo agudo tal que a tangente da metade desse ângulo é igual a* $\frac{n}{m}$.

Vejamos outro fato que surge desse encontro entre Teoria dos Números, Geometria, Álgebra e Trigonometria.

Uma vez que $2\alpha + 2\beta = \frac{\pi}{2}$, então $\alpha + \beta = \frac{\pi}{4}$. Substituindo os valores de α e β pelos arco-tangentes, temos:

$$\mathrm{tg}^{-1}\left(\frac{m-n}{m+n}\right) + \mathrm{tg}^{-1}\left(\frac{n}{m}\right) = \frac{\pi}{4}$$

Essa relação trigonométrica tem consequências. Se fizermos $m = 1$ e $n = 2$, temos o retângulo pitagórico $(3, 4, 5)$, e a relação fica

$$\mathrm{tg}^{-1}\left(\frac{1}{2}\right) + \mathrm{tg}^{-1}\left(\frac{1}{3}\right) = \frac{\pi}{4}.$$

É um fato em que, sempre que há interações entre os diferentes ramos da Matemática, grandes resultados são obtidos [8].

A seguir vamos voltar à fórmula de Heron.

3.3. Os fatores na fórmula de Heron

Foi provado anteriormente que a fórmula de Heron para a área de um triângulo com os lados a, b. c em termos do semiperímetro s é dada por:

$$A = \sqrt{s(s-a)(s-b)(s-c)}.$$

Nesta subseção, mostramos o significado geométrico dos fatores no radical que às vezes parecem estranhos a alguns estudantes. A prova original de Heron usa um argumento geométrico complexo que começa com a construção do incírculo, como pode ser visto em [6]. A seguir, analisaremos a importância dos fatores que aparecem sob o radical [1].

Seja o triângulo ABC ilustrado na Figura 9. Sejam P, Q e R os pontos onde o incírculo tangencia os lados do triângulo. Provaremos que os fatores na fórmula de Heron são dados por:

$$s - a = z = AP = AQ, \quad s - b = x = BP = BR, \quad s - c = y = CQ = CR$$

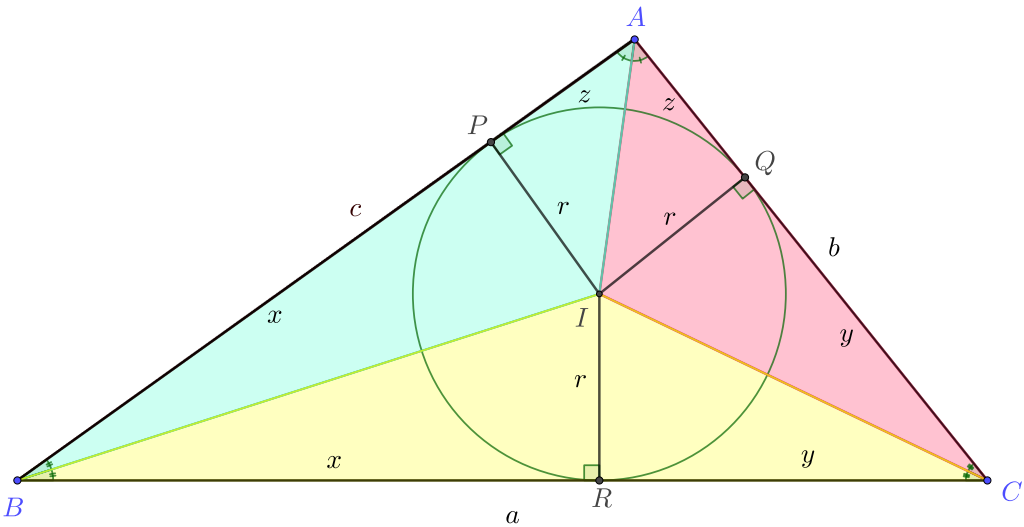


Figura 9: Pontos P, Q e R onde o incírculo tangencia os lados do triângulo.

Vemos que

$$\text{a} + \text{b} + \text{c} = 2\text{x} + 2\text{y} + 2\text{z} \text{ e como } \text{s} = \frac{(\text{a}+\text{b}+\text{c})}{2}, \text{ logo } 2\text{s} = \text{a} + \text{b} + \text{c} = 2\text{x} + 2\text{y} + 2\text{z},$$

e assim temos,

$$\text{s} = \text{x} + \text{y} + \text{z}.$$

Vemos imediatamente a partir da Figura 9 que

$$\text{a} = \text{x} + \text{y}, \quad \text{b} = \text{y} + \text{z}, \quad \text{c} = \text{x} + \text{z}.$$

Façamos s–a = z, s – b = x e s–c = y. Isso completa nossa prova.

Mostramos que o incírculo de um triângulo divide os lados do triângulo em segmentos que são os fatores que aparecem na fórmula de Heron.

Na subseção seguinte, comentaremos como encontrar triângulos não retângulos com lados inteiros e inraios inteiros.

3.4. Triângulos pseudopitagóricos

Em geral, um triângulo não pitagórico com lados inteiros terá um incírculo cujo raio provavelmente será irracional. No entanto, é fácil criar triângulos com lados inteiros com inraios inteiros que chamaremos de pseudopitagóricos, como mostraremos agora. Na Figura 10, começamos com dois triângulos pitagóricos: $(5, 12, 13)$ e $(3, 4, 5)$.

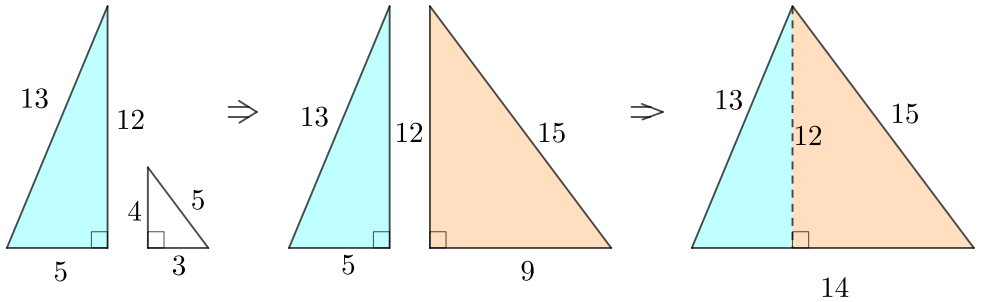


Figura 10: Triângulos pseudopitagóricos.

Então, ampliamos $(3, 4, 5)$ multiplicando cada lado por 3. Agora os dois lados verticais são 12, e assim os triângulos podem ser unidos para formar um novo triângulo não pitagórico com lados (13, 14, 15). Os triângulos pitagóricos sempre têm área inteira, porque um dos catetos é sempre um número par. Desse modo, o triângulo criado unindo dois triângulos pitagóricos deve ter área inteira. Pela Figura 11, vemos que a área é $A = \frac{12.14}{2} = 84$. O Teorema 1 afirma que o inraio r do incírculo para esse triângulo $(13, 14, 15)$ é dado por $r = \frac{A}{s} = \frac{84}{21} = 4$ (Ver Figura 11) .

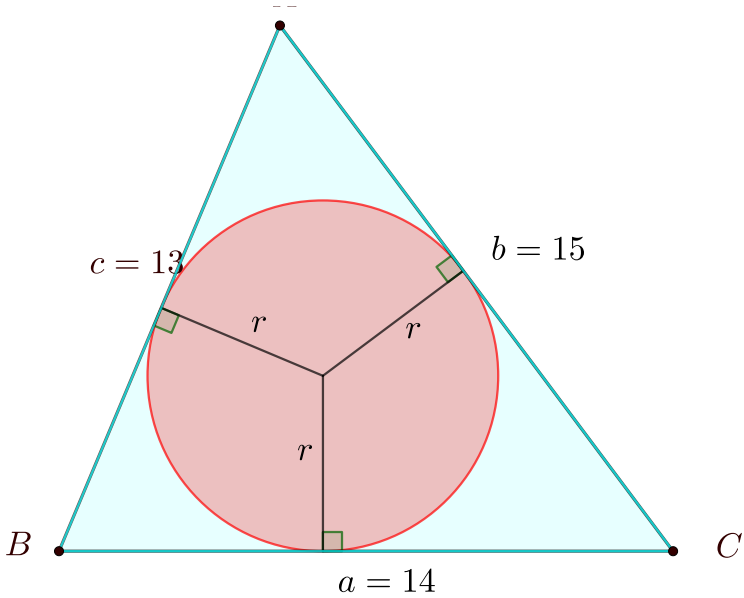


Figura 11: Inraio r do incírculo para o triângulo de lados $(13, 14, 15)$.

Podemos repetir o procedimento acima começando com quaisquer dois triângulos pitagóricos. Ao ampliar um (ou talvez ambos) os triângulos por um fator inteiro, os lados verticais tornam-se iguais e, portanto, podem ser unidos como acima. Este novo triângulo possui área inteira. O

inraio calculado a partir do Teorema 1 é, portanto, um inteiro ou um número racional. Se r for racional, todo o triângulo pode ser ampliado por um fator inteiro apropriado para que o novo inraio seja um inteiro.

Na última subseção, apresentamos uma construção muito singular. A partir do incentro de um triângulo pitagórico, podemos construir um novo triângulo pitagórico

3.5. Triângulos Pitagóricos unidos por um incentro

Um triângulo pitagórico de medidas (3, 4, 5) pode ser encontrado a partir de um triângulo pitagórico de medidas (7, 24, 25) como ilustra a Figura 12.

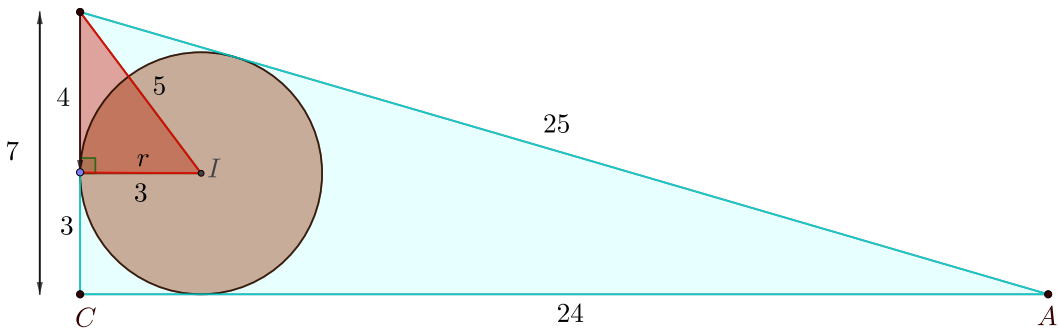


Figura 12: Triângulo pitagórico de medidas (3, 4, 5) a partir de um triângulo pitagórico de medidas (7, 24, 25).

Nesta subseção, generalizaremos tal fato ilustrado na Figura 12 acima [12]. Ou seja, em um triângulo pitagórico BAC, teremos um triângulo pitagórico interno BIQ como ilustrado na Figura 12. Para quais medidas do triângulo pitagórico maior BAC, o triângulo retângulo menor BIQ também é pitagórico?

Abaixo, temos um segundo exemplo (Figura 13), ilustrando a obtenção do triângulo pitagórico BIQ de medidas (35, 84, 91) a partir do triângulo pitagórico BAC de medidas (119, 120, 169).

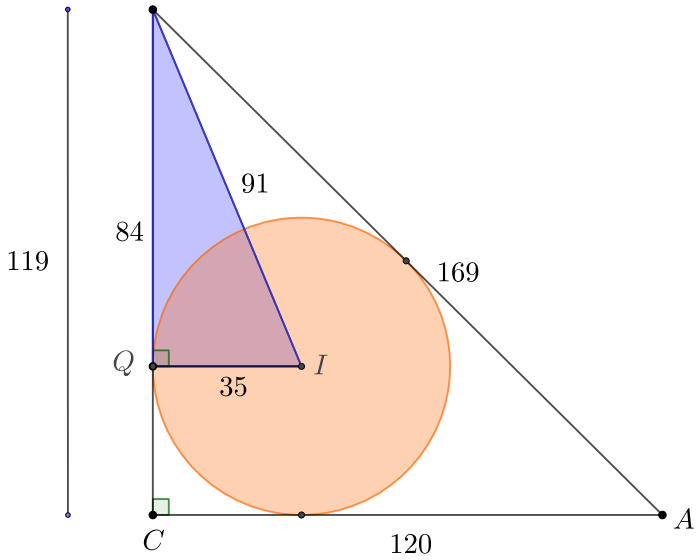


Figura 13: Triângulo pitagórico BIQ de medidas $(35, 84, 91)$ a partir do triângulo pitagórico BAC de medidas $(119, 120, 169)$.

Como o segmento que vai do vértice B até o incentro I é uma bissetriz, temos ângulos de θ e 2θ em B, respectivamente para os triângulos retângulos BIQ e BAC (Figura 14)

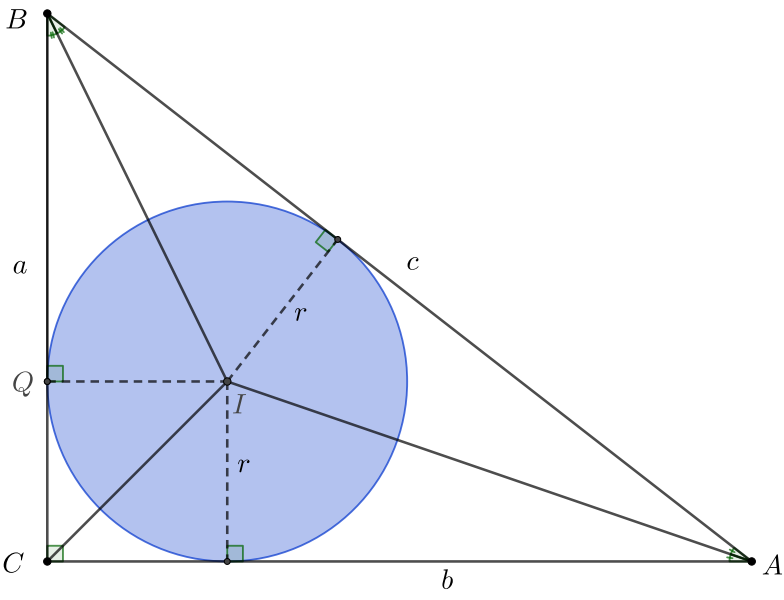


Figura 14: Triângulos retângulos BIQ e BAC.

Se o triângulo BIQ for pitagórico, temos

$$\operatorname{tg}\theta = \frac{m^2-n^2}{2mn} \text{ ou } \operatorname{tg}\theta = \frac{2mn}{m^2-n^2},$$

uma vez que apenas um deles é menor que 1, pois são recíprocos.

Usando a identidade $\operatorname{tg} 2\theta = \frac{2\operatorname{tg}\theta}{1-\operatorname{tg}^2\theta}$, temos:

$$\operatorname{tg} 2\theta = \frac{2\frac{(m^2-n^2)}{2mn}}{1-\left[\frac{(m^2-n^2)}{2mn}\right]^2} = \frac{4mn(m^2-n^2)}{(2mn)^2-(m^2-n^2)^2}$$

ou

$$\operatorname{tg} 2\theta = \frac{2\frac{2mn}{(m^2-n^2)}}{1-\left[\frac{2mn}{(m^2-n^2)}\right]^2} = \frac{4mn(m^2-n^2)}{(m^2-n^2)^2-(2mn)^2}$$

Como esses valores são simétricos, escolhemos o caso para o qual $\operatorname{tg} 2\theta > 0$ ou seja,

$0 < 2\theta < \frac{\pi}{2}$ dependendo se m^2-n^2 é menor ou maior que $2mn$.

Vamos mostrar que o numerador $4mn(m^2-n^2) = 4mn(m+n)(m-n)$ e o denominador $(m^2-n^2)^2-(2mn)^2 = (m^2-n^2+2mn)(m^2-n^2-2mn)$, são relativamente primos. O denominador é ímpar uma vez que m e n têm paridade diferente.

Suponha que um primo $p > 2$, divide $(m+n)$ no numerador e $(m^2-n^2)^2-(2mn)^2 = (m+n)^2(m-n)^2-(2mn)^2$ no denominador. Então p divide $(2mn)^2$, logo p divide m ou divide n. Mas, p divide $(m+n)$, o que implica p é um fator comum de m e n: contradição! Uma contradição semelhante acontece, para garantir que qualquer fator primo ímpar de $(m-n)$ não pode dividir o denominador [17].

Em seguida, se um primo $p > 2$ divide m no numerador e $\pm(m^2-n^2)^2 \pm (2mn)^2$ no denominador, então m divide n^4 implicando que p divide m e n: contradição! Uma contradição semelhante pode ser usada para mostrar que qualquer fator primo ímpar de $(m-n)$ não pode dividir o denominador. Concluímos que o numerador e o denominador não têm fatores comuns.

A partir desses valores de $\operatorname{tg} 2\theta$, o numerador e denominador (possivelmente, vezes um múltiplo comum) correspondem diretamente às medidas dos catetos para o triângulo exterior BAC e a hipotenusa é dada por

$$\{[4mn(m^2-n^2)]^2+[(m^2-n^2)^2]^2\}^{\frac{1}{2}} = (m^2+n^2)^2.$$

Portanto, as medidas, em módulo, do triângulo maior BAC, correspondem ao seguinte triplo pitagórico:

$$(k[4mn(m^2-n^2)], k[(m^2-n^2)^2-(2mn)^2], k(m^2+n^2)^2)$$

Temos o interessante fato de que a hipotenusa do triângulo maior é sempre um múltiplo de um quadrado perfeito.

Como um cateto do triângulo menor BIQ é o inraio, ele é dado por

$$\frac{a+b-c}{2} = \frac{k[4mn(m^2-n^2)-8(mn)^2]}{2} = 2kmn(m^2-n^2-2mn)$$

Assim, as três medidas, em módulo, do triângulo menor BIQ são:

$$(k(m^2 - n^2)(m^2 - n^2 - 2mn), 2kmn(m^2 - n^2 - 2mn), k(m^2 + n^2)(m^2 - n^2 - 2mn))$$

A Figura 15 ilustra o caso geral.

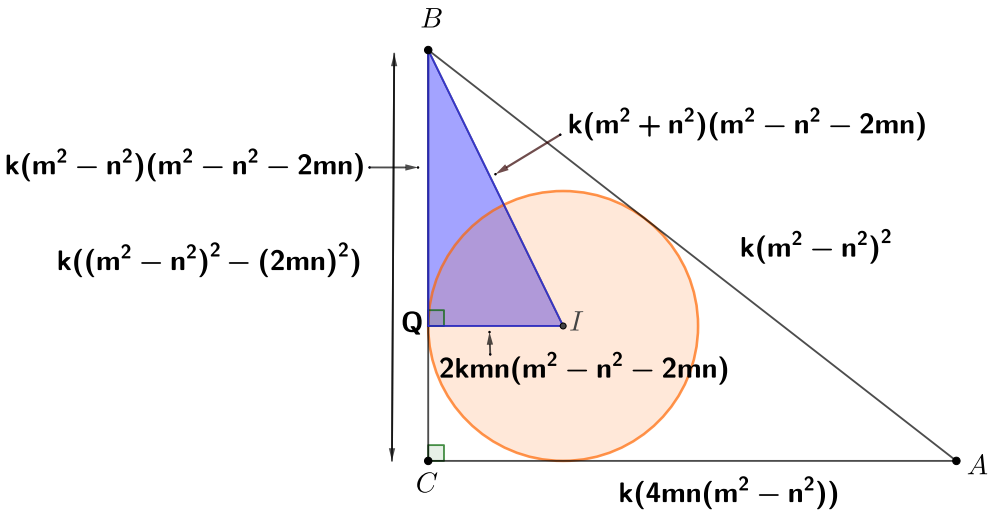


Figura 15: Caso geral de triângulos pitagóricos unidos por um incentro.

A Figura 15, acima, corresponde a $m = 2, n = 1, k = 1$, enquanto a Figura 14 corresponde a $m = 3, n = 2, k = 1$. A próxima construção mais simples seria $m = 4, n = 1, k = 1$, conduzindo ao triplo $(56, 105, 119)$ para o triângulo menor e ao triplo $(161, 240, 289)$ para o triângulo maior, como ilustra a Figura 16.

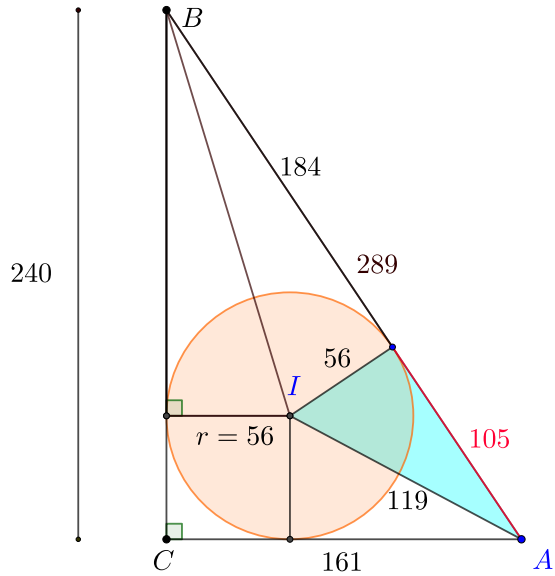


Figura 16: Caso particular de triângulos pitagóricos $(161, 240, 289)$ e $(56, 105, 119)$.

Conforme expusemos nas considerações iniciais, os cinco itens discutidos nesta seção procuram provocar uma reflexão sobre a necessidade de se buscar conteúdos em termos de Escola Básica que permitam uma interação entre a Aritmética, Álgebra e Geometria. E mais exploração do conteúdo do Conjunto dos Números Inteiros em todos os anos dos ensinos fundamental e médio.

4. Conclusão

De acordo com [18, p. 229], "As tarefas com teoria elementar dos números são uma área rica e acessível para aprimorar e sondar o sentido de criação matemática dos alunos". Por essa razão, a utilidade da Aritmética tem sido colocada como um argumento para o ensino e aprendizagem da Matemática. Além disso, para os alunos, a utilidade adicional no contato com conteúdos que envolvam o conjunto dos números inteiros reside no desenvolvimento da apreciação da beleza e do poder da Matemática. O poder e a utilidade no contato com a Teoria dos Números está em desenvolver a habilidade de "trabalhar como um matemático" – conjeturar e testar conjecturas.

O conjunto dos números inteiros positivos é bastante familiar e os problemas são de fácil compreensão (não implicando fácil solução). Usando esse conjunto familiar, o professor, por meio de um processo correto de orientação nas descobertas, pode instigar o genuíno benefício de aprender a pensar de forma independente. Ele deve instruir seus alunos a depender de seus próprios recursos, evitando a todo momento dar as soluções. Incentivar a descobrir que eles têm dentro de si o poder de criar ideias verdadeiramente importantes. Estes são benefícios da prática matemática que se estendem muito além da sala de aula, pois possibilita ao aluno desenvolver uma atitude de questionar e querer aprender respostas ativamente. Não se pode negar que é uma coisa boa em cada empreendimento humano, não apenas na resolução de problemas matemáticos.

Acreditamos que o desenvolvimento do pensamento matemático também se dá através das conexões feitas entre suas mais diversas áreas. Argumentos fracos e incompletos que defendem que a construção do conhecimento matemático só acontece se existir uma aplicabilidade imediata no cotidiano do aluno (empobrecimento da disciplina e utilitarismo pontual) ou através de uma significação dos conteúdos não se sustentam para os que entendem a essência do fazer matemático. É o mesmo tipo de ingenuidade ao se perguntar a um jovem por que ele gosta de jogar video game, se aquilo parece não ter nenhuma utilidade prática para ele...

A falta de motivação para a aprendizagem matemática dá-se pela falta de empatia com as heurísticas. O conhecimento matemático, quando construído através de belos desafios, como uma forma de arte, como um tipo de diversão, dando liberdade para os erros e sempre com respeito, fará todo o sentido para o estudante. Assim como faz ouvir uma música, assistir a um filme, ver a chuva, ler um poema ou ter a curiosidade de saber como os números se relacionam.

Referências

[1] ALTSHILLER-COURT, Nathan. *College Geometry: An Introduction to the Modern Geometry of the Triangle and the Circle*. 2007 (2nd ed.), New York: Barnes & Noble.

[2] BURTON, D. M. *Teoria Elementar dos Números*. 7ª ed. Rio de Janeiro: LTC, 2016.

[3] BRASIL. Ministério da Educação. *Base Nacional Comum Curricular*. Brasília, 2018.

[4] CANTOR, M. *Allgemeine Deutsche Biographie*. Bd. 8. Duncker & Humblot. 1878.

[5] COXETER, H. S. M; S. L. Greitzer. *Geometry Revisited*, New Mathematical Library 19, Mathematical Association of America, Washington, D.C., 1967.

[6] DUNHAM, W. *Journey Through Genius*, Wiley, New York, NY, 1990, pp. 118-127.

[7] LUMPKIN, Beatrice. "The egyptians and pythagorean triples". *Historia Matemathica* 7 (1980), p. 186-187.

[8] MAHONEY, M.S. *The mathematical career of Pierre de Fermat*. Princeton, NJ: Princeton University Press. 1994.

[9] MAOR, Eli. *The Pythagorean Theorem*, Princeton University Press, 2007: Appendix B.

[10] NOBRE, S. *Alguns "porquês" na História da Matemática e suas contribuições para a Educação Matemática*. Caderno Cedes – História e Educação Matemática, Campinas: Papirus, v. 40, p. 29-35, 1996.

[11] OGILVY, C. S; ANDERSON, J. T. *Excursions in Number Theory*. New York: Dover, p. 68, 1988.

[12] O'LOUGHLIN Michael. "Half angles and the inradius of a Pythagorean triangle". *The Mathematical Gazette*, Vol. 94, N° 529 (March 2010), pp. 144-146.

[13] PARRIS, Richard. "Commensurable Triangles". *College Mathematics Journal*. 38 (5): 345–355.2007. doi:10.1080/07468342.2007.11922259. S2CID 218549375

[14] POSAMENTIER, Alfred S. *Advanced Euclidean Geometry: Excursions for Secondary Teachers and Students*, Key College Publishing (Emeryville, CA), 2002.

[15] ROBSON, E. "Neither Sherlock Holmes nor Babylon: a reassessment of Plimpton 322". *Historia Mathematica*, 28, 167-206. 2001.

[16] ROBSON, E. "Words and pictures: New light on Plimpton 322". *The American Mathematical Monthly*, 109(2), 105-120. 2002.

[17] ROSEN, Kenneth H. *Elementary number Theory and its applications*, Addison-Wesley, 1984.

[18] SELDEN, A.; SELDEN, J. "Reflections on mathematics education research questions in elementary number theory". In Campbell, S. R. & Zazkis, R. (Eds.), *Learning and teaching number theory: Research in cognition and instruction* (pp. 213-230). Westport, CT: Ablex Publishing. 2002. p. 229.

[19] SIERPIŃSKI, Wacaw (2003), *Pythagorean Triangles*, Dover.

Rubens Vilhena Fonseca
Universidade do Estado do Pará - Uepa
<rubens.vilhena@uepa.br>

Ana Paula Sales Brito
Graduada em Matemática
<paulasales340@gmail.com>

Gabriel Dias de Pinho
Graduado em Matemática
<gabrieldias141197@gmail.com>

Yuri Albino Marigliani
Graduado em Matemática
<yurialbinomarigliani@gmail.com>

Richard Campos Vilhena Fonseca
Graduando em Física
<richardfonseca207@gmail.com>

Recebido: 21/07/2021
Publicado: 08/08/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1027

Grupos diedrais e simetrias da circunferência: uma abordagem geométrica

Alan de Araújo Guimarães Francisco Thiarly Alves de Souza

Resumo

Seja D_n o grupo diedral, ou seja, o grupo de simetrias de um polígono regular de n lados. Em vários livros de Álgebra Abstrata, o grupo D_n é tratado com enfoque puramente algébrico, sendo visto como um subgrupo do grupo simétrico S_n.

Neste artigo, propomos uma abordagem menos comum do grupo D_n: iremos estudá-lo do ponto de vista geométrico, interpretando-o como um subgrupo do grupo de isometrias do plano que fixam um polígono regular. Provaremos que as únicas simetrias de polígonos regulares são certas rotações e reflexões, além de composições dessas. Por fim, descreveremos o grupo de simetrias da circunferência.

Os resultados aqui apresentados pretendem destacar que certos conceitos da Teoria de Grupos têm sua gênese na Geometria, e podem ser ensinados dessa forma nas disciplinas de Álgebra em nível de Graduação, favorecendo a melhor compreensão dos conceitos por parte dos estudantes.

Este trabalho é fruto da pesquisa de Iniciação Científica do segundo autor sob orientação do primeiro autor.

Palavras-chave: isometrias; polígono regular; grupo diedral.

Abstract

Let D_n be the dihedral group, i. e., the group of symmetries of a regular polygon of n sides. In several Abstract Algebra books, the group D_n is treated with a purely algebraic approach, being seen as a subgroup of the symmetric group.

In this paper, we propose a less common approach of the group D_n: we will study it from the geometric point of view, interpreting it as a subgroup of the isometry group of the plane which fixes a regular polygon. We will prove that the only symmetries of regular polygons are certain rotations and reflections, as well as their composition. Finally, we will describe the group of symmetries of the circle.

The results presented here intend to highlight that certain concepts of Group Theory have their genesis in Geometry, and can be taught in this way in Algebra subjects at the undergraduate level, favoring a better understanding of the concepts by students.

This work is the result of the Scientific Initiation research of the second author under the guidance of the first author.

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

Keywords: isometries; regular polygon; dihedral group.

1. Introdução

Ao estudar o conceito de grupo durante um curso de Graduação, em geral, o estudante tem um primeiro contato com a noção de isometria/simetria de subconjuntos do plano. Nesse momento, o importante grupo diedral D_n é apresentado. O grupo diedral é visto como o conjunto formado pelos movimentos que deixam , a menos da posição dos vértices, um polígono regular invariante. Comumente, na apresentação do grupo D_n, os livros de álgebra focam nos seus aspectos mais algébricos: ordem do grupo, geradores etc.

Daqui por diante, denotaremos por P_n um polígono regular de n lados.

O nosso objetivo aqui é estudar o grupo D_n de um ponto de vista mais geométrico, visualizando-o como um subgrupo do grupo de isometrias do plano que fixam um polígono regular de n lados. Com tal enfoque, teremos condições de deduzir que as únicas simetrias de um polígono regular de n lados são as rotações de ângulo $2k\pi/n$, onde $0 \leq k < n-1$, reflexões e composições dessas. Em particular, seguirá que o grupo diedral D_n é finito (de ordem 2n) e isomorfo a um subgrupo do grupo simétrico S_n.

Na última seção do trabalho, iremos estudar o grupo de simetrias de uma circunferência. Será visto que tal grupo é infinito e consiste de rotações em torno do centro, reflexões em torno de diâmetros e composições dessas.

Muitas vezes, em sala de aula (bem como em livros didáticos), o conceito de Grupo é apresentado de maneira muito abstrata e isolada, e isso pode se tornar um empecilho no processo de ensino e aprendizagem. Acreditamos que a abordagem apresentada neste artigo pode ser adotada em sala de aula (em cursos de Álgebra em nível de Graduação), visando enfatizar as importantes propriedades geométricas do grupo D_n, fortalecendo a compreensão dos alunos e tornando o conceito de Grupo mais natural.

Para uma boa compreensão do texto, são requeridos conhecimentos básicos da Teoria de Grupos e, também, noções de Geometria Euclidiana Plana.

2. Simetrias

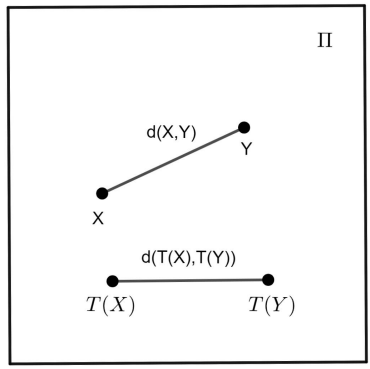
Ao longo do texto, reservaremos o símbolo Π para denotar um plano. Nesse primeiro momento, iremos definir formalmente o grupo de simetrias de um subconjunto $\mathcal{F}$ do plano. Por vezes, iremos chamar $\mathcal{F}$ de *figura*.

Dados os pontos $X, Y \in \Pi$, a medida do segmento XY será denotada por $\overline{XY}$ ou por $d(X,Y)$ (distância euclidiana entre os pontos X e Y).

Definição 1. Uma função $T : \Pi \to \Pi$ é dita isometria, se

$$d(X,Y) = d(T(X), T(Y)),$$

para quaisquer pontos $X, Y \in \Pi$.



Definição 2. Uma isometria $\mathrm{T} : \Pi \to \Pi$ é dita isometria de $\mathcal{F}$ quando $\mathrm{T}(\mathcal{F}) \subset \mathcal{F}$.

De acordo com a definição acima, as isometrias são funções definidas no plano que preservam distâncias.

Observação 1. As seguintes observações são de fácil verificação e podem ser vistas no Capítulo 1 de [4].

(a) Toda isometria é injetiva.

(b) Isometrias de retas e planos são sempre sobrejetivas.

(c) Sejam T uma isometria de $\mathcal{F}$ e $\mathrm{A} \neq \mathrm{B}$ pontos distintos em $\mathcal{F}$. Se $\mathrm{P} \in \mathcal{F}$ está no segmento AB, então T(P) está no segmento T(A)T(B).

(d) Consequência de (c): se T é uma isometria e r é uma reta, então T(r) também será uma reta.

Quando uma isometria T de $\mathcal{F}$ for sobrejetiva, diremos que T é uma *simetria* da figura $\mathcal{F}$. Denotamos o conjunto de todas as simetrias de $\mathcal{F}$ por

$$\mathrm{Isom}(\mathcal{F}).$$

Perceba que uma simetria de $\mathcal{F}$ é uma função bijetora que preserva distâncias. Claramente, a função identidade sempre será uma simetria de $\mathcal{F}$, a qual denotaremos por $\mathrm{Id}_{\mathcal{F}}$.

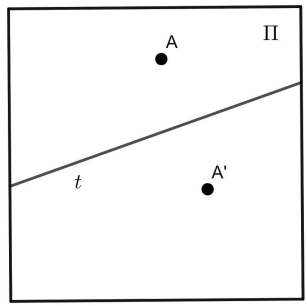
Podemos enxergar $\mathrm{Isom}(\mathcal{F})$ como um subconjunto de $\mathrm{Isom}(\Pi)$. Mais geralmente:

Proposição 1. *Se* $\mathrm{S}, \mathrm{T} \in \mathrm{Isom}(\mathcal{F})$, *então* $\mathrm{S} \circ \mathrm{T}, \mathrm{T}^{-1} \in \mathrm{Isom}(\mathcal{F})$. *Consequentemente,* $(\mathrm{Isom}(\mathcal{F}), \circ)$ *é um subgrupo do grupo* $(\mathrm{Isom}(\Pi), \circ)$.

Exemplo 1. Sejam t uma reta do plano Π e B um ponto fora de t e seja B′ o simétrico de B em relação a t. A função $\mathrm{R_t} : \Pi \to \Pi$, definida por

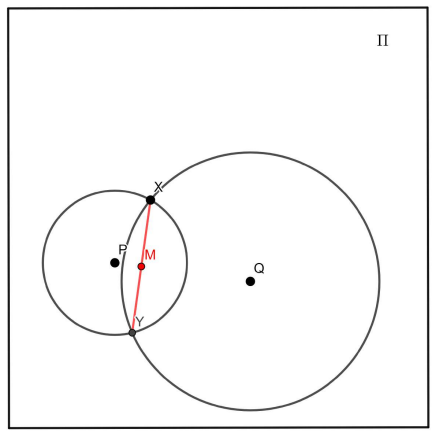
$$\mathrm{R_t}(\mathrm{A}) = \begin{cases} \mathrm{A}, & \text{se } \mathrm{A} \in \mathrm{t} \\ \mathrm{A}', & \text{se } \mathrm{A} \notin \mathrm{t} \end{cases},$$

é uma isometria do plano Π, chamada de reflexão em torno da reta t, e está ilustrada na figura abaixo.



Lema 1. *Seja* T ∈ Isom($\mathcal{F}$) *e suponha que* T *fixa dois pontos distintos, digamos* P *e* Q. *Sendo* R *a reflexão em torno da reta determinada por* P *e* Q, *tem-se* T(X) ∈ {X, R(X)}, *para todo ponto* X *de* $\mathcal{F}$.

Demonstração. Seja X um ponto qualquer da figura $\mathcal{F}$. Como P e Q são fixados por T, então T(X) deve pertencer à circunferência de centro em P que passa por X, e de centro em Q e que passa por X. Caso a interseção das duas circunferências seja o conjunto unitário, segue que T(X) = X, e o resultado está provado. Suponhamos então que exista mais um ponto na interseção, digamos Y, e seja M o ponto médio do segmento XY, conforme ilustrado na figura seguinte.



Observando que o segmento XY é corda comum às duas circunferências, concluímos que PM e MQ

são perpendiculares a XY. Concluímos então que M está no segmento PQ e que XY e PQ são perpendiculares. Assim, segue que $Y = R(X)$. □

Corolário 1. *Se* $T \in \mathrm{Isom}(\mathcal{F})$ *fixa três pontos não colineares, então* $T = \mathrm{Id}_{\mathcal{F}}$.

Demonstração. Suponha que os pontos não colineares P_1, P_2 e P_2 sejam fixados por T e denotemos por r a reta determinada por P_1 e P_2 e por t a reta determinada por P_2 e P_3.

Sendo X um ponto qualquer da figura $\mathcal{F}$, do Lema 1, obtemos

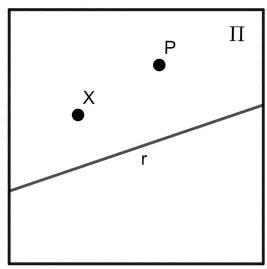
$$T(X) \in \{X, R_r(X)\} \text{ e } T(X) \in \{X, R_t(X)\}.$$

Como as retas r e t são distintas, é claro que $R_r(X) \neq R_t(X)$ e daí $T(X) = X$. □

3. Simetrias de polígonos regulares: grupos diedrais

A Definição 2 fornece-nos uma nova possibilidade de melhor compreender o grupo diedral de um polígono regular de n lados, precisamente: podemos vê-lo como um subgrupo das isometrias do plano que fixam o polígono. Será essa a nossa abordagem daqui por diante.

Dada uma reta r e um ponto P fora de r, seja X um ponto qualquer do semiplano determinado por r e P. Se $T \in \mathrm{Isom}(\Pi)$, sejam $r_1 = T(r)$, $P_1 = T(P)$ e $X_1 = T(X)$.



Com essas notações em mente, temos o seguinte resultado:

Proposição 2. *O ponto* X_1 *está no semiplano determinado por* r_1 *e* P_1.

Demonstração. Por contradição, suponha que X_1 e P_1 estejam em semiplanos distintos determinados por r_1. Assim, o segmento X_1P_1 intersecta a reta r_1, digamos num ponto A_1. Sendo A o ponto de r tal que $T(A) = A_1$, decorre que A está compreendido no segmento XP, o que é contraditório. □

Daqui por diante, iremos denotar um polígono regular de n lados por P_n.

Definição 3. O grupo $\mathrm{Isom}(P_n)$ será chamado de grupo diedral, e será denotado por D_n.

Agora, apresentamos a seguinte caracterização para o grupo D_n:

Proposição 3. *Seja* $T \in D_n$. *Se* V *é um vértice de* P_n, *então* T(V) *também é vértice* P_n. *Consequentemente, o grupo* D_n *é isomorfo a um subgrupo do grupo simétrico* S_n.

Demonstração. Seja W um vértice do polígono tal que V e W formam um lado do polígono. Assim, o polígono fica em um dos semiplanos determinados pela reta que contém o segmento VW. Supondo que T(V) não seja vértice de P_n, decorre que T(W) não estaria no mesmo lado que T(V). Assim, a reta que passa pelos pontos T(V) e T(W) determina dois semiplanos que contêm pontos de P_n, o que contradiz a Proposição 2. □

Corolário 2. *Se* $T \in D_n$, *então o centro de* P_n *é fixado por* T.

Demonstração. Sejam O o centro de P_n e $C(V_i)$ a circunferência centrada no vértice V_i e que passa por O, para cada $i = 1, \ldots, n$. Observemos que

$$C(V_1) \cap \cdots \cap C(V_n) = \{O\}.$$

De acordo com a Proposição 3, os vértices de P_n são permutados, logo

$$C(T(V_1)) \cap \cdots \cap C(T(V_n)) = C(V_1) \cap \cdots \cap C(V_n) = \{O\}.$$

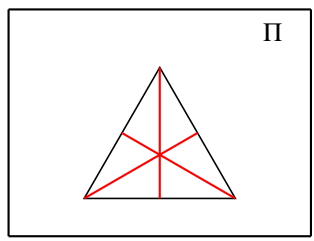
Por outro lado, como T preserva distâncias, concluímos que T(O) pertence à interseção supracitada. Assim, T(O) = O. □

Observação 2. Como consequência da Proposição 3, segue-se que as únicas simetrias do tipo rotação de um polígono P_n são θ_0, $\theta_1 \ldots$, θ_{n-1}, onde θ_k denota a rotação em torno do centro de P_n de ângulo $2k\pi/n$ (que convencionaremos serem no sentido anti-horário).

Observação 3. Para enxergarmos mais simetrias de P_n, precisaremos considerar os seguintes casos:

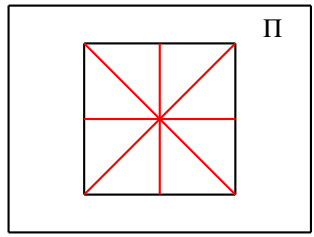
(a) n ímpar: Nesse caso, considere as n medianas que partem de cada vértice de P_n e sejam $R_1, \ldots, R_n$ as reflexões em torno delas.

Abaixo, temos uma ilustração do caso n = 3:



(b) n par: Nesse caso, considere as n/2 diagonais e as n/2 mediatrizes do polígono e sejam $R_1, \ldots, R_{n/2}$ e $U_1, \ldots, U_{n/2}$ as reflexões em torno das diagonais e mediatrizes, respectivamente.

Abaixo, temos uma ilustração do caso n = 4:



Agora, temos todas as informações necessárias para enunciar e provar o principal resultado desta seção.

Teorema 1. *Seja* $T \in D_n$ *um elemento do grupo diedral.*

- *Se* n *for ímpar, então* T *pertence ao conjunto*

$$\{R_t \circ \theta_k \mid 0 \leq k \leq n-1; 1 \leq t \leq n\}.$$

- *Se* n *for par, então* T *pertence ao conjunto*

$$\{R_t \circ \theta_k \mid 0 \leq k \leq n-1; 1 \leq t \leq n/2\} \cup \{U_t \circ \theta_k \mid 0 \leq k \leq n-1; 1 \leq t \leq n/2\}.$$

Consequentemente, a ordem do grupo D_n *é menor ou igual a* n^2.

Demonstração. Faremos somente a demonstração do caso n ímpar, já que o caso n par segue a mesma ideia.

Sejam V um vértice de P_n e O o seu centro. Consideremos R a reflexão do plano em torno da reta determinada por V e O (que é a mediana que parte do vértice V).

Do Corolário 2, sabemos que T fixa O. Logo, se T fixa V, então T terá V e O como pontos fixos. Pelo Lema 1, temos $T(X) \in \{X, R(X)\}$. Se existir X não colinear a V e O que seja fixado, o Corolário 1 garante que $T = Id = \theta_0$. Caso contrário, podemos inferir que $T = R$.

Suponhamos então que $V \neq T(V) = V'$. Consideremos a rotação θ_k^{-1} do plano em torno de O tal que $\theta^{-1}(V') = V$.

Assim, decorre que

$$T \circ \theta_k^{-1}(O) = O$$

e

$$T \circ \theta_k^{-1}(V') = V'.$$

Dessa forma, pelo Lema 3, há as seguintes possibilidades:

$$T \circ \theta_k^{-1} = Id$$

ou

$$T \circ \theta_k^{-1} = \hat{R},$$

onde $\hat{R}$ é a reflexão em torno da mediana que passa por V' e O.

Portanto, das últimas igualdades, obtemos a primeira parte do resultado. A última afirmação do resultado segue trivialmente. □

Na verdade, no que se refere à ordem do grupo diedral, podemos refinar o resultado anterior:

Teorema 2. *O grupo diedral* D_n *tem ordem* $2n$.

Demonstração. Aqui, podemos usar exatamente a mesma ideia da referência [3]. □

Uma pergunta interessante e que vai na contramão do resultado acima é se todo subgrupo finito do grupo $\mathrm{Isom}(\Pi)$ coincide com D_n, para algum polígono regular P_n. O teorema seguinte elucida tal questão.

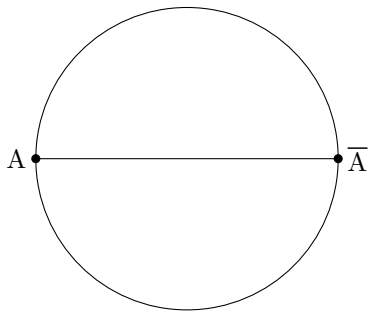
Teorema 3. *Todo subgrupo finito do grupo* $\mathrm{Isom}(\Pi)$ *é isomorfo a* D_n *ou* $\mathbb{Z}_n$*, para algum* n.

Demonstração. Pode ser vista na página 115 da referência [2]. □

4. Subgrupos infinitos de $\mathrm{Isom}(\Pi)$: simetrias da circunferência

Agora, nos propomos a estudar o grupo de simetrias da circunferência. Provaremos que esse grupo é infinito, sendo formado somente por rotações, reflexões em torno de diâmetros e composições dessas.

Iremos denotar uma circunferência pelo símbolo $\mathcal{C}$ e, sendo A um ponto de $\mathcal{C}$, designaremos por $\overline{A}$ o ponto de $\mathcal{C}$ que é diametralmente oposto ao ponto A.



Definição 4. Dizemos que $f \in \mathrm{Isom}(\mathcal{C})$ é uma reflexão de diâmetro $A\overline{A}$ se os únicos pontos de $\mathcal{C}$ fixados por f são A e $\overline{A}$.

Exemplo 2. As seguintes funções são simetrias de $\mathcal{C}$.

(a) Rotações de ângulo qualquer em torno do centro de $\mathcal{C}$.

(b) Reflexões em torno de diâmetros de $\mathcal{C}$.

(c) Composições das simetrias indicadas em (a) e (b).

Proposição 4. *Se* $f \in \mathrm{Isom}(\mathcal{C})$ *fixa dois pontos não diametralmente opostos, então* $f = \mathrm{Id}_{\mathcal{C}}$.

Demonstração. Sejam P e Q pontos de $\mathcal{C}$ que são fixados por f e suponha que $Q \neq \overline{P}$. Observe que

$$d(P, \overline{P}) = d(P, f(\overline{P})),$$

logo $Pf(\overline{P})$ é diâmetro da circunferência, implicando que $f(\overline{P}) = \overline{P}$. Assim, f fixa três pontos não colineares, e, pelo Corolário 1, obtemos $f = \mathrm{Id}_{\mathcal{C}}$. □

Como um corolário, obtemos o seguinte resultado.

Corolário 3. *Suponha que* $f \in \mathrm{Isom}(C)$ *tem pelo menos um ponto fixo em* C*. Então* f *é uma reflexão ou* f *é a identidade.*

Demonstração. Seja P um ponto fixo de f. Pelo visto acima, devemos ter que $\overline{P}$ também será ponto fixo. Se esses são os únicos pontos fixos de f, temos uma reflexão de diâmetro $P\overline{P}$. Caso exista outro ponto fixo, a Proposição 4 implica que f é a identidade. □

Agora, estamos em condições de provar o principal resultado dessa seção.

Teorema 4. *Toda simetria de uma circunferência* C *é uma rotação, ou uma reflexão em torno de algum diâmetro ou é composição dessas.*

Demonstração. Seja f uma simetria de C. Fixemos um ponto $P \in C$ e consideremos a rotação θ^{-1} tal que

$$\theta^{-1}(f(P)) = P.$$

Segue do Corolário 3 que $\theta^{-1} \circ f$ é a identidade ou $\theta^{-1} \circ f$ é uma reflexão em torno de algum diâmetro, e daí o resultado segue. □

5. Considerações finais

Normalmente estudado num primeiro curso de Álgebra Abstrata em nível de Graduação, o grupo diedral é, quase sempre, apresentado aos alunos de forma bastante algébrica, em detrimento de sua importante natureza geométrica. Tal abordagem também é perceptível em boa parte dos livros didáticos. Não obstante, acreditamos que uma abordagem mais geométrica do grupo D_n em sala de aula favorece e amplia a compreensão dos alunos, e torna o conceito de Grupo mais natural. Foi essa a principal motivação para a elaboração do presente artigo, o qual é resultado da pesquisa de Iniciação Científica do segundo autor, tendo orientação do primeiro autor.

Agradecimentos

Os autores agradecem ao revisor pelas sugestões que melhoraram sobremaneira a versão

final do artigo.

Referências

[1] Barbosa, J.L.M, *Geometria Euclidiana Plana*, Sociedade Brasileira de Matemática, décima edição, 2006.

[2] Fraleigh, J.B, *A First Course in Abstract Algebra*, Addison Wesley, sétima edição, 2003.

[3] Garcia, A, *Elementos de Álgebra*, IMPA, quinta edição, 2008.

[4] Lima, E. L, *Isometrias*, Sociedade Brasileira de Matemática, segunda edição, 2007.

Alan de Araújo Guimarães
Universidade Federal do Rio Grande do Norte
Departamento de Matemática
Natal-RN
<alan.guimaraes@ufrn.br>

Francisco Thiarly Alves de Souza
Universidade Federal do Rio Grande do Norte
Departamento de Física
Natal-RN
<thiarly.souza.123@ufrn.edu.br>

Recebido: 04/04/2022
Publicado: 12/08/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1028

O conceito de medida, o *continuum* e o discreto

José Carlos Magossi Vania Rosa Figueiredo Izidoro

Resumo

A palavra "medida" tem sido utilizada ao longo da história da humanidade em quase todos os setores da atividade humana. Não é de espantar que alterações no modo como se mede resultam em alterações no modo como a ciência e as tecnologias são desenvolvidas. Os refinamentos nos critérios de medida, num sentido amplo, ocorrem graças às tecnologias existentes, ou emergem de alguma regra bem definida, escrita em alguma linguagem, com algum fim científico ou prático. Enquanto, num passado remoto, media-se o diâmetro da Terra com base em semelhanças de triângulos, nos tempos atuais as tecnologias dão conta de tornar essas medidas muito mais precisas. Mesmo assim, um consenso ainda não é atingido, haja vista que o *continuum* matemático impõe restrições à realidade voltada às medições. Por exemplo, não há como em laboratórios utilizar π em sua plenitude, uma vez que aproximações são necessárias, levando-se em conta que é um número irracional com infinitas casas decimais. Essas incertezas, no quesito "precisão", podem ser vistas como uma gangorra, em que de um lado há as medidas práticas da realidade em que vivemos e, de outro, as medidas teóricas. O objetivo neste artigo é, por um lado, expor, sob a ótica da matemática, alguns exemplos em que se caracterize a relação entre o *continuum* e o discreto, no quesito "medida". Por outro, mostrar que essa relação pode indicar contradições, num palco de interações entre o mundo prático e o teórico, se não for feita uma leitura cuidadosa. Além de uma digressão histórica com exemplos, mostra-se que algo semelhante ocorre com o conceito de medida visto como quantidade de informação, denominado de entropia por C. E. Shannon. Há também cuidados a serem tomados com relação à entropia, vista sob a ótica de modelos discretos, e sua extensão para modelos contínuos, a entropia diferencial. Enquanto, do lado discreto, a quantidade de informação é positiva, a entropia diferencial, do lado contínuo, pode ser negativa, positiva ou arbitrariamente grande.

Palavras-chave: Medida, *continuum*, discreto, Shannon, entropia diferencial

Abstract

The word "measure" has been used throughout the history of humanity in almost every sector of human activity. It is not surprising that any changes in the way things are measured, also cause impacts in the developent of science and technologies. The refinements in the measurement criteria, in a broad sense, occur thanks to existing technologies, or they emerge from some well-defined rule, written in some language, with some scientific or practical purpose. Whereas, in a remote past, the diameter of the Earth was measured based on similarities of triangles, in modern times technologies made these measures much more precise. Even so a consensus is not yet reached, given that the mathematical *continuum* imposes restrictions on measurement reality. For example,

there is no way to use π in its fullness in laboratories, since approximations are necessary, taking into account that it is an irrational number with infinite decimal places. This characterizes a seesaw, in which, on one hand, there are the practical measures in the reality we live in, and, on the other, the theoretical measures. The goal in this article is to expose that, on one hand, from the perspective of mathematics, some examples characterize the relation between *continuum* and the discrete, in the measured aspect. On the other hand, we show that this relationship can indicate contradictions, in a stage of interactions between the practical and the theoretical world, if no careful reading happens. Apart from a historical digression with examples, it is shown that something similar occurs with the concept of measure when it is seen as an amount of information, called entropy by C. E. Shannon. There is also care to be taken regarding entropy, seen from the point of view of discrete models, and their extension to continuous models, differential entropy. While on the discrete side the amount of information is positive, the differential entropy, on the continuous side, can be negative, positive or arbitrarily large.

Keywords: Measure, *continuum*, discrete, Shannon, differential entropy

1. Introdução

O conceito de medida relaciona-se à possibilidade de passar de um atributo que pode envolver continuidade e quantificadores a uma notação numérica que facilita, com base nas operações numéricas, transmitir informações acerca dos objetos investigados [34]. *Grosso modo*, medir é atribuir números (ou alguma grandeza, uma magnitude) a objetos seguindo determinadas regras. Em matemática o conceito de medida, extensivo a uma teoria da medida, de H. L. Lebesgue (1875-1941) [18], [5], relaciona-se à caracterização do conteúdo de um conjunto por um número real, que alicerça o desenvolvimento da teoria das probabilidades, por exemplo. Uma dificuldade inicial mostra-se quando se pretende elaborar uma definição de medida que seja extensiva o suficiente. Como construir relações entre objetos a serem medidos, com uma linguagem apropriada, de tal forma que haja uma exata interpretação numérica que possibilite leituras práticas de medidas em determinados contextos [30]. É bastante entusiástica a busca por um diálogo mais efetivo entre ciências empíricas e teorias de medida. Isso impacta a inserção de teorias de medidas em setores diversos, tais como educação, psicologia, ciências humanas, informática etc. [20, 27]. Neste artigo, o ponto de discussão caracteriza-se pela relação entre o conceito de medida quando aplicado a modelos discretos, e quando aplicado a modelos contínuos. Em muitos casos, utiliza-se o mesmo critério de medida, a mesma "régua", seja para o caso discreto, seja para o caso contínuo. Por exemplo, ao somar $1 + \frac{1}{2} + \frac{1}{4} + \ldots$, comumente se utiliza o nome "soma infinita". No entanto, a palavra "soma" é reservada para conjuntos finitos de dados, sendo que a palavra "série" aplica-se aos casos em que uma quantidade infinita de parcelas é analisada. Ao escrever "soma infinita" emprega-se, de certa forma, a mesma "régua" para ambos os casos, o finito e o infinito. Caso uma distinção não seja feita, abre-se espaço para perguntas do tipo: "Como somar uma quantidade infinita de parcelas?". De modo análogo, pode-se perguntar quais são as propriedades que se preservam (e quais não) ao se aplicar uma mesma propriedade de um conceito de medida em objetos oriundos de conjuntos discretos e também de conjuntos contínuos. A investigação dessas propriedades auxilia também na distinção entre as ferramentas que podem e as que não podem ser utilizadas com consistência para cada caso. As sutilezas que se escondem nas propriedades que residem, ou não, nos modelos contínuos e modelos discretos talvez possam ser mais bem compreendidas ao se examinar, com os devidos cuidados, o texto escrito no livro *Select Works of A. N. Kolmogorov*:

Se um mapa nos dá informações importantes sobre uma seção da superfície da

> *Terra, a microestrutura do papel e da tinta que ocorre no papel não tem nenhuma relação com a microestrutura da seção da superfície da Terra mostrada sobre esse papel. ([33], p.189) (Tradução dos autores).*

Nesse caso, ao analisar o mapa de um país, exposto numa grande folha de papel, o uso de uma lente de aumento para descobrir, nas ranhuras do mapa, algumas propriedades das ruas de alguma cidade que consta no mapa não vai fornecer resultados consistentes. Nesse caso, a lente de aumento não é uma ferramenta apropriada para obter tais informações, haja vista que o mapa indica propriedades do país no sentido macroscópico e não microscópico. No entanto, algumas propriedades se preservam, seja no sentido macro como no micro, como, por exemplo, a fronteira entre as cidades.

Se o mundo macroscópico fornece (ou não) informações suficientes para uma análise precisa do mundo microscópico, esse é um assunto ainda deveras investigado [10, 11]. De certa forma, isso vem sendo investigado na matemática, tal como o problema da incomensurabilidade de $\sqrt{2}$, que tem sido discutido desde a Grécia antiga e, com base na sua incomensurabilidade, propiciado o surgimento de inúmeros paradoxos. Associar um número a um segmento de reta, tal como se faz nos dias de hoje, indicava, na Grécia antiga, na época de Euclides, ter de resolver, como caso particular, o problema da incomensurabilidade de $\sqrt{2}$. Para evitar esse problema, o geômetra Eudoxo opta por comparar figuras geométricas em vez de associar uma medida a elas. Por exemplo, se um quadrado tem lado a e outro quadrado tem lado β, então se diz que o quadrado de lado a é maior que o quadrado de lado β, em símbolos, $a^2 > \beta^2$, desde que o quadrado de lado β possa ser inserido no quadrado de lado a [19]. Essa ideia de medida procura, de certa forma, escapar às discussões sobre as quantidades infinitamente pequenas [2, 23]. Pode-se especular nesse caso que Eudoxo tenha evitado a relação entre os mundos microscópico e macroscópico e, tal como no exemplo acima, do mapa, tenha procurado por propriedades que fossem comuns a ambos os mundos.

Esse panorama só começa a mudar muito tempo depois, com o surgimento do conceito de limites por A. L. Cauchy (1789-1857) no século *XIX* [12],[13]. O conceito de limites indicou um divisor de águas para a matemática e acelerou inúmeros desenvolvimentos, tais como as alterações no conceito de medida. Assim se deu com a alteração do conceito de medida de áreas, volumes etc., voltado, na época anterior à de Cauchy, apenas às integrais de I. Newton (1643-1727) e G. Leibniz (1646-1716) [37, 22]. Analisar a classe de funções integráveis, que não sejam aquelas obtidas com base em antiderivadas (integrais de Newton-Leibniz) implica, de alguma forma, indicar um processo de medida voltado às partições do domínio da função investigada, no caso das integrais de Cauchy, Riemann, Kurzweil-Henstock, ou da partição do conjunto imagem da função, no caso das integrais de Lebesgue [6]. É certo que essas medições levam em conta o *continuum* matemático, mas é certo também que, com base nelas, desenvolvimentos matemáticos (e tecnológicos) puderam ser elaborados. Pode-se dizer que Cauchy desenvolveu ferramentas apropriadas para "medir" as quantidades infinitamente pequenas. Isto é, ele usou ferramentas adaptadas ao mundo microscópico. Casos clássicos da influência da teoria da medida e integração de Lebesgue, com ferramentas semelhantes, são: teoria das probabilidades, mecânica estatística, teoria da informação, termodinâmica, análise de Fourier etc. Longe de invocar o período de abstração matemática que caracterizou o início do século *XX* ([29], p.173), mas com o viés de que uma linguagem bem estruturada é condição *sine qua non* para sustentar inovações em matemática e tecnologia, entende-se, tal como ocorreu com a teoria da medida e integração de Lebesgue, que caracterizações do conceito de medida sejam desenvolvidas com fins de indicar diversificações na escolha de medidas e com isso possibilitar maior interação entre conceitos, evitando o medir com ferramentas inapropriadas. O importante com isso é diminuir as incertezas presentes na ciência com base no desenvolvimento de novos critérios, e novas tecnologias, associadas aos critérios de medida. As medidas fundadas na

geometria plana auxiliavam os trabalhos de Newton; com N. I. Lobachevsky (1792-1856) e C. F. Gauss (1777-1855), as da geometria não euclidiana auxiliaram os trabalhos de A. Einstein (1879-1955). As incertezas presentes na época de Newton não são as mesmas de hoje, haja vista que física clássica e física moderna são ramificações que indicam a evolução na diminuição dos níveis de incertezas. Conforme L. Brillouin (1889-1969) [10, 11], levando-se em conta a ideia de que um observador é que faz a medida, e em consonância com a ideia de entropia da termodinâmica, na física, a medida de distâncias muito pequenas é fisicamente impossível. Com isso, um ponto interessante é que, para o físico, no sentido operacional, as quantidades infinitamente pequenas (o *continuum*) são apenas abstrações, sem nenhum significado físico [10, 11]. Para Brillouin,

> *O matemático define o infinitamente pequeno, mas o físico é absolutamente incapaz de medi-lo; representa uma pura abstração sem nenhum significado físico. Se adotássemos o ponto de vista operacional, deveríamos eliminar o infinitamente pequeno das teorias físicas, mas, infelizmente, não temos ideia de como alcançar tal programa. ([10], p.x, Tradução dos autores.)*

Não é objetivo trazer à tona as discussões de Brillouin sobre o determinismo ou sobre a impossibilidade de fazer medições para distâncias muito pequenas, mas sim indicar apenas um contexto histórico, uma trajetória de eventos e exemplos, com vistas a justificar a importância de leituras cuidadosas acerca do conceito de medida, nos modelos discretos e contínuos.

Mesmo com tantas incertezas e pluralidade no sentido das interações entre o que se mede e o que poderia ser medido, há problemas interessantes num domínio em que o conceito de medida relaciona-se com o conceito de incerteza, isto é, num domínio pertencente à teoria de Shannon, ou teoria da informação [14]. C. E. Shannon (1916-2001), em seu artigo de 1948 [31], para seu modelo matemático de comunicação, indicou uma medida para a quantidade de informação a ser transmitida entre um emissor X e um receptor Y, através de um canal de comunicação. Com essa medida, denominada por ele de entropia[1], é possível tratar informações e melhorar a eficiência na transmissão de dados em sistemas de comunicação [26, 4, 14]. Se $X = \{x_1, x_2, \ldots, x_i, \ldots, x_m\}$ e $Y = \{y_1, y_2, \ldots, y_j, \ldots, y_n\}$ são variáveis aleatórias discretas, e $p(x_i)$ é a probabilidade *a priori* de que $X = x_i$, então a entropia discreta de X, para um sistema completo de probabilidades,

$$H(X) = -\sum_{i=1}^{M} p(x_i)\log\, p(x_i),$$

mede a quantidade de informação da experiência representada pela variável X. A quantidade de informação *a posteriori* é a incerteza eliminada *a priori*. No caso de variáveis aleatórias contínuas, se $f(x)$ representa uma função de densidade de probabilidade da variável aleatória absolutamente contínua X, então a entropia diferencial de X,

$$h(X) = -\int_{-\infty}^{+\infty} f(x)\log f(x)\,dx,$$

representa, não um número, uma quantidade de informação associada à variável aleatória X, como na entropia para o caso discreto, mas uma medida relativa de incerteza [24] ou uma mudança na incerteza[2]. Com base na medida da quantidade de informação, entropia no sentido de Shannon,

[1] Shannon adotou o mesmo nome utilizado na termodinâmica por R. Clausius (1822-1888) [21].

[2] Note-se, nesse caso, que essa medida fundamenta-se no conceito de integral, haja vista que a existência de $h(X)$ está condicionada à existência da integral presente em sua definição [14].

uma pergunta interessante, em consonância com a discussão aqui apresentada sobre as leituras distintas entre o mundo microscópico e mundo macroscópico, é: Como se dá a relação entre entropia discreta e entropia diferencial? [31, 4, 26].

Esse conceito, de entropia diferencial, que pode ser visto como uma nova leitura da medida da informação para o caso contínuo, tem aplicações em campos além da mecânica estatística e teoria da comunicação, tais como finanças, econometria, processamento de imagens, ecologia, bioestatística etc. [24]. Ou seja, há desafios matemáticos interessantes relacionados à medida de uma quantidade de informação, relacionados ao passar de modelos discretos para modelos contínuos [26]. Mais interessante é que a "régua" utilizada para medir informação para modelos discretos (entropia discreta) é diferente daquela utilizada para medir informações em modelos contínuos.

Na sequência, neste texto, expõem-se, no sentido histórico, exemplos de medidas em modelos contínuos que, quando lidos sob a ótica de modelos discretos, podem incorrer em propensos paradoxos ou contradições. No sentido físico, ilustra-se, de modo breve, a rica discussão, presente em [10, 11], acerca da impossibilidade de medir distâncias muito pequenas. Nesse caso, abre-se espaço para a percepção da importância das ferramentas matemáticas no desenvolvimento de modelos e sua imediata limitação nos modelos do mundo em que habitamos. Expõe-se também o avanço científico que se obtém quando alterações nos modelos contínuos produzem novos desenvolvimentos na matemática, tal como se deu com o conceito de integrais. Finaliza-se o artigo com o conceito de medida relacionado às comunicações. Nesse caso, há uma medida da quantidade de informação (ou incerteza *a priori*), no caso de modelos discretos, mas há um campo novo de investigação que reside na quantidade de informação, incerteza, presente nos modelos contínuos (entropia diferencial). Isso não deixa de ser algo conhecido na história da humanidade, reforçado neste artigo com alguns exemplos, sobre qual é o divisor de águas, se é que existe, entre as ferramentas matemáticas adaptadas para modelos discretos e aquelas adaptadas para os contínuos.

2. Possíveis equívocos com a palavra "medida"

Nesta seção alguns exemplos são expostos com o objetivo de mostrar o quanto de cuidado deve-se ter ao utilizar ferramentas desenvolvidas para modelos discretos com fins de obter resultados em modelos contínuos, ou lançar mão de ferramentas desenvolvidas para modelos contínuos na busca por resultados em modelos discretos. Não que isso não possa ser feito, mas precaução talvez seja a palavra correta, pois contradições podem emergir da leitura, talvez descuidada, da relação entre contínuo e discreto, como a não enumerabilidade de $\mathbb{R}$, incomensurabilidade e conjuntos infinitos. Note-se com os exemplos seguintes que o conceito de medida deve ser pautado em firmes definições, para que contradições não emerjam de leituras não atentas.

2.1. Área infinita e volume finito

Considere-se o cálculo da área da superfície de revolução obtida ao girar a função $y = \frac{1}{x}$ limitada no intervalo $[1, +\infty)$, em torno do eixo x. A fórmula que indica o cálculo da área da superfície desse sólido, obtida por revolução ([17], p.410) em torno do eixo x, é:

$$\text{Área} = \int_1^{+\infty} 2\pi f(x)\sqrt{1 + (f'(x))^2}\,dx.$$

Se $f(x) = \frac{1}{x}$, então $f'(x) = \frac{-1}{x^2}$, e daí:

$$\text{Área} = \int_1^{+\infty} 2\pi f(x)\sqrt{1+\left(\frac{-1}{x^2}\right)^2}\,dx = \int_1^{+\infty} 2\pi\frac{1}{x}\frac{\sqrt{x^4+1}}{x^2}\,dx.$$

$$= \lim_{R\to+\infty}\int_1^R 2\pi\frac{\sqrt{x^4+1}}{x^3}\,dx.$$

Essa integral imprópria não converge; logo, infere-se que a área da superfície de revolução em questão é infinita. Com o auxílio de computadores é possível verificar, para $R = 10^n$ e $n \in \mathbb{N}$, que,

$$\varphi(n) = \int_1^{10^n} 2\pi\frac{\sqrt{x^4+1}}{x^3}\,dx \quad (1)$$

$$= \left(\sqrt{2} - \ln\left(1+\sqrt{2}\right) + \text{arcsenh}(100^n) - 100^{-n}\sqrt{10000^n+1}\right)\pi. \quad (2)$$

Então $\varphi(1) = 15,177$, $\varphi(2) = 29,645$, $\varphi(4) = 58,58$, $\varphi(8) = 116,45$, $\varphi(12) = 174,32$, $\varphi(15) = 217,72$ etc. Ou seja, quanto maior é o valor de n, maior é o valor da integral e, por conseguinte, da área associada à integral. Nesse caso, tem-se que

$$\lim_{n\to+\infty}\varphi(n) = +\infty.$$

Por outro lado, o cálculo do volume desse mesmo sólido, obtido por revolução da função $\frac{1}{x}$ em torno do eixo x, no intervalo $[1,+\infty)$, é feito ([17], p.381) pela seguinte integral:

$$\text{Volume} = \int_1^{+\infty}\pi f(x)^2\,dx = \int_1^{+\infty}\pi\left(\frac{1}{x}\right)^2 dx = \int_1^{+\infty}\left(\frac{\pi}{x^2}\right)dx.$$

Essa é uma integral imprópria, que converge, ou seja,

$$\text{Volume} = \lim_{R\to+\infty}\int_1^R \pi x^{-2}\,dx = \lim_{R\to+\infty}\left[\frac{-\pi}{x}\right]_1^R = \lim_{R\to+\infty}\left[\frac{-\pi}{R}+\frac{\pi}{1}\right] = \pi.$$

Nesse caso, a unidade do valor do volume igual a π vai depender da unidade que possa ser utilizada na descrição do intervalo $[1,+\infty)$. O volume poderá ser expresso em m^3, cm^3 etc. Note-se, então, que a mesma figura, o sólido de revolução com área infinita se $R \to +\infty$, conforme pode ser observado na figura 1, tem volume finito, se $R \to +\infty$. Essa propensa "contradição" advém de leituras discretas em problemas cuja essência volta-se a modelos contínuos. Cabe observar que, em tese, não há contradição, mas a ideia de área infinita e volume finito, para um mesmo sólido[3], pode gerar confusão haja vista não ser algo tão intuitivo. Uma leitura descuidada pode caracterizar que isso seja uma contradição.

[3]Nesse caso considera-se que o sólido existe no intervalo $[1,+\infty)$, algo distante da realidade prática em que vivemos.

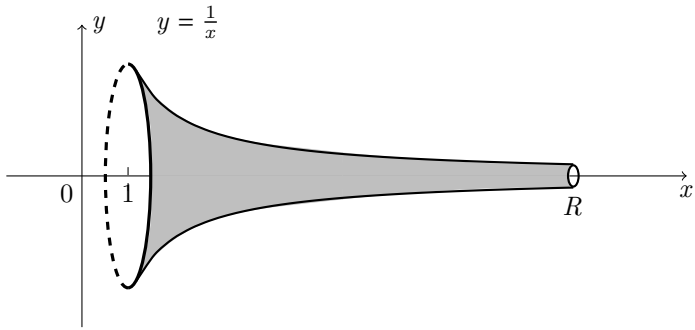


Figura 1: Revolução de $y = \frac{1}{x}$ em torno do eixo x.

2.2. A roda de Aristóteles

Supõe-se a existência de duas circunferências, C_1 e C_2, de tal forma que a circunferência C_2 seja maior que a circunferência C_1. Supõe-se ainda que ambas sejam colocadas uma dentro da outra, isto é, a circunferência C_1 está dentro da circunferência C_2, de tal forma que possam ambas deslizar sobre retas u e v, paralelas entre si. A circunferência C_1 desliza sobre a reta u e a C_2, sobre a reta v. Note-se que cada ponto de uma circunferência está em correspondência biunívoca com cada ponto da outra, conforme pode ser observado na figura 2. No entanto, ambas percorrem o mesmo trajeto de A até B, no mesmo tempo. Se r_2 é o raio da circunferência C_2 e r_1 é o raio da circunferência C_1, então o comprimento da circunferência C_1 é $2\pi r_1$, e o comprimento da circunferência C_2 é $2\pi r_2$.

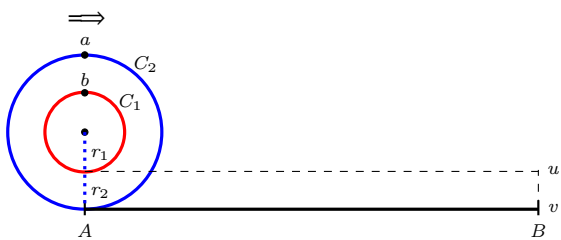


Figura 2: Roda de Aristóteles

Mas, por hipótese, $r_1 < r_2$, então $2\pi r_1 < 2\pi r_2$, isto é, o comprimento da circunferência C_1 é menor do que o comprimento de C_2. Mas, levando-se em conta o desenho, tem-se a impressão de que a trajetória de A até B refere-se ao comprimento de cada circunferência. Se assim for, tem-se então uma possível contradição. No entanto a curva cicloide realizada pela circunferência menor (com base no ponto b e reta suporte u) não é a mesma curva cicloide que a realizada pela circunferência maior (com base no ponto a e reta suporte u), conforme pode ser observado na curva cicloide da figura 3. Note-se que o comprimento do segmento contido na reta suporte u, nesse caso, é $2\pi r_1$.

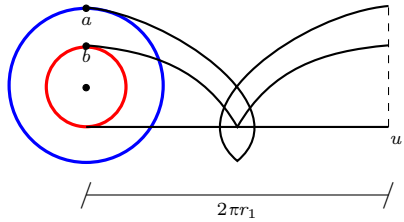


Figura 3: Curva cicloide com início em b sobre a reta u

De modo análogo, a curva cicloide realizada pela circunferência maior (com base no ponto a e reta suporte v) não é a mesma curva cicloide que a realizada pela circunferência menor (com base no ponto b e reta suporte v), conforme pode ser observado na figura 4. Note-se que o comprimento do segmento contido na reta suporte v, nesse caso, é $2\pi r_2$.

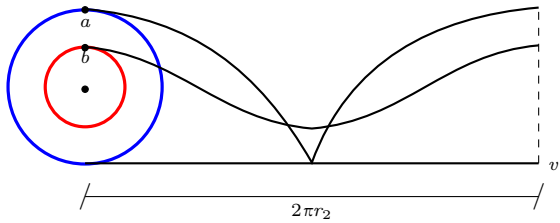


Figura 4: Curva cicloide com início em a sobre a reta v

Assim, conforme for a rotação da roda, o tamanho da reta suporte dependerá do ponto de partida do trajeto. Caso o trajeto seja determinado pela circunferência menor a partir do ponto b, ao longo da reta u, então o percurso é menor que o trajeto iniciado no ponto a, com base na circunferência maior ao longo da reta v. No artigo *Aristotle's Wheel: Notes on the History of a Paradox* [16] encontra-se uma rica discussão sobre esse tema. Além disso, o fato de ambos os conjuntos terem uma correspondência biunívoca (entre cada ponto de C_1 e C_2) não garante que tenham trajetórias idênticas.

2.3. Aquiles e a tartaruga

Na literatura, atribui-se a Zenão de Eleia, da Grécia antiga, um paradoxo acerca de uma corrida entre o guerreiro Aquiles e uma tartaruga. Nessa corrida, a tartaruga tem uma vantagem sobre Aquiles, pois está à sua frente antes do início da corrida. A ideia de Zenão é, com essa simulação, mostrar que Aquiles nunca venceria a corrida, pois nunca alcançaria a tartaruga. Quando Aquiles chegar ao ponto em que a tartaruga saiu (dada a vantagem inicial), ela já terá percorrido um certo trajeto, e estará num ponto, digamos P_1. Quando Aquiles chegar a P_1, a tartaruga já estará em outro ponto, P_2, e assim sucessivamente. Se isso se repetir *ad infinitum,* então Aquiles nunca alcançará a tartaruga. Esse é o paradoxo de Zenão de Eleia, século V antes de Cristo, na Grécia antiga. De certa forma, pode-se inferir que Zenão discutia acerca das quantidades infinitamente pequenas [23] e das contradições que emergem de sua utilização, como no caso de Aquiles e a tartaruga. Se um objeto desloca-se de um ponto A até um ponto B, esse objeto precisa passar

pela metade do caminho, diga-se C, que une A a B. De modo análogo, precisa passar pela metade do caminho que une C até o ponto final B. E assim sucessivamente. Como, argumenta Zenão, há infinitos pontos a percorrer, o objeto nunca chegará ao ponto B. Ou seja, se a distância de A até B é de u metros, então para ir de A até B é preciso percorrer as distâncias, medidas em metros,

$$\frac{u}{2} + \frac{u}{4} + \frac{u}{8} + \dots .$$

Essa soma é uma série geométrica de razão $\frac{1}{2}$ e converge para u. Essa convergência é uma conclusão com base na matemática e na teoria de limites, em que quantidades infinitamente pequenas são levadas em conta. Não é uma conclusão no sentido intuitivo, mas no sentido formal fundamentado numa teoria de limites e convergência, desenvolvido muitos anos após a conhecida estória de Zenão. No entanto Zenão, sem o conhecimento de limites (desenvolvido por Cauchy em 1821), levantava discussões acerca dessas quantidades e de sua conexão com o mundo em que vivemos. Nesse caso, pode-se citar A. Alexander, que, de certa forma, traz à luz do artigo um raciocínio elaborado por Zenão:

> *Mas se os paradoxos de Zenão e o problema da incomensurabilidade provam alguma coisa, é que o sonho de um encaixe perfeito entre matemática e o mundo físico é insustentável. Na escala dos infinitamente pequenos, números não correspondem a objetos físicos, e qualquer tentativa de forçar esse encaixe conduz a paradoxos e contradições.* ([2], pp.19-20)

Nesse caso, nota-se que a palavra "soma"destina-se a operações com um número finito de parcelas. A palavra "série" refere-se ao processo em que há um número infinito de parcelas. Assim, "soma infinita" é uma expressão que pode gerar dúvidas, pois devemos lembrar a utilização de operações finitárias, em cenários não finitários.

2.4. Medidas de ângulos: graus e radianos

As medidas de ângulos em graus e em radianos são muito utilizadas. A medição em radianos é uma das medidas que muitas vezes geram confusão nos meios escolares. Um grau é $\frac{1}{360}$ de uma circunferência, isto é, uma parte de 360 numa circunferência. Um radiano é o ângulo central de uma circunferência unitária C, conforme pode ser visto na figura 5, que corresponde a um arco, cujo comprimento é igual ao raio unitário da circunferência C. A relação entre ângulos em graus e radianos é dada pela seguinte expressão:

$$2\pi \text{ radianos} \approx 360^o.$$

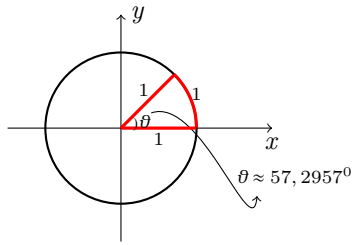


Figura 5: Ângulo θ equivalente a 1 radiano

Note-se nessa expressão que, de um lado, há o número irracional π, e do outro, o número inteiro 360^o. Isso não deixa de ser uma relação entre contínuo e discreto. Nesse caso,

$$1 \text{ radiano} \approx 57,2957^o.$$

No ensino fundamental e médio, nos tópicos sobre trigonometria e medida de ângulos, é comum utilizar medidas em radianos em vez de medidas em graus[4]. Conforme pode ser observado no artigo [35], as medidas de ângulos em graus e radianos impactam o conceito de derivadas. Ou seja, se a medida de ângulos for em graus, então a derivada da função $\operatorname{sen} x$ será $0,01753 \cos x$. Por outro lado, se a medida de ângulos for em radianos, então a derivada da função $\operatorname{sen} x$ será a função $\cos x$. Isso ocorre, pois, para que a derivada da função seno seja a função cosseno, o limite de $\frac{\operatorname{sen} x}{x}$ deve ser 1 quando x tende a zero. Mas, no caso de medida em graus, tem-se que:

$$\lim_{x \to 0} \frac{\operatorname{sen} x}{x} = \frac{\pi}{180} = 0,017453\ldots.$$

3. Medidas (e não medidas) para modelos contínuos

Nesta seção, expõem-se três exemplos. Os dois primeiros exemplos de medidas para modelos contínuos são o problema de Plateau e a medida do calor em uma barra metálica. O de Plateau é um problema com simples enunciado, de fácil intuição, no entanto de difícil solução, tanto é que sua solução está relacionada à primeira *medalha Fields* em matemática[5]. O problema de condução de calor numa barra metálica é também de "natureza" contínua e exibido no presente artigo, pois sua solução, exposta no início do século *XIX*, foi considerada formalmente correta, mas inadequada, haja vista não haver na época de sua solução ferramentas matemáticas sólidas o suficiente para garantir que as hipóteses da solução, proposta por J. Fourier (1768-1830) em 1807, fossem confirmadas. Nesses dois exemplos, ferramentas de modelos contínuos foram utilizadas para sua solução, quais sejam, equações diferenciais. O terceiro exemplo mostra a impossibilidade, no sentido físico, da implementação do conceito de medida em sua forma geral, que, de certa maneira, coloca um limite no "medir". Nesse caso, mostra-se a dificuldade em relacionar o contínuo com o discreto.

[4]Em alguns casos, utiliza-se a medida de ângulos em grados, que é a centésima parte de um ângulo reto. Isto é, uma circunferência dividida em 400 partes.

[5]J. Douglas (1897-1865) e L. V. Ahlfors (1907-1996) foram os primeiros ganhadores da medalha Fields em 1936. https://www.mathunion.org/imu-awards/fields-medal. Acesso em 8 de junho de 2021, às 17h25.

3.1. O problema de Plateau

O problema de Plateau [3] é o de encontrar uma superfície, delimitada por uma curva num espaço de três dimensões, com a menor medida de área possível. Esse problema deve-se ao físico belga J. A. F. Plateau (1801-1883), que mostrou, em 1849, que uma superfície mínima pode ser obtida quando se mergulha, por exemplo, um arame numa vasilha com água e sabão. A superfície S que se forma com a água e o sabão é a superfície com a menor área possível tendo o arame como fronteira, conforme pode ser observado na figura 6. Essa típica experiência com água e sabão, que pode ser estendida para outras formas de fronteira (que não seja apenas um arame como uma curva simples fechada), produz uma superfície em três dimensões que é a superfície de área mínima que pode ser obtida tendo o arame como fronteira.

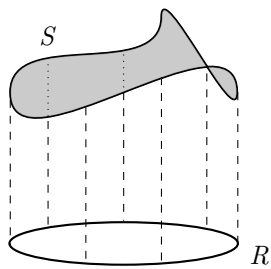


Figura 6: Exemplo de uma superfície de Plateau

Esse tipo de problema data da época de L. Euler (1707-1783) e J. L. Lagrange (1736-1813), e hoje se insere na área do Cálculo de Variações. Esse é um problema de medida que tem uma explicação intuitiva e pode ser observado de modo muito simples via experiências práticas. No entanto a demonstração da veracidade dessas experiências práticas não é trivial, muito menos simples. Ela foi exposta pelo matemático americano J. Douglas [15], e de modo independente pelo matemático húngaro-americano T. Radó (1895-1965) [25]. No caso do problema de Plateau, a medida mínima é obtida levando-se em conta o *continuum* real; caso contrário, num modelo discreto, a estimativa pode se resumir apenas à visualização da referida superfície e à intuição de que seja mínima.

3.2. Medida da temperatura em uma barra metálica

Com fins de resolver o problema de condução de calor em uma barra metálica[6], Fourier indica, em 1807, uma solução matemática formal para a equação diferencial parcial $a^2 u_{xx} = u_t$, cuja resposta [9] é:

$$u(x,t) = \sum_{n=1}^{+\infty} b_n e^{\frac{-n^2\pi^2a^2t}{L^2}} \sin\left(\frac{n\pi x}{L}\right).$$

O objetivo com sua solução é medir a temperatura $u(x,t)$ da barra em qualquer instante $t > 0$ do tempo na posição x. Considera-se que a barra tem comprimento $0 \leq x \leq L$, e leva-se em conta que $u(0,t) = 0$ e $u(L,t) = 0$ (a temperatura nas extremidades da barra mantém-se a zero grau). Considera-se ainda que existe uma distribuição inicial de temperatura na barra, $f(x) = u(x,0)$ para

[6]Problema proposto pelo Institut de France, Paris, que conferiria um prêmio a quem fornecesse a melhor solução.

$0 \leq x \leq L$, conforme pode ser observado na figura 7. Para Fourier, em sua solução, as condições iniciais deveriam satisfazer:

$$f(x) = \sum_{n=1}^{+\infty} b_n \sin\left(\frac{n\pi x}{L}\right) \quad \text{para} \quad b_n = \frac{2}{L}\int_0^L f(x)\sin\left(\frac{n\pi x}{L}\right) dx.$$

Sua solução não convenceu o júri encarregado de analisar os trabalhos que concorriam ao referido prêmio, pois, segundo eles, havia dúvidas acerca das funções que poderiam ser escritas como séries infinitas de senos e cossenos. Essas dúvidas seriam resolvidas a partir do momento em que se entendessem com mais precisão as ideias de convergência em séries e integrais. Com os desenvolvimentos de Lebesgue, em 1902, sobre um novo conceito de integral fundamentado numa teoria da medida, a solução formal de Fourier pôde ser analisada [36]. Com ela, os problemas de Fourier (fundamentados em convergências de séries e integrais) foram resolvidos. Note-se que um problema prático de condução do calor que pode ser verificado ao esquentar uma barra metálica, tal como o cabo de uma panela que vai ao fogo, precisou de quase cem anos para que sua solução fosse comprovada. Isso se deve ao fato de Lebesgue ter introduzido medidas para o trato com o *continuum* real.

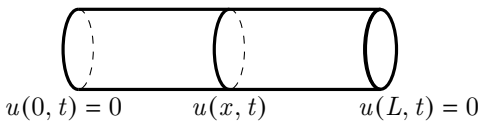


Figura 7: Barra metálica

3.3. Incerteza no medir com "régua"

Quantidades infinitamente pequenas fazem parte do dia a dia do trabalho do matemático. Aproximações são elaboradas e processos de convergência são investigados. O mesmo não se dá no mundo físico em que vivemos, haja vista que aproximações são utilizadas e análises dos erros são levadas em conta. A migração de modelos discretos para modelos contínuos, e vice-versa, implica análises cuidadosas acerca das ferramentas utilizadas e das aproximações, principalmente se o foco reside no conceito de medida.

No que concerne a discussões acerca da impossibilidade de medir distâncias muito pequenas, Brillouin ([11], p.32) indica a impossibilidade de, por exemplo, medir uma distância muito menor do que 10^{-15} cm, pois não há nenhuma "régua" disponível para medir distâncias tão pequenas. Suponha-se, segundo Brillouin, que se queira medir algo da ordem de 10^{-50} cm. O único comprimento padrão que possibilitaria levar adiante tal medida, como comparação de magnitudes, conforme consta em [11], seria o comprimento λ de uma onda eletromagnética. Note-se que, quanto menor for o comprimento de onda (maior frequência), maior será a precisão, no entanto maior será a energia cedida pela radiação em virtude da relação de M. Planck (1858-1947) entre energia e frequência da radiação

$$E = h.v,$$

em que E é a energia do fóton, h é a constante de Planck $(6,62607015\times10^{-34} J.s)$ e v é a frequência da radiação. Assim, para tal medida, levando-se em conta a comparação com o comprimento de

onda λ, tem-se:

$$E = hv = h.\frac{c}{\lambda} \approx \frac{2.10^{-16}}{10^{-50}} \approx 2.10^{34} \quad C.G.S.$$

Ainda segundo Brillouin [11], à página 32, isso representa uma quantidade de energia suficiente para destruir todo o laboratório em que a medida seria realizada, e também o planeta Terra. Desse modo, é possível inferir que, se algo não é possível de ser medido, então não deve ser levado em conta nas experiências laboratoriais. Seguindo essa linha de pensamento, pode-se conjecturar que no trabalho do matemático há estruturas em que quantidades infinitamente pequenas são utilizadas, quantidades essas que não deixam de ser abstrações que correspondem a situações físicas impossíveis ([10], p.236). Por outro lado, não há como não dizer que essas quantidades infinitamente pequenas sejam parte de desenvolvimentos matemáticos que acabam por auxiliar na criação de tecnologia,

> *O matemático define cuidadosamente os números irracionais. O físico nunca encontra esses tais números. Não importa se o que ele mede é representado por um número finito, com muitas figuras, e com uma certa quantidade de incerteza. O matemático estremece com a incerteza e tenta ignorar os erros experimentais.([11], p.33) (Tradução dos autores).*

Ainda segundo Brillouin, para o físico essas quantidades são apenas abstrações, as quais estão muito além das realizações laboratoriais. Num laboratório, a menor distância que pode ser observada é aquela que pode ser medida de acordo com a quantidade de energia disponível nesse laboratório ([10], p.236).

Desse modo, uma linguagem bem definida, bem estruturada, seja no sentido abstrato, seja no laboratorial, é parte integrante da ciência e, por mais que haja incerteza, tanto na linguagem abstrata como na laboratorial, elas acabam por se complementar. Pode-se inferir que o avanço da ciência implica a diminuição das incertezas. No caso do presente artigo, a diminuição das incertezas referentes ao conceito de medida.

4. Integrais: medir intervalos de números reais

O conceito de medida está presente na matemática dos intervalos de números reais. Com vistas a expor a relevância do conceito de medida nos intervalos de números reais, expõem-se algumas mudanças significativas que ocorreram quando pequenas alterações no trato com os intervalos de números reais indicaram alterações no desenvolvimento do conceito de integrais[7]. Nesse caso, alterações foram desenvolvidas no processo de medição com ferramentas de modelos contínuos (sentido microscópico). Há outros exemplos da matemática que podem igualmente ser mencionados, tais como os voltados à topologia, aos intervalos encaixantes, aos intervalos de Cantor etc. Nem sempre há uma designação clara acerca de como medir, nem há uma unidade representativa, haja vista que normalmente a magnitude associada à medida é um número puro, sem unidades.

4.1. Cauchy

Cauchy, em sua definição de integrais, utilizou uma partição de um intervalo $[a, b]$. Se $I = [a, b]$ é um intervalo fechado limitado em $\mathbb{R}$, então uma **partição** de I é um conjunto finito, ordenado,

[7]Nessa seção segue-se o exposto no artigo [22], bem como os livros [6, 7].

$\mathcal{P} = \{x_0, x_1, \ldots, x_{n-1}, x_n\}$ de pontos em I, tal que $a = x_0 < x_1 < x_2 < \ldots < x_n = b$ ([7], pp.199-200). Os pontos de $\mathcal{P}$ são usados para dividir $I = [a, b]$ em subintervalos fechados que não se sobrepõem,

$$I_1 = [x_0, x_1], I_2 = [x_1, x_2], \ldots, I_n = [x_{n-1}, x_n],$$

cuja união é $[a, b]$. Representa-se uma partição de $[a, b]$ por

$$\mathcal{P} = \{[x_{i-1}, x_i]\}_{i=1}^{n}.$$

Cauchy elaborou somas, para cada partição, de modo a obter a área da região limitada entre função $f(x)$ e o eixo x. Se $\mathcal{P} = \{[x_{i-1}, x_i]\}_{i=1}^{n}$ é uma partição de $[a, b]$, então a **soma de Cauchy** de uma função contínua $f : [a, b] \to \mathbb{R}$ correspondente a $\mathcal{P}$ é o número

$$S(f; \mathcal{P}) = \sum_{i=1}^{n} f(x_{i-1})(x_i - x_{i-1}).$$

Para cada retângulo que será parte da área da região sob a curva $f(x)$, Cauchy utilizou $(x_i - x_{i-1})$ como base do retângulo e lançou mão de $f(x_{i-1})$ (os pontos x_{i-1} à esquerda de cada subintervalo I_i da partição de $[a, b]$) como sua altura. Pode-se escrever que Cauchy utilizou uma "régua", conforme pode ser observado na figura 8, com uma escala limitada. Com base nisso, escreve que uma função contínua $f : [a, b] \to \mathbb{R}$ é dita ser **Cauchy integrável** em $[a, b]$, se existe um número $L \in \mathbb{R}$, em símbolos $C\int_a^b f(x)dx = L$, tal que para cada $\varepsilon > 0$ existe um $\delta > 0$ tal que se $\mathcal{P}$ é uma partição de $[a, b]$ com $||\mathcal{P}|| < \delta$, então

$$|S(f; \mathcal{P}) - L| < \varepsilon.$$

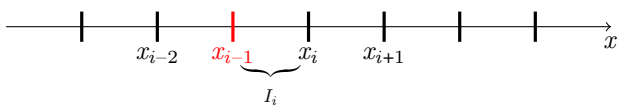


Figura 8: "Régua" de Cauchy

4.2. Riemann

As somas de Cauchy consideram, em cada subintervalo de uma partição, o valor da esquerda, x_{i-1}, do subintervalo $[x_{i-1}, x_i]$ como argumento da função f. Por outro lado, B. Riemann (1826-1866) aprofunda os estudos sobre a classe de funções integráveis e, em vez de escolher, em cada partição, o valor x_{i-1} (tal como fez Cauchy), escolhe um valor qualquer, ou seja, considera um valor $t_i \in [x_{i-1}, x_i]$. A "régua" de Riemann, conforme pode ser observado na figura 9, é, com abuso de linguagem, bem semelhante às que utilizamos no dia a dia.

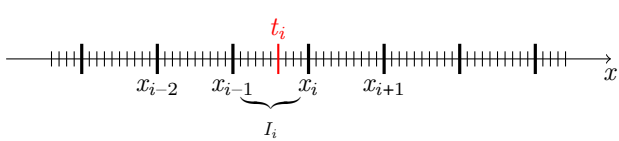


Figura 9: "Régua" de Riemann

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

Essa flexibilidade permite estabelecer condições necessárias e suficientes para a existência de uma integral. Riemann aprimorou a régua utilizada por Cauchy e em sua régua escalas mais diversificadas eram permitidas, quaisquer pontos num intervalo podem ser utilizados. Se $\mathcal{P} = \{[x_{i-1}, x_i]\}_{i=1}^n$ é uma partição do intervalo $I = [a, b]$, uma **etiqueta** é um ponto $t_i \in I_i = [x_{i-1}, x_i]$, para $i = 1, 2, \ldots, n$. Uma **partição etiquetada** de $I = [a, b]$ é um conjunto de pares ordenados

$$\dot{\mathcal{P}} = \{([x_{i-1}, x_i], t_i)\}_{i=1}^n$$

de subintervalos I_i e suas respectivas etiquetas t_i. Se $\dot{\mathcal{P}} = \{([x_{i-1}, x_i], t_i)\}_{i=1}^n$ é uma partição etiquetada, então a **soma de Riemann** de uma função $f : [a, b] \to \mathbb{R}$ correspondente a $\dot{\mathcal{P}}$ é o número

$$S(f; \dot{\mathcal{P}}) = \sum_{i=1}^{n} f(t_i)(x_i - x_{i-1}).$$

Uma função $f : [a, b] \to \mathbb{R}$ é dita ser **Riemann integrável** em $[a, b]$ se existe um número $L \in \mathbb{R}$, em símbolos $\mathcal{R}\int_a^b f(x)\,dx = L$, tal que, para cada $\varepsilon > 0$, existe um $\delta > 0$ tal que, se $\dot{\mathcal{P}}$ é uma partição etiquetada de $[a, b]$ com $||\dot{\mathcal{P}}|| < \delta_\varepsilon$, então

$$|S(f; \dot{\mathcal{P}}) - L| < \varepsilon.$$

4.3. Kurzweil e Henstock

Ainda com fins de aumentar a classe de funções integráveis, e quiçá inovar nas possibilidades de medir todos os subconjuntos de $\mathbb{R}$ [32], J. Kurzweil e R. Henstock (1923-2007) desenvolvem uma "régua", ao estilo de Riemann, mas com escalas flexíveis. Nessa nova "régua", que inclui a "régua" de Riemann, as escalas de medida podem ser ajustadas de acordo com o que se vai medir. Para isso utiliza o termo calibre [7]. Uma função **calibre** em um intervalo $I = [a, b]$ é uma função estritamente positiva definida em I. Se δ é um calibre em I, então uma partição **etiquetada** $\dot{\mathcal{P}}$ de $[a, b]$, em que $I_i = [x_{i-1}, x_i]$ e t_i é uma etiqueta de I_i, é dita ser δ–**fina** se

$$t_i \in I_i \subseteq [t_i - \delta(t_i), t_i + \delta(t_i)] \text{ para } i = 1, 2, \ldots, n.$$

Uma função $f : [a, b] \to \mathbb{R}$ é dita ser **Kurzweil-Henstock integrável** [6, 7], em $[a, b]$ se existe um número $L \in \mathbb{R}$, em símbolos $\mathcal{KH}\int_a^b f(x)\,dx = L$, tal que, para cada $\varepsilon > 0$, existe um calibre $\delta_\varepsilon > 0$ em $[a, b]$, tal que, se $\dot{\mathcal{P}}$ é qualquer partição δ_ε–fina de $[a, b]$, então

$$|S(f; \dot{\mathcal{P}}) - L| < \epsilon.$$

Do mesmo modo que, com simples alterações na "régua" utilizada por Cauchy, Riemann expandiu sua classe de funções integráveis, as integrais de Kurzweil-Henstock foram expandidas graças também a simples alterações na "régua" utilizada por Riemann, tal como pode ser observado na figura 10. Nela nota-se que, de acordo com o calibre δ_ε, as escalas na régua alteram-se em tamanho.

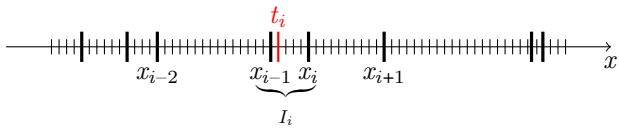


Figura 10: "Régua" de Kurzweil-Henstock

Note-se a importância que o conceito de medida tem no desenvolvimento da matemática, haja vista que pequenas alterações na "régua" utilizada para "medir" intervalos de números reais acarretaram profundas alterações na classe das funções integráveis. Há ainda as medidas (e teoria da medida) de Lebesgue [18, 5], não tratadas neste artigo, que de modo análogo impactaram significativamente muitos ramos da matemática.

O objetivo da discussão sobre as medidas em intervalos de números reais e o conceito de integrais relacionam-se também com a próxima seção, que indicará como o conceito de medida pode também ser caracterizado como medida de quantidade de informação. Como será exibido na próxima seção, a diferença entre medir informação para modelos discretos e modelos contínuos reside na utilização, *grosso modo*, do sinal de somatório $\sum$ para modelos discretos e do sinal de integral $\int$ para modelos contínuos. Ou seja, a existência de medidas de informação para o caso contínuo envolve a existência de integrais, e, por conseguinte, a existência de funções integráveis. Ou seja, a "ponte" entre o discreto e o contínuo, no quesito "medida de informação", passa pelo conceito de integral.

5. Medidas de informação discreta e contínua

É bem plausível escrever que a palavra "medir" esteja relacionada à utilização de alguma régua, de alguma escala numérica, para medir alguma coisa. É o caso também da medida de informação, ou medidas de incerteza, desenvolvidas por Shannon [31]. Shannon indicou uma medida de informação, denominou-a de entropia, para um modelo matemático de comunicação, a qual é essencial na caracterização da era digital, nos tempos atuais. Os processos de comunicação valem-se de sinais, contínuos ou discretos, que são transmitidos (codificados e decodificados) por canais de comunicação (fios, antenas, cabos etc). Shannon tratou da comunicação entre dois pontos levando em conta a existência de ruídos (interferências no canal de comunicação). Os modelos de comunicação, no sentido da entropia de Shannon, podem ser lidos de acordo com os conceitos da área de engenharia, levando-se em conta sinais, recepção, emissão, redundância, codificação, decodificação, filtro, canais etc.

Ao se levar em conta que a entropia "mede" a quantidade de informação, então essa propensa "régua" precisa de ajustes ao lidar com medidas em modelos discretos e contínuos. Para modelos discretos tem-se a entropia discreta, para modelos contínuos tem-se a entropia diferencial. Note-se que, nos modelos contínuos, a entropia diferencial de Shannon não compartilha das mesmas leituras que a dos modelos discretos. Ou seja, há propriedades da entropia discreta que não valem na entropia diferencial. *Grosso modo*, no caso da medida de informação, entropia discreta e diferencial não compartilham da mesma "régua". No entanto, ao se fazer uma extensão para o caso de duas variáveis aleatórias contínuas, X e Y, então a medida da informação mútua $I(X;Y)$ compartilha de propriedades comuns ao caso discreto ([26], p.269), ([4], p.236) e [24]. Ou seja, há propriedades da entropia diferencial que valem para o caso discreto, mas não valem para o caso contínuo, e há propriedades da informação mútua que valem para ambas. Isso acaba por

possibilitar outras leituras, e aplicações, da entropia diferencial, em áreas que não a da teoria da informação [24].

5.1. Modelos discretos

Em seu artigo de 1948 [31], Shannon utilizou probabilidades para caracterizar uma medida de incerteza ou, como é comumente escrito, uma medida de informação. Shannon trabalhou com a estrutura da informação como sendo derivada de considerações estatísticas, não levando em conta aspectos semânticos, valores ou significados relacionados à palavra informação. Quanto maior a incerteza *a priori* associada a um experimento, maior será a quantidade de informação (incerteza eliminada após o experimento). A seguinte fórmula, para símbolos $x_1, x_2, \ldots, x_i, \ldots, x_m$ com respectivas probabilidades *a priori*

$$p(x_1) = p_1, p(x_2) = p_2, \ldots, p(x_i) = p_i, \ldots, p(x_m) = p_m,$$

representa a quantidade de informação por símbolo:

$$H(p_1, p_2, \ldots, p_m) = -K \sum_{i=1}^{m} p_i \ln p_i.$$

A constante K determina a unidade dessa informação. Se o alfabeto é binário, então $K = \frac{1}{\ln 2} = \log_2 e$, e daí se pode escrever que a quantidade de informação é medida em bits.

$$H(p_1, p_2, \ldots, p_m) = -\frac{1}{\ln 2} \sum_{i=1}^{m} p_i \ln p_i = -\log_2 e \sum_{i=1}^{m} p_i \left(\frac{\log_2 p_i}{\log_2 e} \right)$$

$$= -\sum_{i=1}^{m} p_i \log_2 p_i \quad \frac{\text{bits}}{\text{símbolo}}.$$

Se cada símbolo consome um tempo t em segundos, então se tem a medida em $\frac{\text{bits}}{\text{segundos}}$.

No caso em que se tem eventos equiprováveis $p_1 = p_2 = \frac{1}{2}$, tal como no lançamento de uma moeda "honesta", então

$$H(p_1, p_2) = -\sum_{i=1}^{2} p_i \log_2 p_i = -\sum_{i=1}^{2} \frac{1}{2} \log_2 \frac{1}{2} = -\left(\frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{2} \log_2 \frac{1}{2} \right) = 1.$$

Ou seja, a medida da quantidade de informação no lançamento de uma moeda é 1 bit.

Shannon generalizou sua fórmula de entropia para variáveis aleatórias discretas,

$$X = \{x_1, x_2, \ldots, x_i, \ldots, x_m\},$$

com $p(x_i) = p_i$ para $1 \leq i \leq m$ e $\sum_{i=1}^{m} p_i = 1$. Para um alfabeto binário,

$$H(X) = -\sum_{i=1}^{m} p(x_i) \log_2 p(x_i)$$

é a fórmula de **entropia discreta** de Shannon, e denota uma medida de quantidade de informação.

5.2. Modelos contínuos

A transmissão de informações pode se dar por meio de símbolos discretos, ou por sinais contínuos, ou por ondas elétricas, ou como uma função contínua em relação ao tempo, estabelecida num intervalo $t \in [a, b]$. Nesse intervalo a amplitude do sinal assume valores contínuos com base numa função de densidade de probabilidade ([26], p.267). Tal como em outros setores da matemática, a mudança de discreto para contínuo exige cuidado. No caso da fórmula de entropia para modelos discretos, $H(X) = -\sum_{i=1}^{m} p(x_i) \log_2 p(x_i)$, sua extensão para o caso contínuo é dada pela **entropia diferencial**, em que $f(x)$ é uma função densidade de probabilidade,

$$h(X) = -\int_{-\infty}^{+\infty} f(x) \log_2 f(x)\, dx.$$

Em consonância com o que tem sido exposto neste artigo, $H(X)$ tem propriedades que $h(X)$ não tem. Ou seja, enquanto $H(X)$ é positiva, $h(X)$ pode ser negativa ("informação negativa"), infinita ("quantidade infinita de informação") ou mesmo positiva. Isso indica que, para modelos contínuos, $h(X)$ não pode ser considerada, de imediato, como uma medida de informação, a menos que restrições apropriadas sejam indicadas [28].

5.3. Entropia diferencial $h(X)$ negativa

Nesta seção o objetivo é exibir um exemplo em que a entropia diferencial pode ser negativa. No caso em que X é uma variável aleatória discreta que pode assumir os valores $x_1, x_2, \ldots, x_n$, com respectivas probabilidades $p(x_1) = p_1, p(x_2) = p_2, \ldots, p(x_n) = p_n$, tal que $\sum_{i=1}^{n} p_i = 1$, a entropia $H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$ é sempre um número não negativo, haja vista que a função $x \log_2 x$ é negativa para valores entre 0 e 1, conforme pode ser observado na figura 11.

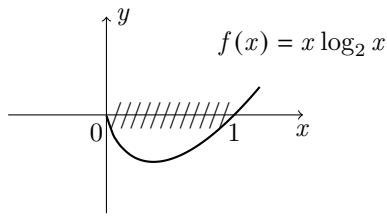


Figura 11: Função logarítmica $y = x \log_2 x$

Já para o caso de uma variável aleatória contínua X, com função densidade de probabilidade $f(x)$, a seguinte condição deve ser satisfeita:

$$\int_{-\infty}^{+\infty} f(x)\, dx = 1.$$

Essa condição é análoga à condição $\sum_i p_i = 1$ em variáveis aleatórias discretas. A construção de exemplos em que se tenha a entropia negativa leva em conta a determinação de uma função

$f(x) \geq 0$, cuja área no plano xy seja 1, de acordo com a variação de alguns parâmetros. Por exemplo, para números reais $a, h \geq 0$, seja $f(x) = \frac{h}{a}x$ se $0 \leq x \leq a$, conforme pode ser observado na figura 12. Note-se que os infinitos valores de a e h que satisfazem $\frac{ah}{2} = 1$ implicam que a área hachurada A será igual a 1 (como é o caso quando $a = 1$ e $h = 2$). Entende-se então que há valores de a e h tais que $\frac{ah}{2} = 1$ e que, ao assumir, como hipótese, que a área da região A vale 1, tem-se então que $A = \frac{ah}{2} = 1$.

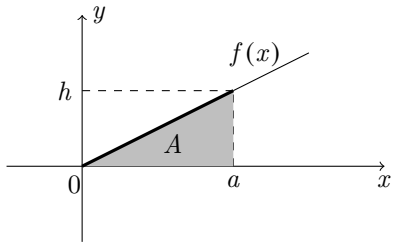


Figura 12: Função densidade de probabilidade $f(x) = \frac{hx}{a}$.

Com base nessa definição da função f, mostra-se que ela é uma função densidade de probabilidade, ao mostrar que $\int_{-\infty}^{+\infty} f(x) = 1$ e que $f(x) \geq 0$. A função f é maior ou igual a zero por construção. Resta então mostrar que

$$\int_{-\infty}^{+\infty} f(x) = 1.$$

$$\int_{-\infty}^{+\infty} f(x)\,dx = \int_0^a \frac{hx}{a}\,dx = \left[\frac{hx^2}{2a}\right]_0^a = \left[\frac{ha^2}{2a} - 0\right] = \frac{ha}{2}.$$

Como, por hipótese, a área $A = \frac{ah}{2} = 1$, tem-se então que

$$\int_{-\infty}^{+\infty} f(x)\,dx = \frac{ah}{2} = 1,$$

e $f(x)$ é uma função densidade de probabilidade.

Com base nessa função $f(x)$, que é uma função densidade de probabilidade, torna-se possível determinar o valor de $h(X)$. Assim, ao considerar, sem perdas de generalidade, que o logaritmo é expresso na base e, tem-se:

$$h(X) = -\int_{-\infty}^{+\infty} f(x)\log f(x)\,dx = -\int_{-\infty}^{+\infty} \frac{h}{a}x\log\frac{h}{a}x dx.$$

Ao fazer a substituição $u = \frac{hx}{a}$, tem-se que $du = \frac{h}{a}dx$. Logo,

$$h(X) = -\int_{-\infty}^{+\infty} u\log u\left(\frac{h}{a}\right)du = -\frac{h}{a}\int_{-\infty}^{+\infty} u\log u du = -\frac{h}{a}\int_0^a u\log u du.$$

$$= \frac{h}{a}\left[\frac{u^2}{2}.\log u - \frac{u^2}{4}\right]_0^a = \frac{h}{a}\left[\frac{a^2}{2}.\log a - \frac{a^2}{4} - 0\right] = \frac{ah}{2}\log a - \frac{ah}{4}.$$

Portanto,

$$h(X) = \frac{ah}{2}\left[\log a - \frac{1}{2}\right].$$

Como, por hipótese, tem-se que $\frac{ah}{2} = 1$, então o valor de $\log a - \frac{1}{2}$ determinará o valor de $h(X)$. Por exemplo, se $a = \sqrt{2}$, então

$$h(X) = \frac{ah}{2}\left[\log a - 1\right] = 1.\left[\log\sqrt{2} - 1\right] = 0,3465 - 0,5 = -0,1534 < 0.$$

Ou seja, $h(X) < 0$.

Assim, levando-se em conta que o logaritmo é expresso na base e, tem-se:

- Se $a = \sqrt{e}$, então $h(X) = 0$.

$$\log a - \frac{1}{2} = 0 \quad \Rightarrow \quad \log a = \frac{1}{2} \quad \Rightarrow \quad a = e^{\frac{1}{2}} \quad \Rightarrow \quad a = \sqrt{e}.$$

- Se $a < \sqrt{e}$, então $h(X) > 0$.

$$\log a - \frac{1}{2} < 0 \quad \Rightarrow \quad \log a < \frac{1}{2} \quad \Rightarrow \quad a < e^{\frac{1}{2}} \quad \Rightarrow \quad a < \sqrt{e}.$$

- Se $a > \sqrt{e}$, então $h(X) < 0$.

$$\log a - \frac{1}{2} > 0 \quad \Rightarrow \quad \log a > \frac{1}{2} \quad \Rightarrow \quad a > e^{\frac{1}{2}} \quad \Rightarrow \quad a > \sqrt{e}.$$

A entropia diferencial $h(X)$ pode ser nula, positiva ou negativa. Ou seja, enquanto no caso discreto a quantidade de informação $H(X)$ é um número positivo ou nulo, no caso contínuo $h(X)$ pode ser nula, positiva ou negativa. Isso mostra que a "medida de informação" para o caso contínuo é diferente da medida de informação para o caso discreto.

5.4. A informação mútua $I(X;Y)$.

Nesta seção, sem pretensões de completude na exposição, expõe-se, com base em referências bibliográficas, o conceito de informação mútua. Para o caso discreto, tal como pode ser observado em [26], [4] ou [14], a informação mútua pode ser expressa como

$$I(X;Y) = H(X) - H(X|Y).$$

Nesse caso, tanto $H(X)$ quanto a entropia condicional $H(X|Y)$ são positivas ou nulas. Daí, $I(X;Y) \geq 0$ para o caso discreto. Para o caso contínuo, a informação mútua $I(X;Y)$ tem propriedades semelhantes à da entropia discreta, isto é, é maior ou igual a zero. Para verificar essa condição, consideram-se duas variáveis aleatórias contínuas, a variável aleatória contínua X e a variável aleatória contínua Y. Considera-se também uma função densidade de probabilidade conjunta $f(x,y)$, tal que $\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\,dxdy = 1$. Assim, conforme pode ser observado em [26], à

página 276, tem-se que:

$$I(X;\,Y) = -\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\log\frac{f(x,y)}{f_X(x)f_Y(y)}\,dxdy$$

$$I(X;\,Y) = -\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\log\frac{f_X(x)}{f(x|y)}\,dxdy$$

$$\geq -\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\left[\frac{f_X(x)}{f(x|y)}-1\right]\log e\;dxdy$$

$$= -\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f_Y(y)f_X(x)\log e\;dxdy + \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\log e\;dxdy$$

$$= 1.1.\log e - \log e = 0.$$

Portanto, $I(X;\,Y) \geq 0$.

Desse modo, mostrou-se que, enquanto a entropia diferencial $h(X)$ e a entropia discreta $H(X)$ sofrem alterações na medida da quantidade de informação quando se alteram os modelos de discreto para contínuo, a informação mútua, isto é, a informação que transita pelo canal de comunicação, se mantém-se inalterada. Ou seja, a medida de ambas é não negativa. Essa é uma propriedade que reside na intersecção dos modelos discretos e contínuos.

6. Conclusões

Na matemática, vista como uma linguagem composta de estruturas e objetos [17], não somente abstrações são possíveis, mas também uma abertura total para processos imaginativos que permitem a criação de estruturas adaptadas aos, por exemplo, processos de medição. Isso não assegura que todos esses processos tenham uma contraparte presente na realidade do mundo em que vivemos. Ou seja, não há uma regra específica que indique quais devam ser os desenvolvimentos que não sejam apenas uma multiplicação de estruturas matemáticas, e quais os que impactam a construção de novas tecnologias. Não há também como indicar impedimentos nesses desenvolvimentos. O conceito de medida, a noção intuitiva de medir alguma coisa, apresenta-se na história da humanidade e vem se desenvolvendo ao longo dos tempos. Medidas na época de G. Galilei (1564-1642) são muito distintas das medidas nos tempos atuais. Isso não significa que se está no ápice do estado da arte dos processos de medição. Tal como indicado por Brillouin, a menor distância possível a ser medida depende da quantidade de energia à disposição no laboratório em que a medida será realizada. Isso revela que novos desenvolvimentos podem ser feitos de modo a diminuir as incertezas, aumentar as precisões no quesito "medida", como por exemplo, a clássica e fantástica história da definição da medida "metro", na França, em 1792 [1], que impactou os sistemas de medida ao redor do mundo. Neste artigo, exemplos foram exibidos com vistas a mostrar que há oscilação, em relação ao conceito de medida, entre as leituras advindas de ferramentas discretas para modelos contínuos e leituras advindas de ferramentas contínuas para modelos discretos. Mostrou-se que há casos em que, mesmo que a leitura seja descuidada, o resultado é equivalente, haja vista a utilização de uma ferramenta que serve aos dois propósitos, quais sejam, a medida em modelos discretos e nos contínuos.

Há também contradições, ao se limitar a leitura ao "mundo discreto" quando o objetivo é observar o "mundo contínuo". Como exemplo, pode-se citar a importância de ter leituras atentas a propriedades advindas do *continuum* real. Atenção deve-se ter, por exemplo, para não concluir que

o conjunto $\mathbb{R}$ é "maior" que um intervalo dele mesmo[8]. Isso pode levar a contradições, se uma atenção maior não for empregada à distinção entre o todo e a parte. Ou seja, esse é um exemplo de uma leitura do mundo macroscópico acerca de modelos do mundo microscópico. Há também, não abordada neste artigo, a teoria da medida de Lebesgue, presente no início do século XX, e também todas as discussões acerca de medidas (não de Lebesgue), voltadas às ciências humanas, que elencam critérios de medida apropriados a cada cenário em particular. Note-se, com base na figura 13, a existência de alguns pontos-chave que impactaram (e podem ainda impactar) o conceito de medida ao longo da história da matemática.

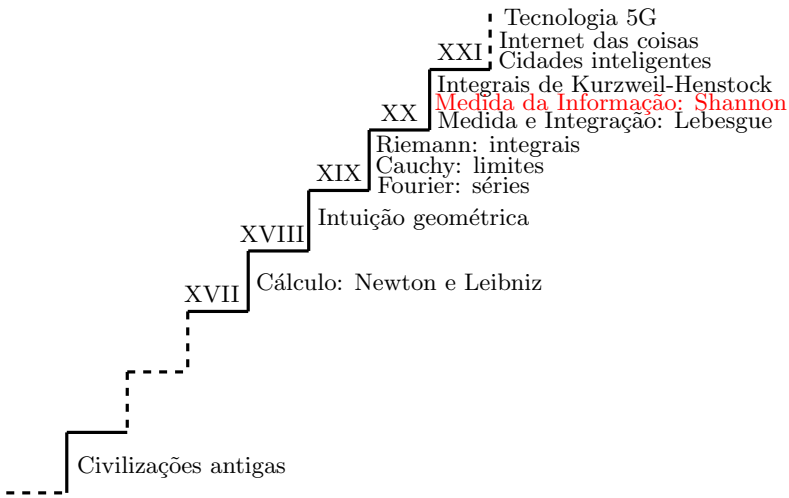


Figura 13: Evolução do conceito de medida ao longo dos séculos.

Estima-se, com este artigo, que a proposta da análise do conceito de medida em patamares discretos e contínuos, e da análise de quais são as propriedades que pertencem a ambos os patamares, possa incentivar novos desenvolvimentos e auxiliar na elucidação de equívocos, ou aparentes contradições. Em particular, estima-se que novos desenvolvimentos possam surgir das investigações acerca das medidas de informação, e das leituras operacionais possíveis, no sentido das propriedades pertencentes aos modelos discretos e contínuos. Note-se que desenvolvimentos nessa área impactam os desenvolvimentos tecnológicos que podem propiciar melhorias nas comunicações e no desenvolvimento humano, tais como tecnologia 5G, internet das coisas, cidades inteligentes etc.

Referências

[1] Alder, K. *Mesurer le monde: L'incroyable histoire de l'invention du mètre.* Traduction: Martine Devillers-Argouac'h. Éditeur Flammarion, 2015.

[2] Alexander, A. *Infinitesimal - A teoria matemática que mudou o mundo.* Jorge Zahar Editor Ltda, Rio de Janeiro, 2014.

[3] Almgren, F. J. *Plateau's Problem: An Invitation to Varifold Geometry.* American Mathematical Society (First Edition, 1966). UK Edition, 2001.

[8] Nesse caso, a função $f : \mathbb{R} \to (-1, 1)$, tal que $f(x) = \frac{x}{1+|x|}$, é uma função bijetora, ou seja, tanto $\mathbb{R}$ quanto $(-1, 1)$ têm o mesmo número de elementos, conforme exposto nos trabalhos de G. Cantor sobre teoria de conjuntos [8].

[4] Ash, R. B. *Information Theory.* Dover Publications, New York, 1990. (Originalmente publicado pela Interscience Publishers, New York, 1965).

[5] Bartle, R. G. *The Elements of Integration and Lebesgue Measure.* John Wiley & Sons, Inc., New York, 1966.

[6] Bartle, R. G. "A Modern Theory of Integration". *Graduate Studies in Mathematics*, Volume 32. American Mathematical Society, Providence, Rhode Island, 2001.

[7] Bartle, R.G.; Sherbert, D.R. *Introduction to Real Analysis*, Fourth Edition, John Wiley & Sons, New York, 2011.

[8] Belna, J. P. *Cantor.* Figuras do Saber. Tradução Guilherme João de Freitas Teixeira, Revisão Técnica Michel Paty. Editora Estação Liberdade, São Paulo, 2011.

[9] Boyce, W. E.; DiPrima, R. C. *Equações diferenciais elementares e problemas de valores de contorno.* LTC- Editora, sexta edição. Rio de Janeiro, 1998.

[10] Brillouin, L. *Science and information theory.* Dover edition, first published in 2013 (is an unabridged republication of the second edition (1962) of the work originally published in 1956 by Academic Press, Inc, New York).

[11] Brillouin, L. *Scientific Uncertainty and information.* Academic Press Inc. New York, 1964.

[12] Cauchy, A. L. *Cours d'analyse (Cours d'analyse de l'école royale polytechnique.* 1^{re} *partie: analyse algébrique.* Paris, 1821.

[13] Cauchy, A. L. *Résumé des leçons données à l'école royale polytechnique sur le calcul infinitésimal.* Vol. 1. Imprimerie royale, 1823.

[14] Cover, T. M.; Joy A. T. *Elements of Information Theory*, John Wiley & Sons, 1991.

[15] Douglas, J. *Solution of the problem of Plateau.* Transactions of the American Mathematical Society. Published by American Mathematical Society , Jan., 1931, Vol. 33, n° 1, pp. 263-321, 1931.

[16] Drabkin, I. E. *Aristotle's Wheel: Notes on the History of a Paradox.* Osiris, Vol. 9, pp. 162-198. The University of Chicago Press on behalf of The History of Science Society. 1950.

[17] Lang, S. *A First Course in Calculus.* Fifth Edition. Springer-Verlag, New York, 1986.

[18] Lebesgue, H. L. *Intégrale, longueur, aire.* Annali di Mathematica Pura ed Applicata (3), 7: 231-359, 1902.

[19] Lintz, R. G. *História da Matemática.* v. I. Blumenau: EdFURB, 1999.

[20] Luce, R. D. *The Ongoing Dialog between Empirical Science and Mesasurement Theory.* Journal of mathematical psychology 40, 7898, 1996.

[21] Magossi, J. C.; Paviotti, J. R. "Incerteza em Entropia". *Revista Brasileira de História da Ciência.* Rio de Janeiro, V.12, n° 1, pp.84-96, janeiro-junho, 2019.

[22] Magossi, J. C.; Barros, A. C. C. "O conceito de Integrais nos cursos de Cálculo". *Revista do Professor de Matemática Online.* Sociedade Brasileira de Matemática. PMO, pp.239-262, v.7, n° 2, 2019.

[23] Magossi, J. C. "O sonho de Lagrange". *Professor de Matemática Online* – PMO, Sociedade Brasileira de Matemática, v.8, n° 1, pp.43-63, 2020.

[24] Michalowicz, J. V.; Nichols, J. M.; Bucholtz, F. *Handbook of differential entropy.* CRC Press, Taylor & Francis Group, A Chapman $ Hall Book. New York, 2014.

[25] Rado, T. *On Plateau's Problem.* Published by Mathematics Department, Princeton University. Annals of Mathematics , Jul., 1930, Second Series, Vol. 31, No. 3, pp.457-469, 1930.

[26] Reza, F. M. *An Introduction to Information Theory.* McGraw-Hill, New York, 1961.

[27] Rossi, G. B. *Measurement and Probability: a probabilistic theory of measurement with applications.* Springer Series in Measurement Science and Technology. Springer, Dordrecht, 2014.

[28] Rioul, O. *Teoria da Informação e da Codificação.* Editora da Unicamp e Editora Universidade de Brasília. Campinas, 2018. (Tradução do original em francês por José Carlos Magossi).

[29] Salsburg, D. *Uma senhora toma chá... como a estatística revolucionou a ciência no século XX.* Jorge Zahar Editor Ltda, Rio de Janeiro, RJ, 2009.

[30] Scott, D.; Suppes, P. "Foundational Aspects of Theories of Measurement. Association for Symbolic Logic". *The Journal of Symbolic Logic*, Vol. 23, N° 2, pp.113-128, Jun., 1958.

[31] Shannon, C. E. "A mathematical theory of communication". *Bell System Technical Journal*, v. 27, pp.379-423, 623-656, 1948.

[32] Shenitzerand, A.; Steprian, S. *The evolution of integration.* The American Mathematical Monthly, Vol. 101, No. 1 (Jan., 1994), pp.66-72

[33] Shiryayev, A. N. *Select works of A. N. Kolmogorov. Volume III. Information theory and the Theory of Algorithms.* Springer-Science+Business Media, B.V. Dordrecht, 1993.

[34] Volken, H. "Les fondements : mesure pour mesure". Revue européenne des sciences sociales. Tome XLV, n° 138, pp.41-53, 2007. (*European Journal of Social siences*). http://journals.openedition.org/ress/192;DOI:10.4000/ress.192

[35] Watanabe, R. G. "Seno de 30 é um meio ?" *Revista do Professor de Matemática* – RPM. Número 30, pp.26-32, São Paulo, 1996.

[36] Wilcox, H. J.; Myers, D. L. *An Introduction to Lebesgue Integration and Fourier Series.* Dover Publications, New York, 1978.

[37] Yee, L. P.; Výborný, R. *The Integral: An Easy Approach after Kurzweil and Henstock.* Cambridge University Press, Cambridge, 2000.

José Carlos Magossi
Universidade Estadual de Campinas
<magossi@unicamp.br>

Vania Rosa Figueiredo Izidoro
Centro Estadual de Educação Tecnológica Paula Souza - Nova Odessa
<vania.izidoro@etec.sp.gov.br>

Recebido: 10/09/2021
Publicado: 17/08/2022

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1029

Uma fórmula para o número de permutações circulares com repetição via ações de grupos

Guilherme F. S. Silva João A. M. Gondim

Resumo

Na Análise Combinatória que é estudada nos cursos de segundo grau e de início de faculdade, muita ênfase é dada nas permutações. São tratadas permutações lineares simples e com repetição, bem como permutações circulares de elementos distintos, mas nada é mencionado sobre permutações circulares com elementos repetidos. O objetivo deste trabalho é fornecer uma referência em língua portuguesa para uma fórmula usada para tal problema, assim como sua demonstração, a qual passa pela Teoria de Ações de Grupos e pelo Lema de Burnside. Esses tópicos são, também, tratados de forma resumida ao longo deste texto para efeito de completude.

Palavras-chave: Permutações circulares com repetição; Ações de grupos; Lema de Burnside.

Abstract

In the Combinatorics studied in high school and in the early stages of college, a lot of emphasis is given to permutations. Linear permutations with either distinct or repeated elements are treated, as well as circular permutations with distinct elements, but nothing is mentioned regarding circular permutations with repeated elements. The goal of this work is to provide a reference in Portuguese for a formula that can be used in this problem, accompanied by its demonstration, which relies on the Theory of Group Actions and Burnside's Theorem. These topics are also briefly treated in this paper for completeness purposes.

Keywords: Circular permutations with repetitions; Group actions; Burnside's Lemma.

1. Introdução

Permutações são um dos principais conteúdos de Análise Combinatória estudados no Ensino Médio. Inicialmente, aprendemos que o número de formas de se ordenar n objetos distintos é n! e chamamos cada uma dessas ordenações de uma *permutação simples* dos n objetos. Em seguida, consideramos permutações com elementos repetidos, sendo β_i elementos do tipo i, $i \in \{1, \ldots, \ell\}$, com

$$\beta_1 + \ldots + \beta_\ell = n.$$

Nesse caso, o número de permutações desses n objetos é dado por

$$\frac{n!}{\beta_1! \cdot \ldots \cdot \beta_\ell!}.$$

Finalmente, os primeiros estudos de permutações costumam ser encerrados tratando das permutações circulares. Se n objetos distintos estão dispostos ao longo de um círculo, então as n! permutações simples acima contam cada uma das ordenações circulares n vezes, uma vez que, escolhida uma das posições, podemos girar o círculo e colocar qualquer um dos n objetos nessa posição. Assim, o número de permutações circulares de n objetos distintos é $(n-1)!$.

Todos esses conteúdos são tratados com profundidade em uma vasta literatura em português, da qual podemos destacar [1], [2] e [3]. No entanto, não há referências sobre permutações circulares com repetição. Seguindo a mesma linha de raciocínio dos casos acima, poderíamos imaginar que bastaria dividir o número de permutações lineares com as mesmas repetições de objetos por n, mas o seguinte exemplo mostra que esse raciocínio está incorreto.

Exemplo 1. Quantas permutações circulares distintas dos elementos da sequência ●●●● existem?

Existem $\dfrac{4!}{2!2!} = 6$ permutações lineares distintas desses quatro elementos. Dessa forma, dividindo 6 pelo número de objetos, um total de quatro, obtemos um número que não é nem inteiro, o que mostra que o raciocínio anterior não funciona. Por inspeção, as duas permutações circulares distintas são as duas da Figura 1.

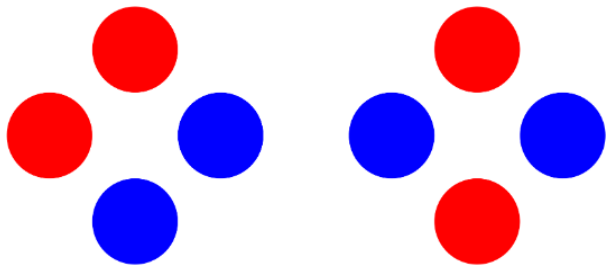


Figura 1: As duas permutações circulares distintas dos elementos ●●●●.

Como devemos proceder, então? Em [4], o autor apresenta uma fórmula. Considere n objetos de ℓ tipos distintos tais que há β_i objetos do tipo i para todo $i \in \{1, \ldots, \ell\}$. Se $\mathrm{PC}(\beta_1, \ldots, \beta_\ell)$ e $\mathrm{PL}(\beta_1, \ldots, \beta_\ell)$ são, respectivamente, os números de permutações circulares e lineares desses n objetos, sabemos que

$$\mathrm{PL}(\beta_1, \ldots, \beta_\ell) = \frac{n!}{\beta_1! \cdot \ldots \cdot \beta_\ell!}. \tag{1}$$

Então

$$\mathrm{PC}(\beta_1, \ldots, \beta_\ell) = \frac{1}{n} \sum_{d|N} \varphi(d) \mathrm{PL}\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right), \tag{2}$$

onde $N = \mathrm{mdc}(\beta_1, \ldots, \beta_\ell)$ e φ é a função totiente de Euler [5, Definição 2.6], a qual fornece o número de inteiros positivos $m \leq n$ tais que m e n são relativamente primos. De fato, no Exemplo 1 temos $\beta_1 = \beta_2 = 2$, logo $N = 2$. Os divisores de 2 são 1 e 2, portanto (2) diz-nos que

$$\mathrm{PC}(2,2) = \frac{1}{4}\left(\varphi(1)\mathrm{PL}(2,2) + \varphi(2)\mathrm{PL}(1,1)\right) = \frac{1 \cdot 6 + 1 \cdot 2}{4} = 2,$$

como queríamos.

Uma discussão mais profunda sobre problemas semelhantes a esse pode ser encontrada tanto em [6] quanto em [7]. O objetivo deste trabalho é apresentar uma demonstração para a fórmula (2). Para efeito de completude do trabalho, as principais técnicas envolvidas na argumentação são expostas nas próximas duas Seções. Primeiramente, ações de grupos são abordadas na Seção 2. Em seguida, o Lema de Burnside, principal resultado usado na prova de (2), é tratado na Seção 3. A demonstração é feita na Seção 4, a qual conclui o trabalho.

2. Grupos e Ações de grupos

Começamos esta seção com um resumo sobre os principais tópicos da Teoria de Grupos necessários para as Seções posteriores. Um grupo trata-se de conjunto G, munido de uma operação binária

$$\begin{array}{ccc} G \times G & \to & G \\ (g, h) & \mapsto & gh \end{array}$$

tal que

(i) $(g_1g_2)g_3 = g_1(g_2g_3)$ para todos $g_1, g_2, g_3 \in G$.

(ii) existe um elemento $e \in G$ (chamado *identidade*) tal que $ge = eg = g$ para todo $g \in G$.

(iii) para todo $g \in G$ existe $g^{-1} \in G$ tal que $gg^{-1} = g^{-1}g = e$.

Por exemplo, os inteiros, com a operação de adição, configuram um grupo. Um subconjunto não vazio H de um grupo G é um *subgrupo* de G se $g^{-1}h \in H$ para todos $g, h \in H$. Se H é subgrupo de G, chamamos o conjunto

$$gH = \{gh : h \in H\}$$

de *classe lateral à esquerda* de H. É sabido que as classes laterais à esquerda de um subgrupo H particionam o grupo G, e que $gH = hH$ se, e somente se, $g^{-1}h \in H$. O número de classes laterais à esquerda de H em G é chamado de *índice* de H em G e é denotado por $[G : H]$. A *ordem* de um grupo G, denotada por $|G|$, é dada pelo seu número de elementos. Quando G é finito, o Teorema de Lagrange [8, Teorema 1.2] garante que

$$|G| = [G : H]|H|.$$

Um importante conceito, fundamental para este trabalho, é definido a seguir.

Definição 1. Sejam G um grupo e X um conjunto. Uma *ação* de G sobre X é uma aplicação

$$\begin{array}{rccc} \phi : & G \times X & \to & X \\ & (g, x) & \mapsto & \phi(g, x) = g \cdot x \end{array}$$

satisfazendo

(i) $e \cdot x = x$ para todo $x \in X$, onde e é a identidade de G.

(ii) $g_1 \cdot (g_2 \cdot x) = (g_1g_2) \cdot x$ para todos $g_1, g_2 \in G$ e $x \in X$.

O leitor interessado pode encontrar ótimas introduções à Teoria de Grupos e às Ações de Grupos em [8], [9] e [10]. Nosso foco cairá sobre dois conceitos importantes que estão associados a toda ação.

Definição 2. Considere uma ação de um grupo G sobre um conjunto X. Dado $x \in X$, a *órbita* de X é o conjunto

$$\mathrm{Orb}_x = \{g \cdot x : g \in G\} \subset X.$$

O *estabilizador* de x é o conjunto

$$\mathrm{Stab}_x = \{g \in G : g \cdot x = x\} \subset G.$$

A relação das ações de grupos com esse trabalho aparece quando representamos cada permutação linear (com repetição) de n objetos como uma função

$$C : \{1, \ldots, n\} \longrightarrow \{1, \ldots, \ell\}$$

que leva cada um dos n elementos no tipo correspondente, de modo que

$$|C^{-1}(i)| = \beta_i, \quad i = 1, \ldots, \ell, \tag{3}$$

onde $C^{-1}(i)$ denota a imagem inversa de $\{i\}$ pela função C.

Seja X o conjunto de todas as funções C como acima. Vamos considerar a ação de $\mathbb{Z}_n = \{\overline{1}, \overline{2}, \ldots, \overline{n}\}$ sobre X tal que, se $\overline{k} \in \mathbb{Z}_n$ e $C \in X$, então $\overline{k} \cdot C$ é a função $\overline{k} \cdot C : \{1, \ldots, n\} \longrightarrow \{1, \ldots, \ell\}$ dada por

$$\overline{k} \cdot C(m) = C(r), \tag{4}$$

em que r é o resto da divisão de $m + k$ por n (a menos que $m + k$ seja múltiplo de n. Nesse caso, $r = n$ devido à forma como definimos $\mathbb{Z}_n$). Dessa forma, duas permutações lineares correspondem à mesma permutação circular se, e somente se, pertencerem à mesma órbita dessa ação.

Exemplo 2. Voltamos à mesma situação do Exemplo 1. Suponha que o tipo 1 corresponde a 🔴 e que o tipo 2 corresponde a 🔵. Nesse caso, o conjunto X possui seis elementos, que estão indicados na Tabela 1.

Permutação	C(1)	C(2)	C(3)	C(4)
🔴🔴🔵🔵	1	1	2	2
🔴🔵🔴🔵	1	2	1	2
🔴🔵🔵🔴	1	2	2	1
🔵🔵🔴🔴	2	2	1	1
🔵🔴🔵🔴	2	1	2	1
🔵🔴🔴🔵	2	1	1	2

Tabela 1: Uma outra maneira de representar permutações com elementos repetidos.

Observe que há apenas duas órbitas nesta ação. Uma delas é formada por 🔴🔴🔵🔵, 🔴🔵🔵🔴, 🔵🔵🔴🔴 e 🔵🔴🔴🔵, enquanto a outra é formada por 🔴🔵🔴🔵 e 🔵🔴🔵🔴. Essas órbitas correspondem às duas permutações circulares distintas desses elementos.

Basta-nos, portanto, contar o número de órbitas dessa ação, o que será feito na próxima seção. Antes disso precisaremos de mais alguns fatos sobre órbitas e estabilizadores.

Teorema 1. *Considere uma ação de um grupo* G *sobre um conjunto* X*. Então:*

(i) As órbitas da ação particionam X*.*

(ii) Para todo $x \in X$*,* $Stab_x$ *é subgrupo de* G*.*

(iii) Se $g, h \in G$ *e* $x \in X$*, então* $gStab_x = hStab_x$ *se, e somente se,* $g \cdot x = h \cdot x$*.*

(iv) Para todo $x \in X$ *vale*

$$|Orb_x| = [G : Stab_x].$$

Demonstração. Para o item (i), dado $x \in X$ temos $x = e \cdot x \in Orb_x$. Se $y \in Orb_x \cap Orb_{x'}$, então existem $g_1, g_2 \in G$ tais que $y = g_1 \cdot x = g_2 \cdot x'$. Se $g \cdot x \in Orb_x$, então $g \cdot x = g \cdot (g_1^{-1} \cdot y) = (gg_1^{-1}) \cdot y = (gg_1^{-1}) \cdot (g_2 \cdot x') = (gg_1^{-1}g_2) \cdot x' \in Orb_{x'}$, portanto $Orb_x \subset Orb_{x'}$. Analogamente, mostra-se que $Orb_{x'} \subset Orb_x$, logo duas órbitas quaisquer ou são iguais ou são disjuntas, como queríamos.

Para o item (ii), como $e \cdot x = x$, temos que $e \in Stab_x$. Se $g, h \in Stab_x$, então $g \cdot x = x$ e $h \cdot x = x$, logo $g^{-1} \cdot x = x$, e $(g^{-1}h) \cdot x = g^{-1} \cdot (h \cdot x) = g^{-1} \cdot x = x$, logo $g^{-1}h \in Stab_x$, o que prova que $Stab_x$ é subgrupo de G.

Para o item (iii), note que $gStab_x = hStab_x$ se, e somente se, $g^{-1}h \in Stab_x$, o que equivale a dizer que $(g^{-1}h) \cdot x = x$, ou seja, que $h \cdot x = g \cdot x$, como queríamos.

Finalmente, considere o mapa

$$\begin{array}{rccc} \phi: & Orb_x & \to & G/Stab_x \\ & g \cdot x & \mapsto & gStab_x \end{array}$$

Esse mapa é claramente sobrejetivo, e pelo item (iii), é injetivo, logo é uma bijeção. Daí, concluímos que

$$|Orb_x| = |G/Stab_x| = [G : Stab_x],$$

provando o item (iv).

□

Para finalizar esta seção note que, pelo item (iv) do Teorema 1 e pelo Teorema de Lagrange, podemos escrever

$$|Orb_x| = \frac{|G|}{|Stab_x|} \tag{5}$$

sempre que o grupo G for finito.

3. O Lema de Burnside

Agora que já sabemos contar quantos elementos há em cada órbita usando a equação (5), vamos determinar quantas órbitas existem.

Teorema 2 (Lema de Burnside)**.** *Dados um grupo finito* G*, um conjunto* X *e uma ação de* G *sobre* X*, o número de órbitas distintas é dado por*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|, \tag{6}$$

onde $X^g = \{x \in X : g \cdot x = x\}$ *é o conjunto dos elementos de* X *que são fixados pela ação de* $g \in G$*.*

Demonstração. Primeiramente, note que

$$\sum_{g\in G}|X^g| = |\{(g,x)\in G\times X : g\cdot x = x\}| = \sum_{x\in X}|\mathrm{Stab}_x|. \tag{7}$$

Por (5),

$$\frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}_x| = \frac{1}{|G|}\sum_{x\in X}\frac{|G|}{|\mathrm{Orb}_x|} = \sum_{x\in X}\frac{1}{|\mathrm{Orb}_x|}. \tag{8}$$

O item (i) do Teorema 1 diz-nos que as órbitas da ação particionam X. Assim, vamos reescrever a equação (8) agrupando todos os elementos de uma mesma órbita. Se $O\in X/G$, então para todo $x\in O$ tem-se $|\mathrm{Orb}_x| = |O|$. Ficamos com

$$\sum_{x\in X}\frac{1}{|\mathrm{Orb}_x|} = \sum_{O\in X/G}\sum_{x\in O}\frac{1}{|O|} = \sum_{O\in X/G}1 = |X/G|. \tag{9}$$

Combinando (7), (8) e (9) obtemos (6). □

4. A fórmula para permutações circulares com repetição

Considere n objetos de ℓ tipos distintos tais que há β_i objetos do tipo i para todo $i\in\{1,\dots,\ell\}$. Se $PC(\beta_1,\dots,\beta_\ell)$ e $PL(\beta_1,\dots,\beta_\ell)$ são, respectivamente, os números de permutações circulares e lineares desses n objetos, sabemos que

$$PL(\beta_1,\dots,\beta_\ell) = \frac{n!}{\beta_1!\cdot\ldots\cdot\beta_\ell!}.$$

Nosso objetivo nesta seção é provar a fórmula (2), isto é, que

$$PC(\beta_1,\dots,\beta_\ell) = \frac{1}{n}\sum_{d|N}\varphi(d)PL\left(\frac{\beta_1}{d},\dots,\frac{\beta_\ell}{d}\right),$$

onde $N = \mathrm{mdc}(\beta_1,\dots,\beta_\ell)$ e φ é a função totiente de Euler. Comecemos, como na Seção 2, representando cada permutação linear dos n objetos como uma função

$$C : \{1,\dots,n\}\longrightarrow\{1,\dots,\ell\}$$

que leva cada um dos n elementos no tipo correspondente, de modo que

$$|C^{-1}(i)| = \beta_i,\quad i = 1,\dots,\ell. \tag{10}$$

Seja X o conjunto de todas as funções C como acima. Vamos novamente considerar a ação de $\mathbb{Z}_n$ sobre X dada por (4), ou seja, se $\overline{k}\in\mathbb{Z}_n$ e $C\in X$, então $\overline{k}\cdot C : \{1,\dots,n\}\longrightarrow\{1,\dots,\ell\}$ dada por

$$\overline{k}\cdot C(m) = C(r), \tag{11}$$

como definida na Seção 2. Note que as permutações C_1 e C_2 pertencem à mesma órbita dessa ação se, e somente se, correspondem à mesma permutação circular dos n elementos. Basta, portanto, calcular o número de órbitas $|X/\mathbb{Z}_n|$ dessa ação, que, pelo Lema de Burnside, é dado por

$$|X/\mathbb{Z}_n| = \frac{1}{n}\sum_{\overline{k}\in\mathbb{Z}_n}|X^{\overline{k}}|. \tag{12}$$

Sejam $\overline{k} \in \mathbb{Z}_n$ e $d = |\langle \overline{k} \rangle|$, isto é, a ordem do (subgrupo gerado pelo) elemento $\overline{k}$. Se a ação de $\overline{k}$ sobre C fixa C, isto é, se $\overline{k} \cdot C = C$, então

$$C(m) = C(m+k) = C(m+2k) = \cdots = C(m+(d-1)k) \tag{13}$$

para todo $m \in \{1, \ldots, n\}$. Observe que os d elementos de $\{1, \ldots, n\}$ indicados na equação acima são distintos. Com efeito, se dois deles fossem iguais, concluiríamos que $j_1 k \equiv j_2 k \mod n$, com $j_1, j_2 \in \{0, \ldots, d-1\}$ distintos, o que contradiz o fato de d ser a ordem de $\overline{k}$ em $\mathbb{Z}_n$. Daí, segue que o número de elementos de cada tipo é sempre um múltiplo de d, portanto d divide $N = \text{mdc}(\beta_1, \ldots, \beta_\ell)$.

Afirmamos que se $|\langle \overline{k_1} \rangle| = |\langle \overline{k_2} \rangle| = d$, então $X^{\overline{k_1}} = X^{\overline{k_2}}$. Com efeito, existe apenas um subgrupo de $\mathbb{Z}_n$ com ordem d [9, Theorem 7, Section 2.3]. Dessa forma, existe $n_0 \in \mathbb{Z}$ tal que $\overline{k_1} = n_0 \overline{k_2}$, ou seja, $k_1 \equiv n_0 k_2 \mod n$, o que nos permite escrever

$$k_1 = n_0 k_2 + \alpha n,$$

com $\alpha \in \mathbb{Z}$. Com isso, se $\overline{k_2}$ fixa C, então

$$C(m + k_1) = C(m + n_0 k_2 + \alpha n) = C(m + n_0 k_2) = C(m)$$

para todo $m \in \{1, \ldots, n\}$, ou seja, $\overline{k_1}$ fixa C, de modo que $X^{\overline{k_1}} \supset X^{\overline{k_2}}$. A outra inclusão é análoga e, com ela, a afirmação está provada.

Como há exatamente $\varphi(d)$ elementos de ordem d em $\mathbb{Z}_n$ [9, Proposition 6, Section 2.3], podemos calcular a quantidade de elementos fixados pela ação de $\overline{\frac{n}{d}}$ e multiplicar esse número por $\varphi(d)$ em (12). Note que, agora, faremos a soma sobre todos os divisores de $N = \text{mdc}(\beta_1, \ldots, \beta_\ell)$, ou seja, (12) torna-se

$$|X/\mathbb{Z}_n| = \frac{1}{n} \sum_{d|N} \varphi(d) |X^{\overline{n/d}}|. \tag{14}$$

Assim, podemos direcionar nossa atenção a $k = \frac{n}{d}$. De fato, esse é o motivo de consideramos os representantes das classes em $\mathbb{Z}_n$ de 1 a n ao invés da escolha usual de 0 a $n-1$, pois isso evita termos que tratar o caso $d = 1$ separadamente. Se $C \in X^{\overline{n/d}}$ e $m \in \{1, \ldots, n\}$, temos

$$C(m) = C\left(m + \frac{n}{d}\right) = C\left(m + 2\frac{n}{d}\right) = \cdots = C\left(m + (d-1)\frac{n}{d}\right). \tag{15}$$

Na equação acima, a função C é calculada em d elementos distintos de $\{1, \ldots n\}$, os quais formam uma progressão aritmética de razão $\frac{n}{d}$ quando escritos em ordem crescente. Logo, o menor desses elementos está entre 1 e $\frac{n}{d}$.

Com isso, segue de (15) que toda função $C \in X^{\overline{n/d}}$ fica totalmente determinada pelos elementos do conjunto

$$S_d = \left\{1, 2, \ldots, \frac{n}{d}\right\},$$

pois as imagens dos demais elementos são obtidas repetindo essa sequência inicial. Basta olhar, portanto, para a restrição

$$C_d = C|_{S_d} : \left\{1, 2, \ldots, \frac{n}{d}\right\} \longrightarrow \{1, \ldots, \ell\},$$

que é tal que $|C_d^{-1}(i)| = \frac{\beta_i}{d}$, $i = 1, \ldots, \ell$. Como há $PL\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right)$ dessas funções (por (1)), segue que

$$|X^{\overline{n/d}}| = PL\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right) \tag{16}$$

e, por (14),

$$PC(\beta_1, \ldots, \beta_\ell) = \frac{1}{n}\sum_{d|N} \varphi(d) PL\left(\frac{\beta_1}{d}, \ldots, \frac{\beta_\ell}{d}\right), \tag{17}$$

como queríamos.

Referências

[1] Santos, J. P. O.; Mello, M. P.; Murari, I. T. C. *Introdução à análise combinatória*. Campinas: Editora da Unicamp, 1995.

[2] Morgado, A. C. O. M.; Carvalho, J. B. P. C.; Carvalho, P. C. P.; Fernandez, P. *Análise Combinatória e Probabilidade*. 9ª ed. Rio de Janeiro: SBM, 2006.

[3] Hazzan, S. *Fundamentos de Matemática Elementar, 5: Combinatória, Probabilidade*. 8ª ed. São Paulo: Atual, 2013.

[4] MacMahon, P. A. *Applications of a Theory of Permutations in Circular Procession to the Theory of Numbers*. Proceedings of the London Mathematical Society, v. 1, n° 1, p. 305-318, 1891.

[5] Santos, J. P. O. *Introdução à Teoria dos Números*. 3ª ed. Rio de Janeiro: Impa, 2009.

[6] Kajimoto, H., Osabe, M. *Circular and necklace permutations*. Bulletin-Faculty of Education Nagasaki University Natural Science, v. 74, 2006.

[7] Mestrovic, R. *Different classes of binary necklaces and a combinatorial method for their enumerations*. arXiv preprint arXiv:1804.00992, 2018.

[8] Martin, P. A. *Grupos, Corpos e Teoria de Galois*. São Paulo: Editora Livraria da Física, 2010.

[9] Dummit, D. S.; Foote, R. M. *Abstract Algebra*. Hoboken: Wiley, 2013.

[10] Gonçalves, A. *Introdução à Álgebra*. 5ª ed. Rio de Janeiro: Impa, 2009.

Guilherme F. S. Silva
Universidade Federal de Pernambuco
Departamento de Matemática
<guilherme.fssilva@ufpe.br>

João A. M. Gondim
Universidade Federal Rural de Pernambuco
Unidade Acadêmica do Cabo de Santo Agostinho
<joao.gondim@ufrpe.br>

Recebido: 11/03/2022
Publicado: 18/08/2022

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

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

Inteiros de Eisenstein

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

Resumo

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

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

Abstract

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

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

1. Introdução

Um *inteiro de Eisenstein* é um número complexo da forma $a + b\omega$, em que a e b são números inteiros e $\omega = (-1 + i\sqrt{3})/2$. O número complexo ω é uma raiz cúbica primitiva da unidade, isto é, $\omega^2 + \omega + 1 = 0$, já que $x^3 - 1 = (x - 1)(x^2 + x + 1)$. A outra raiz cúbica primitiva da unidade é $\omega^2 = -1 - \omega = \overline{\omega}$, onde $\overline{\omega}$ é o conjugado de ω. O conjunto formado por todos os inteiros de Eisenstein munido das operações usuais de adição e multiplicação de números complexos é um anel comutativo com unidade, o qual é denotado por $\mathbb{Z}[\omega]$. Em símbolos,

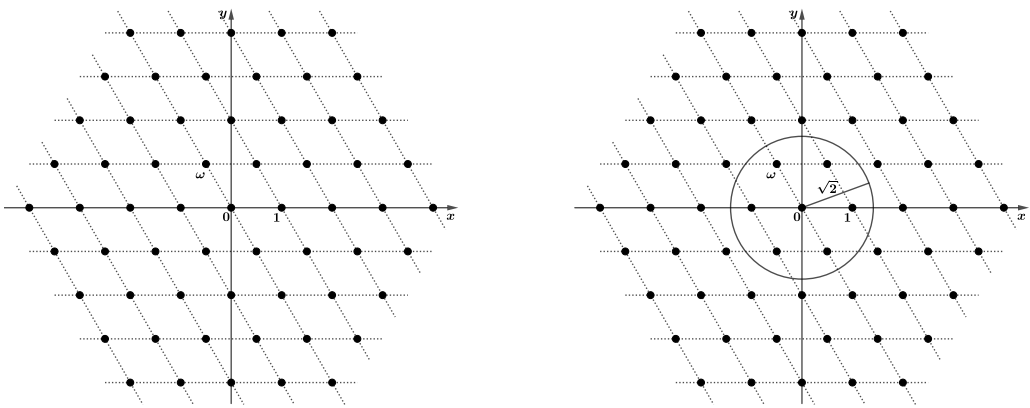
$$\mathbb{Z}[\omega] = \{a + b\omega;\ a, b \in \mathbb{Z}\}.$$

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

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

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

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



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

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

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

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

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

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

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

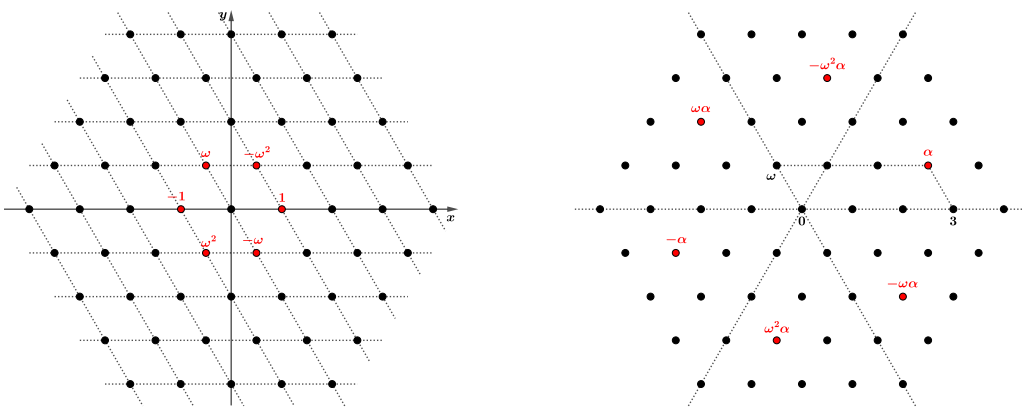
Definição 2. Um inteiro de Eisenstein α é dito *invertível* em $\mathbb{Z}[\omega]$, se existir um elemento $\beta \in \mathbb{Z}[\omega]$ tal que $\alpha \cdot \beta = 1$. Os elementos invertíveis em $\mathbb{Z}[\omega]$ também são chamados de *unidades* de $\mathbb{Z}[\omega]$, ou simplesmente de *unidades*,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

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

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

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

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



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

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

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

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

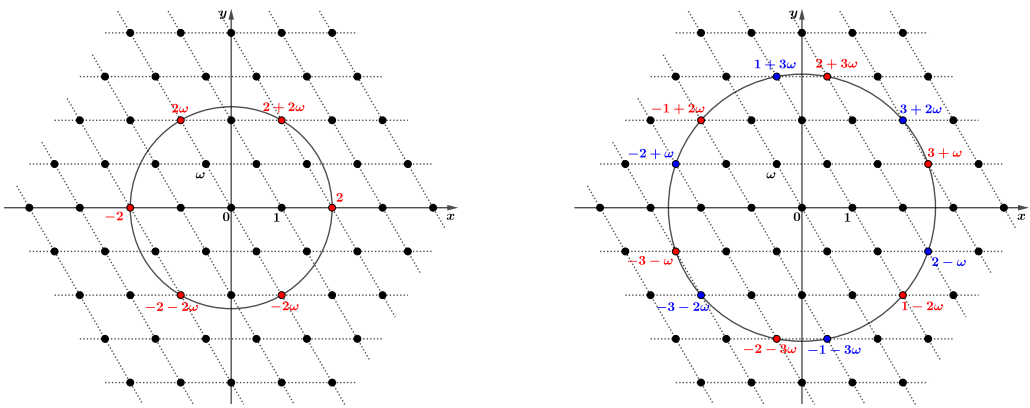
(ii) Se α *e* β *são associados, então* $N(\alpha) = N(\beta)$.

Demonstração. Consequência imediata do Teorema 2. □

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

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

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



(a) Norma igual a 4

(b) Norma igual a 7

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

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

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

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

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

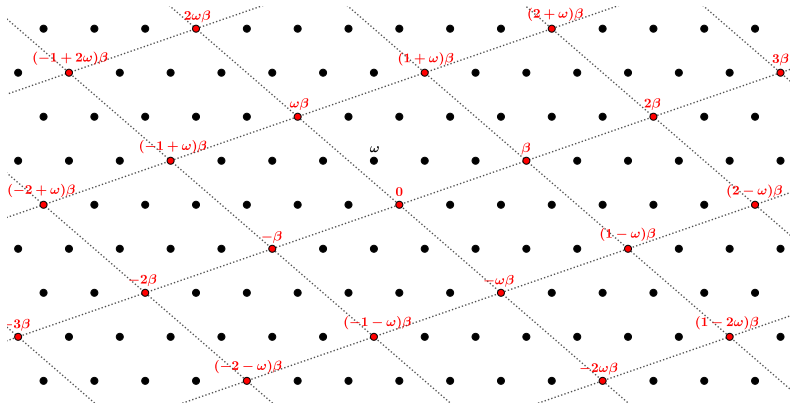


Figura 4: Múltiplos de $\beta = 3 + \omega$.

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

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

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

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

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

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

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

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

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

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

2. Teorema da Divisão

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

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

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

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

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

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

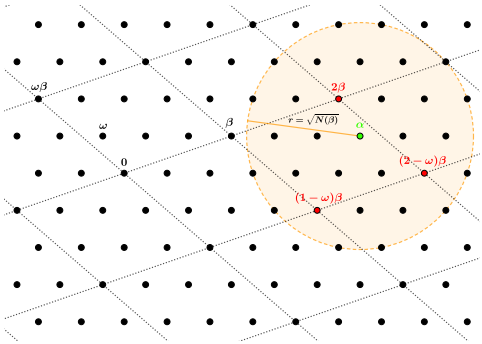
Como $\rho = \beta(\alpha/\beta - \gamma)$ e $\beta \neq 0$, segue que $\mathrm{N}(\rho) = |\rho|^2 = |\beta|^2 \cdot \left|\alpha/\beta - \gamma\right|^2 \leq 3/4 \cdot |\beta|^2 < |\beta|^2 = \mathrm{N}(\beta)$. Portanto existem $\gamma, \rho \in \mathbb{Z}[\omega]$ tais que $\alpha = \gamma\beta +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

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

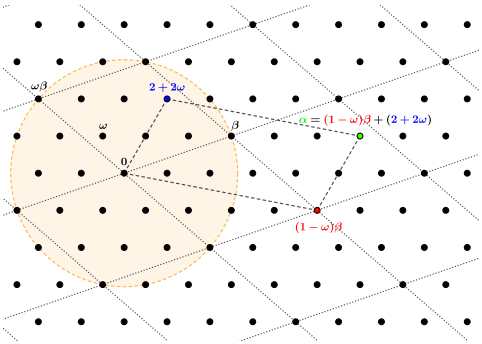
Exemplo 6. Sejam $\alpha = 6+\omega$ e $\beta = 3+\omega$. Dizer que um inteiro de Einsentein ρ satisfaz $\mathrm{N}(\rho) < \mathrm{N}(\beta)$ significa que ρ, representado no plano complexo pelo par ordenado $(\mathrm{Re}(\rho), \mathrm{Im}(\rho))$, pertence ao interior do círculo centrado na origem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

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

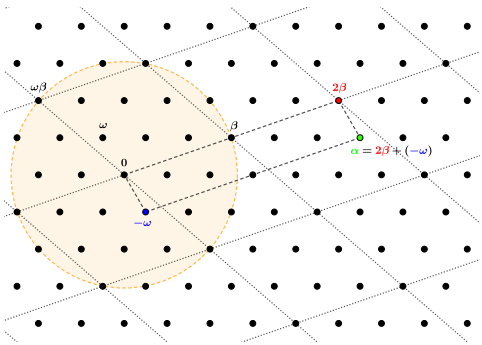
Dados inteiros de Eisenstein α e β, com $\beta \neq 0$, o Teorema 7 garante a existência de inteiros de Eisenstein γ e ρ tais que $\alpha = \gamma\beta + \rho$ e $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. No enunciado do teorema não há informação



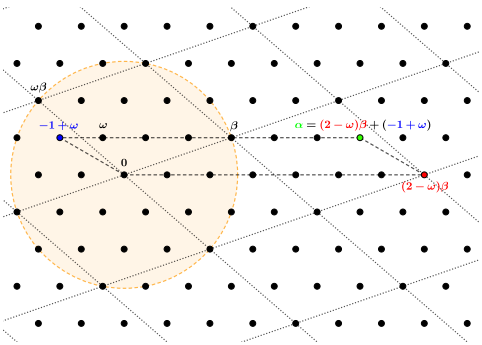
(a) Múltiplos de β próximos de α.



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



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



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

Figura 5: Divisão de α por β.

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

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

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

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

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

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

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

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

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

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

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

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

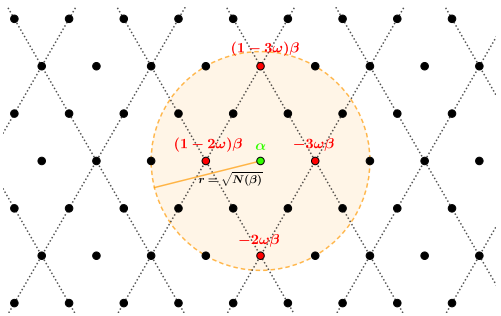


Figura 6: Múltiplos de β próximos de α

3. Algoritmo de Euclides

Iniciaremos introduzindo o conceito de máximo divisor comum.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Teorema de Bézout

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Substituindo (3) em (4), obtemos

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

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

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

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

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

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

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

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

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

5. Primos de Eisenstein

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Demonstração. Ver ([2], Página 31). □

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

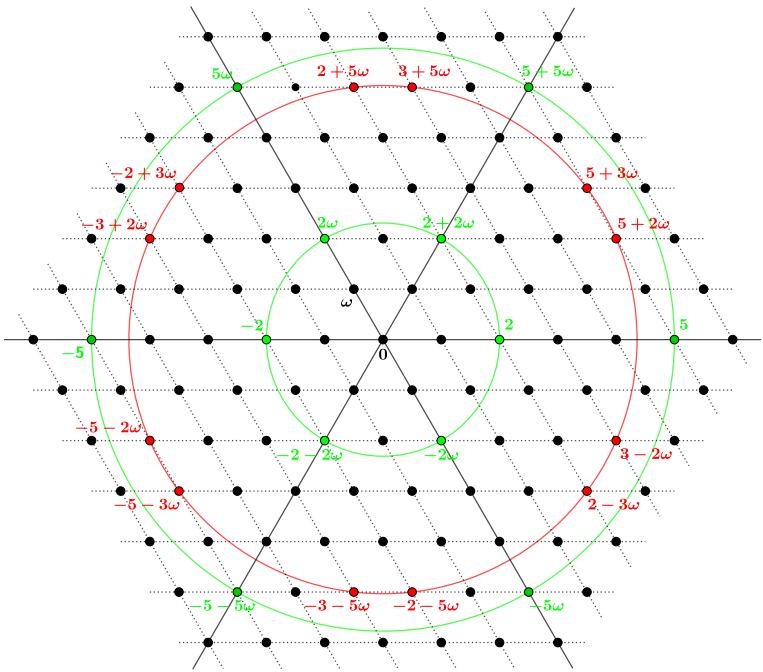


Figura 7: Primos de Eisenstein de norma igual a $4, 19$ e 25.

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

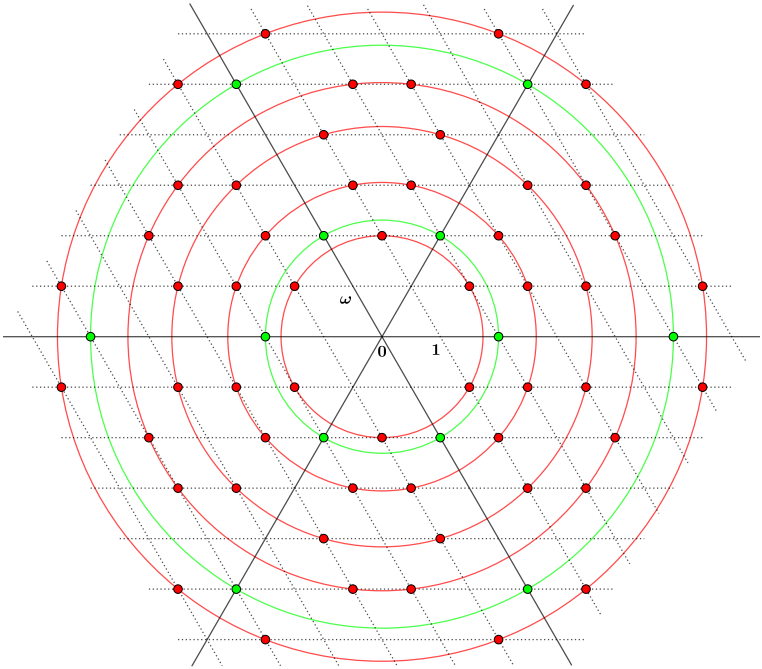


Figura 8: Primos de Eisenstein de norma menor ou igual a 31.

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

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

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

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

foi discutido acima.

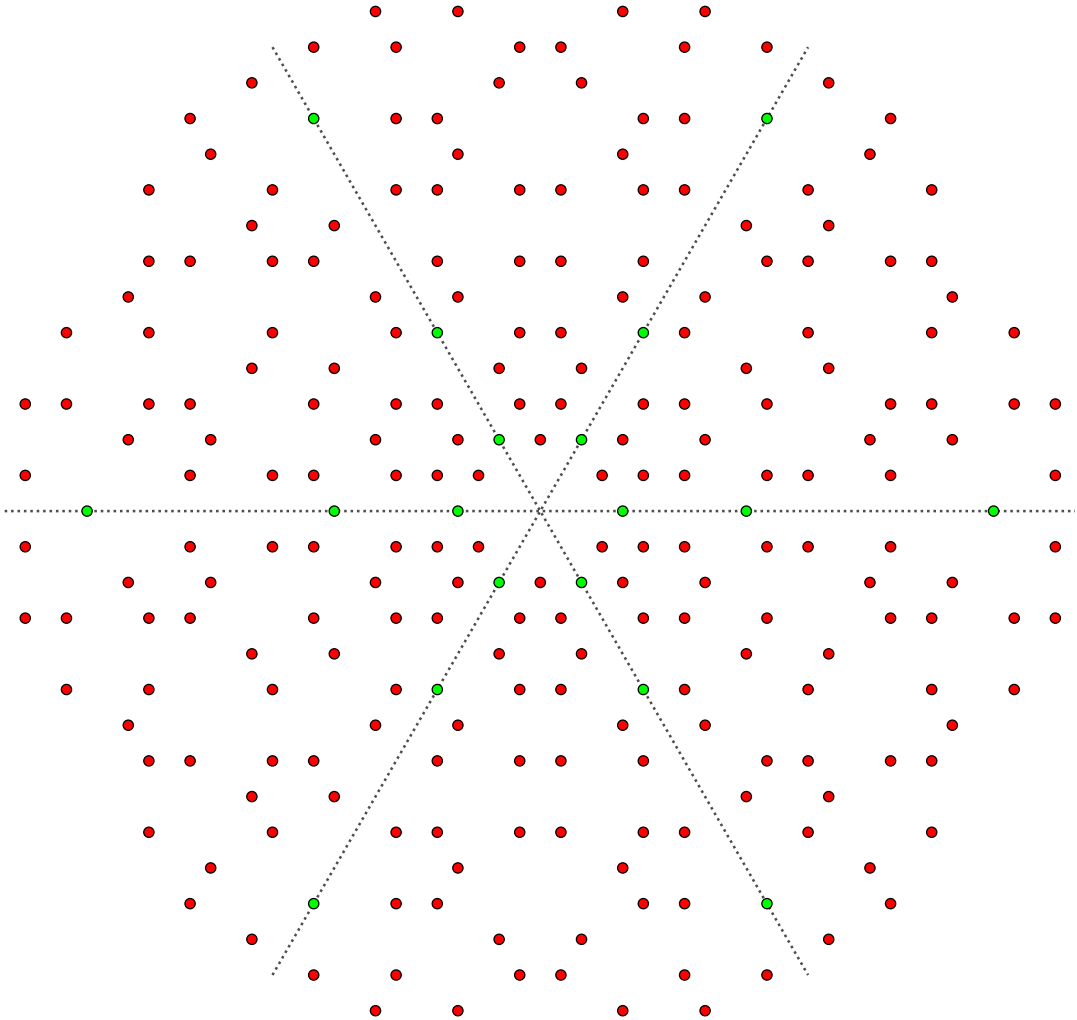


Figura 9: Primos de Eisenstein de norma menor ou igual a 169

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

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

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

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

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

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

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

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

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

6. Fatoração Única

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

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

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

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

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

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

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

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

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

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

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

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

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

Exemplo 19. O número de soluções da equação diofantina $x^2 - xy + y^2 = n$ é divisível por 6. De fato, se a equação $x^2 - xy + y^2 = n$ não admite solução, o resultado é trivial. Suponha, então, que ela admite solução. Temos que (x, y) é uma solução da equação se, e somente se, o inteiro de Eisenstein $x + y\omega$ possui norma igual a n. Ou seja, existe uma correspondência biunívoca entre o conjunto solução da equação e o conjunto dos inteiros de Eisenstein de norma igual n. Por outro lado, o número de inteiros de Eisenstein de norma igual a n é múltiplo de 6 (Observação 2). Portanto o número de soluções da equação diofantina $x^2 - xy + y^2 = n$ é divisível por 6.

Exemplo 20. O objetivo deste exemplo é determinar as soluções da equação diofantina $x^2 - xy + y^2 = 19$. Para isso, basta determinar os inteiros de Eisenstein $x + y\omega$ de norma igual a 19, uma vez que $N(x + y\omega) = x^2 - xy + y^2$. Se $x + y\omega$ tem norma igual a 19, então $(x + y\omega)(\overline{x + y\omega}) = 19$. Como 19 é um primo e $19 \equiv 1 \mod 3$, segue que $x + y\omega$ e $\overline{x + y\omega}$ são primos de Eisenstein. Em particular, $5 + 2\omega$ e $\overline{5 + 2\omega}$ são primos de Eisenstein, pois $N(5 + 2\omega) = (5 + 2\omega)(\overline{5 + 2\omega}) = 19$. Logo, pelo Teorema da Fatoração Única, os inteiros de Eisenstein $x + y\omega$ de norma igual a 19 são exatamente os associados de $5 + 2\omega$ e os associados de $\overline{5 + 2\omega}$, isto é, $5 + 2\omega$, $3 - 2\omega$, $-5 - 2\omega, -2 + 3\omega, 2 - 3\omega, -3 - 5\omega, 3 + 5\omega, -3 + 2\omega, 2 + 5\omega, -2 - 5\omega, -5 - 3\omega$ e $5 + 3\omega$ (esses elementos estão ilustrados em vermelho na Figura 7). Portanto as soluções da equação diofantina $x^2 - xy + y^2 = 19$ são $(5, 2), (3, -2), (-5, -2), (-2, 3), (2, -3), (-3, -5), (3, 5), (-3, 2), (2, 5), (-2, -5), (-5, -3)$ e $(5, 3)$.

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

Agradecimentos

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

Referências

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

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

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

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

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

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

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

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

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

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

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

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