# Anais da

# XI Semana de Matemática

A Semana de Matemática é um encontro bianual de natureza científica promovido pela Unidade Acadêmica de Matemática – UAMat. Seu objetivo é reunir alunos, professores, pesquisadores e demais interessados em Matemática. Para este fim, abrimos um leque de atividades como palestras, minicursos, oficinas, comunicações, propiciando um encontro com a pesquisa de ponta na área da Matemática, trabalhos de iniciação científica, discussões e reflexões sobre a Educação Matemática no Brasil e no mundo.

Considerando a situação sanitária atual e as incertezas quanto ao fim da pandemia da COVID-19 no Brasil, a comissão organizadora da XI Semana de Matemática da UAMat decidiu por organizar o evento na modalidade virtual. Desse modo, a XI Semana de Matemática acontecerá virtualmente através das plataformas Even3, YouTube e GoogleMeet no período de **24 a 26 de novembro de 2021**.

Os organizadores da XI Semana de Matemática expressam sua gratidão a todos os convidados, autores e participantes que contribuíram para o sucesso de mais uma edição.

## Comitê Organizador

Angelo Roncalli F. Holanda
Alânnio Barbosa Nobrega
Jefferson Abrantes dos Santos
Josefa Itailma da Rocha
Pammella Queiroz de Souza
Romildo Nascimento de Lima

## Comitê Científico

Daniel Cordeiro de Morais Filho
Diogo Diniz Pereira da Silva e Silva
Henrique Fernandes de Lima
Marco Aurélio Soares Souto
Severino Horácio da Silva

# Sumário

# Programação

<table>
<tr><th>Horário</th><th>24/11/2021<br>Quarta feira</th><th>25/11/2021<br>Quinta feira</th><th colspan="2">26/11/2021<br>Sexta feira</th></tr>
<tr><td rowspan="5">08:00–12:30</td><td>Abertura<br>09:20 – 09:40</td><td>Palestra<br>Pacelli Bessa – UFC<br>09:00 – 09:40</td><td>Abertura<br>(PROFMAT)<br>09:00 – 09:20</td><td>Mesa Redonda<br>OCM<br>08:00 – 09:45</td></tr>
<tr><td>Palestra Abertura<br>Claudianor Alves – UFCG<br>09:40 – 10:20</td><td>Palestra<br>Hilario Alencar – UFAL<br>09:40 – 10:20</td><td>Palestra<br>Cristina Vaz – UFPA<br>09:20 – 10:10</td><td rowspan="3">Batalha OCM<br>10:00 – 12:00</td></tr>
<tr><td>Palestra<br>Juliana Pimentel – UFRJ<br>10:30 – 11:10</td><td rowspan="2">Mesa Redonda<br>10:30 – 12:00</td><td>Comunicação Oral<br>10:20 – 11:20</td></tr>
<tr><td>Palestra<br>Aparecido Souza – UFPB<br>11:20 – 12:00</td><td>Colação de grau do PROFMAT/<br>Encerramento<br>11:30 – 12:30</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td rowspan="3">14:00–18:00</td><td>Minicurso/Oficina/<br>Workshop<br>14:00 – 16:00</td><td>Minicurso/Oficina/<br>Workshop<br>14:00 – 16:00</td><td colspan="2" rowspan="5"></td></tr>
<tr><td>Momento PET Matemática<br>16:00 – 17:20</td><td>Momento PET<br>Matemática-Estatística<br>16:00 – 17:20</td></tr>
<tr><td>Comunicação Oral<br>17:20 – 18:00</td><td>Comunicação Oral<br>17:20 – 18:00</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="2">18:00–20:40</td><td>Minicurso/Oficina<br>18:00–20:00</td><td>Minicurso/Oficina<br>18:00–20:00</td></tr>
<tr><td>Palestra<br>Paulo Caetano – UFSCar<br>20:00 – 20:40</td><td>Palestra<br>Sergio Oliva – IME–USP<br>20:00 – 20:40</td></tr>
</table>

**Mesa redonda:** Importância da Iniciação Científica para a formação dos alunos de Graduação
**Mediador:** Severino Horácio da Silva
Diogo Diniz Pereira da Silva e Silva (UFCG)
Matheus Augusto De Bittencourt Pasquali (UFCG)
Michelli Karine Barros da Silva (UFCG)
Rodrigo Marques Faustino (Aluno - UFCG)

**Mesa redonda OCM:** Olimpíadas de Matemática: preparação, desafios e oportunidades
**Mediadora:** Deise Mara Barbosa de Almeida
Carlos Alexandre Gomes da Silva (UFRN)
Yuri Gomes Lima (UFC)
Joanilda Alves Ferreira (EMEF Cândido de Assis Queiroga; Colégio Motiva Jardim Ambiental)
José de Arimatéia Fernantes (UFCG)

## Programação Minicursos/Oficinas

| Horário | 24/11/2021<br>Quarta feira | 25/11/2021<br>Quinta feira |
|---|---|---|
| 14:00–16:00 | **Oficina:** Aprendendo Manipulando: O Uso Do LEM como alternativa para o ensino de Matemática | **Oficina:** Aprendendo Manipulando: O Uso Do LEM como alternativa para o ensino de Matemática |
| 14:00–16:00 | **Minicurso:** A equação de difusão e algumas aplicações à engenharia de alimentos | **Minicurso:** A equação de difusão e algumas aplicações à engenharia de alimentos |
| 14:00–16:00 | **Minicurso:** Introdução aos princípios de contagem | **Minicurso:** Introdução aos princípios de contagem |
| 14:00–16:00 | **Minicurso:** Ensino de funções com tecnologia | **Minicurso:** Ensino de funções com tecnologia |
| 18:00–20:00 | **Oficina:** GeoGebra, Matemática e Arte | **Oficina:** GeoGebra, Matemática e Arte |
| 18:00–20:00 | **Minicurso:** Introdução ao Latex | **Minicurso:** Introdução Ao Latex |
| 18:00–20:00 | **Oficina:** O Uso Do Software Geoboard Como Ferramenta Facilitadora No Ensino e Aprendizagem De Matemática | **Oficina:** O Uso Do Software Geoboard Como Ferramenta Facilitadora No Ensino e Aprendizagem De Matemática |

## Programação Workshop da Pós Graduação

| 24/11/2021<br>Quarta feira | 25/11/2021<br>Quinta feira |
|---|---|
| Sessão Temática de Análise | Sessão Temática de Análise |
| Sessão Temática de Análise Funcional | |
| | Sessão Temática de Geometria |
| Sessão Temática de Probabilidade e Estatística | |
| | Sessão Temática de Matemática Aplicada |
| Sessão Temática de Álgebra | Sessão Temática de Álgebra |

| Sessão temática de Análise | | |
|---|---|---|
| 24 e 25 de novembro de 2021 | | |
| Org.: Jefferson Abrantes | | |
| | **24 de novembro de 2021** | **25 de novembro de 2021** |
| 14h00–14h40 | Gaetano Siciliano (USP/São Paulo) | Harish Shrivastava (TIFR-CAM/India) |
| 14h50–15h30 | José Carlos (UFPE/Recife) | Uberlandio Severo (UFPB/João Pessoa) |
| 15h40–16h20 | Gabrielle Nornberg (DIM/Chile) | Gelson Santos (UFPA/Belém) |
| 16h30–17h10 | Kaye da Silva (UFG/Goiânia) | Gustavo Madeira (UFSCAR/São Carlos) |
| 17h20–18h00 | Eugênio Massa (USP/São Carlos) | Marcelo Furtado (UnB/Brasília) |

| Sessão temática de Análise Funcional | |
|---|---|
| **24 de novembro de 2021** | |
| Org.: Gustavo Araújo | |
| 14h00–14h50 | María Pilar Rueda Segado (Universitat de València) |
| 15h00–15h50 | Vinícius Vieira Fávaro (Universidade Federal de Uberlândia) |
| 16h00–16h20 | Web Coffee |
| 16h20–17h10 | Thaís Jordão (ICMC/USP) |
| 17h20–18h10 | Daniel Núñez Alarcón (Universidad Nacional de Colombia) |

| Sessão temática de Probabilidade e Estatística | |
|---|---|
| **24 de novembro de 2021** | |
| Org.: Manoel Santos-Neto | |
| 14h00–14h50 | José Mir Justino da Costa (UFAM – Brasil) |
| 15h00–15h50 | Tiago Maia Magalhães (UFJF - Basil) |
| 16h00–16h50 | Antônio Marcos Batista do Nascimento (UFRN – Brasil) |
| 17h00–17h50 | Eliardo Guimarães da Costa (UFRN – Brasil) |

| Sessão temática de Álgebra | | |
|---|---|---|
| **24 e 25 de novembro de 2021** | | |
| Org.: Diogo Diniz da Silva | | |
| | **24 de novembro de 2021** | **25 de novembro de 2021** |
| 14h00–14h50 | Thyago Souza (UFCG) | Lucio Centrone (Università degli Studi de Bari) |
| 15h00–15h50 | Felipe Yukihide Yasumura (USP) | Manuela Souza (UFBA) |
| 16h00–16h50 | Viviane Ribeiro da Silva (UFMG) | Claudemir Fidelis Bezerra Júnior (UFCG) |

| Sessão temática de Matemática Aplicada | |
|---|---|
| **25 de novembro de 2021** | |
| Org.: Severino Horácio Silva | |
| 14h00–14h40 | Silvia Sastre (Universidad de Sevilla – Espanha) |
| 14h40–15h30 | Diego Souza (Universidad de Sevilla – Espanha) |
| 15h40–16h20 | Flank Bezerra (UFPB - Brasil) |

| Sessão temática de Geometria | |
|---|---|
| **25 de novembro de 2021** | |
| Org.: Marco Antonio Lázaro | |
| 14h00–14h50 | Allan George de Carvalho Freitas (UFPB – Brasil) |
| 15h00–15h50 | Brian Grajales (Universidad de Pamplona - Colombia) |
| 16h00–16h50 | Weiller Felipe Chaves Barboza (UFCG – Brasil) |
| 17h00–17h50 | André Felipe Araujo Ramalho (UFCG – Brasil) |

# Programação (Momento PETs/Comunicações Orais)

**24 de novembro de 2011, 16h às 18h**

Momento PET Matemática

- A Matemática da Criptografia RSA
- Uma Demonstração Bem Diferente Do Excêntrico Paul Erdös
- Uma aplicação não muito convencional da Topologia na Aritmética: uma demonstração da infinitude dos números primos
- Sequências de P.A.s Contendo Infinitos Números Primos – Parte II.
- Matemática e Cálculos Mentais Auxiliando Nos Juros Da Economia Doméstica: Erros comuns, acertos e sugestões

Comunicações Orais

- Equidistribuição E Números Naturais: A Lei do Primeiro Dígito em Potenciações.
- Solução De Energia Mínima Para Problemas Elípticos Envolvendo A Equação De Choquard
- Existência E Unicidade De Soluções Para O Modelo De Keller-Segel Para A Quimiotáxia
- Avaliação Do Uso Da Metodologia De Resolução De Problemas No Ensino De Matemática

**25 de novembro de 2011, 16h às 18h**

Momento PET Matemática e Estatística

- Uma Curiosa Aplicação Da Teoria De Bases De Gröbner: O Problema Da Pertinência
- Calculando Uma Integral Imprópria Utilizando O Teorema De Resíduos
- Produto Semidireto
- O Teorema Dos Quatro Quadrados
- Um Estudo Sobre Raízes Primitivas E Uma Caracterização Dos Números Que As Possuem
- Funções Diferenciáveis E Polinômio De Taylor
- Unidade Do Anel Dos Inteiros Quadráticos

Comunicações Orais

- O Problema Isoperimétrico
- Atuações Do Pibid Durante A Pandemia Do Covid-19 Na Preparação De Alunos Para O Enem

## Programação (Comunicações Orais - PROFMAT)

**26 de novembro de 2011, 10h20 às 11h20**

- Uma Proposta Histórico-Construtivista dos Logaritmos
- Uma estratégia para resolver questões de Análise Combinatória no ENEM
- Cálculo De Área: Resumo Expandido
- Pesquisas Com Sala De Aula Invertida E Instrução Por Pares Na Matemática Do Ensino Médio

# Plenária de Abertura

# Ensino Remoto: Um desafio para todos

Claudianor Oliveira Alves
Unidade Acadêmica de Matemática
Universidade Federal de Campina Grande

**Resumo**

Nesta palestra vamos conversar um pouco sobre o impacto da pandemia na educação, que trouxe a necessidade de utilizar o ensino remoto em escolas e universidades que não estavam preparadas para esse tipo de ensino. Iremos refletir como esse tipo de ensino afeta a rotina de professores, alunos e familiares, levando em consideração os pontos positivos e negativos do mesmo.

# Palestras

# Atratores globais para a equação do calor

Juliana Fernandes Pimentel
Departamento de Matemática
Universidade Federal do Rio de Janeiro

**Resumo**

Apresentaremos alguns resultados principais sobre a estrutura de Morse-Smale dos sistemas dinâmicos gerados pela classe das equações escalares semilineares parabólicas. Para evitar complexidades não essenciais, a discussão será baseada no caso mais simples e clássico da equação de Chafee-Infante. Veremos finalmente a consequência de tal estrutura na decomposição do atrator global associado.

# Apoio Computacional ao Ensino de Matemática

Aparecido Jesuino de Souza
Departamento de Computação Científica
Universidade Federal da Paraíba

**Resumo**

Nesta palestra de caráter geral pretendemos abordar tópicos do ensino da disciplina matemática constantes de algumas ementas de disciplinas presentes na grade curricular dos cursos das áreas de exatas e engenharias com uma metodologia alternativa de fixação dos conceitos via a programação dos mesmos em linguagem acessível, bem como a utilização de softwares disponíveis para a realização de operações envolvidas.

# Harry Potter em busca do "pi" no conjunto de Mandelbrot

Paulo Silvani Caetano
Departamento de Matemática
Universidade Federal de São Carlos

**Resumo**

Vamos definir o conjunto de Mandelbrot no plano complexo e apresentar como o número "pi" aparece nesse conjunto.

# Teoremas da Esfera

Pacelli Feitosa Bessa
Departamento de Matemática
Universidade Federal do Ceará

**Resumo**

Apresentar uma coletânea de teoremas da esfera em Geometria.

# Provas Geométricas e Animações de Alguns Problemas de Matemática da Educação Básica

Hilário Alencar da Silva
Instituto de Matemática
Universidade Federal de Alagoas

**Resumo**

Loren C. Larson, em seu consagrado livro Problem-Solving Through Problems, lista doze estratégias para a resolução de problemas. Inspirado nas estratégias propostas, construímos resoluções de alguns problemas de Matemática, mediante uma sequência de figuras e a corresponde animação. Aliás, observamos que das estratégias listadas por Larson, utilizamos com maior predominância, a segunda, sexta e sétima estratégias, que são, respectivamente, trace uma figura, explore as simetrias e divida em casos.

# Human mobility as an instrument for dynamical analysis of COVID-19 pandemics in Brazil

Sérgio Muniz Oliva
Instituto de Matemática e Estatística
Universidade de São Paulo

**Abstract**

The COVID-19 pandemic has become a challenge for several areas of science and proven to be a major burden in the population, causing deaths and economic impacts. In the beginning, without vaccines or proven drugs, the disease spread quickly and challenged society and government. The control was based mainly on non-pharmaceutical methods seeking either to reduce the odds of contact with an infected individual causing an infection, such as mask-use and handwashing, or to avoid the contact between an infected and susceptible individual, such as social distancing, lockdown, etc.. Our research interest is the spatial dynamics of this disease, using anonymized mobility data in Brazil from cell phones, we explore some aspects of the epidemic.

# Matemática e Arte: uma experiência inovadora no ensino-aprendizagem da Matemática

Cristina Lucia Vaz
Instituto de Ciências Exatas e Naturais
Universidade Federal do Pará

**Resumo**

Nesta palestra pretendemos inspirar professores e futuros professores de matemática na implementação de práticas inovadoras promovendo um diálogo interdisciplinar entre a Matemática e a Arte. A proposta é inspirada na cultura Maker e na metodologia STEAM (Science, Technology, Engineering, Arts and Mathematics), tendências mundiais de ensino e aprendizagem que surgiram em contraponto às metodologias tradicionais. Para isto, apresentaremos alguns projetos e produtos educacionais que visam promover uma aprendizagem criativa em Matemática. Entre eles, destacamos: Trilhar interdisciplinar pela arte dos azulejos de Belém, A matemática na obra do artista Antônio Peticov, Inventário-artístico matemático com instrumento pedagógico, Monitor Maker: a matemática da arte cinética, Festival de Matemática da UFPA.

# Minicursos

# A equação de difusão e algumas aplicações à engenharia de alimentos

Aluízio Freire da Silva
Unidade Acadêmica de Física e Matemática
Universidade Federal de Campina Grande

**Resumo**

A Equação de Difusão é uma Equação Diferencial Parcial (EDP) com diversas aplicações em problemas da física e das engenharias. No presente minicurso essa EDP será apresentada no contexto de problemas de transferência de calor e transferência de massa, com foco em algumas geometrias, condições de contorno e hipóteses para alguns de seus parâmetros. Finalmente, esses conceitos abordados serão aplicados em alguns problemas da engenharia de alimentos.

**Carga Horária:** 4h

# Introdução aos princípios de contagem

André Gustavo Campos Pereira
Departamento de Matemática
Universidade Federal do Rio Grande do Norte

**Resumo**

Neste minicurso introduziremos os princípios aditivo e multiplicativo e, a partir deles, desenvolveremos outras ferramentas, como a permutação, a combinação, o arranjo, a permutação com elementos repetidos e as combinações completas, as quais nos auxiliam na resolução de problemas de contagem mais complexos. Veremos, a medida que formos desenvolvendo essas ferramentas, em que situações elas podem ser utilizadas, bem como a diferença de uma para outra. Ao final do curso, seremos capazes de construir uma árvore de decisões que nos auxilie na escolha da ferramenta mais adequada para resolver cada situação específica, nas etapas de resolução de um problema de contagem.

**Público alvo:** Alunos e professores do ensino médio

**Carga Horária:** 4h

# Ensino de funções com tecnologia

Gladson Octaviano Antunes; Michel Cambrainha
Departamento de Métodos Quantitativos
Universidade Federal do Estado do Rio de Janeiro

**Resumo**

Nos últimos anos muito tem se debatido sobre o uso de novas tecnologias no ensino de conceitos matemáticos. Em especial, com a adoção do ensino remoto devido à pandemia de COVID-19 as discussões sobre esse tema ganharam centralidade. Sabemos que funções é um tópico que ocupa boa parte do currículo de matemática dos Ensinos Fundamental e Médio e, apesar disso, as pesquisas em educação matemática têm evidenciado uma grande dificuldade que os estudantes encontram em articular suas diferentes representações (gráfico, expressão algébrica, descrição por palavras, tabelas). Neste minicurso pretendemos abordar esta e outras questões mostrando na prática como as ferramentas digitais podem auxiliar os professores a resgatar a natureza dinâmica do conceito de função, diversificar as representações e transitar entre elas.

**Carga Horária:** 4h

# Introdução Ao Latex

Reginaldo Amaral Júnior
Unidade Campus Itabaiana
Instituto Federal da Paraíba

**Resumo**

O LaTeX é uma linguagem de formatação padrão para produção de textos impressos de alta qualidade, especialmente em matemática, física e outras áreas da ciência fortemente matematizadas.
No LaTeX o texto é digitado a partir de comandos no arquivo de entrada que são traduzidos como símbolos em um arquivo de saída, como PDF. Por esse motivo, com o conhecimento básico dos códigos é possível escrever textos com simbologia matemática que na maioria das vezes não são acessíveis em outros programas.
Nesse sentido, o minicurso tem como objetivo uma breve introdução ao LaTex com ênfase na edição de textos matemáticos.

**Carga Horária:** 4h

# Oficinas

# Aprendendo Manipulando: O Uso Do LEM como alternativa para o ensino de Matemática

Joelson Joventino Santos; Lívia Tito Ribeiro; Rafael Alves Silva; Wilton dos Santos;
Jacqueline Félix de Brito Diniz; Larise Carmélia de França Silva
Unidade Acadêmica de Matemática
Universidade Federal de Campina Grande

**Resumo**

O ensino da matemática e ainda hoje um dos mais tradicionais e presos a modelos utilizados há anos, e pensando nisso e tendo em mente que a aprendizagem pode ocorrer de outras maneiras, não apenas através de aulas expositivas, que preparamos esta oficina. Aqui iremos abordar a importância do uso do LEM (Laboratório de Ensino da Matemática) em nossas aulas. Assim como discutir diversas ideias e propostas, juntos construiremos materiais didáticos de fácil acesso e simples manuseio, tornando assim as aulas de matemática mais interessantes, cativando a interação e resultando em momentos mais atrativos aos alunos.

**Carga Horária:** 4h

# GeoGebra, Matemática e Arte

Sérgio Carrazedo Dantas
Campus Apucarana
Universidade Estadual do Paraná

Carmen Vieira Mathias
Departamento de Matemática
Universidade Federal de Santa Maria

**Resumo**

Uma das definições da matemática é que ela é "uma ciência de padrões e temas". No âmbito desta definição, as tecnologias digitais facilitam a criação de elementos visuais e padrões. Assim, a oficina proposta tem como objetivo realizar uma releitura de algumas obras de arte utilizando o software GeoGebra. Para tanto, os participantes serão convidados a produzir imagens que possuem padrões esteticamente agradáveis e ao mesmo tempo resolver problemas, utilizando os quatro pilares do pensamento computacional: decomposição, abstração, percepção de padrões e algoritmos.

**Carga Horária:** 4h

# O Uso Do Software Geoboard Como Ferramenta Facilitadora No Ensino e Aprendizagem De Matemática

Diego Rawalyson Marques de Souza, Eliel Marques Brito, Sérgio Victor de Melo Soares, Wander Ícaro Guedes Medeiros, Jacqueline Félix de Brito Diniz, Larise Carmélia de França Silva
Unidade Acadêmica de matemática
Universidade Federal de Campina Grande

**Resumo**

Durante esse período de pandemia surgiu a extrema necessidade de aulas remotas, tornando necessário a adaptação de professores para trabalhar não mais na sala de aula, mas em um ambiente virtual. Essa oficina visa capacitar os alunos, futuros professores, na utilização de um software on-line que ir a auxiliá-los na ministração de alguns conteúdos nas aulas de matemática, o Geoboard. Ele é uma versão digital de um material já utilizado há algum tempo, o Geoplano. Estaremos juntos construindo e compartilhando um conhecimento que facilitará a aprendizagem tanto nas aulas remotas quanto nas presenciais.

**Carga Horária:** 4h

# Workshop Pós-Graduação

# Workshop Pós-Graduação

# Sessão Temática de Análise

# Analysis of ground states for an elliptic system with local and nonlocal nonlinearities

Gaetano Siciliano
USP/São Paulo – Brasil

**Resumo**

Nessa palestra apresentamos um sistema elíptico em todo o espaço em presença de não–linearidades de tipo local e não local. Nosso objetivo é a análise dos ground states ao depender de um parâmetro real dentro da não linearidade. Usando métodos variacionais mostramos a existência e o comportamento dos ground states quando o parâmetro  e muito grande ou muito pequeno.
Os resultados apresentados foram obtidos em colaboração com L. Maia (UnB, BR) e P. d'Avenia (Poliba, IT).

# On fractional magnetic Schrodinger equations with potential vanishing at infinity

José Carlos
UFPE/Recife – Brasil

**Abstract**

In this talk we discuss the existence of solutions for the following class of fractional magnetic Schrodinger equations

$$(-\Delta)_A^S u + V(x)u = g(|u|^2)u + \lambda|u|^{q-2}u, \qquad in\ \mathbb{R}^N,$$

where $(-\Delta)_A^S$u is the fractional magnetic Laplacian, A:$\mathbb{R}^N \to \mathbb{R}^N$ is the magnetic potential, s ∈ (0, 1), N > 2s, $\lambda \geq 0$, V: $\mathbb{R}^N \to \mathbb{R}$ is a potential function that may decay to zero at infinity, g: $\mathbb{R}_+ \to \mathbb{R}$ is a continuous function and $q \geq 2_S^*$:= 2N/(N - 2s). Our approach is based on variational methods combined with penalization technique and $L^\infty$–estimates.

Joint work with Jose Luando Santos (Federal University of Pernambuco).

# Existence and nonexistence results for Lane-Emden type systems.

Gabrielle Nornberg
DIM – Chile

**Abstract**

In this talk we discuss the existence, nonexistence and uniqueness of positive radial solutions for a class of Lane-Emden type systems and their recent extensions to fully nonlinear uniformly elliptic operators.

# The bering method applied to the level sets of a family of functionals

Kaye da Silva
UFG/Goiânia – Brasil

**Abstract**

Given an one-parameter family of $C^1$–functionals, $\Phi_\mu: X \to \mathbb{R}$, defined on an uniformly convex Banach space X, we describe a method that permit us find critical points of at some energy level c ∈ $\mathbb{R}$. In fact, we show the existence of a sequence $\mu$(n, c), n ∈ $\mathbb{N}$, such that $\Phi_{\mu(n,c)}$ has a critical level at c ∈ $\mathbb{R}$, for all n ∈ $\mathbb{N}$. Moreover, we show some good properties of the curves $\mu$(n,c), with respect to c (for example, they are Lipschitz), and as a consequence of this analysis, we recover many know results on the literature concerning bifurcations of elliptic partial differential equations. Furthermore we prove new results for a large class of elliptic partial differential equations, which includes, for example, Ouyang, Lane-Enden, Concave-Convex, Kirchhoff and Schrödinger-Bopp-Podolsky type equations.

# Comportamento “côncavo-convexo" para Equações de tipo Kirchhoff com coeficiente degenerado

Eugênio Massa
USP/São Carlos – Brasil

**Resumo**

Introduziremos as equações elípticas com operador de tipo Kirchhoff e mostraremos alguns resultados em que a interação entre o coeficiente não local e a não linearidade produzem fenômenos tópicos dos problemas de tipo côncavo–convexo. Veremos como a degeneração do coeficiente (caso ainda pouco estudado em literatura) joga um papel fundamental para obter estes comportamentos.

# Variational free transmission problems of Bernoulli type

Harish Shrivastava
TIFR-CAM – India

**Abstract**

We will discuss some known results pertaining to regularity theory of variational free transmission problems of Bernoulli type. We point out the key ingredients that allow the improvement of known regularity results.

# Existence and asymptotic behavior of ground states for linearly coupled systems with exponential growth

Uberlandio Severo
UFPB/João Pessoa – Brasil

**Abstract**

In this talk we study a class of linearly coupled systems in the plane involving a positive parameter lambda and the nonlinearities are continuous functions with critical exponential growth in the sense of Trudinger-Moser inequality. First, for any value of the parameter in the open interval (0; 1), by using minimization arguments and minimax estimates we prove the existence of positive ground state solutions. Moreover, we study the asymptotic behavior of these solutions when the parameter lambda goes to zero.

# Existence of solution for a class of quasilinear Schrödinger equation in $\mathbb{R}^N$ with zero-mass

Gelson C. G. dos Santos
UFPA/Belém – Brasil

**Abstract**

We present recent results on the existence of solutions for the following quasilinear Schrödinger problem with zero-mass:

$$\begin{cases} -\Delta u - \Delta(u^2)u = h(x)u^q \ \ in\ \mathbb{R}^N \\ u \geq 0, \qquad u \in D^{1,2}(\mathbb{R}^N) \cap L^\infty(\mathbb{R}^N) \end{cases}$$

where k > 0, $0 \leq q < 2 \cdot 2^* - 1$ and $2^* = 2N/(N-2)$; $N \geq 3$ is the critical Sobolev exponent and $h \in L^\infty_{loc}(\mathbb{R}^N)$ is a function that can change sign. To establish existence results we used the variational method. More precisely, we used a change of variables combined with the Ekeland Variational Principle, Mountain Pass Theorem, careful estimates on energy functionals and an argument of passing to the limit.

This is joint work with Sabado Saide Muhassuab (Universidade Rovuma–Nampula Mo cambique).

# Positive solutions of elliptic Neumann problems with nonlocal and convection terms

Gustavo Madeira
UFSCAR/São Carlos – Brasil

**Abstract**

We prove in this talk the existence of positive solutions of elliptic Neumann problems with nonlocal and convection terms satisfying some general conditions. The result is applied to some classes of equations involving source terms usually occuring in the applications.

# Two solutions for a singular elliptic equation with critical growth at infinity

Marcelo Furtado
UnB/Brasília – Brasil

**Abstract**

We look for positive solutions for the singular equation

$$-\Delta u - \frac{1}{2}(x \cdot \nabla u) = \mu h(x) u^{q-1} + \lambda u + u^{(N+2)/(N-2)}, \qquad in\ \mathbb{R}^N,$$

where N≥3, $\lambda > 0$, $\mu > 0$ is a parameter, 0 < q < 1 and h has some summability properties. By using a perturbation method and critical point theory, we obtain two solutions when max{1,N/4} < $\lambda$ < N/2 and the parameter $\mu > 0$ is small.

This is joint work with Karla Sousa (UFG).

# Workshop Pós-Graduação

# Sessão Temática de Análise Funcional

# The biduality problem in certain Banach spaces

Pilar Rueda
Universitat de València – Espanha

**Resumo**

The biduality problem deals with the description of the bidual of certain Banach spaces of analytic functions of several complex variables, when endowed with a weight. This problem has remained open since the 1960s. We will review some of the most important results concerning the biduality problem and examine recent partial solutions that have been jointly obtained by C. Boyd and the author.

# Um panorama do tema lineabilidade em conjuntos de sequências

Vinícius Vieira Fávaro
UFU – Brasil

**Resumo**

Nessa palestra pretendemos abordar um tópico de intensa atividade de pesquisa nos últimos anos na área de Análise: lineabilidade/espaçabilidade. A "teoria de lineabilidade e espaçabilidade" se preocupa com o estudo de estruturas lineares em subconjuntos, digamos, exóticos de espaços vetoriais. Nos últimos 15 anos, esta busca por linearidade tem sido explorada em diversos contextos: Teoria de Conjuntos, Teoria de Probabilidade, Análise Funcional, Teoria de Medida, etc. Nesta palestra pretendemos apresentar um pouco do desenvolvimento deste tópico, principalmente no que diz respeito aos principais espaços de sequências estudados na Análise Funcional.

# Teoremas do tipo de Titchmarsh

Thaís Jordão
ICMC/USP – Brasil

**Resumo**

O estudo do decaimento da transformada/coeficientes de Fourier é um tema clássico em Análise de Fourier. Neste cenário, o matemático britânico Edward C. Titchmarsh (1899 - 1963) mostrou que o decaimento da transformada de Fourier que se tinha podia ser melhorado para funções de uma variável real satisfazendo certa condição de Lipschitz generalizada. Atualmente, resultados desta natureza são reconhecidos por teoremas do tipo de Titchmarsh. Tais resultados podem ser interpretados como caracterizações de espaços de Lipschitz generalizados em termos do decaimento da transformada de Fourier. Nesta palestra, o teorema original de Titchmarsh será revisitado e discutido do ponto de vista da atualidade e em termos do conceito de suavidade generalizada.

# As desigualdades de Hardy–Littlewood em espaços $\ell p$

Daniel Núñez Alarcón
Universidad Nacional de Colombia – Colômbia

**Resumo**

Em 1930, J.E. Littlewood deu início à investigação da relação entre as normas usuais de formas bilineares em $c_0 \times c_0$ (a norma do sup) com as somas dos coeficientes dessas formas bilineares. Em 1934, em um trabalho em colaboração com G.H. Hardy, J.E. Littlewood estendeu o resultado anterior para espaços $\ell p$. O principal objetivo desta palestra é apresentar versões $m$-lineares do resultado de Hardy e Littlewood e o estado da arte deste tema.

# Workshop Pós-Graduação

# Sessão Temática de Probabilidade e Estatística

# Estimativa de parâmetro e simulação direta de experimentos por hipertermia-quimioterapia in vitro

José Mir Justino da Costa
UFAM – Brasil

**Resumo**

Para estimar os parâmetros de um modelo de aquecimento por laser de diodo de uma cultura de células cancerígenas sob o efeito de um quimioterápico, dois modelos matemáticos foram propostos para representar o problema físico durante o aquecimento: a convecção natural foi considerada no modelo completo, enquanto o modelo reduzido foi dado por um sistema de parâmetros concentrados (lumped system). O dano térmico causado nas células pelo aquecimento foi modelado como uma reação de primeira ordem. Para estimar os parâmetros do modelo foi usado o MCMC, via algoritmo Metrópolis-Hastings. A abordagem do Modelo de Erro de Aproximação (AEM) foi usada para acelerar os cálculos da solução do problema inverso quando o modelo de completo foi substituído pelo modelo reduzido para o cálculo das variáveis dependentes. Simulações de Monte Carlo também foram realizadas para calcular a variação transitória do número de células durante os períodos antes e depois do aquecimento imposto.

# A class of categorization methods for credit scoring models

Tiago M. Magalhães
UFJF – Brasil

**Resumo**

Credit scoring models are usually developed using logistic regression. For several reasons, professionals of this area frequently categorize the quantitative covariates before using them in the model. In this work, we introduce a class of methods for covariate categorization in regression models for binary response variables. Applications to real data and a Monte Carlo simulation study suggest that one of the methods of this class has a better predictive performance and a smaller computational cost than other methods available in the literature.

**Joint work with:** Diego M. B. Silva and Gustavo H. A. Pereira.

# Multiple Phase Transitions for an Infinite System of Spiking Neurons

Antonio Marcos Batista do Nascimento
UFRN – Brasil

**Resumo**

We consider a stochastic model describing the spiking activity of a countable set of neurons spatially organized into a homogeneous tree of degree $d$, $d \geq 2$; the degree of a neuron is just the number of connections it has. Roughly, the model is as follows. Each neuron is represented by its membrane potential, which takes non-negative integer values. Neurons spike at Poisson rate 1, provided they have strictly positive membrane potential. When a spike occurs, the potential of the spiking neuron changes to 0, and all neurons connected to it receive a positive amount of potential. Moreover, between successive spikes and without receiving any spiking inputs from other neurons, each neuron's potential behaves independently as a pure death process with death rate $\gamma \geq 0$. In this article, we show that if the number $d$ of connections is large enough, then the process exhibits at least two phase transitions depending on the choice of rate $\gamma$: For large values of $\gamma$, the neural spiking activity almost surely goes extinct; For small values of $\gamma$, a fixed neuron spikes infinitely many times with a positive probability, and for ``intermediate'' values of $\gamma$, the system has a positive probability of always presenting spiking activity, but, individually, each neuron eventually stops spiking and remains at rest forever.

# Verifying compliance with ballast water standards: a decision-theoretic approach

Eliardo G. Costa
UFRN – Brasil

**Resumo**

We construct credible intervals to estimate the mean organism (zooplankton and phytoplankton) concentration in ballast water via a decision-theoretic approach. To obtain the required optimal sample size, we use a total cost minimization criterion defined as the sum of the sampling cost and the Bayes risk either under a Poisson or a negative binomial model for organism counts, both with a gamma prior distribution. Such credible intervals may be employed to verify whether the ballast water discharged from a ship is in compliance with international standards. We also conduct a simulation study to evaluate the credible interval lengths associated with the proposed optimal sample sizes.

**Joint work with:** Julio Singer (IME–USP) and Carlos Daniel Paulino (Universidade de Lisboa

# Workshop Pós-Graduação

# Sessão Temática de Álgebra

# Transposta de Auslander e módulos G-perfeitos reduzidos no contexto relativo

Thyago Souza
UFCG – Brasil

**Resumo**

Módulo semidualizante, dimensão de Gorenstein, e transposta de Auslander são conceitos fundamentais na Álgebra homológica. Nesta palestra, apresentaremos a dimensão de Gorenstein e a transposta de Auslander ambas no contexto relativo a um modulo semidualizante C, bem como outras noções relativas que nos permitem definir uma certa classe de módulos, chamados $G_C$–perfeitos reduzidos. Estudaremos conexões entre essa classe de módulos e a transposta de Auslander com respeito a C, investigaremos quando a $G_C$–perfeição reduzida é preservada pela C–transposta, e exploraremos algumas consequências envolvendo o operador ligação horizontal.

# Graduações Na Álgebra De Incidência

Felipe Yukihide Yasumura
IME/USP – Brasil

**Resumo**

Álgebras de incidência constituem uma estrutura rica do ponto de vista combinatorial, e é uma construção útil para exibir exemplos e contra–exemplos de propriedades algébricas. Graduações em álgebra surgem como uma forma de estudar simetrias (em algum sentido) de uma dada álgebra. Nesta apresentação, mostrarei a construção das álgebras de incidência e introduzirei o conceito de graduações por grupos em álgebras. Em seguida, apresentarei exemplos de graduações sobre álgebras de incidências, e apresentarei uma descrição de todas as suas possíveis graduações. Se o tempo permitir, falarei do problema inverso: dada uma graduação $\Gamma$ em uma álgebra triangular, seria possível encontrar uma graduação $\Gamma'$ sobre alguma álgebra de incidência de modo que $\Gamma \cong \Gamma'$?

# On the minimal varieties of PI-algebras graded by finite cyclic groups and the factorability of their T–ideals

Viviane Ribeiro Tomaz da Silva
UFMG – Brasil

**Abstract**

Let F be a eld of characteristic zero. In 2003, Giambruno and Zaicev established some interesting results relating minimal varieties of a given exponent and the factorability of their T–ideals. In this talk, we deal with varieties generated by PI-algebras graded by finite cyclic groups and we present some recent results concerning the minimality of these varieties and the factorability of their graded polynomial identities.

# Formal languages and monomial algebras with polynomial identities

Lucio Centrone
Università degli Studi di Bari – Itália

**Abstract**

In this lecture, we would like to outline some basic facts about formal languages and we would like to apply them to monomial algebras with polynomial identities.

# Aplicações da Álgebra Linear

Manuela da Silva Souza
UFBA – Brasil

**Resumo**

A álgebra linear, principalmente matrizes e sistemas lineares tem aplicações em várias áreas do conhecimento, como por exemplo física, biologia, engenharias etc. Nessa palestra, falarei um pouco sobre algumas dessas aplicações.

# Graded identities in Lie algebras with Cartan gradings: the algorithm

Claudemir Fideles Bezerra Jr.
UFCG – Brasil

**Resumo**

The classification of finite-dimensional semisimple Lie algebras in characteristic 0 is one of the great achievements of Algebra in the first half of 20th century. Tells us that, in characteristic 0, every finite-dimensional Lie algebra is a semidirect product of a semisimple Lie algebra and a solvable ideal (the solvable radical of the algebra). The classification of the finite–dimensional semisimple Lie algebras (once again in characteristic 0) was obtained during the last decade of the 19th century by Killing and by Cartan. According to the Killing–Cartan classification, the isomorphism classes of simple Lie algebras, over an algebraically closed field of characteristic zero, are in one-to-one correspondence with irreducible root systems. Such classification is well known, and it consists of the Classical and Exceptional Lie algebra. In the infinite-dimensional case the situation is more complicated, and the so-called algebras of Cartan type appear. It is somewhat surprising that graded identities for Lie algebras have been relatively few results to that extent. In this talk, we will be to present some results obtained so far and also an algorithm that can help to obtain a basis for all graded identities in Lie algebras with Cartan gradings. In particular, over an any infinite field, we will apply this algorithm to provide a basis for every graded identities of U1, the Lie algebra of the derivations of the algebra of Laurent polynomials K[t, $t^{-1}$], and prove that they do not admit any finite basis. Many results present in this talk were obtained in recent research projects, and these were joint works with D. Diniz (UFCG), D. Macêdo (UFRPE), P. Koshlukov (UNICAMP), and F. de Souza (UFCG).

# Workshop Pós-Graduação

# Sessão Temática de Matemática Aplicada

# Equações não locais em domínios perfurados

Silvia Sastre
Universidade de Sevilla – Espanha

**Resumo**

Neste trabalho analisamos o comportamento das soluções para equações de evolução não local com um termo de reação não linear não local em um domínio perfurado perturbado. Este domínio perfurado é pensado como um conjunto fixo de onde removemos um subconjunto denominado orifícios. Escolhemos famílias apropriadas de funções limitadas para lidar com as condições de Neumann e de Dirichlet nos buracos que definem uma condição de Dirichlet fora do domínio. Estudamos o limite das soluções fornecendo uma equação homogeneizada não local.

# Controle de problemas de fronteira livre

Diego Araujo de Souza
Universidade de Sevilla – Espanha

**Resumo**

Nesta palestra apresentaremos as principais ideias para deduzir resultados de controlabilidade para problemas de fronteira-livre bifásico por meio de controles distribuídos em um domínio unidimensional. Este tipo de problema de fronteira livre modela processos de solidificação ou fusão. Cada uma das fases está regida por uma equação parabólica completada com as condições iniciais e de contorno; as fases estão separadas por uma interface de mudança de fase, onde uma condição de fronteira livre adicional é imposta. Permitindo que duas fontes localizadas atuem no sistema (uma em cada fase) como mecanismos de controle (aquecendo ou resfriando), provamos que é possível conduzir as temperaturas de cada uma das fases a temperatura de equilíbrio e, além disso, as interfaces podem ser direcionadas a um local desejado, desde que os dados iniciais e a posição inicial da interface estejam suficientemente próximos dos alvos. Adicionalmente, quando apenas um controle está presente em uma das fases, provamos que não é possível controlar ambas temperaturas. Concluiremos a palestra apresentando algumas observações finais e formulando algumas questões interessantes que ainda permanecem em aberto.

# Equações diferenciais lineares de ordem superior em espaços de Banach

Flank D. M. Bezerra
UFPB – Brasil

**Resumo**

Neste trabalho estudamos problemas de Cauchy do tipo

$$\begin{cases} \dfrac{d^n u}{dt^n}(t) + Au(t) = 0, t > 0, \\ u^{(k)}(0) = u_k(0), k = 0, 1, \ldots, n-1, n \geqslant 3, \end{cases}$$

sob o ponto de vista da teoria de potências fracionárias de operadores fechados e densamente definidos em espaços de Banach. Aqui, A : D(A) ⊂ X → X denota um operador linear, o qual é gerador infinitesimal de um semigrupo fortemente contínuo de operadores lineares e limitados em um espaço de Banach X. Questões sobre resolubilidade deste problema e de aproximações fracionárias deste problema são discutidas.

# Workshop Pós-Graduação

# Sessão Temática de Geometria

# Free-Boundary minimal hypersurfaces in rotational domains

Allan George de Carvalho Freitas
UFPB – Brasil

**Abstract**

In this lecture, we deal with domains whose boundary is a regular level set of a function F in $\mathbb{R}^n$. For such domains we obtain a Minkowski-type identity for compact free-boundary minimal hypersurfaces contained in it. We use this identity to study the particular case where the function F is a quadratic polynomial and therefore, the boundary of domain is a quadric domain. This permits unify the study of existence and uniqueness for free-boundary boundary minimal hypersurfaces contained in some remarkable domains such as cones, circular paraboloids, parabolic cylinders, slabs, hyperboloid of one sheet and many others. Furthermore, we also intend to approach gap results where the ambient space is a rotational ellipsoid or a ball. This is a joint work with E. Barbosa, R. Melo and F. Vitório announced in [1].

**References:**

[1] E. Barbosa, A. Freitas, R. Melo and F. Vitório, “Uniqueness of free-boundary minimal hypersurfaces in rotational domains”, arXiv:2108.00441v1 [math.DG].

# Real flag manifolds of type $G_2$

Brian Grajales
Universidad de Pamplona – Colombia

**Abstract**

A generalized flag manifold of a non-compact, simple real Lie algebra g is the homogeneous space $\mathbb{F}_\theta = G/P_\theta$, where G is a connected Lie group with associated Lie algebra g and $P_\theta$ is a parabolic subgroup. In this talk, we present a construction of real flag manifolds of type $G_2$ and give a brief description of their invariant metrics.

**References:**

[1] M. Patrão, Luiz A. B. San Martin, "The isotropy representation of a real flag manifold: Split real forms", Indagationes Matematicae 26 (2015) 547-579.
[2] Luiz A. B. San Martin, "Algebras de Lie", Editora Unicamp (2010).

# On the umbilicity of Linear Weingarten Spacelike Submanifolds Immersed in the de Sitter Space

Weiller Felipe Chaves Barboza
UFCG – Brasil

**Abstract**

We investigate the umbilicity of n-dimensional complete linear Weingarten spacelike submanifolds immersed with parallel normalized mean curvature vector field in the de Sitter space $\mathbb{S}_p^{n+p}$ of índex p > 1. We recall that a spacelike submanifold is said to be linear Weingarten when its mean curvature function H and its normalized scalar curvature R satisfy a linear relation of the type R = aH + b , for some constants a, b ∈ $\mathbb{R}$. Under suitable constraints on a and b, we apply a generalized maximum principle for a modified Cheng-Yau operator L in order to show that such a spacelike submanifold must be either totally umbilical or isometric to a product $M_1 \times \cdots \times M_k$, where the factors $M_i$ are totally umbilical submanifolds of $\mathbb{S}_p^{n+p}$ which are mutually perpendicular along their intersections. Moreover, we also study the case in which these spacelike submanifolds are $\mathcal{L}$–parabolic.

**References:**

[1] W.F.C. Barboza, E.L. Lima, H.F. de Lima; Marco A.L. Velásquez. “On the umbilicity of linear Weingarten spacelike submanifolds immersed in the de Sitter space”, Bulletin of Mathematical Sciences, v. 10, p. 1-12, 2020.

# Bifurcation and local rigidity of constant second mean curvature hypersurfaces in Riemannian warped products

André Felipe Araújo Ramalho
UFCG – Brasil

**Resumo**

In a Riemannian warped product $I \times_f M^n$, where I $\subset \mathbb{R}$ is an open interval, f is a positive real function defined on I and $M^n$ is a compact Riemannian manifold without boundary, we use equivariant bifurcation theory in order to establish sufficient conditions, in terms of f and the spectrum of the Laplacian on $M^n$, that allow us to guarantee the existence of bifurcation instants or the local rigidity of a certain family of open sets whose boundaries are $H_2$–hypersurfaces, namely, whose boundaries are hypersurfaces with constant second mean curvature $H_2$. For each of our results, we have provided a considerable number of examples that verify all the assumptions under consideration.

**References:**

[1] Marco A.L. Velásquez, A.F.A. Ramalho, J.F. Silva, J.Q. Oliveira, "Bifurcation and local rigidity of constant second mean curvature hypersurfaces in Riemannian warped products". Nonlinear Analysis, v. 197, p. 111865, 2020.

# Comunicações Orais

# A Matemática da Criptografia RSA

**Isabella Tito de Oliveira Silva**[1] **- isabella.tito@estudante.ufcg.edu.br**
**Maria Débora de Oliveira Silva**[1]**- debora.oliveira@estudante.ufcg.edu.br**
**Daniel Cordeiro de Morais Filho**[1] **- daniel@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil. Parcialmente financiado pelo MEC/FNDE/PET

***Resumo:*** *Desde a antiguidade, a humanidade buscou um jeito de esconder informações sigilosas sem que pessoas indesejadas tivessem acesso a elas. Durante anos, foram buscadas formas para se, acaso uma mensagem fosse interceptada, ela não pudesse ser lida, um exemplo bastante simples são as mensagens cifradas trocando letras por símbolos. Porém, havia um problema: se o interceptor encontrasse o artifício utilizado para esconder as mensagens, o método de criptografia estaria quebrado e não seria mais útil. Dessa forma, era necessário estabelecer uma maneira segura na qual o receptor tivesse acesso ao método utilizado, podendo decodificar e ler a mensagem, gerando o que chamamos Problema da Distribuição de Chaves. Em decorrência desse Problema, surgiu um método muito conhecido e utilizado para a segurança de dados, a Criptografia RSA. Sendo assim, o objetivo desse trabalho é entender como ocorre a codificação e decodificação do método RSA, além de compreender a matemática desse método, que permite a troca segura de mensagens e evita qualquer tipo de violação. Vale ressaltar que o presente trabalho é fruto de uma atividade do Grupo PET-Matemática-UFCG, sob orientação do Tutor Prof. Dr. Daniel Cordeiro de Morais Filho, utilizando bibliografias sobre o assunto, como livros e dissertações.*
***Palavras-chave****: Problema da Distribuição de Chaves; Codificação de mensagens; Números primos.*

## 1. Introdução

Esconder uma mensagem é uma atividade muito comum, seja em uma situação banal, como brincar com a *língua do P* ou decifrar uma frase em um jogo de gibi ou, em outra situação, esconder informações importantes, como dados pessoais ou segredos governamentais. Manter essas informações importantes em segurança é uma tarefa de extrema necessidade, visto que, uma vez em mãos erradas, podem afetar uma nação, causar dívidas, problemas pessoais, entre outros. Por esse motivo, foram criados diversos métodos com a finalidade de que uma mensagem interceptada não pudesse ser decifrada. A técnica utilizada para transmitir informações cifradas chama-se *criptografia*.

Na criptografia, as *chaves* desenvolvem um papel muito relevante, elas guardam as informações utilizadas nos processos de codificação e decodificação, que dão acesso às mensagens. O termo "chave" faz analogia a uma mensagem trancada em uma caixa com um cadeado, onde apenas a chave certa fornece a mensagem guardada. É chamada *chave simétrica ou única* quando tanto o emissor quanto o receptor possuem a chave para abrir o cadeado, enquanto é chamada *chave assimétrica* quando o emissor utiliza um cadeado e apenas o receptor tem a chave para abri-lo.

Inicialmente, foram pensadas em *criptografias de chave simétrica*, como, por exemplo, a troca de letras por símbolos. Neste caso, em um texto extenso, o interceptador consegue perceber um padrão na repetição dos símbolos e, assim, pode facilmente decodificar a mensagem. Outro problema desse método é que o receptor deve conhecer a chave utilizada para criptografar a mensagem, ou seja, o emissor deve informá-lo do método. No entanto, nem sempre é possível informar pessoalmente esse código, tendo de confiar em uma terceira pessoa para fazer o intermédio, arriscando ter essas informações divulgadas.

Com as descobertas científicas e avanços tecnológicos, os computadores se tornaram amplamente acessíveis às corporações, implicando em um maior uso dos métodos de criptografia, e consequentemente, necessitando de mais pessoas para distribuir as chaves. Este problema foi denominado *Problema da distribuição de chaves*, no qual muitos pesquisadores e estudiosos se dedicaram a resolver. Segundo Singh (2004), um deles foi o matemático Whitfield Diffie (1944- ), que pensou em um método de criptografia no qual a chave utilizada para codificar não pudesse ser usada para decodificar, chamada *criptografias de chave assimétrica*.

No entanto, após anos de estudo junto ao criptógrafo Martin Hellman (1945 - ), ele não conseguiu elaborar um método como havia pensado, mas acreditava em sua ideia. Por isso, em 1975, Diffie publicou um resumo com a teoria da chave assimétrica, dando a largada a corrida pelo método. Os primeiros a passar pela linha de chegada foram os cientistas da computação, Ronald Rivest (1947 - ) e Adi Shamir (1952 - ), e o matemático Leonard Adleman (1945 - ), em 1977, dando início ao sistema *Criptografia RSA*.

A criptografia RSA é principalmente utilizada por sites para gerar certificados digitais que comprovam a autenticidade e integridade de uma mensagem. Um exemplo de empresas que usam esse tipo de criptografia é a *Amazon.com, Inc.* e, segundo Bonfim (2017), o site do Banco do Brasil.

## 2. Metodologia

O trabalho foi realizado em atividades do Grupo PET-Matemática-UFCG, através de revisões bibliográficas com textos renomados sobre o assunto, como o livro *Números Inteiros e Criptografia RSA*, do Professor Doutor Severino Collier Coutinho, e *O livro dos códigos*, de Simon Singh, Ph.D. em Física e ex editor de Ciência da BBC. Após os estudos e análise dos textos, foram realizadas reuniões com o tutor, Prof. Dr. Daniel Cordeiro, para orientação e desenvolvimento do trabalho. Em seguida, foi elaborado uma apresentação para o *XI Workshop Didático-Pedagógico de Prática de Ensino em Matemática*, uma das atividades do Grupo PET-Matemática-UFCG. Neste Workshop foi trabalhado a matemática por trás do método de Criptografia RSA, gerando discussões importantes sobre o assunto e sugestões de melhoria do trabalho.

## 3. Resultado e discussão

Como já citado, a Criptografia RSA é uma criptografia de chave assimétrica, isso significa que são utilizadas duas chaves para o processo, chamadas *Chave pública* e *Chave privada*. A chave pública é aquela divulgada pelo receptor para que as pessoas possam lhe enviar mensagens, enquanto a chave privada deve ser guardada para si, pois ela permite que a mensagem seja descriptografada pela pessoa que a possui. A forma como ocorre o processo de codificação e decodificação e como são definidas as chaves serão explicados mais à frente, mas antes iremos enunciar alguns resultados preliminares estudados.

### 3.1 Resultados preliminares

**Definição 1.** *Seja $\bar{a} \in \mathbb{Z}_n$. Dizemos que a classe $\bar{a'} \in \mathbb{Z}_n$ é o inverso multiplicativo de $\bar{a}$ se a igualdade $\bar{a} \cdot \bar{a'} = \bar{1}$ é satisfeita em $\mathbb{Z}_n$. (COUTINHO, 2005)*

**Teorema 1.** *(Teorema da inversão.) A classe $\bar{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$ se, e somente se, $mdc(a, n) = 1$. (COUTINHO, 2005)*

**Teorema 2.** *(Teorema de Bézout.) Sejam $a, b \in \mathbb{Z}$ e $d = mdc(a, b)$. Então existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. (MILIES; COELHO, 2006)*

**Teorema 3.** *(Pequeno Teorema de Fermat.) Seja $p$ um número primo e $a$ um inteiro que não é divisível por $p$. Então $a^{p-1} \equiv 1 \ (mod\ p)$. (COUTINHO, 2005)*

**Definição 2.** *(Função de Euler.) O número $\phi(n)$ é o número de inteiros positivos menores do que ou iguais a $n$, que são relativamente primos com $n$. Em especial, se $p$ é um número primo, então todos os inteiros positivos menores que $p$ são primos com $p$, ou seja, $\phi(p) = p - 1$. (COUTINHO, 2005)*

**Teorema 4.** *Se $m$, $n$ são inteiros positivos tais que $mdc(m, n) = 1$, então $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$. (COUTINHO, 2005)*

**Teorema 5.** *(Teorema Chinês dos Restos.)*

*Sejam $n_1, n_2, \ldots, n_k$ inteiros, relativamente primos dois a dois. Então o sistema*

$$\begin{aligned} x &\equiv a_1 \ (mod\ n_1) \\ &\vdots \\ x &\equiv a_k \ (mod\ n_k) \end{aligned}$$

*tem uma única solução em $\mathbb{Z}_{n_1 \cdot n_2 \cdots n_k}$. (MILIES; COELHO, 2006)*

### 3.2 Codificação

Antes de iniciar o processo de codificação é necessário que o receptor disponibilize sua chave pública contendo dois parâmetros: $n$ e $e$. Para isso, o receptor deve escolher dois primos distintos $p$ e $q$, e o produto entre eles será $n$. O parâmetro $e$ deve ser escolhido de forma que seja invertível módulo $\phi(n)$, em outras palavras, pelo Teorema 1, precisamos ter o $mdc(e, \phi(n)) = 1$. Recordando que, pelo Teorema 4 e Definição 2, podemos calcular $\phi(n)$.

Vamos dar um exemplo. Consideraremos $p = 3$ e $q = 17$, logo $n = 51$. Desse modo, aplicando o Teorema 4 e a Definição 2 em $n = 51$, temos $\phi(51) = 32$, e assim, consideraremos $e = 11$, pois $mdc(11, 32) = 1$. Portanto, a chave pública a ser disponibilizada será $(51, 11)$.

Conhecendo a chave pública escolhida pelo receptor, vamos fazer um teste e checar se o método funciona. Desse modo, criptografaremos a frase *Bombas de Turing*, remetendo a máquina criada pelo matemático e criptógrafo Alan Turing (1912–1954). Segundo o Singh (2004), a máquina recebeu esse apelido, pois sua abordagem mecânica tinha uma semelhança passageira com a *bomba de Marian Rejewski (1905-1980)*. Esse mecanismo ajudou a decifrar o código da máquina *Enigma* utilizada pelos alemães durante a guerra.

Dividiremos o processo de codificação em três passos:

1. **Pré-codificação**

   Primeiro de tudo, é necessário transformar a mensagem que desejamos enviar em números. Dessa forma, é utilizada uma tabela pré-formulada e de domínio público. Nesta tabela é necessário que todos os números tenham a mesma quantidade de dígitos para não gerar ambiguidades durante a decodificação. No exemplo a seguir, vamos utilizar a relação estabelecida na Figura 1.

Figura 1: Relação estabelecida pelos autores

| A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | **Espaço** |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 |

Fonte: Os autores

Fazendo a troca de letras pelos números na frase *Bombas de Turing*, encontramos o seguinte número:

$$12252312112937141537031281924 17. \tag{1}$$

2. **Separação em blocos**

   Feito a pré-codificação, o número obtido em (1) deve ser separado em pequenos blocos, de forma a serem menores que o parâmetro $n$ e não podem começar com zero. Vale ressaltar que esta separação não é única, podendo ser feita de diversas formas. Assim, para $n = 51$, separaremos a expressão (1) da seguinte maneira:

$$12 - 25 - 2 - 31 - 21 - 1 - 29 - 37 - 1 - 41 - 5 - 37 - 30 - 3 - 12 - 8 - 19 - 2 - 41 - 7. \tag{2}$$

3. **Codificação**

   Considerando $b$ cada um dos blocos separados em (2), neste passo será utilizado a *Aritmética Modular* para encontrar o resto da divisão de $b^e$ por $n$. Desse modo, basta calcularmos a forma reduzida de

$$C(b) := b^e (mod\ n). \tag{3}$$

Lembrando que o parâmetro $e = 11$, teremos cada um dos blocos elevados a 11.° potência. Desse modo, para facilitar os cálculos, será utilizada a linguagem de programação *Python* com a fórmula $[(b^{**}e)\ \%\ n]$, onde "$**$" indicam o expoente e o símbolo "%" encontra o resto da divisão de $(b^{**}e)$ por $n$. Efetuando as operações usando a *Aritmética Modular*, temos

$$12^{11} \equiv 6\ (mod\ 51) \quad 25^{11} \equiv 19\ (mod\ 51) \quad 2^{11} \equiv 8\ (mod\ 51) \quad 31^{11} \equiv 10\ (mod\ 51) \quad 21^{11} \equiv 30\ (mod\ 51)$$
$$1^{11} \equiv 1\ (mod\ 51) \quad 29^{11} \equiv 23\ (mod\ 51) \quad 37^{11} \equiv 7\ (mod\ 51) \quad 41^{11} \equiv 14\ (mod\ 51) \quad 5^{11} \equiv 11\ (mod\ 51)$$
$$30^{11} \equiv 21\ (mod\ 51) \quad 3^{11} \equiv 24\ (mod\ 51) \quad 8^{11} \equiv 2\ (mod\ 51) \quad 19^{11} \equiv 25\ (mod\ 51) \quad 7^{11} \equiv 31\ (mod\ 51).$$

Assim, chegamos nos seguintes blocos codificados:

$$6 - 19 - 8 - 10 - 30 - 1 - 23 - 7 - 1 - 14 - 11 - 7 - 21 - 24 - 6 - 2 - 25 - 8 - 14 - 31. \tag{4}$$

O número enviado para o receptor é o encontrado em (4). Não devemos juntar os blocos novamente, pois caso o fizesse, poderia causar confusão no momento da decodificação.

### 3.3 Decodificação

Na etapa de decodificação dos blocos cifrados, o receptor precisará apenas de duas informações: $n$ e o inverso de $e$ em $\phi(n)$ (Teorema 1) que chamaremos de $d$. Pelo Teorema 2, temos $ed = 1 + k\phi(n)$, com $k$ inteiro, e assim pode-se obter $d$ da seguinte forma:

$$d \cdot e \equiv 1\ (mod\ (p-1)(q-1)).$$

Como apenas o receptor conhece os números primos $p$ e $q$, somente ele conseguirá facilmente resolver a equação usando *Aritmética Modular* sem precisar fatorar $n$, chegando em $d = 3$. Assim, a chave privada, que deve ser apenas do conhecimento do receptor, será $(p, q, d)$.

Por último, para decodificar a mensagem cifrada, ele deve encontrar o resto da divisão de $a^d$ por $n$, onde $a$ é cada um dos blocos codificados de (4). Isto é,

$$D(a) := a^d\ (mod\ n). \tag{5}$$

Aplicando os blocos (4) da mensagem codificada em (5), obtemos

$$6^3 \equiv 12\ (mod\ 51) \quad 19^3 \equiv 25\ (mod\ 51) \quad 8^3 \equiv 2\ (mod\ 51) \quad 10^3 \equiv 31\ (mod\ 51) \quad 30^3 \equiv 21\ (mod\ 51)$$
$$1^3 \equiv 1\ (mod\ 51) \quad 23^3 \equiv 29\ (mod\ 51) \quad 7^3 \equiv 37\ (mod\ 51) \quad 14^3 \equiv 41\ (mod\ 51) \quad 11^3 \equiv 5\ (mod\ 51)$$
$$21^3 \equiv 30\ (mod\ 51) \quad 24^3 \equiv 3\ (mod\ 51) \quad 2^3 \equiv 8\ (mod\ 51) \quad 25^3 \equiv 19\ (mod\ 51) \quad 31^3 \equiv 7\ (mod\ 51).$$

Observe que reescrevendo os blocos com essa nova relação de congruência, temos

$$12 - 25 - 2 - 31 - 21 - 1 - 29 - 37 - 1 - 41 - 5 - 37 - 30 - 3 - 12 - 8 - 19 - 2 - 41 - 7,$$

justamente o conjunto de blocos obtidos em (2). Neste momento, podemos juntar os números novamente e separá-los de dois em dois para utilizar a relação entre números e letras da Figura 1. Feita a relação chegamos na mensagem desejada: *Bombas de Turing*.

### 3.4 Por que funciona?

Já vimos como ocorre o processo de codificação e decodificação do método RSA, mas até agora só mostramos um caso particular. A pergunta que fica é: será que o método funciona para outros números que seguem as condições citadas, ou esse foi um caso isolado? E se funcionar para qualquer número, por que funciona? Nesta seção pretendemos responder essas perguntas.

A ideia do método é que os passos de codificação e decodificação sejam inversos, ou seja, conseguiremos voltar para o bloco pré-codificado utilizando as funções (3) e (5), além dos parâmetros definidos. Em outras palavras, desejamos mostrar que $D(C(b)) \equiv b \ (mod\ n)$, onde $C(b)$ é o resto da divisão de $b^e$ por $n$ e $D(a)$ é o resto da divisão de $a^d$ por $n$. Dessa forma, $D(C(b)) \equiv (b^e)^d \ (mod\ n) \equiv b^{ed} \ (mod\ n)$.

Logo, pelo Teorema 2, como o $mdc(e, \phi(n)) = 1$ existem $d$ e $k$ inteiros tais que $ed = 1 + k\phi(n)$. Além disso, pelo Teorema 1, concluímos que $d$ é inverso de $e$ módulo $\phi(n)$. Portanto,

$$b^{ed} \equiv b^{1+k\phi(n)} \equiv b \cdot (b^{\phi(n)})^k \equiv b \cdot b^{k(p-1)(q-1)} \ (mod\ n).$$

Sabendo que $p$ e $q$ são números primos distintos e $n = pq$, pelo Teorema 5, podemos calcular a forma reduzida de $b^{ed}$ módulo $p$ e $b^{ed}$ módulo $q$. Comecemos por $p$. Assim, temos dois casos a considerar: $p$ não divide $b$ ou $p$ divide $b$. Se a primeira situação ocorre, então pelo Teorema 3, segue

$$b^{p-1} \equiv 1(mod\ p) \Rightarrow b^{ed} \equiv b \ (mod\ p).$$

Caso contrário, temos

$$b^{p-1} \equiv 0(mod\ p) \Rightarrow b^{ed} \equiv b \ (mod\ p).$$

De forma análoga, fazemos para módulo $q$ e chegamos a conclusão de que a congruência vale para quaisquer $p$ e $q$. Em outras palavras, $b^{ed} - b$ é divisível por $p$ e $q$. Além disso, $p$ e $q$ são números primos distintos tais que $mdc(p, q) = 1$, então temos $b^{ed} - b$ é divisível por $n$, concluindo

$$b^{ed} \equiv b \ (mod\ n), \text{ para qualquer inteiro } b.$$

Um fator muito importante para a segurança desse método é a escolha dos números $p$ e $q$. A nível de exemplo, utilizamos números primos muito pequenos, de forma que facilmente o parâmetro $n$ possa ser fatorado, o que permite a qualquer pessoa obter $p$ e $q$ e decifrar a mensagem. Dessa forma, é necessário utilizar números primos muito grandes, dificultando ainda mais a fatoração do parâmetro $n$ e garantindo que ninguém além do receptor irá ler as mensagens enviadas. No livro de Coutinho (2005) explica como escolher esses números para o uso do método, pois não podemos apenas escolher números primos grandes, mas devemos nos certificar que a diferença entre eles não é pequena.

## 4. Conclusões

Durante o processo de criptografia apresentado neste trabalho, é possível perceber o quão importante a matemática foi para o desenvolvimento do método RSA. As propriedades da *Aritmética Modular* e o uso dos números primos, possibilitaram o desenvolvimento desse método seguro. Vale salientar, que a dificuldade de identificar a fatoração de números muito grandes em produtos de potências de primos, torna a mensagem cifrada difícil de ser quebrada.

## Agradecimentos

O presente trabalho foi parcialmente financiado pelo FNDE, Fundo Nacional de Desenvolvimento da Educação-Brasil, por meio da bolsa fornecida para o Grupo PET-Matemática-UFCG, do qual os autores fazem parte.

## Referências

BONFIM, D. H. *Criptografia RSA*. [s.n.], 2017. 49-51 p. Disponível em: ⟨https://teses.usp.br/teses/disponiveis/55/55136/tde-06042017-164507/publico/DanieleHelenaBonfim_revisada.pdf⟩. Citado na página 2.

COUTINHO, S. *Números inteiros e criptografia RSA*. [S.l.]: IMPA, 2005. Citado 2 vezes nas páginas 2 e 5.

MILIES, C. P.; COELHO, S. P. *Números: uma Introdução à Matemática*. [S.l.]: Edusp, 2006. ISBN 978-8531404580. Citado na página 2.

SINGH, S. *O livro dos códigos*. RECORD, 2004. ISBN 9788501055989. Disponível em: ⟨https://books.google.com.br/books?id=yUpTa5WLWv0C⟩. Citado 2 vezes nas páginas 1 e 3.

# UMA DEMONSTRAÇÃO BEM DIFERENTE DO EXCÊNTRICO PAUL ERDÖS

**Jonas Barros Lima de Medeiros**[1] **- jonas.lima@estudante.ufcg.edu.br**
**Rodrigo Marques Faustino da Silva**[1] **- rodrigo.marques@estudante.ufcg.edu.br**
**Daniel Cordeiro de Morais Filho**[1] **- daniel@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil - Parcialmente Financiado pelo MEC/FNDE/PET

***Resumo:*** *As demonstrações matemáticas são ferramentas utilizadas pelos matemáticos para mostrar a veracidade de algumas sentenças matemáticas, podendo variar em diversos tipos e tecnicidades. Este trabalho tem como objetivo explanar uma demonstração inusitada da infinitude dos números primos feita por um brilhante e excêntrico matemático húngaro, chamado Paul Erdös (1913 - 1996). Com isto, pretendemos alcançar, principalmente os discentes da graduação, estimulando sua curiosidade matemática, exibindo uma demonstração possivelmente ainda não vista, inusitada e que vale a pena ler aos auspícios de seu criador. Esse trabalho foi realizado por meio de uma atividade do Grupo PET-Matemática-UFCG, intitulada "Pesquisa em competências básicas no uso da língua escrita e oral, em idioma estrangeiro e na área de tecnologias de informação e comunicação", na qual o Prof. Tutor Daniel Cordeiro sugeriu uma referência, que foi lida e estudada pelos autores petianos, para que posteriormente fosse desenvolvido, pelo autores, um trabalho, com um conteúdo que tivesse uma abordagem mais acessível, didática e com as notações simplificadas. Vale salientar que, além do presente trabalho ser revisado e lido pelos demais integrantes do PET, foi exposto no Workshop Didático-Pedagógico, com intuito de testar a metodologia que foi usada para torná-lo mais inteligível para um nível de conhecimento dos alunos inciantes dos cursos de Matemática. Por fim, esperamos que os leitores deste trabalho apreciem essa belíssima demonstração da infinitude dos números primos e agreguem mais conhecimento à sua caminhada acadêmica.*
***Palavras-chave****: Demonstração Inusitada; Números Primos; Paul Erdös*

## 1. Introdução

Segundo Filho (2016), uma demonstração matemática é uma cadeia dedutiva de raciocínio que usa argumentos válidos e uma sequência finita de sentenças, que podem ser axiomas, teoremas, definições, hipóteses ou até mesmo uma sentença resultante da anterior. Nesse contexto, podemos ressaltar que nem sempre as demonstrações matemáticas são fáceis de serem compreendidas pelos iniciantes, pois existem casos em que os argumentos são carregados de notações e resultados técnicos ou muito sofisticados. Ainda mais, pela natureza das demonstrações matemáticas, existem diversos tipos delas e, como todas as obras primas, vão das mais simples às mais elegantes demonstrações.

Mostrar que o conjunto dos números primos é infinito pode parecer uma tarefa fácil, como fez parecer o matemático Euclides de Alexandria (300 a.C - desconhecida), que provou essa afirmação utilizando o método de demonstração *ad adsurdum* e um raciocínio extremamente brilhante, até hoje admirado e utilizado (BOYER; MERZBACH, 2010). Segundo Ribenboim (2001), vários matemáticos já demonstraram essa afirmação de formas totalmente distintas, tais como: Ernt Kummer (1810 - 1893), Chales Hermite (1822 - 1901), Christian Goldbach (1690 - 1764), Leonard Euler (1707 - 1783) etc. Porém, neste trabalho, vamos voltar nossos olhos para uma elegante, inesperada e inusitada demonstração feita por um engenhoso matemático húngaro chamado Paul Erdös (1913 - 1996).

Filho de professores de Matemática, em sua infância, Paul Erdös já mostrava seus talentos na Matemática. Segundo Brusamarello e Carmelo (2009), enquanto brincava com os números, após uma pessoa dizer o ano que tinha nascido, ele devolvia rapidamente a quantidade de dias, horas e segundos que ela tinha vivido. Quando adulto, Erdös era bastante conhecido por seu diferente e exótico estilo de vida. Passando por diversos países, trabalhando com os mais variados matemáticos, ele não via prazer em angariar bens materiais devido às suas

contribuições, Erdös adaptava-se rapidamente aos diversos ambientes para qual viajava com um único propósito: resolver os problemas "mais difíceis"da Matemática. Erdös deixou diversas contribuições em várias áreas da Matemática, no entanto, trabalhou mais diretamente nas áreas de Teoria dos Números e Análise Combinatória. Segundo Brusamarello e Carmelo (2009), a contribuição desse notável matemático foi tão reconhecida que ele foi homenageado com um número, chamado Número de Erdös, que "mede"a proximidade de um pesquisador que trabalhou com esse matemático.

A demostração que iremos expor neste trabalho pode ser encontrada no livro intitulado: *Proofs From the Book*, (ZIEGLER; HOFMANN, 2014), cuja tradução para o português ficou como "Provas do Livro". Para Erdös, existem demostrações que são consideradas verdadeiras obras de arte, assim, era necessário reunir as melhores e mais elegantes demostrações de cada resultado matemático em um único livro que as contenham, não um livro qualquer, mas "O livro". Além de deixar sua marca registrada neste livro, Paul Erdös indicou demonstrações e soluções de outros matemáticos, entretanto, acabou falecendo antes da publicação do livro.

Passemos à parte matemática de nosso artigo. Podemos evidenciar um fato muito interessante que acontece quando começamos a manipular os números naturais. Observe que, ao olharmos para os inversos dos números naturais, $1/n$ tal que $n \in \mathbb{N}$, podemos deduzir: quanto maior o número $n$, mais o valor da fração se aproxima de zero. Entretanto, impressionantemente, a sequência das somas parciais da série

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots$$

não vai para zero, em verdade, tende para mais infinito. Essa série anterior é muito importante no Cálculo Diferencial e Integral e é chamada de Serie Hârmonica (THOMAS, 2012). Mais surpreendentemente ainda, Erdös, seguindo as ideias da demonstração feita por Euler, (ZIEGLER; HOFMANN, 2014), selecionou os inversos dos números primos e, com o mesmo raciocínio anterior, apostou suas expectativas na divergência dessa parte da Série Harmônica

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} \dots$$

A aposta de Erdos foi bastante ousada, pois quando selecionamos uma quantidade infinita de números naturais, mas não todos, a série formada pelos inversos dos números selecionados pode convergir ou não para um número real. A saber, se selecionarmos as potências de 2 e considerarmos a série dos inversos desses números, $\sum(1/2)^n$, obtemos uma série geométrica, que sabemos ser convergente. E, assim, Euler abriu um caminho para Erdös exibir uma nova forma de demonstrar a infinitude dos números primos.

Neste trabalho, provaremos que a série dos inversos dos primos diverge e, consequentemente, obteremos uma demonstração da infinitude dos números primos!

## 2. Metodologia

O presente trabalho é fruto das atividade do Grupo PET-Matemática-UFCG, intitulada: "Pesquisa em competências básicas no uso da língua escrita e oral, em idioma estrangeiro e na área de tecnologias de informação e comunicação", "Workshop Didático-Pedagógico" e "Redação e Participação em Encontros Científicos". Inicialmente, o Prof. Tutor Daniel Cordeiro, indicou uma referência em inglês para que fosse lida e estudada pelos tutorandos. Logo após realizada a leitura e o estudo, os discentes desenvolveram um conteúdo específico, visando trazer uma abordagem mais simplificada e didática do tema tratado, abrandando as notações e, assim, promovendo um melhor entendimento dos resultados. Além disso, em sua fase de escrita, o trabalho foi lido pelos demais integrantes do PET com o intuito de que fossem feitos apontamentos para aprimoramento do texto. Por fim, foi apresentado em outra atividade do Grupo, intitulada como: Workshop Didático-Pedagógico, com o objetivo de testar a metodologia e encontrar uma melhor maneira para ser exposto.

## 3. Resultado e discussão

Antes de exibir a inesperada demonstração do matemático Paul Erdös sobre a infinitude dos números primos, iremos vislumbrar alguns resultados e definições preliminares para ajudar no entendimento da demonstração do teorema principal.

A partir do Princípio da Boa Ordem, consideremos a sequência dos números primos $(p_1, p_2, p_3, \ldots)$ ordenada de forma crescente. Sejam $N$ e $k$ números naturais fixos a serem escolhidos posteriormente, definamos os conjuntos

$$A_k = \{p_1, p_2, p_3, \ldots, p_k\} \text{ e } B_k = \{p_{k+1}, p_{k+2}, \ldots, p_m, \ldots\}.$$

Agora, a partir de $A_k$ e $B_k$, definamos os conjuntos:

$$D_N^{A_k} := \{n \in \mathbb{N}; n \leq N \text{ e, ou } n = 1 \text{ ou } n \text{ é divisível somente por elementos de } A_k\},$$

$$D_N^{B_k} := \{n \in \mathbb{N}; n \leq N \text{ e } n \text{ é divisível por algum elemento de } B_k\}.$$

Observe que $D_N^{A_k}$ e $D_N^{B_k}$ são finitos, pois os elementos deles também são números naturais menores do que $N$.

Vejamos a seguinte propriedade entre os conjuntos $D_N^{A_k}$ e $D_N^{B_k}$.

***Lema 1:*** Os conjuntos $D_N^{A_k}$ e $D_N^{B_k}$ são finitos, disjuntos e

$$card(D_N^{A_k}) + card(D_N^{B_k}) = card(D_N^{A_k} \cup D_N^{B_k}) = N.$$

***Demonstração.*** Observemos que se $n \in D_N^{A_k}$, então $n$ é divisível apenas por elementos de $A_k$, logo, não é divisível por nenhum elemento de $B_k$ e, assim, $n \notin D_N^{B_k}$. Dessa forma, $D_N^{A_k} \cap D_N^{B_k} = \emptyset$.

Provemos agora que sendo $n \leq N$ natural, temos $n \in D_N^{A_k} \cup D_N^{B_k}$. Notemos que $1 \in D_N^{A_k} \cup D_N^{B_k}$. Agora, seja $n$ um número natural tal que $1 \leq n \leq N$, então existe, pelo Teorema Fundamental da Aritmética, um número primo $p_i$ que divide $n$. Se $n$ é divisível apenas por números primos de $A_k$, então $n \in D_N^{A_k}$, caso contrário, existiria um $p_i$ de $B_k$ que dividiria $n$ e, assim, $n \in D_N^{B_k}$. Daí, se $n \leq N$, então $n \in D_N^{A_k} \cup D_N^{B_k}$. Portanto, o conjunto $\{1, \ldots, N\} \subset D_N^{A_k} \cup D_N^{B_k}$ e, por definição, $D_N^{A_k}, D_N^{B_k} \subset \{1, \ldots, N\}$. Desse modo, $D_N^{A_k} \cup D_N^{B_k} = \{1, \ldots, N\}$. Portanto, $card(D_N^{A_k}) + card(D_N^{B_k}) = card(D_N^{A_k} \cup D_N^{B_k}) = N$. ***C.Q.D***

Segundo Filho (2016), pelo Princípio da Contrapositividade, uma sentença $(H \Rightarrow T)$ será válida se, e somente se, sua contrapositiva $(^{\sim}T \Rightarrow ^{\sim} H)$ for válida. Logo, se demonstrarmos $(^{\sim}T \Rightarrow ^{\sim} H)$, temos assegurada a validade de $(H \Rightarrow T)$, onde $H$ é a hipótese e $T$ a tese de uma sentença matemática. Tendo isso em vista, para mostrar que o conjunto dos números primos $\mathbb{P}$ é infinito, basta utilizarmos a seguinte lógica: Se $\mathbb{P}$ é finito, então $\sum \frac{1}{p_i}$ converge. A contrapositiva é:

$$\text{Se } \sum \frac{1}{p_i} \text{ diverge, então } \mathbb{P} \text{ é infinito.}$$

Assim, provaremos que $\sum \frac{1}{p_i}$ diverge, com $p_i \in \mathbb{P}$, e consequentemente, teremos que o conjunto dos números primos é infinito. Vejamos a demostração do resultado principal.

***Teorema:*** O conjunto dos números primos é infinito.

***Demonstração.*** Primeiramente, suponhamos por contradição que $\sum_{i=1}^{\infty} \frac{1}{p_i}$ converge. Desse modo, obtemos a soma dos últimos termos se aproximando de zero:

$$\lim_{k\to\infty} \left( \sum_{i=k+1}^{\infty} \frac{1}{p_i} \right) = \lim_{k\to\infty} \left( \sum_{i=1}^{\infty} \frac{1}{p_i} - \sum_{i=1}^{k} \frac{1}{p_i} \right) = 0.$$

Portanto, pela definição de limite, existe $k_0 \in \mathbb{N}$ tal que, para $k > k_0$, temos

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2} \Rightarrow \sum_{i=k+1}^{\infty} \frac{N}{p_i} < \frac{N}{2}. \tag{1}$$

Sejam $k \geq k_0$ fixo e $N$ um número natural fixo. Consideremos os conjuntos $A_k, B_k, D_N^{A_k}$ e $D_N^{B_k}$ conforme definido inicialmente. Mostraremos que, para um número natural $N$ adequado,

$$card(D_N^{A_k}) + card(D_N^{N_k}) < N$$

o que contraria o Lema 1.

Definamos $\lfloor x \rfloor$ como sendo o piso de $x \in \mathbb{R}$ , onde $\lfloor x \rfloor$ é o maior número inteiro menor do que ou igual a $x$. Logo, de (1), segue que

$$\sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \leq \sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2} \Rightarrow \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}, \tag{2}$$

sendo $\left\lfloor \frac{N}{p_i} \right\rfloor$ a imagem de $\frac{N}{p_i}$ pela função piso. Agora, estimemos a quantidade de elementos de $D_N^{B_k}$. Se $m \in D_N^{B_k}$, então $m \leq N$ e existe um número primo $p_i \in B_k$ que divide $m$, logo $m$ é um múltiplo de $p_i$, com $p_i \in B_k$. Assim, todo elemento de $D_N^{B_k}$ é múltiplo de algum $p_i$ de $B_k$ e é menor do que ou igual a $N$. Portanto,

$$D_N^{B_k} \subset M := \{rp_i; r \in \mathbb{N}, p_i \in B_k \text{ e } rp_i \leq N\}.$$

Observe que $\left\lfloor \frac{N}{p_i} \right\rfloor$ é a quantidade de múltiplos de $p_i$ menores do que $N$. Observe também que $M$ é finito, pois, para primos suficientemente grandes, teremos $rp > N$ para todo $n \in \mathbb{N}$. Logo, na soma a seguir, há apenas uma finidade de parcelas não nulas:

$$card(M) = \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \Rightarrow card(D_N^{B_k}) \leq card(M) = \sum \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \tag{3}$$

Estimemos a quantidade de elementos de $D_N^{A_k}$. Para auxiliar na estimativa de quantos elementos $D_N^{A_k}$ possui, decomponhamos os elementos $m$ de $D_N^{A_k}$ como produto de números primos, isto é, $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, com $p_i \neq p_j$ para $i \neq j$, o que é possível pelo Teorema Fundamental da Aritmética (SANTOS, 2003). Utilizando o Algoritmo da Divisão de Euclides, reescrevendo as potências da forma $\alpha_i = 2l_i + \beta_i$, com $l_i \geq 0$ e $\beta_i \in \{0, 1\}$, podemos reescrever $m$ da seguinte maneira:

$$m = (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}) \cdot (p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_k^{l_k})^2 = a_m \cdot b_m^2,$$

onde $a_m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ e $b_m = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_k^{l_k}$. Pelo fato de que $m \in D_N^{A_k}$ e $a_m$ ser livre de quadrados, segue-se que $a_m$ é o produto de diferentes elementos de $A_k$ e $a_m \leq a_m b_m^2 = m \leq N$. Concluímos, pelo Princípio Fundamental da Contagem, que existem até $2^k$ diferentes números $a_m$ livres de quadrado. Ou seja, a quantidade de termos $Q(a_m)$ de $a_m$ cumpre

$$Q(a_m) \leq 2^k. \tag{4}$$

Daí, encontramos uma cota superior para $Q(a_m)$.

Agora, note que

$$a_m \geq 1 \Rightarrow a_m b_m^2 \geq b_m^2 \Rightarrow m \geq b_m^2 \Rightarrow b_m \leq \sqrt{m}.$$

Ainda mais, como $m \leq N$, verifica-se

$$\sqrt{m} \leq \sqrt{N} \Rightarrow b_m \leq \sqrt{m} \leq \sqrt{N}.$$

Daí, encontramos uma conta superior para a quantidade $Q(b_m)$ de possíveis $b_m$. A saber:

$$Q(b_m) \leq \sqrt{N}. \tag{5}$$

De (4) e (5) segue-se que

$$Q(a_m) \leq 2^k \text{ e } Q(b_m) \leq \sqrt{N} \Rightarrow card(D_N^{A_k}) = Q(a_m) \cdot Q(b_m) \leq 2^k \sqrt{N}.$$

Recordando que $card(D_N^{B_k}) \leq \frac{N}{2}$, resta encontrar um $N$ natural tal que

$$card(D_N^{A_k}) = 2^k\sqrt{N} \leq \frac{N}{2}.$$

Ou seja, precisamos encontrar um $N$ tal que

$$2^k\sqrt{N} \leq \frac{N}{2} \Leftrightarrow 2^{k+1}\sqrt{N} \leq N \Leftrightarrow 2^{2(k+1)}N \leq N^2 \Leftrightarrow 2^{2(k+1)} \leq N.$$

Com essa finalidade, basta tomar $N = 2^{(2k+2)}$, que, por conseguinte,

$$card(D_N^{B_k}) < \frac{N}{2} \text{ e } card(D_N^{A_k}) \leq \frac{N}{2} \Rightarrow card(D_N^{A_k}) + card(D_N^{B_k}) < \frac{N}{2} + \frac{N}{2} = N.$$

O que contraria o Lema 1. Portanto, o conjunto dos números primos é infinito. ***C.Q.D.***

## 4. Conclusões

O presente trabalho possibilitou que os petianos envolvidos treinassem e aperfeiçoassem suas habilidades na língua estrangeira inglês, através de uma elegante e criativa demontração feita pelo excêntrico matemático Paul Erdös. Além disso, com a tradução e simplificação das notações, eles também puderam trabalhar a parte de redação e escrita matemática aguçando, assim, suas habilidades para redigir demonstrações. Ainda mais, pôde-se aperfeiçoar as habilidades pedagógicas a fim de tornar a demonstração original mais acessível e atraente para os alunos iniciantes nos cursos de Matemática.

A demonstração vista é um tanto inusitada, pois Paul Erdös colocou todas as suas apostas nos ensinamentos do grande mestre Euler, que também demonstrou a infinitude dos números primos. Ainda mais, ao fazer a própria demonstração da infinitude dos números primos, inspirado por Euler, provando a divergência da série dos inversos dos números primos, Erdös utilizou técnicas e ferramentas belíssimas que nos faz abrir a mente admirando-se com essa inusitada criatividade.

## Agradecimentos

O presente trabalho foi parcialmente financiado pelo FNDE, Fundo Nacional de Desenvolvimento da Educação - Brasil, por meio da bolsa fornecida para o Grupo PET-Matemática-UFCG, do qual somos integrantes. Particularmente, agradecemos ao nosso Prof. Tutor Daniel Cordeiro que, com muito entusiamo, nos apresentou essa belíssima demostração, e nos guiou sabiamente, sendo imprescindível em seus apontamentos. Ainda mais, agradecemos imensamente aos nossos colegas de Grupo que demandaram do seu tempo e energia para revisar e tecer sugestões de aperfeiçoamentos para melhoria do nosso trabalho.

## Referências

BOYER, C.; MERZBACH, U. C. *A History of Mathematics*. United States of America: Jhon Wiley Sos, 2010. Citado na página 1.

BRUSAMARELLO, R.; CARMELO, E. L. M. Paul erdös, o mago. *Matemática Universitária*, v. 43, p. 74–81, 2009. Citado 2 vezes nas páginas 1 e 2.

FILHO, D. C. D. M. *Um Convite à Matemática*. Rio de Janeiro: SBM, 2016. Citado 2 vezes nas páginas 1 e 3.

RIBENBOIM, P. *Números Primos: Mistérios e Recordes*. Rio de Janeiro: IMPA, 2001. Citado na página 1.

SANTOS, J. P. D. O. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2003. Citado na página 4.

THOMAS, G. B. *Cálculo*. São Paulo: Pearson Education do Brasil, 2012. Citado na página 2.

ZIEGLER, G. M.; HOFMANN, K. H. *Proofs From the Book*. United States of America: Springer, 2014. Citado na página 2.

# Uma aplicação não muito convencional da Topologia na Aritmética: uma demonstração da infinitude dos números primos

**Bruna Alves da Silva Santos**[1] **- bruna.silva@estudante.ufcg.edu.br**
**Matheus da Silva Nascimento**[1] **- matheus.s.nascimento@estudante.ufcg.edu.br**
**Daniel Cordeiro de Morais Filho**[1] **- daniel@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil - Parcialmente financiado pelo MEC/FNDE/PET

***Resumo:*** *Após o matemático Henri Poincaré (1854-1912) publicar um artigo intitulado Analysis situs (POINCARÉ, 1895), que foi pioneiro na criação da Topologia, essa área de pesquisa avançou bastante e passou a contribuir indispensavelmente nas principais áreas de estudo de Matemática. Neste trabalho, desenvolvido pelo Grupo PET-Matemática-UFCG e orientado pelo professor Daniel Cordeiro, perceberemos o quanto a linguagem topológica pode ser abrangente, fato que exemplificaremos por meio de um uso nada convencional da topologia na demonstração do famoso Teorema de Euclides sobre a infinitude dos números primos (FURSTENBERG, 1955). Tal demonstração é fundamentada na introdução de uma topologia no conjunto discreto $\mathbb{Z}$, baseada em uma definição bastante criativa de conjunto aberto, intuitivamente bem diferente da que estudamos nos espaços euclidianos completos usuais.*
***Palavras-chave****: Topologia; Números primos; Conjuntos abertos*

## 1. Introdução

Dentre as principais linhas de estudo de Matemática, podemos dizer que a Topologia é a mais nova delas. Segundo Eves (2011), o primeiro artigo inteiramente dedicado à Topologia, foi publicado no final do século XIX, com o título de *Analysis situs* (POINCARÉ, 1895), sob a autoria de Henri Poincaré (1854-1912). Após essa publicação de Poincaré, esse campo de estudos tornou-se indispensável na Matemática e passou a receber a contribuição de um número cada vez maior de pesquisadores.

Durante a graduação do estudante de Matemática, a primeira vez em que ouvimos o termo "Topologia"é nos cursos de Cálculo e de Análise Matemática. Neles somos apresentados à topologia dos espaços euclidianos, cujos conceitos são a base para o estudo de limites de funções, continuidades etc. Apesar desses serem os exemplos mais comuns de topologias, eles não são os únicos, aliás, os conceitos topológicos são bem mais abrangentes.

Por outro lado, os números primos é um tema que encanta matemáticos de todas as épocas, em especial a infinitude desse conjunto de números já recebeu diversas demonstrações, com as mais variadas argumentações. Uma demonstração da infinitude dos números primos, muito interessante, foi dada por Hillel Fürstenberg (1935), publicada na revista *American Mathematical Monthly* (FURSTENBERG, 1955), na qual foram utilizados conceitos da Topologia. Esta demonstração, posteriormente, também apareceu no famoso livro *Proofs from the book* (ZIEGLER; HOFMANN, 2014), que por sua vez, contém belíssimas demonstrações de resultados famosos da Matemática.

Em geral, a ideia que um estudante de Matemática pode ter, a princípio, é que os conceitos de Topologia só aparecem para conjuntos contínuos. Neste trabalho, faremos uma demonstração da infinitude dos números primos, por meio de conceitos topológicos, a medida que introduziremos uma topologia em um conjunto discreto, neste caso, o conjunto dos números inteiros, que foge as situações mais usuais. Tal demonstração não só encanta pela imparidade dos argumentos utilizados, mas também pelo uso da linguagem topológica que é capaz de proporcionar uma excelente degustação, até mesmo para aqueles que por ventura já conhecem este campo de estudos da Matemática.

## 2. Metodologia

Este trabalho é oriundo de uma atividade do Grupo PET-Matemática-UFCG, que visa o desenvolvimento de trabalhos de caráter científico na área de Matemática. A metodologia é exploratória bibliográfica, na qual de

início o Tutor do Grupo nos apresentou o artigo sobre a infinitude dos números primos de autoria do matemático Hillel Fürstenberg. A partir daí, buscamos outras referências, em português e em língua estrangeira, para estudar sobre topologia e assim explorar e dar uma apresentação pessoal, usando os argumentos presentes na demonstração que aparece no artigo do Hillel Fürstenberg. Desse modo, o desenvolvimento deste trabalho também coincidiu com a atividade intitulada "Pesquisa em Competências Básicas no Uso da Linguagem Escrita e Oral, em Idioma Estrangeiro e na Área de Tecnologias de Informação e Comunicação", uma vez que usamos textos em inglês para elaboração do trabalho.

Ao longo do desenvolvimento do trabalho foram reservados horários de estudo individual, bem como de horários de reuniões com o Tutor, para que fossem feitas as devidas orientações para o estudo e a confecção do trabalho final. Ademais, também foi elaborado uma apresentação para os seminários internos do Grupo PET-Matemática-UFCG, relacionados à atividade intitulada "XI Workshop Didático-Pedagógico de Prática de Ensino em Matemática".

## 3. Resultado e discussão

### 3.1 Resultados básicos

Primeiro, vamos definir topologia, para isso escolhemos a definição adaptada de Lima (2009):

**Definição 1.** *Seja $X$ um conjunto qualquer. Uma topologia em $X$ é uma coleção $\tau$ de subconjuntos de $X$, denominados **abertos** (segundo a topologia $\tau$), que cumpre as seguintes condições:*

*i) $X$ e $\emptyset$ são abertos;*

*ii) Se $A_1, A_2, \cdots, A_n$ são subconjuntos abertos de $X$, então a interseção $A_1 \cap A_2 \cap \cdots \cap A_n$ é um conjunto aberto;*

*iii) Se $(A_\alpha)_{\alpha \in L}$ é uma coleção qualquer de subconjuntos abertos de $X$, então a união $\bigcup_{\alpha \in L} A_\alpha$ é um conjunto aberto.*

Para nossas finalidades precisaremos também da definição de conjuntos fechados e de uma importante propriedade deles:

**Definição 2.** *Um subconjunto $F$ de $X$ é dito **fechado**, quando seu complementar $F^C$, em relação a $X$, for um conjunto aberto.*

Ao longo do texto, faremos o uso de duas notações para tratar do complementar de um conjunto, a saber $F^C$ e $X \setminus F$.

**Proposição 1.** *A união de dois subconjuntos fechados $F_1$ e $F_2$ de $X$, resulta em um conjunto fechado.*

***Demonstração.*** De fato, pela Lei de De Morgan, podemos escrever

$$(F_1 \cup F_2)^C = F_1^C \cap F_2^C.$$

Ademais, como os conjuntos $F_1$ e $F_2$ são fechados, então pela Definição 2, os conjuntos $F_1^C$ e $F_2^C$ são abertos. Consequentemente, pelo item ii) da Definição 1 a interseção desses abertos resultará em um conjunto aberto, ou seja, $(F_1 \cup F_2)^C$ é aberto e portanto, o conjunto $F_1 \cup F_2$ é fechado. ■

**Corolário 1.1.** *A união finita de subconjuntos fechados $F_1, F_2, \cdots, F_n$ de $X$, é ainda um conjunto fechado.*

### 3.2 A definição da topologia

A partir de agora, voltaremos nossa atenção para o conjunto dos números inteiros, daí precisaremos adotar uma estratégia para estabelecer quando um subconjunto de $\mathbb{Z}$ é aberto. Nossa estratégia vai se basear em progressões aritméticas, fundamentada na seguinte definição:

**Definição 3.** *Dados $a, b \in \mathbb{Z}$, com $b > 0$, uma progressão aritmética será uma sequência (infinita) da forma*

$$P_{a,b} = \{a + bn\,;\, n \in \mathbb{Z}\}\,.$$

**Exemplo 1.** *Considerando $a = 0$ e $b$ um número inteiro positivo, a progressão aritmética obtida $P_{0,b}$, será exatamente o conjunto dos múltiplos inteiros de $b$, isto é*

$$P_{0,b} = \{bn\,;\, n \in \mathbb{Z}\} = \{\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots\} = b\mathbb{Z}.$$

De posse da Definição 3, vamos caracterizar os pretensos subconjuntos abertos de $\mathbb{Z}$, para em seguida verificar se essa família de subconjuntos introduz uma topologia em $\mathbb{Z}$.

**Definição 4.** *Diremos que $A \subseteq \mathbb{Z}$ é aberto, se $A$ for vazio ou, se para cada $a \in A$ exista $b > 0$ tal que $P_{a,b} \subseteq A$.*

**Exemplo 2.** *O conjunto $\mathbb{Z}$ é aberto. Com efeito, dado qualquer número $a \in \mathbb{Z}$, seja qual for $b$ inteiro positivo, podemos concluir que $P_{a,b} \subseteq \mathbb{Z}$.*

**Proposição 2.** *Dados $a, b \in \mathbb{Z}$, com $b > 0$, a progressão aritmética $P_{a,b}$ é um conjunto aberto.*

***Demonstração.*** De fato, considerando $a_0 \in P_{a,b}$, podemos escrever $a_0 = a + bn_0$, para algum $n_0 \in \mathbb{Z}$. Vamos mostrar que $P_{a_0,b} \subseteq P_{a,b}$. Para tanto, desde que $m \in P_{a_0,b}$, deve existir $n_1 \in \mathbb{Z}$ tal que $m = a_0 + bn_1$. Consequentemente,

$$m = (a + bn_0) + bn_1 = a + b(n_0 + n_1) \in P_{a,b},$$

pois, $n_0 + n_1 \in \mathbb{Z}$. E portanto $P_{a_0,b} \subseteq P_{a,b}$. ■

**Exemplo 3.** *A Proposição 2, nos diz que as progressões aritméticas que vimos na Definição 3, são subconjuntos abertos de $\mathbb{Z}$, isto é, satisfazem a Definição 4. Desse modo, obtemos uma infinidade de subconjuntos abertos de $\mathbb{Z}$.*

Finalmente, vamos verificar que os subconjuntos abertos de $\mathbb{Z}$, segundo a Definição 4, satisfazem a Definição 1 de topologia:

i) Note que, por definição, $\emptyset$ é um conjunto aberto. Ademais, $\mathbb{Z}$ também é aberto, segundo o Exemplo 2;

ii) Sejam $A_1$, $A_2$, $\cdots$, $A_n$ abertos, vamos mostrar que $A_1 \cap A_2 \cap \cdots \cap A_n$ é aberto. Para tanto, mostraremos primeiro que, para $n = 2$, o resultado é válido. De fato, dados $A_1$ e $A_2$ abertos, caso $A_1 \cap A_2 = \emptyset$, é imediato que $A_1 \cap A_2$ é aberto. Por outro lado, se $A_1 \cap A_2 \neq \emptyset$, então podemos considerar $a \in A_1 \cap A_2$ e, como esses conjuntos são abertos, devem existir $b_1 > 0$ e $b_2 > 0$ tais que

$$P_{a,b_1} \subseteq A_1 \;\text{ e }\; P_{a,b_2} \subseteq A_2.$$

Ademais, a progressão $P_{a,b_1b_2}$ está contida nas progressões $P_{a,b_1}$ e $P_{a,b_2}$, logo $P_{a,b_1b_2} \subseteq A_1 \cap A_2$. Daí, concluímos que $A_1 \cap A_2$ é aberto, e assim, que o resultado é válido para $n = 2$. Suponhamos agora, que o resultado é válido para algum $k \in \mathbb{N}$, isto é, que se $A_1$, $A_2$, $\cdots$, $A_k$ são abertos, então $A_1 \cap A_2 \cap \cdots \cap A_k$ é aberto. Vejamos que isso implica que o resultado também será válido para $k + 1$. Com efeito, sendo $A_{k+1}$ aberto então a intersecção dos dois conjuntos abertos

$$(A_1 \cap A_2 \cap \cdots \cap A_k) \cap A_{k+1},$$

resulta em um conjunto aberto, logo o resultado também é válido para $k + 1$. Portanto, fica provado o resultado para qualquer $n$ natural.

iii) Considere uma coleção qualquer $(A_\alpha)_{\alpha\in L}$ de conjuntos abertos, iremos mostrar que a união $\underset{\alpha\in L}{\cup} A_\alpha$ é um conjunto aberto. De fato, se todos esses conjuntos forem vazios, devemos ter $\underset{\alpha\in L}{\cup} A_\alpha = \emptyset$, assim $\underset{\alpha\in L}{\cup} A_\alpha$ é aberto. Para o caso em que $A_{\alpha_0} \neq \emptyset$ para algum $\alpha_0 \in L$, então podemos considerar $a \in A_{\alpha_0}$ e como $A_{\alpha_0}$ é aberto, existe $b > 0$ tal que $P_{a,b} \subseteq A_{\alpha_0}$ e, consequentemente

$$P_{a,b} \subseteq \underset{\alpha\in L}{\cup} A_\alpha.$$

Isso mostra que $\underset{\alpha\in L}{\cup} A_\alpha$ é um conjunto aberto.

As condições que acabamos de verificar, garantem que a família de subconjuntos abertos que apresentamos na Definição 4, de fato, introduzem uma Topologia em $\mathbb{Z}$.

### 3.3 Resultados principais

**Proposição 3.** *Todo subconjunto aberto e não vazio de $\mathbb{Z}$ é infinito.*

***Demonstração.*** Seja $A \subset \mathbb{Z}$ aberto e não vazio. Como $A$ é não vazio, podemos considerar $a \in A$. Além disso, como $A$ é aberto, então para $a \in A$ deve existir $b \in \mathbb{Z}$, sendo $b > 0$, tal que $P_{a,b} \subseteq A$. Ora, $P_{a,b}$ é um subconjunto infinito de $A$, portanto, $A$ também é infinito. ■

Para esta última conclusão, usamos a contrapositiva do resultado que diz que todo subconjunto de um conjunto finito é finito, tal resultado pode ser consultado em Lima (2004).

**Proposição 4.** *Se $p$ é um número inteiro positivo, então*

$$P_{0,p} = \mathbb{Z} \setminus \cup_{i=1}^{p-1} P_{i,p}.$$

***Demonstração.*** Seja $x \in P_{0,p}$, então $x = np$ para algum $n \in \mathbb{Z}$. Queremos mostrar que

$$x \in \mathbb{Z} \setminus \cup_{i=1}^{p-1} P_{i,p}.$$

Suponha por contradição que $x \in \cup_{i=1}^{p-1} P_{i,p}$, assim $x = i + n_1 p$, para algum $i \in \{1, 2, ..., p-1\}$ e $n_1 \in \mathbb{Z}$, daí

$$np = n_1 p + i \Rightarrow i = (n - n_1)p.$$

Ou seja, $p$ divide $i$, o que é um absurdo, pois $i \in \{1, 2, ..., p-1\}$. Logo, somos levados a admitir que $x \notin \cup_{i=1}^{p-1} P_{i,p}$ e, consequentemente, que

$$x \in \mathbb{Z} \setminus \cup_{i=1}^{p-1} P_{i,p}.$$

Por outro lado, para mostrar a inclusão contrária, basta garantir que $x \in P_{0,p}$, ou seja, $x = np$, para algum $n \in \mathbb{Z}$. Sabemos que $x \notin P_{i,p}$, assim

$$x \neq np + i, \ \forall\, i \in \{1, 2, ..., p-1\} \text{ e } n \in \mathbb{Z}. \tag{1}$$

Ademais, pelo algoritmo da divisão existem $n_0, r \in \mathbb{Z}$, tais que

$$x = n_0 p + r, \ \text{ com } \ 0 \leq r \leq p - 1. \tag{2}$$

Logo, por (1) e (2), para todo $i \in \{1, 2, ..., p-1\}$, segue-se que $n_0 p + r \neq n_0 p + i$, logo $r \neq i$. Assim, resta apenas que $r = 0$ e portanto $x = n_0 p$, mostrando que $x \in P_{0,p}$. ■

**Corolário 4.1.** *Se $p$ é um número inteiro positivo, então a progressão $P_{0,p}$ é um conjunto fechado.*

***Demonstração.*** Com efeito, pela Proposição 4, sabemos que

$$P_{0,p} = \mathbb{Z} \setminus \cup_{i=1}^{p-1} P_{i,p}.$$

Por outro lado, vimos na Proposição 2 que as progressões aritméticas $P_{i,p}$ são conjuntos abertos. Logo, a união

$$\cup_{i=1}^{p-1} P_{i,p}$$

é um conjunto aberto e consequentemente, seu complementar $P_{0,p}$ é fechado. ■

### 3.4 A demonstração da infinitude dos números primos

Enfim, chegamos a tão esperada demonstração da infinitude dos números primos utilizando Topologia.

**Teorema 1.** *O conjunto $\mathbb{P}$ dos números primos é infinito.*

***Demonstração.*** Pelo Teorema Fundamental da Aritmética (COUTINHO, 2005), todo número $m$ inteiro, diferente de -1 e 1, possui um divisor $p_0$ primo, assim $m \in P_{0,p_0}$. Consequentemente, de modo geral, podemos escrever

$$\bigcup_{p\in\mathbb{P}} P_{0,p} = \mathbb{Z} \setminus \{-1, 1\}.$$

Pelo Corolário 4.1, cada progressão $P_{0,p}$ é um conjunto fechado. Logo, se $\mathbb{P}$ fosse finito, então o Corolário 1.1, nos asseguraria que a união finita $\bigcup_{p\in\mathbb{P}} P_{0,p}$ seria um conjunto fechado, e consequentemente, seu complementar $\{-1, 1\}$, deveria ser um conjunto aberto. Absurdo! Pois, se $\{-1, 1\}$ fosse aberto, então pela Proposição 3, este aberto não vazio deveria ser infinito, o que não é verdade.

Portanto, concluímos que a união $\bigcup_{p\in\mathbb{P}} P_{0,p}$ não pode ser uma união finita, isto é, o conjunto dos números primos $\mathbb{P}$ é infinito. ■

## 4. Conclusões

Ao lado da Análise, da Álgebra e da Geometria, a Topologia constitui uma das partes fundamentais da Matemática. De fato, seus conceitos penetraram diversos ramos da Matemática e proporcionaram o desenvolvimento de cada desses ramos, como por exemplo o estudo das Equações Diferenciais e da Geometria Diferencial que carregam muitos aspectos da topologia. No entanto, sua influência é ainda mais abrangente, a exemplo do nosso trabalho, fomos capazes de introduzir uma topologia em um conjunto discreto e, a partir de uma definição de conjunto aberto nada convencional, que foge da nossa intuição, demonstrar o magnífico Teorema de Euclides sobre a infinitude do conjunto dos números primos.

## Agradecimentos

O presente trabalho foi parcialmente financiado pelo FNDE, Fundo Nacional de Desenvolvimento da Educação - Brasil, por meio da bolsa fornecida para o Grupo PET-Matemática-UFCG, do qual somos integrantes. Agradecemos também ao Tutor Daniel Cordeiro e aos demais integrantes do Grupo PET-Matemática UFCG.

## Referências

COUTINHO, S. C. *Números inteiros e criptografia RSA*. [S.l.]: IMPA, 2005. Citado na página 5.

EVES, H. W. *Introdução à história da matemática*. [S.l.]: Unicamp, 2011. Citado na página 1.

FURSTENBERG, H. On the infinitude of primes. *The American Mathematical Monthly*, v. 62, n. 5, p. 353, 1955. Citado na página 1.

LIMA, E. L. Curso de análise vol 1. 11a edição. *Rio de Janeiro: IMPA*, 2004. Citado na página 4.

LIMA, E. L. *Elementos de topologia geral, textos universitários*. [S.l.]: SBM, 2009. Citado na página 2.

POINCARÉ, H. *Analysis situs*. [S.l.]: Gauthier-Villars Paris, France, 1895. Citado na página 1.

ZIEGLER, G. M.; HOFMANN, K. H. *Proofs from the Book*. [S.l.]: Springer, 2014. Citado na página 1.

# Sequências de P.A.s Contendo Infinitos Números Primos – Parte II

**Fábio Lima de Oliveira**[1] **- fabiolimaoliveira99@gmail.com**
**Gabriel Pereira de Figueiredo**[1] **- gabrielpdf97@gmail.com**
**Daniel Cordeiro de Morais Filho**[1] **- daniel@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil - Parcialmente financiado pelo MEC/FNDE/PET

***Resumo:*** *A descoberta de grandes números primos contribui para a melhoria do método usado pela Criptografia RSA, que é uma ferramenta importante na segurança da comunicação nas mídias digitais. O estudo dos números primos não é tão atual quanto a Criptografia, séculos atrás, Euclides de Alexandria (360-295 a.C) já havia dado uma demonstração da infinidade dos números primos. O matemático Johann Peter Gustav Lejeune Dirichlet (1805-1859) relacionou o estudo sobre a infinidade de números primos com progressões aritméticas (P.A.s) provando que qualquer progressão aritmética de termo geral* $a+nq$*, com* $n \in \mathbb{N}$ *e* $a, q \in \mathbb{Z}$*, tais que* $mdc(a, q) = 1$*, possui infinitos números primos (SHIELDS, 1989). Esse é o conhecido Clássico Teorema de Dirichlet. Aqui, abordaremos alguns casos particulares de P.A.s associadas a esse teorema como continuação de um trabalho já publicado nessa direção (FIGUEIREDO et al., 2020). Para o desenvolvimento do trabalho, realizamos uma pesquisa bibliográfica sobre o tema, inclusive por meio de leituras em língua estrangeira. Após os estudos proveninetes dessas pesquisas, sob a orientação do Tutor Prof. Daniel Cordeiro, do Grupo PET-Matemática-UFCG, elaboramos uma apresentação para ser exposta na atividade Workshop didático-pedagógico desenvolvida pelo Grupo. Ao se debruçar sobre essa temática, é perceptível que mesmo com as dificuldades em trabalhar com números primos, as P.A.s surgem como uma forma de manter um certo controle sobre números primos, ainda que não se possa saber quais dos termos dessas P.A.s são números primos e onde estão.*
***Palavras-chave****: Infinidade dos Números Primos; Progressões Aritméticas; Teorema de Dirichlet.*

## 1. Introdução

É possível que em algum momento se ouça a notícia da descoberta de um grande número primo, até então desconhecido, fato que é considerado como um novo recorde no campo de pesquisa por grandes números primos. Muitos pesquisadores dedicam grande parte de seu tempo e de seu esforço na busca por quebrar esses recordes, seja por curiosidade ou até mesmo por motivações financeiras. Um exemplo é o GIMPS (Great Internet Mersenne Prime Search), um grupo que reúne pesquisadores na busca por grandes números primos de Mersenne (WOLTMAN; KUROWSKI, 2021).

Independentemente do que os move, esses feitos tem ajudado, por exemplo, no aprimoramento da Criptografia RSA, que é uma ferramenta muito importante para o envio de mensagens seguras. De forma geral, a Criptografia consiste no conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor conheçam a mensagem (COUTINHO, 2000).

A principal relação entre a Criptografia RSA e a obtenção de grandes números primos está justamente no fato de que, quanto maior for um número primo, maior é a segurança dos códigos estabelecidos na criptografia. No entanto, encontrar esses números grandes é uma tarefa difícil, pois nunca foi encontrado e, certamente, não existe um padrão na sequência infinita dos números primos.

Desde a antiguidade, já se sabia da infinidade dos números primos com a demonstração dada por *Euclides de Alexandria* (360-295 a.C). Posterior à demonstração dada por Euclides, tiveram muitas outras, cada uma com sua forma peculiar de observar o mesmo fato. Um pesquisador de muito prestígio, *Pierre de Fermat* (1601-1665) também se debruçou sobre o tema e tentou uma fórmula de gerar números primos, a qual nem todos os números dessa sequência são primos, porém ficaram conhecidos como *Números de Fermat* (EVES, 2004).

Já no século XIX, o matemático *Johann Peter Gustav Lejeune Dirichlet* (1805-1859) apresentou uma nova forma de olhar para a infinidade dos números primos, quando exibiu um vínculo entre a infinidade desses números e as Progressões Aritméticas (P.A.s) (SHIELDS, 1989). O resultado de Dirichlet é o *Clássico Teorema de Dirichlet* (RIBENBOIM, 2001), que pode ser enunciado da seguinte forma:

**Teorema 1.** *Sejam $r \geq 2$ e $a \neq 0$ inteiros primos entre si, então a progressão aritmética*

$$a, a + r, a + 2r, \ldots, a + nr, \ldots$$

*contém uma infinidade de números primos.* (SILVA JUNIOR, 2017)

A demonstração para esse teorema é extremamente técnica e pode ser encontrada em Selberg (1949). Diante disso, o presente trabalho é a continuação de um estudo inicial que pode ser lido em Figueiredo et al. (2020), no qual pretende-se abordar mais alguns casos particulares do Teorema de Dirichlet. Diferente do primeiro, nessa continuação as P.A.s exigem alguns resultados preliminares, para só então seguirmos para o modelo de demonstração, cujas ideias germinais, já se encontram no Teorema da Infinitude dos Números Primos de Euclides.

## 2. Metodologia

Este trabalho é proveniente de duas das atividades realizadas pelo Grupo PET-Matemática-UFCG, intituladas "Pesquisa em competências básicas no uso da linguagem escrita e oral, em idioma estrangeiro e na área de tecnologias de informação e comunicação" e "Workshop didático-pedagógico de prática de ensino em Matemática". Para o desenvolvimento do trabalho, realizamos uma pesquisa bibliográfica sobre o tema, por meio da leitura de livros, artigos e pesquisa em sites. Após os estudos provenientes da pesquisa, sob a orientação do Tutor do Grupo, Prof. Daniel Cordeiro, partimos para a fase de elaboração de uma apresentação em slides para ser exposta no Workshop didático-pedagógico.

## 3. Resultado e discussão

Em um trabalho já publicado demonstramos alguns casos particulares de P.A.s contendo uma infinidade de números primos (FIGUEIREDO et al., 2020). Nele podemos perceber um certo "padrão" de demonstração, também encontrado na demonstração do Teorema da Infinidade de Números Primos dada por Euclides. Nesse sentido, apresentaremos agora mais dois casos de progressões aritméticas com uma infinidade de números primos, cujas demonstrações desse fato apresentam algumas peculiaridades.

Ademais, para nossa abordagem utilizaremos alguns resultados preliminares que apresentaremos a seguir.

**Teorema 2** (Teorema Fundamental da Aritmética)**.** *Seja $n \in \mathbb{N}$ e $n > 1$. Existem números primos $p_1 < p_2 < \cdots < p_k$ e $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$, com $k \in \mathbb{N}$, tais que*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}.$$

*Essa decomposição é única, a menos de ordem* (VIEIRA, 2015).

**Teorema 3** (O Pequeno Teorema de Fermat)**.** *Se $q$ é primo e $s \in \mathbb{N}$, então $q \mid s^q - s$. Ou ainda em termos de congruência*

$$s^q \equiv s \ (mod\ q)$$

(VIEIRA, 2015).

### 3.1 A P.A. $(1, 5, \ldots, 4k + 1, \ldots)$

Para demonstrarmos a infinitude de números primos na P.A. $(1, 5, \ldots, 4k + 1, \ldots)$ necessitamos do seguinte lema:

**Lema 3.1.** *Todo número da forma $s^2+1$, com $s \in \mathbb{N}$ e $s > 1$, tem algum divisor primo da P.A. $(5, 9, \ldots, 4k + 1, \ldots)$ e não pode ter divisores primos na P.A. $(7, 11, \ldots, 4k + 3, \ldots)$* (RIBENBOIM, 2001).

***Demonstração:*** Observemos que $s^2 + 1 \neq 2^r$, com $r \in \mathbb{N}$ e $r > 2$. De fato, se $s$ for par, então $s^2 + 1$ é ímpar e não há o que discutir. Por outro lado, se $s$ for ímpar, isto é, $s = 2m + 1$, então $s^2 + 1$ é um número da forma $4k + 2$, com $k \in \mathbb{N}$, donde segue que $4 \nmid s^2 + 1$, mas $4 \mid 2^r$, pois $r > 2$.

Além disso, o Teorema 2 garante que existe $p$ primo tal que $p \mid s^2 + 1$. Desse modo, como $p \neq 2$ teremos $p$ da forma $4k + 1$ ou $4k + 3$, para algum $k \in \mathbb{N}$. Mostraremos que $p$ só pode ser da forma $4k + 1$. Com efeito, suponha por contradição que $p = 4k + 3$, para algum $k \in \mathbb{N}$. Assim, podemos observar que

$$p = 4k + 3 = 4m - 1, \text{ onde } m = k + 1 \text{ para algum } k \in \mathbb{N}.$$

Ademais, como $p \mid s^2 + 1$, da definição de congruência, segue que

$$s^2 \equiv -1(mod\ p). \tag{1}$$

Das propriedades de congruência, podemos elevar ambos os lados de (1) pela potência $\frac{p-1}{2} \in \mathbb{N}$, e assim, temos

$$\begin{aligned}(s^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}(mod\ p) &= (-1)^{\frac{4m-2}{2}}(mod\ p)\\ &= (-1)^{2m-1}(mod\ p)\\ &= -1(mod\ p).\end{aligned}$$

Daí, segue que

$$s^{p-1} \equiv -1(mod\ p) \Rightarrow p \mid s^{p-1} + 1.$$

Logo, $p \mid s^p + s$. Além disso, pelo Teorema 3, $p \mid s^p - s$. Assim, tem-se

$$p \mid (s^p + s) - (s^p - s) = 2s.$$

Dessa forma, sendo $p$ um primo ímpar segue que $p \mid s$ e, consequentemente, $p \mid s^2$. Como $p \mid s^2 + 1$, obtemos

$$p \mid s^2 + 1 - s^2 = 1,$$

o que é um absurdo. Portanto, $p = 4k + 1$ para algum $k \in \mathbb{N}$. ■

Com isso, partiremos para a demonstração do Teorema.

**Teorema 4.** *Na P.A.* $(1, 5, \ldots, 4k + 1, \ldots)$ *há uma infinidade de números primos.*

***Demonstração:*** Suponhamos, por contradição, que exista uma quantidade finita de números primos na P.A. $(5, 9, \ldots, 4k + 1, \ldots)$, com $k \in \mathbb{N}$, digamos

$$P := \{5, 13, \ldots, 4k_0 + 1\}.\ (1^{a}\ Etapa)$$

Considere o número $n = (2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2 + 1 > 1$ ($2^{a}$ *Etapa*). Temos $n > p$ para qualquer $p \in P$ e daí, como $(2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2 > 1$, pelo Lema 3.1, existe $q = 4k + 1$ primo, para algum $k \in \mathbb{N}$, tal que $q \mid n$ ($3^{a}$ *Etapa*).

Ora, $q \notin P$, pois caso contrário $q \mid (2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2$ e como $q \mid n$, teríamos

$$q \mid [n - (2 \cdot 5 \cdot \ \ldots \ \cdot (4k_0 + 1))^2] = 1,$$

o que é um absurdo ($4^{a}$ *Etapa*).

Portanto, deve existir uma infinidade de números primos na P.A. $(1, 5, \ldots, 4k + 1, \ldots)$. ■

Observe que o número $n$ foi tomado como um número da PA, pois $n = 4(5 \cdot 13 \cdot \ \ldots \ \cdot (4k_0 + 1))^2$. Daí, na demonstração anterior, podemos notar algumas etapas semelhantes as encontradas em Figueiredo et al. (2020), apenas diferenciando-se por informações adicionais. Agora, veremos um caso mais geral.

### 3.2 P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$, com $r>2$ e $k\in\mathbb{N}$

Para demonstrarmos a infinitude de números primos na P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$ precisaremos do seguinte lema:

**Lema 4.1.** *Sejam $p$ um número primo e $M, n\in\mathbb{N}$, com $mdc(M,n)=1$, tais que $p \mid M^n-1$. Seja $b\geq 1$ o menor natural tal que $p\mid M^b-1$. Então $b\mid n$.*

***Demonstração:*** Inicialmente, observe que a existência de $b$ é garantida pelo Teorema 3 e pelo Princípio da Boa ordenação.

Ademais, nas condições dadas, temos

$$M^n \equiv 1 (mod\ p) \tag{2}$$

e

$$M^b \equiv 1 (mod\ p). \tag{3}$$

Daí, pelo Algoritmo da Divisão, segue que $n=qb+r$, onde $q>0$ e $0\leq r<b$.

Suponha que $r>0$, ou seja, $r\geq 1$. Segue de 3 e das propriedades de congruência que

$$\begin{aligned}(M^b)^q \equiv 1^q\ (mod\ p) &\Rightarrow (M^b)^q M^r \equiv 1^q\cdot M^r\ (mod\ p)\\ &\Rightarrow M^n = M^{(qb+r)} \equiv M^r\ (mod\ p)\end{aligned}$$

Daí, observando 2 tem-se $M^r\equiv 1\ (mod\ p)$, o que contraria a minimalidade de $b$, pois $1\leq r<b$. Portanto, $r=0$ e $b\mid n$. ■

**Teorema 5.** *A progressão aritmética $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$, com $r>2$ fixo e $k\in\mathbb{N}$, contém uma infinidade de números primos.*

***Demonstração:*** Suponhamos que exista uma quantidade finita de números primos na P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$, digamos

$$\mathcal{P} := \{p_1, p_2, \ldots, p_n\}, n\in\mathbb{N}.$$

Desse modo, os elementos de $\mathcal{P}$ são os únicos primos tais que $2^r | p_i-1$, para $1\leq i\leq n$.

Considere o número $N=2\cdot p_1\cdot p_2\cdot\ \ldots\ \cdot p_n$ e $M=N^{2^{r-1}}$. Desse modo, mostraremos que existe $p$ primo tal que $2^r | p-1$ e $p\neq p_i$ para $1\leq i\leq n$.

Com efeito, nas condições dadas tem-se $M-1>1$ e, além disso, observe que $M^2-1=(M-1)(M+1)$, ou seja, $M-1\mid M^2-1$. Ademais, como $1<M-1<M^2-1$, pelo Teorema 2, segue que existe $p$ primo tal que

$$p\mid \frac{M^2-1}{M-1}=\frac{(M-1)(M+1)}{M-1}.$$

isto é, $p\mid M+1$.

Assim, se $p\mid M-1$, como $p\mid M+1$ então $p\mid M+1-(M-1)=2$. Daí, sendo $p$ primo tem-se $p=2$, donde segue que

$$p\mid M=N^{2^{r-1}}=(2\cdot p_1\cdot p_2\cdot\ \ldots\ \cdot p_n)^{2^{r-1}}$$

e, consequentemente, $p\mid M-(M-1)=1$, o que nos leva a um absurdo. Logo,

$$p\nmid M-1=N^{2^{r-1}}-1 \tag{4}$$

Por outro lado, sabendo que $p\mid M+1$, tem-se

$$p\mid (M+1)(M-1)=M^2-1=N^{2^r}-1. \tag{5}$$

Observe que se $p\in\mathcal{P}$, então $p\mid N$ e, por conseguinte, $P\mid M$ donde teríamos $p\mid M+1-M=1$, o que é um absurdo. Logo, $mdc(p,N)=1$ e assim, pelo Teorema 3 obtemos

$$p\mid N^{p-1}-1. \tag{6}$$

Sabendo que $p \notin \mathcal{P}$, para concluírmos a demonstração, basta mostrarmos que $2^r \mid p-1$, chegando a uma contradição.

De fato, de 5 e 6, sendo $t \geq 1$ o menor natural tal que $p \mid N^t - 1$, segue pelo Lema 4.1 que $t \mid 2^r$ e $t \mid p-1$, respectivamente. Ademais, de 4 tem-se que $t \nmid 2^{r-1}$, isto é, $t \neq 2^s$ para $1 \leq s < r$. Logo, $t = 2^r$, donde obtém-se $2^r \mid p-1$, o que é uma contradição.

Portanto, existe uma infinidade de números primos na P.A. $(1, 1+2^r, 1+2\cdot 2^r, \ldots, 1+k\cdot 2^r, \ldots)$. ■

Com isso, encontramos uma forma para obter alguns dos números primos, o que nos dá um certo controle, no entanto, não conhecemos esses números primos e nem sabemos onde estão.

## 4. Conclusões

De acordo com o apresentado, pode-se perceber a dificuldade em trabalhar com os números primos, uma vez que não conhecemos todos, ou seja, não temos uma fórmula que descreva todo o conjunto dos números primos. Entretanto, ao trabalhar com certos tipos de progressões aritméticas, temos um "controle" sobre uma infinidade de números primos mesmo sem saber quem são e onde estão.

As P.A.s vistas neste trabalho remetem à demonstração de Euclides, porém fornecendo uma nova forma de observar a infinidade de números primos, trabalhando com outros resultados importantes da Teoria dos números.

## Agradecimentos

Agradecemos ao FNDE, Fundo Nacional de Desenvolvimento da Educação Brasil, pelo financiamento e aos demais integrantes do Grupo PET-Matemática-UFCG, pela colaboração.

## Referências

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. 2. ed. IMPA: SBM, 2000. Citado na página 1.

EVES, H. *Introdução a história da matemática*. Campinas: Unicamp, 2004. Tradução: Hygino H. Domingues. Citado na página 1.

FIGUEIREDO, G. P. de; OLIVEIRA, F. L. de; GUEDES, P. H. A.; DE MORAIS FILHO, D. C. P.a.s com infinitos números primos que ninguém sabe onde estão. *VII ECMAT*, 2020. 10 p. Citado 3 vezes nas páginas 1, 2 e 3.

RIBENBOIM, P. *Números Primos: mistérios e recordes*. 1. ed. IMPA: SBM, 2001. Citado 2 vezes nas páginas 1 e 2.

SELBERG, A. An elementary proof of dirichlet's theorem about primes in an arithmetic progression. *Annals of Mathematics*, v. 50, n. 2, 1949. 297-304 p. Disponível em: ⟨https://www.jstor.org/stable/1969454⟩. Citado na página 2.

SHIELDS, A. Lejeune dirichlet and the birth of analytic number theory: 1837-1839. *The Mathematical Intelligencer*, v. 11, n. 4, p. 07–11, 1989. Citado na página 1.

SILVA JUNIOR, J. C. *O teorema de Dirichlet: primos em progressão aritmética*. Dissertação (Mestrado), João Pessoa, 2017. Citado na página 2.

VIEIRA, V. L. *Um curso básico em Teoria dos números*. Campina Grande: EDUEPB, 2015. 560 p. Citado na página 2.

WOLTMAN, G.; KUROWSKI, S. Great internet mersenne prime search (gimps). PrimeNet, 2021. Disponível em: ⟨https://www.mersenne.org/primes/⟩. Citado na página 1.

# MATEMÁTICA E CÁLCULOS MENTAIS AUXILIANDO NOS JUROS DA ECONOMIA DOMÉSTICA: ERROS COMUNS, ACERTOS E SUGESTÕES

**Amanda de Araújo Queiroz[1] - amanda.araujoqueiroz91@gmail.com**
**Cecília Nunes Magalhães[1] - cecilianmagalhaes@gmail.com**
**Hayalla Alves Cabral[1] - hayallaalves@gmail.com**
**Daniel Cordeiro de Morais Filho[1] - daniel@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil. Parcialmente financiado pelo MEC/FNDE/PET.

***Resumo:*** *A economia doméstica está intimamente ligada à Matemática, em especial à Matemática Financeira, com temas relacionados a juros e porcentagem. Assim sendo, no período atual de crise econômica, agravada pela Pandemia da Covid-19, e o consequente aumento nos valores dos insumos básicos, acaba por levar a uma maior busca pela população por descontos e promoções. Este trabalho foi realizado por meio de atividades desenvolvidas pelo Grupo PET-Matemática-UFCG, sob orientação do Tutor Professor Doutor Daniel Cordeiro de Morais Filho. Aqui, analisamos as propagandas que oferecem descontos e o método que os cálculos são realizados pela maioria da população que pesquisamos, pessoas com maior ou menor formação em Matemática básica. Nessa análise, relatada neste resumo, detectamos os principais erros cometidos, bem como os acertos e sugerimos como identificar a maneira mais simples e intuitiva do real desconto na compra de um produto ou nos juros de um empréstimo propalados pelas propagandas nas ruas e em supermercados. Com isso, busca-se refletir sobre a importância do estudo da Matemática Financeira na educação básica.*
***Palavras-chave****: Economia Doméstica; Juros; Matemática Financeira*

## 1. Introdução

Na Economia Doméstica, a Matemática é algo sempre presente, figurando em cálculos de valores, orçamentos de gastos mensais, comparações de preços, estimativas de descontos, entre muitas outras ocasiões, as quais requerem conhecimento de Matemática básica, em especial o cálculo de juros. No atual cenário de crise sanitária associada à crise econômica que ora se instala e que, consequentemente, vem acarretando o aumento dos preços dos insumos básicos, as pessoas tendem a procurar mais por itens em promoção ou com algum desconto, visando aumentar seu poder de compra, ou por empréstimos com menores juros.

Nesse sentido, os juros são muito importantes no cotidiano das famílias, estão presentes em supermercados, postos de gasolina, lojas de roupas e móveis. Os juros aparecem em descontos por compra de itens em maior quantidade, descontos na compra da segunda peça, ou na busca por empréstimos em situações de endividamento.

Atualmente, a Matemática Financeira está presente em todos os níveis da educação básica, e não se pode relegar ao segundo plano sua importância para a compreensão das relações econômicas e financeiras atuais. Desse modo, a apropriação dos significados dos conceitos da área da Matemática Financeira é fundamental. No cálculo dos juros, existe a necessidade de relacionar os demais conceitos da Matemática Financeira, como razão, proporção, porcentagem e regra de três para a resolução dos problemas, conforme previsto nos critérios e competências da Matemática da Base Nacional Comum Curricular (2018, p. 269),

> Assim, podem ser discutidos assuntos como taxas de juros, inflação, aplicações financeiras (rentabilidade e liquidez de um investimento) e impostos. Essa unidade temática favorece um estudo interdisciplinar envolvendo as dimensões culturais, sociais, políticas e psicológicas, além da econômica, sobre as questões do consumo, trabalho e dinheiro. (BRASIL, 2018)

Santos (2005) define juro como sendo "[...] aquela quantia que é cobrada ou recebida a mais sobre um valor emprestado ou aplicado durante certo tempo à referida taxa. Entretanto, juro pode ser definido sob diferentes prismas, como o político, o econômico, o jurídico ou até filosófico".

Alencar (2006), nos diz que a economia conceitua juro como sendo a remuneração paga, pelo tomador de um empréstimo, ao detentor do capital emprestado. Juridicamente, os juros são ditos "frutos civis" do capital, remuneração pela disponibilidade de uma importância em dinheiro por determinado tempo (GRANDO; SCHNEIDER, 2010).

Os juros são classificados em simples ou compostos, dependendo do regime de capitalização. No caso do juro simples, a taxa percentual incide somente sobre o capital inicial e não se incorpora no capital, mesmo que, com o passar do tempo, tenha um crescimento linear. No juro composto, o regime de capitalização é diferente, porque a cada período que o juro gerado é incorporado ao capital atual (saldo devedor) e sua acumulação se dá de forma exponencial (LIMA et al., 2004).

Assim, a maioria das propagandas que menciona descontos ou promoções, podem levar o consumidor a pensar e calcular de maneira equivocada a real redução no valor daquela compra, as pessoas podem acreditar que estão tendo vantagens e economizando além do que realmente estão. Se as pessoas soubessem, pelo menos, comparar o total do valor a prazo (montante) com o valor à vista (capital inicial), utilizando o recurso da proporção ou da porcentagem, teriam uma noção do valor a mais que estariam pagando na modalidade a prazo, mesmo não sabendo calcular exatamente a taxa de juros mensais incluída nas transações com lojas ou financeiras.

Nesse trabalho, buscamos analisar as propagandas com promoções e descontos, como os consumidores são levados a fazerem cálculos equivocados desses descontos e o quanto isso é comum, tendo em vista as confusões acarretadas pela pressa do dia a dia. Nesse sentido, contamos com que um consumidor possa ser capaz de fazer alguns cálculos mentais e, para isso, ensinamos alguns métodos diretos e simples.

## 2. Metodologia

A metodologia utilizada no trabalho é a coleta de dados, instrumentalizada através da captação de materiais de propagandas nas ruas, mercados e lojas de e-commerce, com a aplicação de juros, bem como algumas entrevistas que fizemos a pessoas com diferentes níveis de formação matemática. Assim, conforme Gil (1999), a pesquisa será exploratória, na medida em que

> [...] são desenvolvidas com o objetivo de proporcionar visão geral, de tipo aproximativo, acerca de determinado fato. Este tipo de pesquisa é realizado especialmente quando o tema escolhido é pouco explorado e torna-se difícil sobre ele formular hipóteses precisas e operacionalizáveis.

Desse modo, foi desenvolvida uma análise das propagandas que utilizam juros, sejam de empréstimos ou de descontos, e como as pessoas podem realizar o cálculo desses juros, o que pode causar erros, os quais detectamos e nos causou bastante surpresa. Esse trabalho foi elaborado como atividade do Grupo PET-Matemática-UFCG, sob orientação do Tutor Professor Doutor Daniel Cordeiro de Morais Filho e financiado pelo MEC/FNDE/PET.

## 3. Resultado e discussão

Existem diversas situações no dia a dia onde podemos nos deparar com o conceito de juros. Por exemplo, é muito comum irmos ao supermercado e encontrarmos promoções do seguinte tipo: "Leve 4 pague 3". Em casos como esse, podemos nos perguntar "o preço do produto interfere no desconto?" ou "é possível calcular o valor dos juros sem saber o valor do produto?".

Vejamos os exemplos a seguir:

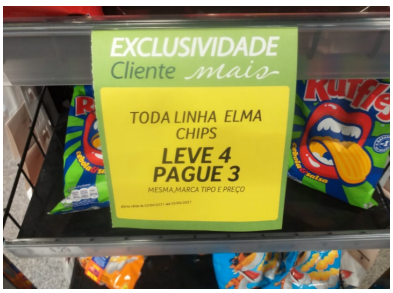



Figura 1: Leve 4 pague 3


Desodorante Dove Original Aerosol 50% de Desconto na Segunda Unidade de 150ml cada

Figura 2: 50% de desconto na segunda unidade

No caso da Figura 1, é possível fazer alguns cálculos mentais simples para calcular a porcentagem do descontos, que ensinamos agora:

Supondo que cada produto custe $R\$100,00$, o cliente pagaria $R\$400,00$ para levar os 4 produtos, mas irá pagar $R\$300,00$, ou seja, teve um desconto de $R\$100,00$. Assim, o desconto final é de 25%, pois $R\$100,00$ equivale a 25% de $R\$400,00$.

Desse modo, descobrimos que, em casos como este, independentemente do valor do produto, sempre haverá uma redução de 25%, ou seja, o preço não interfere no real desconto. Esse é um fato interessante para um consumidor comum, que pode, sem dificuldade, replicar esse método em diversas ocasiões.

Outro exemplo de situação com cálculos de juros muito corriqueira é: "50% de desconto na 2ª unidade!!" (Figura 2). Esse número "50%"parece ser mágico nesses anúncios. Mas se nos perguntarmos se o real desconto é mesmo 50%, a resposta é não.

Assim como no caso anterior, se o cliente supor que cada desodorante custa $R\$100,00$, sem o desconto ele iria pagar $R\$200,00$ ao final dessa compra e com o desconto, ele pagaria $R\$150,00$. Logo, o desconto seria de $R\$50,00$, que equivale a 25% de $R\$200,00$.

A ideia, nesses tipos de propaganda, é levar o cliente a acreditar que pagaria a metade do valor, quando na verdade o desconto é somente na segunda peça, então o desconto real é de 25% no valor total. Esses tipos de propagandas, na verdade são estratégias de marketing, pensadas e formuladas com o intuito de passar a ideia que o cliente estará fazendo um ótimo negócio, quando nem sempre é tão ótimo assim.

Vejamos as imagens a seguir:


Figura 3: Propagandas


Figura 4: Empréstimo

Estes são exemplos muito comuns em várias cidades, inclusive em Campina Grande – PB (onde as imagens abaixo foram feitas), em que vários postes de iluminação contêm propagandas de empréstimos, convidativos e, aparentemente, fáceis de serem feitos. As duas imagens trazem problemas de empréstimo, mas focaremos no empréstimo da Figura 4, pois tem dados numéricos mais simples, induzindo ainda mais facilmente a erros, por recaírem em cálculos mais simples. A figura 4 mostra a propaganda de um empréstimo de $R\$1000,00$ que será pago em prestações de $12 \times R\$100,00$, totalizando $R\$1200,00$. Realizamos uma pesquisa com diferentes pessoas para saber como elas calculariam os juros desse empréstimo.

A maioria das pessoas cometeu o mesmo erro ao calcular os juros desse tipo de problema, acreditando ser um caso de juros simples, como no caso dos juros expostos anteriormente. Observemos abaixo alguns dos erros cometidos pelos entrevistados:

Em algumas tentativas, alguns dividem o acréscimo, pela quantidade de meses:

$$\frac{R\$200,00}{12} = 16,66\ldots$$

E daí, calculam os juros:

$$\frac{16,66}{100} = 0,166\%.$$

Em outras, tentaram de forma errada, com cálculos simples mentais, e no fundo utilizaram a fórmula de juros simples, vide Lima et al. (2004):

$$J = C \cdot i \cdot t$$

onde $J$ são os juros; $C$, como o primeiro capital investido; $i$, a taxa de juros (em porcentagem) e $t$ o tempo, representado, normalmente, em meses. Daí, aplicando os valores do problema na fórmula, obtêm-se:

$$200 = 1000 \cdot i \cdot 12$$
$$i \approx 1,6\%$$

Para detectar e convencer do erro que esse procedimento pode causar, coloquemos essa taxa de juros aplicado a cada mês:

**1º. Mês:** $R\$1000,00$+ juros de $1,6\% = R\$1016,00$
Paga $R\$100,00$, falta $R\$1016,00 - R\$100,00 = R\$916,00$

**2º. Mês:** $R\$916,00$+ juros de $1,6\% = R\$930,66$
Paga $R\$100,00$, falta $R\$930,66 - R\$100,00 = R\$830,66$
$\vdots$
**11º. Mês:** $R\$96,60$+ juros de $1,6\% = R\$98,42$
Paga $R\$100,00$, quita sua dívida e ainda sobra $R\$1,58$

Ou seja, se os cálculos estivessem corretos, antes mesmo dos 12 meses, a pessoa já teria quitado sua dívida. Podemos então perceber que este problema não é resolvido utilizando-se o conceito de juros simples. Na verdade, este problema é resolvido com o conceito de juros compostos! Um ponto importante é a dificuldade que existe em resolver esse tipo de problema, visto que os cálculos envolvem exponencial e logaritmo, onde juros simples têm crescimento linear e juros compostos têm crescimento exponencial, mas pessoas podem ser levadas a utilizar simples cálculos mentais.

Assim como os entrevistados, mesmo sem termos meios científicos para assegurarmos isso, acreditamos que a grande parte das pessoas comete erros ao calcular os juros e descontos na hora de compras ou empréstimos. Às vezes os erros ocorrem por falta de conhecimento para efetuar os cálculos, outras vezes, pelas pessoas serem levadas a ideias errôneas por meio das propagandas. Em todos os casos, não resta dúvida que o conhecimento sobre juros é importantíssimo na formação de qualquer cidadão.

Os cálculos mentais podem nos dar a ilusão de que estamos resolvendo bem o problema, mas, como frisado anteriormente, o cálculo de juros compostos de forma mental é, na grande maioria das vezes, bem mais trabalhoso. Dessa forma, vejamos como podemos resolver o referido problema, utilizando a fórmula dos juros compostos, vide Lima et al. (2004), para enfim saber a verdadeira taxa de acréscimo no empréstimo em questão:

$$M = C(1+i)^t$$

onde $M$ é o montante, $C$ é o capital inicial, $i$ é a taxa de juros e $t$ é o tempo. Substituindo os valores, temos

$$1200 = 1000\,(1+i)^{12} \implies \frac{1200}{1000} = (1+i)^{12} \implies 1,2 = (1+i)^{12} \implies \sqrt[12]{1,2} = 1+i.$$

Dessa forma,

$$1+i = 1,01531 \implies i = 1,01531 - 1 \implies i = 0,01531 \cdot 100 \implies i = 1,531\%.$$

Assim, encontramos a taxa de juros correta, que é $1,531\%$.

## 4. Conclusões

É possível observar que é imprescindível o modo como se realiza e se aprende sobre juros e como aplicá-los no dia a dia, mesmo que alguns métodos, longe da realidade da população, possam ser questionados. Há indivíduos que podem ter dificuldades em resolver alguns problemas de matemática básica e financeira, pois alguns cálculos de juros não são tão simples de se realizar mentalmente e podem exigir mais trabalho do que se possa pensar.

Ademais, é comum anúncios que podem levar a uma interpretação tendenciosamente errada, de modo que uma propaganda sobre juros compostos pode fazer o indivíduo acreditar que se trata de juros simples, assim também como um anúncio sobre desconto na segunda peça pode levar o consumidor a pensar que o desconto é muito vantajoso. Deste modo, esperamos ajudar muitas pessoas com esse trabalho, a fim de abrirmos seus olhos para não cair mais nas famosas "propagandas enganosas" e saberem como realizar cálculos simples mentalmente, assim como também possam entender a distinção entre juros simples e compostos.

## Referências

ALENCAR, M. F. Noções básicas sobre juros e o combate histórico à usura. *Jus Navigandi, Teresina*, v. 10, 2006. Citado na página 2.

BRASIL. *Base Nacional Comum Curricular*. Ministério da Educação, 2018. Citado na página 1.

GIL, A. Métodos e técnicas de pesquisa social. editora atlas. *São Paulo–SP*, 1999. Citado na página 2.

GRANDO, N. I.; SCHNEIDER, I. J. Matemática financeira: alguns elementos históricos e contemporâneos. *Zetetiké*, v. 18, n. 1, 2010. Citado na página 2.

LIMA, E. L. et al. A matemática do ensino médio, volume 2, 5ª edição. *Coleção do Professor de Matemática, Sociedade Brasileira de Matemática*, 2004. Citado 3 vezes nas páginas 2, 4 e 5.

SANTOS, G. d. C. *Educação financeira: a matemática financeira sob nova perspectiva. 2005*. Tese (Doutorado) — Dissertação (Mestrado em Educação para a Ciência)–Faculdade de Ciências ..., 2005. Citado na página 2.

# EQUIDISTRIBUIÇÃO E NÚMEROS NATURAIS: A Lei do Primeiro Dígito em Potenciações.

**Heric Corrêa da Silva**[1] **- heric@ufrj.br**
**Janaíne Geralda Mesquita Martins**[2] **- janaine.martins@ufv.br**

[1]Universidade Federal do Rio de Janeiro, Instituto de Matemática - Rio de Janeiro, RJ, Brasil
[2]Universidade Federal de Viçosa, Campus Florestal - Florestal, MG, Brasil

***Resumo:*** *Será mostrado que as sequências $(b^n)_n$ formadas pelas potências com uma base $b$ não nula, e diferentes de quaisquer potências de 10, é equidistribuída no sentido de Weyl e, como consequência, satisfaz a Lei do Primeiro Dígito de Newcomb-Benford..*
***Palavras-chave****: Equidistribuição; Lei de Benford; Potenciação.*

## 1. Introdução

Seja qual for o seu número favorito, mostraremos neste trabalho que ele está no começo de uma potência de 2. Mais do que isso, ele também está no começo de uma potência de 3, 4, 5, e várias outras. Especificamente, o que queremos dizer é sintetizado no seguinte teorema

Teorema 1. *Seja $b$ um número natural não nulo e diferente de qualquer potência de 10. Então para todo natural não nulo $d$ existe algum $n$ natural tal que $b^n$ começa com $d$.*

Por exemplo, se $b = 2$:

| $\forall\, d$ | $\exists\, n$ | $2^n$ |
|---|---|---|
| 51 | 9 | $2^9 = 512$ |
| 335 | 25 | $2^{25} = 33554432$ |
| 4 294 967 | 32 | $2^{32} = 4294967296$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

Em especial, olhando apenas para os primeiros dígitos da sequência, conforme figura a seguir

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^n$ | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | ... |

observa-se que, se continuarmos até os 100 primeiros elementos desta progressão, obteríamos precisamente a seguinte proporção:

| $d$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $P^{100}(d)$ | 30% | 17% | 13% | 10% | 7% | 7% | 6% | 5% | 5% |

Em que

$$P^{100}(d) := \frac{\text{Quantidade de dígitos que começa com } d \text{ até os 100 primeiros}}{100 \text{ números no total}}.$$

Ademais, uma vez que uma sequência possui infinitos termos, queremos avaliar como essa proporção se comporta à medida que a quantidade de termos tende à infinito. Isto é, quais os valores (se é que existe) dos limites

$$\lim_{m\to\infty} P^m(d) := \lim_{m\to\infty} \frac{\text{Quantidade de dígitos que começa com } d \text{ até os } m \text{ primeiros}}{m \text{ números totais}}.$$

Um *spoiler* interessante é que o limite existe e permanece próximo da distribuição da tabela anterior. Precisamente, temos para cada $d \in \{1,2,3,4,5,6,7,8,9\}$ que

$$\lim_{m\to\infty} P^m(d) = \log\left(1+\frac{1}{d}\right). \tag{1}$$

Todo conjunto de números cuja distribuição do primeiro dígito é dada pela equação (1) é dito satisfazer a *lei de Benford* ou a *lei do primeiro dígito*. Essa distribuição está presente em várias fontes de casos reais, como, contas de energia elétrica, quantidade das populações de cidades de um país, primeiros dígitos dos números da sequência de Fibonacci, entre outros.

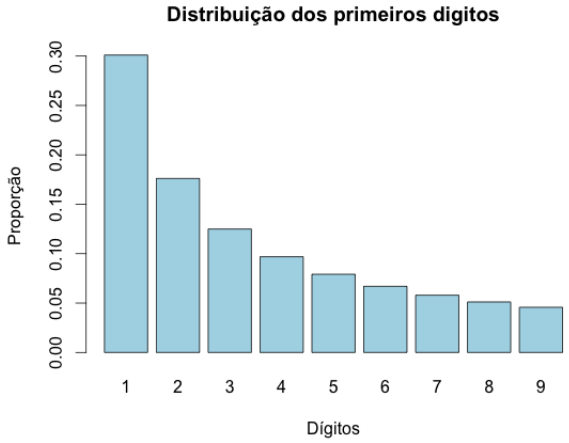



**Figura 1.** *Primeiros dígitos de um conjunto de dados satisfazendo a Lei de Benford*

Neste trabalho, mostraremos que essa lei é válida para uma família de sequências de números naturais, a saber mostraremos o seguinte Corolário 1:

Corolário 1. *A sequência $(b^n)_{n\in\mathbb{N}}$ dada pelas potências de um número natural não nulo $b$, diferente de qualquer potência de 10, satisfaz a Lei de Benford.*

## 2. Metodologia

O autor Heric Corrêa da Silva foi aluno de Iniciação Científica nas áreas de Sistemas Dinâmicos e Teoria Ergódica durante sua graduação na Universidade Federal de Minas Gerais (UFMG), sob orientação dos professores José Antônio Miranda e Carlos Carballo. A autora Janaíne G. Mesquita Martins é aluna de Iniciação Científica nas áreas de Álgebra Abstrata e Estatística na Universidade Federal de Viçosa (UFV) sob orientação respectiva de .... Este trabalho foi uma iniciativa dos alunos-autores que se reuniram semanalmente para debater e aprender sobre o tema que é uma intersecção interessante entre aritmética, dinâmica e estatística.

## 3. Resultado e discussão

Seja $(x_1, x_2, \ldots, x_n, \ldots)$ uma sequência de números reais, doravante denotada por $(x_n)_n$. Sempre podemos, associada à esta, construir uma nova sequência

$$(\mathrm{fr}(x_n))_n := (\mathrm{fr}(x_1), \mathrm{fr}(x_2), \ldots, \mathrm{fr}(x_n), \ldots)$$

onde $\text{fr}(x_n)$ denota a parte fracionária de cada elemento $x_n$.

Note que todos os elementos da sequência $(\text{fr}(x_n))_n$ pertencem ao intervalo $[0,1)$. Com isso, dado um subintervalo $(a,b) \subset [0,1)$, seja $P^m_{(a,b)}$ um subconjunto dos números naturais definido pela igualdade

$$P^m_{(a,b)} = \{j \in \mathbb{N} \mid j < m,\ \text{fr}(x_j) \in (a,b)\}.$$

Sem grande rigor, estamos apenas contabilizando a quantidade de vezes em que as partes fracionárias dos elementos da sequência $(x_n)_n$ "caem"em um subintervalo pré-determinado $(a,b)$.

**Definição 3.2. (Equidistribuição)** *Uma sequência de números reais $(x_n)_n$ é dita* ***equidistrbuída****, ou* ***uniformemente densa*** *no intervalo $[0,1)$ se para qualquer intervalo $(a,b) \subset [0,1]$* vale

$$\lim_{m\to\infty} \frac{1}{m} \#P^m_{(a,b)} = b - a, \tag{2}$$

*onde $\#$ indica a quantidade de elementos de um conjunto finito.*

Informalmente, uma sequência é equidistribuída no intervalo $[0,1)$ quando a razão do tempo que a sequência permanece em um subintervalo $(a,b)$ é igual ao comprimento deste intervalo. Em um contexto probabilístico, isso significa que escolhendo ao acaso um elemento da sequência, a probabilidade de que ele esteja dentro do intervalo $(a,b)$ é precisamente igual ao comprimento deste intervalo. Esse resultado foi enunciado e provado a primeira vez por Weyl em (**??**) e, mais tarde ampliado para um contexto bem mais geral dando origem à um braço forte da teoria dos Sistemas Dinâmicos: a Teoria Ergódica.

**Observação 3.3.** A equação (2) pode ser reescrita da seguinte maneira:

$$\lim_{m\to\infty} \frac{1}{m} \sum_{j=0}^{m-1} \chi_{(a,b)}(\text{fr}(x_j)) = \int_0^1 \chi_{(a,b)}(x)\, dx. \tag{3}$$

Na qual $\chi_{(a,b)}$ é a função característica do intervalo $(a,b)$, i.e,

$$\chi_{(a,b)}(x) = \begin{cases} 1 & \text{se } x \in (a,b), \\ 0 & \text{se } x \notin (a,b). \end{cases}$$

**Proposição 3.4 (Critérios de Weyl parte 1).** *Considerando a sequência de números reais $(x_n)_n$, as seguintes afirmações são equivalentes:*

*(a) $(x_n)_n$ é equidistribuída.*

*(b) Para cada função Riemann-integrável $f\colon [0,1] \to \mathbb{C}$ vale que*

$$\lim_{m\to\infty} \frac{1}{m} \sum_{j=0}^{m-1} f(\text{fr}(x_j)) = \int_0^1 f(x)\, dx.$$

*Explicação 3.4.* Uma sequência ser equidistribuída significa que a sequência das partes fracionárias de seus elementos, quando o tempo tende ao infinito, se distribuem de forma uniforme ao longo do intervalo $[0,1)$. Dessa forma, podemos considerar que estamos tomando partições cada vez mais refinadas no intervalo, o que justifica, por definição de integral de Riemann, o item *(b)* ser equivalente ao item *(a)*.

□

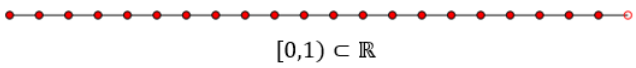



Figura 1: Equidistribuição no intervalo.

**Definição 3.5 (Exponencial).** *A seguinte função será chamada de* ***exponencial***

$$\begin{aligned} e\colon \mathbb{R} &\longrightarrow \mathbb{C} \\ x &\mapsto e(x) = \cos(2\pi x) + i\,\mathrm{sen}(2\pi x). \end{aligned}$$

Note que tal função é periódica com período 1. Além disso, a restrição $e_{|_{[0,1)}}$ é um homeomorfismo (Função bijetora contínua cuja inversa também é contínua) de $[0,1)$ sobre a circunferência unitária no plano complexo, denotada por $S^1$. Isso quer dizer, topologicamente, que o intervalo $[0,1)$ em algum sentido se assemelha à circunferência no plano complexo. Esse fato é importante no que se segue.

**Proposição 3.6 (Critérios de Weyl parte 2).** *Considerando a sequência de números reais $(x_n)_n$, as seguintes afirmações são equivalentes:*

*(b) Para cada função Riemann-integrável $f\colon [0,1] \to \mathbb{C}$ vale que*

$$\lim_{m\to\infty} \frac{1}{m} \sum_{j=0}^{m-1} f(\mathrm{fr}(x_j)) = \int_0^1 f(x)\,dx.$$

*(c) Para cada $k$ inteiro não nulo,*

$$\lim_{m\to\infty} \frac{1}{m} \sum_{j=0}^{m-1} e(kx_j) = 0.$$

*Explicação 3.6.* O item *(c)* lança mão da função que chamamos de exponencial, essa função transforma, de forma biunívoca e contínua, o intervalo $[0,1) \subset \mathbb{R}$ na circunferência $S^1 \subset \mathbb{C}$ conforme imagem a seguir.

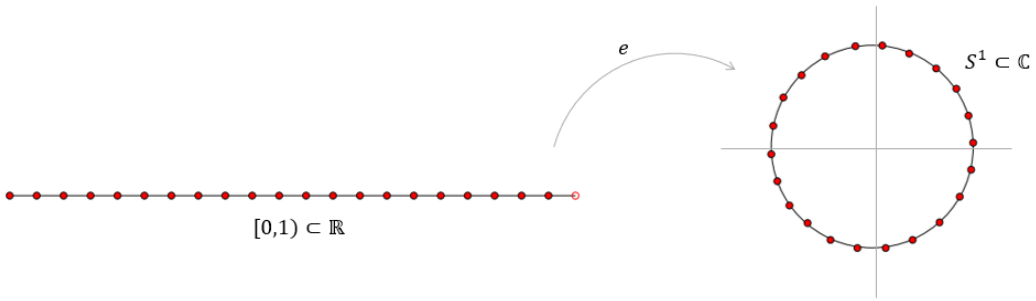



**Figura 2.** *Equidistribuição e exponencial.*

Logo, aproveitando a simetria de $S^1$, a distribuição uniforme da sequência nos permite concluir (informalmente) que o somatório dos elementos da sequência no plano complexo tende para 0.

□

Essas caracterizações de uma sequência ser uniformemente densa num intervalo, juntamente com os resultados a seguir são suficientes para demonstração do Teorema e do Corolário.

**Proposição 3.** *Seja $b$ um número natural não nulo e que não seja uma potência de 10. Então o logaritmo de $b$ na base 10 é um número irracional.*

**Proposição 4.** *Seja $d$ um número natural não nulo. Então o número de algarismos de $d$, denotado por $N_d$, é tal que*

$$N_d = 1 + \lfloor \log d \rfloor,$$

*onde $\lfloor \cdot \rfloor$ denota a parte inteira do número. Além disso, $N_d$ satisfaz*

$$\log(d+1) \leq N_d.$$

**Proposição 5.** *O Teorema 1 é equivalente à seguinte proposição: Dado um número arbitrário $d$ natural, não nulo e diferente de qualquer potência de 10. Então para todo número $d$ natural não nulo, existe um $n$ natural tal que a seguinte desigualdade é verdadeira*

$$0 \leq \log\left(\frac{d}{10^{N_d-1}}\right) \leq \mathrm{fr}(n \log b) \leq \log\left(\frac{d+1}{10^{N_d-1}}\right) < 1.$$

E, por fim,

**Proposição 5.** *Seja $\alpha$ um número irracional, então a sequência $(\alpha n)_n$ é equidistribuída.*

São os resultados necessários para se mostrar o teorema e o corolário.

## 4. Conclusões

Equidistribuição de Weyl, além de uma excelente introdução para um resultado mais amplo e geral: Teorema Ergódico; é bem efetivo para estudar e inferir resultados em Teoria dos Números, como neste caso, que pudemos obter propriedades sobre as potências de números naturais por meio de critérios clássicos, sem lançar mão dos aspectos técnicos de Teoria Ergódica.

## Agradecimentos

Heric Corrêa agradece à toda orientação, parceria e amizade dos professores Carlos Maria Carballo e José Antônio Miranda. Janaíne Martins agradece..

## Referências

Monteiro, F. C. (2017). Rotações e Números Naturais: Uma Introdução aos Sistemas Dinâmicos. *Acta Legalicus*, n.6. Nenhuma citação no texto.

Weyl, H. (1916). Über die Gleichverteilung von Zählen mod. Eins. *AMath. Ann.*, 77, pp. 313–352. Citado na página 3.

Kosma, J. F. (1935). Ein mengentheoretischer Satz über die Gleichverteilung modulo Eins *Compositio Mathematica,* p. 250-258 Nenhuma citação no texto.

# SOLUÇÃO DE ENERGIA MÍNIMA PARA PROBLEMAS ELÍPTICOS ENVOLVENDO A EQUAÇÃO DE CHOQUARD

**Eduardo Dias Lima**[1] **- duardo.dias16@hotmail.com**
**Edcarlos Domingos da Silva**[2] **- edcarlos@ufg.br**

[1]Universidade Federal de Goiás, Instituto de Matemática e Estatística - Goiânia, GO, Brasil
[2]Universidade Federal de Goiás, Instituto de Matemática e Estatística - Goiânia, GO, Brasil

***Resumo:*** *Neste trabalho, apresentamos um estudo sobre a existência de solução de energia mínima para a seguinte equação de Choquard não linear*

$$\begin{cases} -\triangle u + V(x)u = \left( \displaystyle\int_{\mathbb{R}^N} \frac{Q(y)F(u(y))}{|x-y|^\mu}\, dy \right) Q(x)f(u(x)) \\ u \in \mathcal{D}^{1,2}(\mathbb{R}^N), \end{cases} \tag{1}$$

*onde* $N \geq 3$, $0 < \mu < N$, $V \in \mathcal{C}(\mathbb{R}^N,\ [0,+\infty))$, $Q \in \mathcal{C}(\mathbb{R}^N,\ (0,+\infty))$, $f \in \mathcal{C}^1(\mathbb{R},\mathbb{R})$ *e* $F(t) = \displaystyle\int_0^t f(s)ds$. *A não-linearidade* $f : \mathbb{R} \to \mathbb{R}$ *é contínua e tem comportamento assintoticamente linear no infinito. Além disso, sobre certas condições da variedade de Nehari* $\mathcal{N}$ *e algumas outras desigualdades, estabelecidas no trabalho, a equação (1) tem uma solução de energia mínima.*
***Palavras-chave****: Variedade de Nehari, Equação de Choquard, Minimização em Variedade.*

## 1. Introdução

A equação de Choquard também é conhecida como equação Schrödinger-Newton em modelos acoplados, que foi proposta por Penrose em 1996, como um modelo de matéria autogravitante. Neste caso, a existência de soluções não triviais foi comprovada por métodos variacionais de Lieb, Lions e Menzala [3]. Neste trabalho, explicitamos a existência de solução de energia mínima por meio do conjunto de Nehari,

$$\mathcal{N} := \{u \in E \setminus \{0\} : \langle \Phi'(u), u\rangle = 0\}.$$

Para isso, garantimos que o funcional $\Phi$ associado ao problema (1) possui a Geometria do Passo da Montanha, utilizando as hipóteses de crescimento assumidas sobre a função $f$ acima, e asseguramos a existência de uma sequência limitada de Cerami $\{u_n\}_{n\in\mathbb{N}}$ para $\Phi$. Por fim, evidenciamos que o funcional $\Phi$ possui ínfimo e é atingido para algum elemento $\overline{u} \in H^1(\mathbb{R}^N)$. Note que $(2N-\mu)/(N-2)$ e $(2N-\mu)/N$ são, respectivamente, expoentes críticos superior e inferior, no sentido da desigualdade de Hardy-Littlewood-Sobolev.

## 2. Metodologia

Para a elaboração deste trabalho, seguimos os artigos [1], [2] e [4]. Em 2018, os autores Sitong Chen e Shuai Yuan estudaram a seguinte equação de Choquard não linear dado em (1). Consequentemente, expressaram o conjunto $E$ de modo que

$$E := \left\{ u \in \mathcal{D}^{1,2}(\mathbb{R}^N) : \int_{\mathbb{R}^N} V(x)u^2 dx < +\infty \right\},$$

afim de obter solução fraca para (1), cujo objetivo é encontrar um ponto crítico não trivial para $\Phi$. Por meio de métodos variacionais, podemos definir o funcional energia natural associado ao problema (1), $\Phi : E \to \mathbb{R}$ por

$$\Phi(u) = \frac{1}{2}\int_{\mathbb{R}^N} |\nabla u|^2 dx + \frac{1}{2}\int_{\mathbb{R}^N} V(x)u^2 dx - \frac{1}{2}\int_{\mathbb{R}^N}\int_{\mathbb{R}^N} \frac{Q(y)F(u(y))}{|x-y|^\mu} dy Q(x)F(u(x))dx.$$

Mostramos que $\Phi$ é de classe $\mathcal{C}^1(E,\mathbb{R})$. Recentemente, muitos pesquisadores começaram a se concentrar na equação de Choquard com a não linearidade não homogênea satisfazendo as seguintes hipóteses:

(F0) $f \in \mathcal{C}(\mathbb{R},\mathbb{R})$ satisfaz

$$\lim_{t\to 0}\frac{F(t)}{|t|^{(2N-\mu)/N}}=0 \qquad \text{e} \qquad \lim_{|t|\to+\infty}\frac{F(t)}{|t|^{(2N-\mu)/(N-2)}}=0,$$

existe uma constante $C_0>0$ tal que

$$|tf(t)|\le C_0\left(|t|^{(2N-\mu)/N}+|t|^{(2N-\mu)/(N-2)}\right), \quad \forall\, t\in\mathbb{R}.$$

(Q1) $V(x)$, $Q(x)>0$; $\forall\, x\in\mathbb{R}^N$, $V\in\mathcal{C}(\mathbb{R}^N,\mathbb{R})$ e $Q\in\mathcal{C}(\mathbb{R}^N,\mathbb{R})\cap L^\infty(\mathbb{R}^N,\mathbb{R})$;

(Q2) Se $\{A_n\}\subset\mathbb{R}^N$ é uma sequência do conjunto de Borel tal que a medida de Lebesgue para $A_n$ é menor do que $\delta$, $\forall\, n$ e algum $\delta>0$, então

$$\lim_{r\to+\infty}\int\limits_{A_n\cap B_r^c(0)}[Q(x)]^{\frac{2N}{2N-\mu}}dx=0, \text{ uniformemente em } n\in\mathbb{N};$$

(Q3) $\dfrac{Q}{V}\in L^\infty(\mathbb{R}^N)$;

(Q4) Existe $p\in(2,2^*)$ tal que

$$\frac{[Q(x)]^{\frac{2N}{2N-\mu}}}{[V(x)]^{\frac{2^*-p}{2^*-2}}}\longrightarrow 0, \qquad |x|\to+\infty.$$

(F1) $\lim\limits_{|t|\to+\infty}\dfrac{F(t)}{|t|}=+\infty$;

(F2) $\lim\limits_{t\to 0}\dfrac{F(t)}{|t|^{\frac{2N-\mu}{N}}}=0$, se vale (Q3); ou $\lim\limits_{t\to 0}\dfrac{F(t)}{|t|^{\frac{p(2N-\mu)}{2N}}}=0$, se vale (Q4).

(F3) $\lim\limits_{|t|\to+\infty}\dfrac{F(t)}{|t|^{\frac{2N-\mu}{N-2}}}<+\infty$, se vale (Q3); $\lim\limits_{|t|\to+\infty}\dfrac{F(t)}{|t|^{\frac{p(2N-\mu)}{2N}}}<+\infty$, se vale (Q4).

(F4) $f(t)$ é não-decrescente em $\mathbb{R}$.

Note que $(V,Q)\in\mathcal{K}$ significa o conjunto de todos os potenciais $V$ e $Q$ tais que (Q1)-(Q4) são satisfeitas. Para demonstrar o nosso resultado principal, usamos alguns conceitos, tais como:

**Lema 1:** Suponha que $(V,Q)\in\mathcal{K}$ e $f$ satisfaz (F1)-(F4). Então existe uma constante $c_*\in(0,m]$ e uma sequência $\{u_n\}\subset E$ satisfazendo

$$\Phi(u_n)\to c_*, \qquad \|\Phi'(u_n)\|\,(1+\|u_n\|)\to 0. \tag{2}$$

**Demonstração.** A prova encontra-se em [2]. □

**Lema 2:** Suponha que $(V,Q)\in\mathcal{K}$ e $f$ satisfaz (F1)-(F4). Então a sequência $\{u_n\}\subset E$ satisfazendo

$$\Phi(u_n)\to c\ge 0, \qquad \langle\Phi'(u_n),u_n\rangle\to 0 \tag{3}$$

é limitada em $E$.

**Demonstração.** A prova encontra-se em [2]. □

## 3. Análise/Conclusão

O principal resultado deste trabalho pode ser descrito da seguinte forma:

**Teorema:** Suponha que $(V,Q) \in \mathcal{K}$ e $f \in \mathcal{C}^1(\mathbb{R},\mathbb{R})$ satisfazendo (F1)-(F4). Então (1) tem uma solução de energia mínima $\overline{u} \in E$ tal que $\Phi(\overline{u}) = \inf_{\mathcal{N}} \Phi > 0$.

**Demonstração.** Nesta ocasião, almejamos encontrar uma solução de energia mínima para o problema dado em (1). Para isso, vamos utilizar o fato provado pelas seções anteriores, de que $\Phi$ possui um ponto crítico não trivial. Os Lemas 1 e 2 fornecem uma sequência limitada $\{u_n\} \subset E$ tal que (2) é verificado. Passando para uma subsequência, o Teorema de Banach-Alaoglu assegura que $u_n \rightharpoonup u$ em $E$. Reiteramos que

$$\|u_n - u\|^2 = \Phi'(u_n)(u_n - u) + \int_{\mathbb{R}^N}\int_{\mathbb{R}^N} \frac{Q(x)Q(y)F(u_n(x))f(u_n(y))\,[u_n(y)-u(y)]}{|x-y|^{\mu}}dxdy.$$

Consequentemente, $\|u_n - u\|^2 = o_n(1)$ e devido a convergência forte, segue que $u_n \to u$ em $H^1(\mathbb{R}^N)$. Sabemos que

$$\|\Phi'(u_n)\| \leq \frac{\varepsilon}{1+\|u_n\|} \leq \varepsilon, \qquad \forall\, n \geq n_0.$$

Assim, $\|\Phi'(u)\| \leq \varepsilon$. Pela arbitrariedade de $\varepsilon > 0$, temos

$$\Phi'(u) = 0 \;\Leftrightarrow\; \langle \Phi'(u), h\rangle = 0, \qquad \forall\, h \in H^1(\mathbb{R}^N).$$

Logo,

$$\Phi(u) = c_* \in (0, m],$$

com $u$ solução fraca. Além disso, dado $u \in \mathcal{N}$, encontraremos $\Phi(u) \geq m$ (onde $m$ é a menor de todas as energias), pois se tomarmos $h = u$ temos que $\langle \Phi'(u), u\rangle = 0$. Dessa forma,

$$\Phi(u) \leq m \qquad \text{e} \qquad \Phi(u) \geq m.$$

Segue que

$$\Phi(u) = m > 0, \qquad \forall\, u \in E. \tag{4}$$

Portanto, $u \in E$ é uma solução de energia mínima para (1). □

## Referências

[1] ALVES, C. O.; SOUTO, M. A. S. **Existence of solutions for a class of nonlinear Schrdinger equations with potential vanishing at infinity**. J. Differential Equations, 2013. Nenhuma citação no texto.

[2] CHEN, S.; YUAN, S. **Ground state solutions for a class of Choquard equations with potential vanishing at infinity**, J. Math. Appl. 463: 880-894, 2018. Nenhuma citação no texto.

[3] LIEB, E. H. **Existence and uniqueness of the minimizing solution of Choquard's nonlinear equation**, Stud. Appl. Math. 57: 93-105, 1977. Nenhuma citação no texto.

[4] MOROZ, V.; SCHAFTINGEN, J. V. **Existence of groundstate for a class of nonlinear Choquard equations**, Trans. Amer. Math. Soc. 367: 6557-6579, 2015. Nenhuma citação no texto.

# EXISTÊNCIA E UNICIDADE DE SOLUÇÕES PARA O MODELO DE KELLER-SEGEL PARA A QUIMIOTÁXIA

**Masterson Falcão de Morais Costa**[1] **- masterson.costa@ufpe.br**

[1]Universidade Federal de Pernambuco, CCEN - Departamento de Matemática, PE, Brasil

***Resumo:*** *Neste trabalho, fazendo uso de ferramentas da Análise Funcional, foi estudado o modelo fracionário de Keller-Segel de ordem* $\alpha \in (0,1)$*. O modelo consiste em um sistema acoplado de Equações Diferenciais Parciais em* $\mathbb{R}^n$*, com* $n \geq 2$*. Considerando dados iniciais suficientemente pequenos e fazendo-se estimativas estruturais dos operadores de Mittag-Leffler via estimativas do semigrupo do calor, é demonstrado a existência e unicidade de soluções brandas, no sentido de Hadamard, construídas pelo princípio de Duhamel em espaços de Morrey e Besov-Morrey homogêneos para a classe de Fujita-Kato fazendo uso de um argumento topológico de ponto fixo de Banach. Com a hipótese,* $\gamma = 0$*, apresentamos soluções para o modelo que são invariantes por escala, ou seja, são auto-similares. E por fim, analisamos o comportamento assintótico das soluções, obtendo um resultado de estabilidade no tempo e como decorrência disso temos que cada solução auto-similar é um atrator global (AZEVEDO; CUEVAS; HENRIQUEZ, 2019).*
***Palavras-chave****: Quimiotaxia; Modelo de Keller-Segel Fracionário; Equações de Evolução.*

## 1. Introdução

O Cálculo Fracionário tem sido bastante difundido e utilizado por pesquisadores do mundo todo, mesmo não se tendo um consenso sobre aplicações físicas unificadas do assunto, ele traz melhorias pontuais para cada trabalho, por exemplo, para um modelo biológico como o modelo de Keller-Segel, criado no início da década de 70 por matemáticos estadunidenses. Este trabalho traz o espaços de Besov e Besov-Morrey, que estão tipos de espaços BMO, introduzidos por Mazzucato que são espaços mais gerais que o espaço $L^p$. Foi utilizado uma tecnica de topologia sobre pontos fixos em operadores lineares contínuos em espaços de Banach, para se garantir a existência e unicidades das soluções do modelo. O modelo ainda fornece resultado sobre soluções auto-similares e comportamento assintótico.

## 2. Metodologia

Este trabalho foi apresentado em minha dissertação para obtenção do título de Mestre em Matemática sob orientação do professor Dr. Claudio Cuevas, o artigo do tema é fruto da Tese de Doutorado de Joelma Azevedo.

## 3. Resultado e discussão

Modelos matemáticos necessitam da garantia de boa colocação para que façam sentido na vida real, afinal, não espera-se que um experimento nas mesmas condições, apresentem resultados diferente se você busca padroniza-lo. Isto é feito com maestria neste trabalho.

## 4. Conclusões

Além de divulgar as equações de evolução fracionária, é observado uma excelente técnica de boa colocação em Análise Funcional que pode ser utilizada em trabalhos futuros por estudantes e pesquisadores.

## Referências

AZEVEDO, J.; CUEVAS, C.; HENRIQUEZ, E. Existence and asymptotic behaviour for the time-fractional keller–segel model for chemotaxis. *Mathematische Nachrichten*, Wiley Online Library, v. 292, n. 3, p. 462–480, 2019. Citado na página 1.

# AVALIAÇÃO DO USO DA METODOLOGIA DE RESOLUÇÃO DE PROBLEMAS NO ENSINO DE MATEMÁTICA

**Aylla Gabriela Paiva de Araújo**[1] **- ayllagabriela@uern.br**
**Jeymerson Diogo de Oliveira**[1] **- jeymersonoliveira@alu.uern.br**

[1]Universidade do Estado do Rio Grande do Norte - Mossoró, RN, Brasil

***Resumo:*** *A Resolução de Problemas – RP, é uma metodologia de ensino de matemática que se baseia na construção do conhecimento por meio da investigação do conteúdo abordado ao buscar resolver problemas. Dessa forma, na medida em que problemas matemáticos são resolvidos, ocorre um desenvolvimento da aplicação e articulação dos saberes já apreendidos. Entendendo a importância da resolução de problemas para o ensino-aprendizagem de matemática, busca-se, através deste trabalho, desenvolver uma avaliação do uso dessa tendência da educação matemática em sala de aula. No detalhe, pretende-se entender a compreensão que os professores têm da metodologia, verificar de que modo ela é utilizada e interpretar qualitativamente dados, comparando o observado na prática com a teoria. Para isso, foi realizado pesquisa bibliográfica sobre o tema, pesquisa de campo para coleta de dados, através de aplicação de questionário com professores de matemática de escolas públicas e privadas do município de Mossoró-RN, análise dos dados e interpretação dos resultados analisados à luz da teoria de RP. Os resultados mostram que a utilização de RP é uma realidade presente nas escolas, e que essa metodologia é bem trabalhada com foco, principalmente, na compreensão do problema e na execução do plano de solução. Por outro lado, notou-se que o estímulo à lembrança específica de fórmulas e problemas parecidos, bem como, a realização de retrospecto da resolução, são sugestões da literatura que podem ser mais bem aproveitadas em sala de aula.*
***Palavras-chave****: matemática; resolução de problemas; metodologia*

## 1. Introdução

As práticas inovadoras que se destacam como tendências da Educação Matemática surgem da busca por melhorias no ensino da Matemática. Essas tendências expressam diferentes abordagens que, segundo Flemming, Luz e Mello (2005), são consideradas importantes no processo de ensino-aprendizagem. Entre essas, está a Resolução de Problemas – RP, discutida pela primeira vez por George Polya, em seu livro A arte de resolver problemas (1945).

Por muito tempo, resolver problemas em sala de aula se resumia a uma estratégia de verificação de conteúdos por meio da repetição de um algoritmo matemático. De acordo com Onuchic (1999), essa repetição ainda caracterizava o início do século XX. Porém, anos depois, começou-se a falar em resolver problemas. O matemático húngaro George Polya (1887 – 1985) foi o primeiro a sistematizar a aplicação da Resolução de Problemas no ensino de Matemática, em seu livro A arte de resolver problemas (1945). Seu trabalho serviu de alicerce para muitas pesquisas posteriores.

De acordo com Polya (1995), a resolução de problemas em sala de aula se fundamenta na interação professor aluno e aluno-professor. Para ele, esse processo pode ser dividido em quatro fases: compreender o problema; elaborar um plano; executar o plano; e fazer um retrospecto da resolução.

No entanto, ainda é comum as pessoas confundirem resolução de problemas com resolução de exercício de fixação, por isso, é fácil perceber que em muitas aulas é transmitida a ideia equivocada de que resolver problemas é algo mecânico e repetitivo. Daí, surge a necessidade de verificar a coerência entre a teoria dessa metodologia e a aplicação prática feita por professores de matemática. Dessa necessidade nos vem um questionamento: Qual a melhor maneira de usar a Resolução de Problemas em sala de aula?

Para dar resposta à problemática citada, este trabalho tem como objetivo geral avaliar a metodologia utilizada para resolução de problemas nas aulas de matemática. De forma específica, pretende-se: entender a compreensão dos professores sobre a resolução de problemas; verificar de que modo a RP é trabalhada nas aulas de matemática; comparar pontos da metodologia de RP com a forma utilizada em sala de aula; e inferir

um diagnóstico qualitativo sobre o estudo realizado.

## 2. Metodologia

Para o desenvolvimento deste trabalho, foram definidas e cumpridas as seguintes etapas:
1- Pesquisa bibliográfica sobre o tema;
2- Pesquisa de campo para coleta de dados;
3- Análise dos dados;
4- Interpretação dos resultados analisados à luz da teoria de RP.

Para a realização da primeira etapa, considerou-se trabalhos importantes acerca do tema, a maioria tinha como raiz comum o modelo de Polya para metodologia de RP. Essa pesquisa foi fundamental para adentrar ao tema e construir uma base de conhecimento teórico imprescindível para o desenvolvimento deste trabalho.

A segunda etapa consistiu em uma pesquisa de campo para coleta de dados. Neste trabalho, a coleta de dados foi realizada através de questionário aplicado a 19 professores de Matemática do Ensino fundamental e Médio de escolas públicas e privadas do município de Mossoró – Rio Grande do Norte. O questionário foi realizado no Google Formulários, e o link enviado para os entrevistados pelo Whats Up. Tendo em vista a pandemia, essas ferramentas foram muito úteis para proceder com a entrevista. O questionário era composto por 22 perguntas relacionadas a Resolução de Problemas, sendo todas baseadas nas proposições de modelo de Polya.

A análise dos dados considerou aspectos qualitativos, por meio de identificação de características comuns e organização dessas características em ferramentas como tabelas e gráficos, caracterizando, assim, essa pesquisa como qualitativa.

Após a análise dos dados, foi feita uma interpretação dos resultados através de comparação entre a teoria proposta por Polya para RP e a forma utilizada na prática pelos professores entrevistados.

## 3. Resultado e discussão

Quanto à primeira etapa da resolução de problemas, as ideias do modelo adotado mostram que é preciso compreender o problema, descrevendo-o com notação adequada e perguntando aos alunos sobre informações pertinentes ao problema. Na pesquisa de campo, o observado foi que, de modo geral, os entrevistados não apenas leem o problema mais de uma vez, como estimulam sua leitura, descrevem o problema com outras palavras e tem preocupação em observar se o problema foi bem compreendido pelos alunos, ouvindo-os.

Quanto à elaboração do plano de solução, o modelo de Polya propõe conexão entre o problema e a teoria já conhecida, bem como o uso de problemas auxiliares, de modo que se chegue a uma estratégia de solução, o plano de solução. As respostas às perguntas 9 a 14 indicam que a grande maioria dos entrevistados nem sempre faz associação entre o problema em questão e problemas parecidos sempre, mas mostrou que a maioria faz conexão do problema à teoria já vista, bem como estimular a construção do plano de solução.

Para a terceira etapa da resolução do problema, as proposições de Polya indicam que se deve executar o plano traçado, chegando na solução de modo que seja possível verificar cada passo. Conforme observado nos resultados, de modo geral, os professores entrevistados estimulam os alunos a executar o plano de solução, contribuem para o entendimento dos erros por meio de perguntas direcionadoras e incentivam a verificação dos passos da solução.

A quarta e última etapa do processo deve ser, segundo o modelo adotado, para retrospecto sobre a solução, revisando o caminho utilizado, entendendo o resultado, verificando outros caminhos possíveis e fazendo associações entre o resultado, o conteúdo e outros problemas. Os resultados indicam que a maioria dos entrevistados estimula a reflexão sobre o conteúdo abordado no problema, mas evidenciam que a maioria não tem como rotina realizar retrospecto sobre a solução de modo que haja estímulo à avaliação da estratégia utilizada, o que possibilitaria a comparação com outras estratégias.

## 4. Conclusões

RP é bem trabalhada em sala de aula, com foco, principalmente, na compreensão do problema e na execução do plano de solução, oportunizando-as aos alunos.

Apesar dos entrevistados estimularem os alunos a lembrar de conteúdos já vistos, nem sempre há estímulo à lembrança específica de fórmulas e problemas parecidos.

O retrospecto da resolução, importante para o aluno comparar resoluções já realizadas, nem sempre é trabalhado.

Considerando os resultados obtidos com esta pesquisa, pode-se afirmar, portanto, que uma boa maneira de se trabalhar a resolução de problemas nas aulas de matemática é, tomando como base o modelo de Polya, elaborar um planejamento de aula em que fique claro ao professor as ações necessárias para cada etapa da resolução do problema, de modo que o caminho a ser percorrido seja completamente conhecido e pensado para obtenção dos objetivos da aula.

**Referências**

FLEMMING, D. M.; LUZ, E. F.; MELLO, A. C. C. *Tendências em educação matemática. 2. ed.* [S.l.]: Palhoça: UnisulVirtual, 2005. Citado na página 1.

ONUCHIC, L. L. R. *Ensino-aprendizagem de matemática através da resolução de problemas*. São Paulo: Unesp, 1999. Citado na página 1.

POLYA, G. *A arte de resolver problemas: um novo aspecto do método matemático. Tradução e adaptação de Heitor Lisboa de Araújo*. Rio de Janeiro: Interciência, 1995. Citado na página 1.

# UMA CURIOSA APLICAÇÃO DA TEORIA DE BASES DE GRÖBNER: O PROBLEMA DA PERTINÊNCIA

**Celine Ingrid Gomes dos Santos**[1] **- celineingridgomess@hotmail.com**
**Thyago Santos de Souza**[1] **- thyago@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *A teoria de Bases de Gröbner fora apresentada pela primeira vez na tese de doutorado de Bruno Buchberger e, mais tarde, recebera esse nome em homenagem a Wolfgang Gröbner, orientador de Buchberger. Sinteticamente, uma Base de Gröbner para um ideal polinomial $I$ é um subconjunto $G$ de $I$ em que a igualdade entre o ideal gerado pelos termos líderes dos elementos de $G$ e o ideal gerado pelos termos líderes de $I$ é satisfeita. Dessa forma, neste trabalho, produzido a partir de uma Iniciação Científica vinculada ao Programa de Educação Tutorial (PET) – Matemática e Estatística, apresentaremos alguns resultados referentes a essa teoria. A posteriori, exibiremos as definições de Base de Gröbner Minimal e Reduzida, que serão essenciais para o alcance do nosso principal objetivo: compreender a aplicação de Bases de Gröbner ao problema da pertinência de um polinômio $f$ a um ideal. Por fim, veremos que essas bases também possuem contribuições na Álgebra linear e concluiremos que, em verdade, são uma generalização dos métodos de escalonamento e Eliminação de Gauss-Jordan.*
***Palavras-chave****: Bases de Gröbner; Ideais polinomiais; Pertinência a um ideal; Aplicação.*

## 1. Introdução

As ideias preliminares de Bases de Gröbner surgiram em 1965, por meio do até então estudante de doutorado Bruno Buchberger. Posteriormente, Buchberger, em homenagem ao seu orientador, Wolfgang Gröbner, rebatiza definitivamente sua teoria para Bases de Gröbner, que também são conhecidas como Base Padrão. Atualmente, há diversas aplicações dessa tese em diferentes áreas, como Geometria Algébrica, Engenharia, Álgebra Comutativa e Sistemas Computacionais. (SANTOS, 2020)

Dessa forma, neste trabalho, apresentaremos alguns conceitos e resultados introdutórios necessários para a compreensão da teoria de Bases de Gröbner e, ao final, mostraremos uma curiosa aplicação ao problema da pertinência de um polinômio $f$ a um ideal.

## 2. Metodologia

O presente trabalho é fruto de um projeto de pesquisa de Iniciação Científica, intitulado "Introdução às Bases de Gröbner e Aplicações", ainda em andamento, e que está sendo desenvolvido por meio do Programa de Educação Tutorial (PET) - Matemática e Estatística, da Universidade Federal de Campina Grande (UFCG).

A metodologia que utilizamos para estudo do tema e desenvolvimento deste trabalho fora a pesquisa bibliográfica em um livro de Álgebra e dois trabalhos de conclusão de curso. Todos podem ser encontrados nas referências deste trabalho. Para tanto, foram analisados os tópicos existentes nas obras citadas e, dessa forma, pudemos selecionar os de maior relevância para o contexto da pesquisa.

Dessarte, para estudo do conteúdo, empregamos o mesmo sistema de estudos utilizado no projeto de Iniciação Científica: exposições semanais de seminários sobre o tema. Após a análise desses materiais, fora possível construir o alicerce de fundamentos necessários para desenvolvimento deste trabalho.

## 3. Resultado e discussão

Todos os resultados que serão apresentados nesta seção foram retirados de Mendes (2012) e Coutinho (2012). Recomendamos a leitura circunstanciada dessas obras para a compreensão de todos os tópicos que não serão expostos aqui.

**Definição 1**: Uma **ordenação monomial** sobre $K[x_1, \cdots, x_n]$ é qualquer relação sobre $\mathbb{Z}_+^n$, ou, equivalentemente, qualquer relação $>$ sobre o conjunto de monômios $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_s}$, $\alpha \in \mathbb{Z}_+^n$, satisfazendo:
**(i)** $>$ é uma ordenação total sobre $\mathbb{Z}_+^n$.
**(ii)** Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}_+^n$, então $\alpha + \gamma > \beta + \gamma$.
**(iii)** $>$ é uma boa ordenação em $\mathbb{Z}_+^n$.

**Definição 2 (Ordenação Lexicográfica)**: Sejam $\alpha = (\alpha_1, \cdots, \alpha_n)$ e $\beta = (\beta_1, \cdots, \beta_n)$ pertencentes a $\mathbb{Z}_+^n$. Diremos que $\alpha >_{lex} \beta$ se no vetor diferença $\alpha - \beta \in \mathbb{Z}^n$, a coordenada não nula mais à esquerda de $\alpha - \beta$ é positiva. Escrevemos $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.

**Definição 3**: Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio não nulo em $K[x_1, \cdots, x_n]$ e seja $>$ uma ordenação monomial. Então:

**(i)** O **multigrau** de $f$ é:
$$multigrau(f) = max\{\alpha \in \mathbb{Z}_+^n : a_\alpha \neq 0\}.$$

**(ii)** O **coeficiente líder** de $f$ é:
$$CL(f) = a_{multigrau(f)} \in K.$$

**(iii)** O **monômio líder** de $f$ é:
$$ML(f) = x^{multigrau(f)}$$

**(iv)** O **termo líder** de $f$ é:
$$TL(f) = CL(f) \cdot ML(f).$$

**Teorema 1 (Algoritmo de Divisão em** $K[x_1, \cdots, x_n]$**)**: Fixe uma ordenação monomial $>$ sobre $\mathbb{Z}_+^n$, e seja $F = (f_1, \cdots, f_s)$ uma s-upla ordenada de polinômios em $K[x_1, \cdots, x_n]$. Então todo $f \in K[x_1, \cdots, x_n]$ pode ser escrito como
$$f = a_1 f_1 + \cdots + a_s f_s + r,$$
onde $a_1, \cdots, a_s \in K[x_1, \cdots, x_n]$ e $r = 0$ ou $r$ é uma combinação linear, com coeficientes em $K$, de monômios, tais que nenhum deles é divisível por algum $TL(f_1), \cdots, TL(f_s)$. Chamaremos $r$ de resto da divisão de $f$ por $F$. Além disso, se $f_i \neq 0$, temos, então
$$multigrau(f) \geq multigrau(a_i f_i).$$

**Lema 1**: Seja $I = \langle x^\alpha : \alpha \in A \rangle$ um ideal monomial. Então um monômio $x^\beta$ pertence a $I$ se, e somente se, $x^\beta$ é divisível por $x^\alpha$, para algum $\alpha \in A$.

**Definição 4**: Seja $I \subset K[x_1, \cdots, x_n]$ um ideal não nulo.

**(i)** Denotamos por $TL(I)$ o conjunto de termos líderes dos elementos de $I$. Desse modo,
$$TL(I) = \{cx^\alpha; \exists\ f \in I \text{ com } TL(f) = cx^\alpha\}.$$

**(ii)** Denotamos por $\langle TL(I) \rangle$ o ideal gerado pelos elementos de $TL(I)$.

**Definição 5**: Fixe uma ordenação monomial. Um subconjunto finito $G = \{g_1, \cdots, g_s\}$ de um ideal $I$ é dito uma **base de Gröbner** de $I$ se
$$\langle TL(g_1), \cdots, TL(g_s) \rangle = \langle TL(I) \rangle .$$

Do Lema 1, temos que um conjunto $g_1, \cdots, g_s \subset I$ é uma base de Gröbner se, e somente se, o termo líder de qualquer elemento de $I$ é divisível por um dos $TL(g_i)$.

**Proposição 1**: Seja $G = \{g_1, \cdots, g_s\}$ uma base de Gröbner para o ideal $I \subset K[x_1, \cdots, x_n]$ e seja $f \in K[x_1, \cdots, x_n]$. Então existe um único $r \in K[x_1, \cdots, x_n]$ com as seguintes propriedades:

**(i)** Nenhum termo de $r$ é divisível por nenhum dos $TL(g_1), \cdots, TL(g_s)$.
**(ii)** Existe $g \in I$ tal que $f = g + r$.

Em particular, $r$ é os resto da divisão de $f$ por $G$, não importando como os elementos de $G$ estão ordenados quando usamos o algoritmo da divisão.

Dessa forma, a partir da proposição anterior, podemos enunciar o Corolário 1, que nos dá uma forma de determinar quando um polinômio pertence a um ideal.

**Corolário 1**: Seja $G = \{g_1, \cdots, g_s\}$ uma base de Gröbner para o ideal $I \subset K[x_1, \cdots, x_n]$ e seja $f \in K[x_1, \cdots, x_n]$. Então $f \in I$ se, e somente se, o resto da divisão de $f$ por $G$ é zero.

*Demonstração:* Se o resto é zero, então $f = a_1 g_1 + \cdots + a_s g_s \in I$. Reciprocamente, dado $f \in I$, então $f = f + 0$ satisfaz as duas condições da proposição anterior. Portanto, segue que 0 é o resto da divisão de $f$ por $G$. □

**Definição 6**: Escrevemos $\overline{f}^F$ para o resto da divisão de $f$ pela s-upla ordenada $F = (f_1, \cdots, f_s)$. Se $F$ é uma base de Gröbner para $\langle f_1, \cdots, f_s \rangle$, então podemos considerar $F$ como um conjunto, ou seja, sem nenhuma ordem entre seus elementos.

**Definição 7**: Sejam $f, g \in K[x_1, \cdots, x_n]$ polinômios não nulos.

**(i)** Se $multigrau(f) = \alpha$ e $multigrau(g) = \beta$, então tomamos $\gamma = (\gamma_1, \cdots, \gamma_n)$, em que $\gamma_i = max(\alpha_i, \beta_i)$, para cada $i = 1, 2, \cdots, n$. Chamaremos $x^\gamma$ o **Mínimo Múltiplo Comum** de $ML(f)$ e $ML(g)$, e escreveremos $x^\gamma = MMC(ML(f), ML(g))$.

**(ii)** O **S-polinômio** de $f$ e $g$ é a combinação

$$S(f, g) = \frac{x^\gamma}{TL(f)} \cdot f - \frac{x^\gamma}{TL(g)} \cdot g.$$

**Teorema 2 (Critério de Buchberger)**: Seja $I \neq \{0\}$ um ideal polinomial. Então a base $G = \{g_1, \cdots, g_s\}$ de $I$ é uma base de Gröbner de $I$ se, e somente se, o resto da divisão de $S(g_i, g_j)$ por $G$ é zero, para todos os pares $(i, j)$, com $i \neq j$.

O próximo resultado ilustrará uma maneira de computarmos uma base de Gröbner para um ideal $I$ a partir de um conjunto $\{f_1, \cdots, f_s\}$ que gera $I$.

**Teorema 3 (Algoritmo de Buchberger)**: Seja $I = \langle f_1, \cdots, f_s \rangle \neq \{0\}$ um ideal polinomial. Então uma base de Gröbner pode ser construída em um número finito de passos por meio do seguinte algoritmo:

*Entrada* : $F = (f_1, \cdots, f_s)$
*Saída* : *Uma base de Gröbner* $G = (g_1, \cdots, g_s)$ *para* $I$, *com* $F \subset G$
$G := F$
*REPITA*
  $G' := G$
  *PARA cada par* $\{p, q\}$, *com* $p \neq q$ *em* $G'$ *FAÇA*
  $S := \overline{S(p, q)}^{G'}$
  *SE* $S \neq 0$ *ENTÃO* $G := G \cup \{S\}$
*ATÉ* $G = G'$

**Lema 2**: Seja $G$ uma base de Gröbner do ideal $I$. Seja $p \in G$ um polinômio tal que $TL(p) \in \langle TL(G - \{p\}) \rangle$. Então $G - \{p\}$ é também uma base de Gröbner de $I$.

**Definição 8**: Uma **base de Gröbner minimal** para um ideal polinomial $I$ é uma base de Gröbner $G$ tal que:

**(i)** $CL(p) = 1$, para todo $p \in G$.
**(ii)** Para todo $p \in G$, $TL(p) \notin \langle TL(G - \{p\})\rangle$.

Para obtermos uma base de Gröbner minimal para um ideal $I \neq \{0\}$, utilizamos o Algoritmo de Buchberger e, logo após, o Lema 2 para eliminar os geradores desnecessários que podem ter sido incluídos

**Definição 9**: Uma **base de Gröbner reduzida** para um ideal polinomial $I$ é uma base de Gröbner $G$ para $I$ tal que:

**(i)** $CL(p) = 1$, para todo $p \in G$.
**(ii)** Para todo $p \in G$, nenhum monômio de $p$ pertence a $\langle TL(G - \{p\})\rangle$

**Proposição 2**: Seja $I \neq \{0\}$ um ideal polinomial. Então, para uma dada ordenação monomial, existe uma única base de Gröbner reduzida para $I$.

Vejamos, agora, o problema da pertinência de um polinômio $f$ a um ideal.

**Aplicação**: Como vimos anteriormente, no Corolário 1, podemos resolver o problema da pertinência de um polinômio $f$ a um ideal $I$ apenas calculando uma base de Gröbner $G$ para $I$ e utilizando algoritmo da divisão com $f$ como dividendo e $G$ como divisor. Após isso, concluímos que $f \in I$ se, e somente se, o resto da divisão de $f$ por $G$ é zero.

Dessa forma, vamos mostrar que o polinômio

$$f = 2xw - w - 2zy + y$$

pertence ao ideal $I = \langle f_1, f_2\rangle$, onde

$$f_1 = wx + w - zy \quad \text{e} \quad f_2 = wx - 2w - zy + y.$$

Primeiramente, vamos calcular uma base de Gröbner para esse ideal, relativamente à ordenação lexicográfica, com $x > y > z > w$. Assim, vamos iniciar calculando

$$S(f_1, f_2) = -y + 3w,$$

o qual denotaremos por $f_3$. Como os S-polinômios $S(f_1, f_3)$ e $S(f_2, f_3)$ deixam resto zero relativamente ao conjunto

$$\{f_1, f_2, f_3\},$$

concluímos, pelo Critério de Buchberger, que esse conjunto é uma base de Gröbner de $\langle f_1, f_2\rangle$ relativamente à ordem lexicográfica, com $x > y > z > w$. No entanto, note que $f_1$ e $f_2$ têm o mesmo termo líder, isto é, a base de Gröbner encontrada não é minimal. Para minimalizá-la, removemos $f_2$, obtendo

$$\{f_1, f_3\}.$$

Essa nova base é minimal, porém, não é reduzida, pois o resto da divisão de $f_1$ por $f_3$ é $xw - 3zw + w$. Como o resto da divisão de $f_3$ por $f_1$ é $f_3$, podemos concluir que

$$G = \{xw - 3zw + w, y - 3w\}$$

é uma base de Gröbner reduzida de $\langle f_1, f_2\rangle$.

Por fim, vamos calcular o resto da divisão de $f$ por $G$. Temos,

$$2xw - w - 2zy + y = 2(xw - 3zw + w) + (2z + 1)(y - 3w)$$

ou seja, o resto da divisão é zero. Isso prova que $f$ pertence ao ideal $\langle f_1, f_2 \rangle$, completando, desse modo, essa aplicação.

**Observação**: Vamos ver, ainda, algumas conexões entre o algoritmo de Buchberger e o algoritmo de linha-redução (Eliminação de Gauss-Jordan) para sistemas de equações lineares. O fato interessante aqui é que o algoritmo de linha-redução é, essencialmente, um caso particular do algoritmo geral visto neste trabalho. Vejamos um situação correspondente ao sistema de equações lineares:

$$\begin{cases} 3x - 6y - 2z + 0w = 0 \\ 2x - 4y + 0z + 4w = 0 \\ x - 2y - z - w = 0 \end{cases}$$

Se usarmos linha-operações na matriz dos coeficientes do sistema anterior para colocá-la na forma escalonada, obteremos:

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} (*)$$

Após isso, se computarmos a matriz escalonada reduzida, encontraremos:

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} (**)$$

Agora, seja $I$ o ideal

$$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w \rangle$$

que corresponde ao sistema de equações inicial. Usando a ordenação lexicográfica com $x > y > z > w$, vamos aplicar o Critério de Buchberger a $I$. Assim, $I = \langle \tilde{f}_3, \tilde{f}_4 \rangle = \langle x - 2y + 2w, z + 3w \rangle$ é uma base de Gröbner reduzida. Perceba, ainda, que $I$ é equivalente ao sistema escalonado reduzido apresentado anteriormente em $(**)$.

Um ponto interessante que podemos destacar é que assim como na Álgebra Linear toda matriz pode ser colocada na forma escalonada reduzida de forma única, também temos aqui a unicidade das bases de Gröbner reduzidas.

## 4. Conclusões

Em suma, como fora ilustrado ao longo deste trabalho, a teoria de Bases de Gröbner é uma abrangente e poderosa ferramenta que consegue generalizar os artifícios estudados na Álgebra Linear, sendo capaz de resolver, também, sistemas não lineares.

Além da aplicação apresentada nos resultados deste trabalho, há outros diversos empregos das Bases de Gröbner que podem despertar a curiosidade do leitor. Para tanto, recomendamos a leitura das referências deste trabalho para mais detalhes.

## Referências

COUTINHO, S.C. **Polinômios e Computação Algébrica**. Rio de Janeiro: IMPA, 2012.

MENDES, B. R. A. F. **Bases de Groebner e Aplicações em Álgebra Comutativa.** Monografia (Graduação em Matemática), Universidade Federal de São Carlos. São Carlos, p. 91. 2012.

SANTOS, P. A. D. **Introdução as Bases de Gröbner.** Monografia (Graduação em Matemática) - Faculdade de Matemática, Universidade Federal de Uberlândia. Uberlândia, p. 40. 2020.

# CALCULANDO UMA INTEGRAL IMPRÓPRIA UTILIZANDO O TEOREMA DE RESÍDUOS

**Laryssa Kely Alves Rodrigues** [1] **- lkellyalves@hotmail.com**
**Romildo Nascimento de Lima**[1] **- romildo@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Na disciplina de Cálculo Diferencial e Integral II, os estudantes deparam-se com o cálculo de integrais impróprias reais de funções racionais, e aprendem um método de resolução. Entretanto, objetivamos, neste trabalho, discorrer acerca de um outro modo de calcular esse tipo de integral, utilizando a aplicação do teorema de resíduos, conceito este fornecido pela Análise Complexa que vamos apresentar ao longo deste resumo. Do ponto de vista metodológico, estudamos o conteúdo mencionado em vários livros ao longo dos seminários realizados através de uma Iniciação Científica vinculada ao Programa de Ensino Tutorial (PET) Matemática e Estatística. Por conseguinte, enunciaremos alguns teoremas e definições que são necessárias para compreender como aplicar o teorema de resíduos. E por fim, aplicaremos o que foi estudado através de um exemplo. Mediante o elencado, esperamos que este trabalho desperte o interesse do leitor em aprender sobre o Teorema de Resíduos e suas aplicações.*
***Palavras-chave****: Cálculo de integrais; Teorema de resíduos; Séries de potências; Análise Complexa.*

## 1. Introdução

Inicialmente, é válido pontuar que, um estudante ao ingressar na disciplina de Cálculo Diferencial e Integral II[2], adquire como um dos primeiros conceitos, o cálculo de Integrais Impróprias do tipo I, que consiste em integrais com limites infinitos de integração. Consoante a isso, podemos destacar a definição vista na disciplina, encontrada em Thomas (2012):

Se $f(x)$ é contínua em $(-\infty, \infty)$, então,

$$\int_{-\infty}^{\infty} f(x)\,dx = \int_{-\infty}^{c} f(x)\,dx + \int_{c}^{\infty} f(x)\,dx \tag{1}$$

onde $c$ é qualquer número real. Em decorrência das proposições supramencionadas, neste trabalho, vamos introduzir um método diferente para calcular integrais impróprias de funções racionais aplicando alguns conceitos estudados na Análise Complexa, como Singularidades e o Teorema do Resíduo. Os pré-requisitos que são necessários para a compreensão do assunto que irá ser abordado são: série de Taylor, série de Laurent, singularidades (em particular, do tipo polo) e resíduos.

Para isso, é necessário recordar alguns conceitos que irão servir como base para compreender como calcular integrais aplicando o teorema que irá ser apresentado. Dessa forma, o estudante terá uma outra ferramenta à disposição para o cálculo de integrais, além de agregar novas ideias e conceitos que serão apontados ao longo deste trabalho.

## 2. Metodologia

Este trabalho é resultado de estudos realizados através de um projeto de Iniciação Científica vinculada ao PET Matemática e Estatística da Universidade Federal de Campina Grande, possuindo como título "Estudo de Alguns Elementos da Análise Complexa e Aplicações". Para o desenvolvimento destas atividades, foram executadas pesquisas bibliográficas em alguns livros que abordam o assunto procurado, como os livros do Ávila (2008), Zill e Shanahan (2011) e Brown e Churchill (2009). Atrelado a isso, utilizamos também livros de Cálculo Diferencial e Integral, como os livro de Thomas (2012) e Guidorizzi (2014) para estabelecer comparações.

[2]Estamos nos referindo a uma disciplina cursada na Universidade Federal de Campina Grande - UFCG.

Dessa forma, por intermédio desses materiais e seminários expostos semanalmente acerca do tema, realizou-se a concretização deste resumo.

## 3. Resultado e discussão

Todos os resultados mostrados ao longo do texto foram retirados de ÁVILA(2008), ZILL e SHANAHAN (2011) e Thomas (2012). Caso o leitor tenha interesse em consultar as demonstrações que não foram apresentadas, recomendamos a pesquisa nos livros mencionados nas referências.

É essencial considerar, antes de tudo, o conceito de série de Laurent. Nesse sentido, devemos relembrar também a definição de Série de Taylor, para isso, vejamos essa definição no caso Real. Sabemos que, no caso desta última série, é possivel desenvolver em séries de potências de $z - z_0$ uma função que seja regular em $z_0$.

**Definição 1** (Série de Taylor)**.** *Seja $f$ uma função com derivadas de todas as ordens em algum intervalo contendo $a$ como um ponto interior. Então, a* ***série de Taylor gerada por*** *$f$* ***em*** *$x = a$ é*

$$\sum_{k=0}^{\infty} \frac{f^{(k)}(a)}{k!}(x-a)^k = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + \cdots . \tag{2}$$

Ademais, veremos agora que, o desenvolvimento pode ainda ser possível, mesmo que a função não seja regular em $z_0$, desde que admitam-se potências com expoentes negativos. Esse tipo de série que acabamos de mencionar é intitulada como série de Laurent, isto é, uma generalização da série de Taylor. Seu resultado geral é dado pelo seguinte teorema:

**Teorema 1.** *Seja $f$ uma função univalente e analítica numa região anelar $G$: $r < |z - z_0| < R$. Então, para todo $z$ nesta região,*

$$f(z) = \sum_{n=1}^{\infty} \frac{a_{-n}}{(z-z_0)^n} + \sum_{n=0}^{\infty} a_n (z-z_0)^n \tag{3}$$

*onde os coeficientes $a_n$, $n = 0, \pm 1, \pm 2, ...$, são dados por*

$$a_n = \frac{1}{2\pi i} \int_C \frac{f(s)}{(s-z_0)^{n+1}}\, ds \tag{4}$$

*sendo $C$ um contorno fechado em $G$, envolvendo $z_0$ uma vez no sentido positivo.*

**Demonstração.** Dado $z \in G$, sejam $r_1$ e $r_2$ tais que $r < r_1 < |z - z_0| < r_2 < R$. Designemos por $C_1$ e $C_2$ os círculos de centro $z_0$ e raios $r_1$ e $r_2$, respectivamente, orientados no sentido positivo. Ligando $C_1$ e $C_2$ por um arco $L$, obtemos um contorno fechado $\gamma = C_2 + L - C_1 - L$, numa região de regularidade da função $f$; logo, pela fórmula de Cauchy,

$$f(z) = \frac{1}{2\pi i} \int_{\gamma} \frac{f(s)}{s-z}\, ds. \tag{5}$$

As integrais ao longo de $L$ e $-L$ se cancelam mutuamente, portanto,

$$f(z) = \frac{1}{2\pi i} \int_{C_2} \frac{f(s)}{s-z}\, ds - \frac{1}{2\pi i} \int_{C_1} \frac{f(s)}{s-z}\, ds. \tag{6}$$

A primeira destas integrais é tratada exatamente como no caso da série de Taylor e resulta na série de potências positivas que aparece em (3), em que, substituída em (6), resulta

$$f(z) = \sum_{n=0}^{\infty} a_n (z-a_0)^n - \frac{1}{2\pi i} \int_{C_1} \frac{f(s)}{s-z}\, ds. \tag{7}$$

Quanto a esta última integral, notamos primeiro que

$$\frac{1}{s-z} = \frac{1}{(s-z_0)-(z-z_0)} = \frac{-1}{z-z_0} \cdot \frac{1}{1 - \dfrac{s-z_0}{z-z_0}} = -\sum_{n=0}^{\infty} \frac{(s-z_0)^n}{(z-z_0)^{n+1}}. \tag{8}$$

Esta série converge uniformemente em $s \in C_1$, então

$$-\frac{1}{2\pi i}\int_{C_1}\frac{f(s)}{s-z}\,ds = \frac{1}{2\pi i}\int_{C_1} f(s)\sum_{n=0}^{\infty}\frac{(s-z_0)^n}{(z-z_0)^{n+1}} \tag{9}$$

$$= \sum_{n=0}^{\infty}\frac{1}{(z-z_0)^{n+1}}\cdot\frac{1}{2\pi i}\int_{C_1}\frac{f(s)}{(s-z_0)^{-n}}\,ds. \tag{10}$$

Escrevendo $n+1$ como novo índice $n$, obtemos

$$-\frac{1}{2\pi i}\int_{C_1}\frac{f(s)}{(s-z)}\,ds = \sum_{n=1}^{\infty}\frac{1}{(z-z_0)^{n}}\cdot\frac{1}{2\pi i}\int_{C_1}\frac{f(s)}{(s-z_0)^{-n+1}}\,ds. \tag{11}$$

Substituindo em (7), obtemos o desenvolvimento dado no teorema, já que a integral que aparece em (4) tem o mesmo valor, qualquer que seja o contorno $C$ descrito no teorema, em particular $C_1$ ou $C_2$. ■

Outro fator importante para a compreensão do teorema principal que vamos utilizar, é a definição de resíduos e a definição de polo.

**Definição 2** (Resíduos)**.** *Seja $f$ uma função regular e univalente numa região $R$, exceto numa singularidade isolada $z_0 \in R$. Então, numa vizinhança de $z_0$ vale o desenvolvimento de Laurent,*

$$f(z) = \sum_{n=1}^{\infty}\frac{a_{-n}}{(z-z_0)^n} + \sum_{n=0}^{\infty} a_n(z-z_0)^n$$

os coeficientes $a_n$ sendo dados por

$$a_n = \frac{1}{2\pi i}\int_C \frac{f(s)}{(s-z_0)^{n+1}}\,ds$$

onde C é um contorno fechado de R, envolvendo $z_0$ uma vez no sentido positivo. O coeficiente $a\_1$ é chamado resíduo de $f$ no ponto $z_0$, e denotado $(res.f)(z_0)$

**Teorema 2** (Teorema do resíduo)**.** *Se $f$ é regular e univalente numa região simplesmente conexa $R$, exceto em um número finito de singularidades isoladas, $z_1, ..., z_k$, então*

$$\int_C f(z)\,dz = 2\pi i\sum_{j=1}^{k}(res.f)(z_j)$$

*onde $C$ é um contorno fechado de $R$, envolvendo $z_1, ..., z_k$ uma vez no sentido positivo.*

A demonstração pode ser encontrada em Ávila (2008).

**Definição 3** (Polo)**.** *Vamos considerar, o caso em que no desenvolvimento*

$$f(z) = \sum_{n=1}^{\infty}\frac{a_{-n}}{(z-z_0)^n} + \sum_{n=0}^{\infty} a_n(z-z_0)^n \tag{12}$$

*só aparece um número finito de potências negativas, isto é, existe $m > 0$ tal que $a_{-m} \neq 0$ e $a_{-n} = 0$ para $n > m$. Então, (12) se reduz a*

$$f(z) = \frac{a_{-m}}{(z-z_0)^m} + ... + \frac{a_{-1}}{(z-z_0)} + \sum_{n=0}^{\infty} a_n(z-z_0)^n, a_{-m} \neq 0. \tag{13}$$

*Neste caso, $z_0$ é chamado polo de ordem $m$ da função $f$.*

Além disso, o resíduo $a_{-1}$ no caso de um polo simples é dado pelo seguinte teorema:

**Teorema 3** (Resíduo em um Polo Simples)**.** *Se $f$ tiver um polo simples em $z = z_0$,*

$$(Res.f)(z_0) = \lim_{z \to z_0} [(z - z_0)f(z)] \tag{14}$$

A demonstração acima pode ser consultada no livro de Zill e Shanahan (2011). Nessa perspectiva, depois de ter compreendido alguns pré-requisitos, veremos como o teorema de resíduos pode ser uma alternativa para o cálculo de certas integrais impróprias de funções racionais.

**Exemplo 1.** *Calcule a integral*

$$\int_{-\infty}^{\infty} \frac{1}{x^2+1}\, dx$$

Na disciplina de Cálculo Diferencial e Integral II, aprendemos, da seguinte maneira:

Pela definição, podemos escrever,

$$\int_{-\infty}^{\infty} \frac{1}{1+x^2}\, dx = \int_{-\infty}^{0} \frac{1}{1+x^2}\, dx + \int_{0}^{\infty} \frac{1}{1+x^2}\, dx$$

Dessa forma, resolvemos cada integral imprópria

$$\int_{-\infty}^{0} \frac{1}{1+x^2}\, dx = \lim_{a \to -\infty} \int_{a}^{0} \frac{1}{1+x^2}\, dx \tag{16}$$

$$= \lim_{a \to -\infty} \arctan|_{a}^{0} \tag{17}$$

$$= \lim_{a \to -\infty} (\arctan(0) - \arctan(a)) = \frac{\pi}{2} \tag{18}$$

Agora, note que,

$$\int_{0}^{\infty} \frac{1}{1+x^2}\, dx = \lim_{b \to \infty} \int_{0}^{b} \frac{1}{1+x^2}\, dx \tag{19}$$

$$= \lim_{b \to \infty} \arctan|_{0}^{b} \tag{20}$$

$$= \lim_{b \to \infty} (\arctan(b) - \arctan(0)) = \frac{\pi}{2} \tag{21}$$

Portanto,

$$\int_{-\infty}^{\infty} \frac{1}{x^2+1}\, dx \ = \frac{\pi}{2} + \frac{\pi}{2} = \pi$$

Por conseguinte, vamos calcular utilizando o Teorema de resíduos. Sendo assim,

$$\int_{-\infty}^{\infty} \frac{1}{x^2+1}\, dx \ = \lim_{R \to \infty} \int_{-R}^{R} \frac{1}{z^2+1}\, dz \tag{22}$$

O integrando, $f(z) = \dfrac{1}{z^2+1} = \dfrac{1}{(z-i)(z+i)}$, possui polos simples nos pontos $z = \pm i$. Seja $C_R$ o semicírculo do semiplano $Imz \geq 0$, de raio R e centro na origem. Supondo $R > 1$, o contorno formado pelo segmento $[R, -R]$, seguido de $C_R$, contém o polo $z = i$, onde o resíduo de $f$ é

$$Res(f(z), i) = \lim_{z \to i} (z - i) \frac{1}{(z-i)(z+i)} = \frac{1}{2i}$$

Pelo teorema do resíduo,

$$\int_{-R}^{R} \frac{1}{z^2+1}\,dz + \int_{C_R} \frac{1}{z^2+1}\,dz = 2\pi i \cdot \frac{1}{2i} = \pi$$

Por outro lado, $|f(z)| \leq \dfrac{1}{|z|^2-1}$, donde

$$\left|\int_{C_R} \frac{1}{z^2+1}\right| \leq \frac{1}{R^2-1}\int_{C_R} |dz| = \frac{\pi R}{R^2-1} \tag{24}$$

Isso mostra que

$$\lim_{R\to\infty} \int_{C_R} \frac{1}{z^2+1}\,dz = 0;$$

logo, passando ao limite com $R \to \infty$ em (5.9), obtemos

$$\int_{-\infty}^{\infty} \frac{1}{x^2+1}\,dx = \pi$$

que é o resultado procurado.

Embora esse exemplo seja dos mais simples que se possa imaginar, ele apresenta um procedimento que é aplicável ao cálculo de toda integral de $-\infty$ a $\infty$ de funções racionais $f(z) = \dfrac{P(z)}{Q(z)}$, onde $Q(z)$ não se anula para $z$ real e $grauQ - grauP = m \geq 2$. Dessa forma, esse exemplo foi escolhido, por ser a integral em questão sempre presente nos cursos de cálculo.

## 4. Conclusões

Torna-se evidente, portanto, que o Teorema de resíduos pode auxiliar no cálculo de integrais reais com limites infinitos de integração, sendo um dispositivo diferente para a resolução desse tipo de integral que é apresentada ao aluno durante o curso de Cálculo Diferencial e Integral II. Assim, a inserção dessa ferramenta na vida do estudante poderá desencadear um interesse nos estudos da Análise Complexa.

Diante do exposto, o discente agora poderá escolher qual método for mais apropriado diante de alguma integral que poderá surgir ao longo de sua vida acadêmica. Sendo assim, acreditamos que com o auxílio deste trabalho, tenhamos despertado o interesse pelo estudo do Teorema de resíduos e outras aplicações advindas dessa proposição. Além disso, caso o leitor tenha curiosidade nas demonstrações que não foram exibidas, elas encontram-se demonstradas nos livros que foram citados como referências.

## Referências

ÁVILA, G. Variáveis Complexas e Aplicações. 3 ed. Rio de Janeiro: LTC, 2008.

ZILL, D.G.; SHANAHAN, P.D. Curso Introdutório à Análise Complexa com Aplicações. 2 ed. Rio de Janeiro: LTC, 2011.

BROWN, J.W., CHURCHILL, R.V. Complex Variables and Applications. 8 ed. Boston: Mc-Graw Hill, 2008.

THOMAS, G.B. Cálculo, volume 1. 12 ed. São Paulo: Perason Education do Brasil, 2012.

GUIDORIZZI, H. L. Um curso de Cálculo, vol. 4. 5 ed. Rio de Janeiro: LTC, 2013.

# PRODUTO SEMIDIRETO

**Juan Pablo França Alves Cantalice**[1] **- juanpablo.contato@gmail.com**
**Diogo Diniz Pereira da Silva e Silva**[1] **- diogo@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Na matemática, e em especial na teoria dos grupos, um produto semidireto é uma generalização de um produto direto. Existem dois conceitos intimamente relacionados de produto semidireto, a de produto semidireto interno e externo. Nosso intuito no presente trabalho, é trazer uma abordagem didática e formal sobre produto semidireto, assunto que pouco é visto pelos alunos de graduação em matemática, seja do bacharelado ou licenciatura. O método utilizado foi o de pesquisa teórica, isto é, nosso trabalho é fruto de estudos prévios teóricos nos quais nos baseamos para trazer de forma clara, objetiva e didática tal conteúdo de produto semidireto. Os conceitos de algébra são fundamentais e trabalhados de forma predominante em nossa abordagem, desse modo, acabam proporcionando amadurecimento e a oportunidade do compartilhamento entre a comunidade acadêmica de matemática, em especial, entre os estudantes de graduação, que por muitas vezes, desconhecem tal conteúdo.*
***Palavras-chave****: Teoria de Grupos; Produto Semidireto; Álgebra*

## 1. Introdução

A teoria de grupos, é um importante ramo da álgebra, pois traz diversas aplicações em vários tipos de campos da ciência em geral, além do mais, abre um leque de pesquisa imenso para os matemáticos. A teoria dos grupos tem sua origem no trabalho do matemático francês Évariste Galois (1811-1832) sobre a solubilidade por radicais de equações polinomiais. Outros matemáticos, dentre eles o suíço Leonard Euler (1707-1783), o alemão Carl Friedrich Gauss (1777-1855), o francês Joseph Louis Lagrange (1736-1813), o norueguês Niels Henrik Abel (1802-1829), e o italiano Paolo Ruffini (1765-1822), também colaboraram para o crescimento desta área, com contribuições na teoria das equações algébricas, na teoria de números e na geometria.(SOUZA, 2012)

Um grupo é uma estrutura relativamente simples quando comparada com um anel, tal estrutura possui apenas uma operação binária. Embora simples do ponto de vista álgebrico, a teoria de grupos possui tópicos de extrema complexidade.

Produto semidireto, é um assunto dentro da teoria de grupos que normalmente não é visto pelo alunos da graduação em matemática, tendo isso em mente, em nosso trabalho, apresentaremos o conceito de produto semidireto, abordaremos alguns exemplos, traremos consequências e observações importantes.

## 2. Metodologia

Nosso trabalho é fruto de um conjunto de elementos, tais elementos são os vários encontros de Iniciação Científica feitos no período de 2020 até o presente momento, na qual foram e estão sendo desenvolvidos por meio do Progama de Educação Tutorial (PET) - Matemática e Estatística, da Universidade Federal de Campina Grande (UFCG). Tais encontros proporcionaram um amadurecimento maior nos temas relativos a álgebra. Outro elemento de suma importância na produção desse trabalho, foram os conteúdos vistos na disciplina de Álgebra I, ofertada pela Universidade Federal de Campina Grande (UFCG).

Nossa metologia foi a de pesquisa bibliográfica, isto é, fizemos um estudo prévio através de nossas principais referências, dentre elas (BRANDÃO, 2021), (FRALEIGH, 1994) e (GONÇALVES, 1999). Após visto todos os conteúdos fundamentais e que formam a base da teoria de grupos, podemos pesquisar um pouco mais de modo a construir tal material de produto semidireto.

Foram feitos encontros semanais com o orientador da Iniciação Científica através da plataforma Google Meet, além do mais, houveram exposições semanais bem como momentos para tirar as dúvidas e resolver exercícios. Também podemos incluir as várias dúvidas sanadas através de email, por parte do professor de Álgebra I. Com a junção de tais elementos citados, fora possível fazer o estudo de produto semidireto bem como a produção do presente resumo.

## 3. Resultado e discussão

Como já afirmamos, produto semidireto é um assunto particular da teoria de grupos, portanto é indispensável trazer conceitos de modo que sua abordagem fique suscinta. Um conceito de extrema relevância é o de transversal.

**Definição 1:** Sejam G um grupo, H um subgrupo de G e T um subconjunto não vázio de G. Dizemos que T é:

- Um transversal à direita para H em G se $Ht_1 \neq Ht_2$, para quaisquer $t_1, t_2 \in T$ distintos, $\bigcup_{t\in T} Ht = G$.
- Um transversal à esquerda para H em G se $t_1H \neq t_2H$ para quaisquer $t_1, t_2 \in T$ distintos, e $\bigcup_{t\in T} tH = G$.

**Definição 2:** Sejam G um grupo e H e N subgrupos de G. Dizemos que G é o produto semidireto (interno) de N por H se $G = HN$, $H \cap N = \{e\}$ e $N \trianglelefteq G$.

**Notações:** $G = N \rtimes H$ e $G = H \ltimes N$.

Sendo G um grupo e H e N subgrupos de G, temos que $G = N \rtimes H$ se, e somente se, $N \trianglelefteq G$ e H é um transversal para N em G. Neste caso, temos $H \backsimeq G/N$.

**Exemplo 1:** Todo grupo G é o produto semidireto de G por $\{e\}$ (produto semidireto trivial). Todo produto direto é um produto semidireto.

**Exemplo 2:** Tomando $\gamma = (1\ 2\ 3), \sigma = (1\ 2) \in S_3$, $H = \langle\sigma\rangle$ e $N = \langle\gamma\rangle$, temos que $S_3 = N \rtimes H$.

**Exemplo 3:** Considere o grupo diedral infinito $D_\infty = \mathbb{Z} \times \{1, -1\}$ cuja operação é dada por $(a, n) * (b, m) = (a + nb, nm)$. Tomando $N = \{(a, 1)|a \in \mathbb{Z}\}$ e $H = \{(0, 1), (0, -1)\}$, temos que $D_\infty = N \rtimes H$.

**Exemplo 4:** Tomando em $S_4$ os elementos $\alpha = (1\ 2\ 3\ 4)$ e $\beta = (2\ 4)$, temos que $\beta\alpha\beta^{-1} = \alpha^{-1}$ e daí $\beta \in N_{S_4}(\langle\alpha\rangle)$. Logo, $K = \langle\alpha, \beta\rangle = \langle\alpha\rangle\langle\beta\rangle$. Além disso, $\langle\alpha\rangle \cap \langle\beta\rangle = \{Id\}$. Desta forma, temos $K = \langle\alpha\rangle \rtimes \langle\beta\rangle$.

Tomando agora $\mu = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ e $\sigma = (2\ 3\ 5)(4\ 7\ 6)$ em $S_7$, temos $\sigma\mu\sigma^{-1} = (1\ 3\ 5\ 7\ 2\ 4\ 6) = \mu^2$ e daí que $H = \langle\mu, \sigma\rangle = \langle\mu\rangle\langle\sigma\rangle$. Além disso, $H = \langle\mu\rangle \rtimes \langle\sigma\rangle$ (não é difícil ver que $\langle\mu\rangle \cap \langle\sigma\rangle = \{Id\}$). Observe que H é um grupo não abeliano de ordem 21.

**Exemplo 5:** Tomando

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} | a \in \mathbb{R}^* \right\}$$

temos que H é subgrupo de $GL_2(\mathbb{R})$. Ademais, $GL_2(\mathbb{R}) = SL_2(\mathbb{R}) \rtimes H$.

Sendo $G = N \rtimes H$ e $h \in H$, definamos

$$\begin{aligned} \varphi_h : N &\longrightarrow N \\ x &\longmapsto \varphi_h(x) = hxh^{-1} \end{aligned}$$

Não é difícil ver que $\varphi_h$ é um automorfismo de N, donde podemos definir

$$\begin{aligned} \varphi : H &\longrightarrow Aut\ N \\ h &\longmapsto \varphi(h) = \varphi_h \end{aligned}$$

Com isso observamos que um produto semidireto de N por H induz um homomorfismo de H em $Aut\ N$. Observe que G é o produto direto interno de N por H se, e somente se, o homomorfismo $\varphi$ definido acima é trivial.

Considere agora G e K grupos (denote por $e_G$ e $e_K$, respectivamente, os seus elementos neutros) e suponha

$$\begin{aligned} \psi : G &\longrightarrow Aut\ K \\ g &\longmapsto \psi_g \end{aligned}$$

um homomorfismo de grupos. Considere o conjunto $K \times G$ e a operação " $*_\psi$ " em $K \times G$ definida por

$$(x, g) *_\psi (y, h) = (x\psi_g(y), gh).$$

Temos que $(K \times G, *_\psi)$ é um grupo, chamado produto semidireto (externo) de K por G com homomorfismo $\psi$. Denotamos este grupo por $K \rtimes_\psi G$. Observe que se $\psi$ é o homomorfismo trivial, então $K \rtimes_\psi G$ é exatamente o produto direto de K por G.

**Exemplo 6:** Consideremos o grupo multiplicativo $C_2 = \{1, -1\}$. Sendo G um grupo abeliano, defina

$$\begin{aligned} \psi : C_2 &\longrightarrow Aut\ G \\ n &\longmapsto \psi_n \end{aligned}$$

onde $\psi_n(g) = g^n$. Temos então que $\psi_1$ é a identidade e $\psi_{-1}$ é a inversão. Claramente, $\psi$ é um homomorfismo e a operação " $*_\psi$ " em $G \rtimes_\psi C_2$ é dada por

$$(a, n) *_\psi (b, m) = (a\psi_n(b), nm) = (ab^n, nm)$$

**Exemplo 7:** Sendo G um grupo considere a aplicação identidade de Aut G. Considerando agora o grupo $G \rtimes_{Id} Aut\ G$, temos que sua operação é dada por

$$(g, \varphi)(g_1, \varphi_1) = (g\varphi(g_1), \varphi \circ \varphi_1).$$

O grupo $G \rtimes_{Id} AutG$ é chamado de holomorfo de G e é dentotado por $Hol\ G$.

**Exemplo 8:** Considere G um grupo e suponha $G = N \rtimes H$. Consideremos

$$\begin{aligned} \varphi : H &\longrightarrow Aut\ N \\ h &\longmapsto \varphi(h) = \varphi_h \end{aligned}$$

Temos $G \backsimeq N \rtimes_\varphi H$

## 4. Conclusões

A teoria de grupos é uma teoria na qual há muito a se explorar, o que o torna efetiva para várias aplicações na ciência de uma forma geral. Diante disso, conhecer razoavelmente tal teoria é de extrema relevância para todo aluno(a) e matemático(a). Para a teoria de grupos, é necessário um grande tempo de estudo e amadurecimento matemático, o que por vezes a torna inacessível para muitos alunos. Produto semidireto é um tópico dentro da teoria de grupos, o qual decidimos abordar, pois muitas vezes não se vê tal assunto na graduação. Daí, a importância da divulgação na comunidade acadêmica de temas que por vezes não vemos. Há também vários tópicos que derivam de produto semidireto e que tem uma relevância muito grande no contexto da álgebra, um exemplo disso é o produto entrelaçado e que pode ser encontrada em (BRANDÃO, 2021).

## Agradecimentos

Meus sinceros agradecimentos ao PET – Matemática e Estatística UFCG pela concessão do auxílio financeiro através do FNDE. Agradeço ao professor Diogo Diniz por me orientar nas minhas Iniciações Científicas, pelas várias correções e ensinamentos. Por último e não menos importante, agradeço ao professor Antônio Brandão pelos ensinamentos de Álgebra.

**Referências**

BRANDÃO, A. P. *Notas de aula de álgebra 1*. Campina Grande - PB: Ainda não publicado, 2021. Citado 2 vezes nas páginas 1 e 3.

FRALEIGH, J. B. *A First Course in Abstract Algebra*. Reading Mas: Addison-Wesley, 1994. Citado na página 1.

GONÇALVES, A. *Introdução à Álgebra*. Rio de Janeiro: IMPA, 1999. Citado na página 1.

SOUZA, J. A. Uma nota sobre a teoria dos grupos: Da teoria de galois à teoria de gauge. *Revista Brasileira de História da Matemática*, v. 12 - n° 24, p. 71–81, 2012. Citado na página 1.

# O TEOREMA DOS QUATRO QUADRADOS

**Ísis Vieira Fernandes**[1] **- isisvf11l@email.com**
**Thyago Santos de Souza**[1] **- thyago@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Este trabalho tem como objetivo explorar, de forma breve, a representatividade de números inteiros positivos como soma de dois, três e quatro quadrados inteiros e, por fim, provar que todo número inteiro positivo pode ser escrito como uma soma de quatro quadrados, conhecido como Teorema dos Quatro Quadrados ou Teorema de Lagrange. Este é oriundo de um Projeto de Iniciação Científica vinculado ao PET-Matemática e Estatística (UFCG). A metodologia utilizada para desenvolvimento deste trabalho foi a pesquisa bibliográfica, principalmente uma apostila publicada em um evento matemático.*
***Palavras-chave****: Soma de Quadrados; Números inteiros; Congruência.*

## 1. Introdução

Bem antes do surgimento das escolas pitagóricas, os babilônicos e os gregos já tinham conhecimento de alguns exemplos de triângulos retângulos de lados inteiros e há evidências que, desde a Mesopotâmia, conseguiam determinar trios pitagóricos por meio de uma fórmula. Um exemplo que gera trios pitagóricos, considerando $a, b, c$ os lados do triângulo é $a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2$ com $m$ e $n$ inteiros e $n < m$ e, assim, podemos notar que a hipotenusa $c$ desse triângulo de lados inteiros é uma soma de quadrados. A partir de então, a ideia de representar um número inteiro como soma de quadrados se torna um problema bem antigo e desde Diofanto de Alexandria é estudado.

Séculos mais tarde, Claude Bachet anuncia que todo inteiro positivo pode ser escrito como soma de quatro quadrados, entretanto não demonstrou esse resultado, somente revelou que era válido para os inteiros 1 até 325, por meio da indução. Após quinze anos, Fermat divulga esse resultado, mas, também não expõe uma prova. Apenas em 1770, Joseph Louis Lagrande (1736-1813) demonstra esse problema, baseado-se, também, nas obras de seu amigo Euler e publicado somente em 1798 no artigo intitulado *Essai sur la theorie des nombres.* Dessa forma, por ser o primeiro a provar esse resultado, o teorema leva seu nome e fica conhecido como Teorema de Lagrange ou Teorema dos Quatro Quadrados.

Portanto, esse trabalho tem como objetivo discutir, de forma sucinta, sobre a representatividade de um número inteiro como soma de quadrados de outros inteiros e apresentar o Teorema dos Quatro Quadrados, não exatamente como a demonstração de Lagrange e Euler, mas de uma forma simples baseado em Neto (2015). Entretanto, antes mostraremos uma breve revisão de conceitos e teoremas fundamentais da Teoria dos Números para o entendimento do trabalho, principalmente a noção de congruência.

## 2. Metodologia

Esse trabalho foi desenvolvido durante um Projeto de Iniciação Científica, em andamento, ligado ao PET-Matemática e Estatística da Universidade Federal de Campina Grande (UFCG), intitulado "Anéis de Polinômios e o 17º Problema de Hilbert". É fruto de uma pesquisa bibliográfica e utilizamos como fonte principal a apostila Neto (2015), onde os resultados essenciais podem ser encontrados. Ademais, para a demonstração do Teorema dos Quatro Quadrados utilizamos assuntos básicos da Teoria do Números.

## 3. Resultado e discussão

Inicialmente, é necessário apresentar alguns resultados e propriedades básicas que serão de fundamental importância para o entendimento dos resultados futuros.

**Definição 3.1.** *Se $m \in \mathbb{Z}$, com $m > 1$, dizemos que dois números $a$ e $b$ são congruentes módulo $m$ se $m \mid a - b$.*

*Nesse caso, representamos da seguinte forma:*

$$a \equiv b \ (mod\ m)$$

Quando não houver a relação de congruência escrevemos $a \not\equiv b \ (mod\ m)$.
A relação de congruência possui algumas propriedades:
Sejam $a, b, c, d \in \mathbb{Z}$, então

1. (Reflexividade) $a \equiv a \ (mod\ m)$;
2. (Simetria) Se $a \equiv b \ (mod\ m)$ então $b \equiv a \ (mod\ m)$;
3. (Transitividade) Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$ então $a \equiv c \ (mod\ m)$;
4. Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $a + b \equiv c + d \ (mod\ m)$ e $ab \equiv cd \ (mod\ m)$;
5. Se $a \equiv b \ (mod\ m)$ e $n \in \mathbb{Z}, n > 1$, então $a^n \equiv b^n \ (mod\ m)$;
6. Se $ab \equiv ac \ (mod\ m)$ e $d = mdc(a, m)$, então $b \equiv c \ \left(mod\ \frac{m}{d}\right)$. Em particular, se $mdc(a, m) = 1$, então $b \equiv c \ (mod\ m)$;
7. Se $mdc(a, m) = 1$ então existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \ (mod\ m)$.

Podemos encontrar as demonstrações de algumas dessas propriedades em Domingues e Iezzi (2018).

**Definição 3.2.** *Um sistema completo de restos módulo $m$ é o conjunto $R = \{r_1, ..., r_m\}$ cujos elementos são incongruentes módulo $m$ e para cada $n \in \mathbb{Z}$ existe um inteiro $r \in R$ tal que $n \equiv r \ (mod\ m)$.*

**Teorema 3.3** (Teorema Fundamental da Aritmética)**.** *Se $n$ é um número inteiro diferente de $-1, 0, 1$, então o valor absoluto de $n$ pode ser escrito como produto de primos de modo único, a menos da ordem em que aparecem os fatores, que não são necessariamente distintos.*

Agora, temos as informações fundamentais para entender sobre a representatividade de um número inteiro positivo como soma de quadrados. Nesse sentido, é natural perguntarmos qual a quantidade mínima de somas de quadrados que todo número inteiro positivo pode ser representado.

Primeiramente, podemos analisar que muitos números não podem ser escritos como soma de dois quadrados. De acordo com a identidade de Brahmagupta-Fibonacci, o produto de dois números que são somas de dois quadrados é uma soma de dois quadrados, ou seja,

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2, \forall\ a, b, c, d \in \mathbb{Z}. \tag{1}$$

Dessa forma, como todo número pode ser escrito como produto de números primos, de acordo com o Teorema 3.3, então se todo primo for soma de dois quadrados, obtemos pela igualdade (1) que o número será uma soma de dois quadrados. Entretanto, isso não ocorre, devido ao seguinte teorema

**Teorema 3.4.** *Um número primo ímpar $p$ pode ser escrito como soma de dois quadrados se, e somemte, se $p \equiv 1 \ (mod\ 4)$.*

Como todo número primo ímpar $p$ é congruente a 1 ou a 3 módulo 4, então todos aqueles primos da forma $p = 4k + 3$, com $k \in \mathbb{Z}$ não são soma de dois quadrados.

**Exemplo 3.5.** *O número 7 não é uma soma de dois quadrados, pois $7 \equiv 3 \ (mod\ 4)$.*

Em seguida, também observamos uma infinidade de inteiros que não podem ser escritos como soma de três quadrados.

**Teorema 3.6.** *Todo inteiro que deixa resto 7 quando dividido por 8 não pode ser escrito como soma de três quadrados.*

**Corolário 3.7.** *Um inteiro da forma $4^m(8k+7)$, com $k \in \mathbb{Z}$, não pode ser escrito como soma de três quadrados.*

As demonstrações dos teoremas anteriores podem ser encontradas em Neto (2015).

**Exemplo 3.8.** *O número 55 não é expresso como soma de três quadrados, pois $55 = 8 \cdot 6 + 7$, isto é,*

$$55 \equiv 7 \ (mod\ 8).$$

Por fim, muitos estudiosos afirmaram que todo número inteiro positivo pode ser escrito como soma de quatro quadrados, como Claude Bachet, Fermat e o inglês Waring, mas nenhum apresentou uma demonstração para o problema. Assim, mostraremos a veracidade dessa afirmação baseados nas demonstrações de Joseph Luis Lagrande com contribuições de Euler chamado de Teorema de Lagrande ou Teorema dos Quatro Quadrados (NETO, 2015). Entretanto, precisamos dos seguintes lemas para demostrá-lo.

**Lema 3.9** (Identidade de Euler, 1748)**.** *Se $m$ e $n$ são somas de quatro quadrados, então o produto $mn$ também é uma soma de quatro quadrados.*

**Demonstração.** Suponhamos que $m = a^2 + b^2 + c^2 + d^2$ e $n = A^2 + B^2 + C^2 + D^2$, então

$$mn = r^2 + s^2 + t^2 + u^2$$

com $r = aA + bB + cC + dD$, $s = aB - bA + cD - dC$, $t = aC - bD - cA + dB$ e $u = aD + bC - cB - dA$, o que completa a demonstração. ∎

**Lema 3.10.** *Seja $p > 2$ um inteiro primo. Então a equação*

$$X^2 + Y^2 + 1 \equiv 0 \ (mod\ p)$$

*admite uma solução $x_0, y_0 \in \mathbb{Z}$, com $0 \leq x_0 \leq \frac{p-1}{2}$ e $0 \leq y_0 \leq \frac{p-1}{2}$.*

**Demonstração.** Considere os conjuntos

$$S_1 = \left\{1 + k^2 \mid k = 0, ..., \frac{p-1}{2}\right\} \text{ e } S_2 = \left\{-l^2 \mid l = 0, ..., \frac{p-1}{2}\right\}$$

Queremos mostrar, inicialmente, que se $1+k_1^2 \neq 1+k_2^2$ com $1+k_1^2, 1+k_2^2 \in S_1$, então $1+k_1^2 \not\equiv 1+k_2^2 \ (mod\ p)$. Provaremos a contrapositiva, suponhamos que $1 + k_1^2 \equiv 1 + k_2^2 \ (mod\ p)$, então $p \mid k_1^2 - k_2^2 = (k_1 - k_2)(k_1 + k_2)$. Como $p$ é primo, temos que $p \mid (k_1 - k_2)$ ou $p \mid (k_1 + k_2)$. Como $0 \leq k_1, k_2 \leq \frac{p-1}{2}$, temos $0 \leq k_1 + k_2 \leq p - 1$. Daí, $k_1 + k_2 \equiv 0 \ (mod\ p)$ implica que $k_2 = -k_1$ e $1 + k_1^2 = 1 + k_2^2$. Já $-\frac{p-1}{2} \leq k_1 - k_2 \leq \frac{p-1}{2}$ e, então, $k_1 - k_2 \equiv 0 \ (mod\ p)$, logo, $k_1 = k_2$ e $1 + k_1^2 = 1 + k_2^2$.

De forma análoga, provamos que se $l_1, l_2 \in S_2$ e $l_1 \neq l_2$, então $-l_1^2 \not\equiv -l_2^2 \ (mod\ p)$. Agora, podemos observar que $S_1$ e $S_2$ são conjuntos disjuntos, visto que $S_1$ possui apenas elementos positivos e $S_2$ têm somente elementos negativos. Portanto,

$$|S_1 \cup S_2| = |S_1| + |S_2| = \tfrac{p-1}{2} + 1 + \tfrac{p-1}{2} + 1 = p + 1 > p.$$

Daí, pelo princípio da casa dos pombos (Dirichlet), existem $1 + x_0^2 \in S_1$ e $-y_0^2 \in S_2$ tais que

$$1 + x_0^2 \equiv -y_0^2 \ (mod\ p)$$

com $0 \leq x_0 \leq \frac{p-1}{2}$ e $0 \leq y_0 \leq \frac{p-1}{2}$. ∎

**Teorema 3.11** (Teorema dos Quatro Quadrados)**.** *Todo número inteiro positivo é soma de quatro quadrados.*

**Demonstração.** Inicialmente, utilizando o Teorema Fundamental da Aritmética (3.3), sabemos que todo número inteiro positivo é primo ou pode ser escrito como produto de primos. Logo, se todo número primo for uma soma de quatro quadrados, então pelo Lema 3.9, todo número inteiro positivo também será. Então, basta mostrar que todo número primo é uma soma de quatro quadrados.

Para $p = 2$, o resultado é verificado, pois temos $p = 1^2 + 1^2 + 0^2 + 0^2$. Vamos considerar $p$ um número ímpar, então, pelo Lema 3.10, existem $a = x_0, b = y_0, c = 1$ e $d = 0$ tais que $p \mid a^2 + b^2 + c^2 + d^2$. Logo,

$$Mp = a^2 + b^2 + c^2 + d^2,$$

com $M \in \mathbb{Z}$. Como $Mp$ é uma soma de quadrados e $p > 1$, então $M \geq 0$. Entretanto, $M \neq 0$, pois supondo o contrário, teríamos $0 = a^2 + b^2 + c^2 + d^2 = x_0^2 + y_0{}^2 + 1^2 + 0^2 \geq 1$, ou seja, um absurdo. Portanto, $M \geq 1$.

Além disso, pelo Lema 3.10,

$$0 \leq x_0 \leq \tfrac{p-1}{2} < \tfrac{p}{2} \text{ e } 0 \leq y_0 \leq \tfrac{p-1}{2} < \tfrac{p}{2}.$$

Daí, temos $Mp = x_0^2 + y_0{}^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2$. Assim, $M < p$ e, portanto, $1 \leq M < p$. Dessa forma, pelo Princípio da Boa Ordenação, podemos escolher um $m$ como o menor inteiro que satisfaz as condições anteriores, isto é, $mp = a^2 + b^2 + c^2 + d^2$. Nesse caso, $m$ é um número ímpar. De fato, se $m$ fosse par $mp = a^2 + b^2 + c^2 + d^2 \equiv 0 \ (mod\ 2)$ e como $(a+b+c+d)^2 = a^2 + b^2 + c^2 + d^2 + 2(ab + ac + ad + bc + bd + cd)$ temos $(a+b+c+d)^2 \equiv a^2 + b^2 + c^2 + d^2 \ (mod\ 2)$ e , assim, $a+b+c+d \equiv 0 \ (mod\ 2)$. Considerando, sem perca de generalidade, que $a + b \equiv 0 \ (mod\ 2)$ e $c + d \equiv 0 \ (mod\ 2)$, logo, $a + b, c + d, a - b, c - d$ seriam pares e então,

$$\frac{m}{2}p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$$

com todos os termos em parênteses sendo números inteiros. Mas, isso contradiz a minimalidade de $m$. Portanto, $m$ é um número ímpar.

Queremos mostrar que $m = 1$. Para isso, suponhamos por contradição que $m \geq 3$. Daí, sejam $a_0, b_0, c_0, d_0 \in \mathbb{Z}$ tais que

$$a_0 \equiv a \ (mod\ m), b_0 \equiv b \ (mod\ m), c_0 \equiv c \ (mod\ m), d_0 \equiv d \ (mod\ m) \text{ e } -\frac{m}{2} < a_0, b_0, c_0, d_0 < \frac{m}{2}. \tag{2}$$

Isso é possível pois $\left\{-\frac{m-1}{2}, ..., \frac{m-1}{2}\right\}$ é um sistema completo de restos módulo $m$.

Logo, temos $a_0^2 + b_0{}^2 + c_0^2 + d_0^2 \equiv a^2 + b^2 + c^2 + d^2 \ (mod\ m)$, então existe $n \in \mathbb{Z}$ e $n > 0$ tal que

$$a_0^2 + b_0{}^2 + c_0^2 + d_0^2 = mn. \tag{3}$$

Caso $n = 0$, teríamos $a_0^2 + b_0{}^2 + c_0^2 + d_0^2 = 0$ e das congruências em (2), obteríamos $a \equiv b \equiv c \equiv d \equiv 0 \ (mod\ m)$. E, assim, existiriam $k_i \in \mathbb{Z}$ com $1 \leq i \leq 4$ tais que $a = k_1 m$, $b = k_2 m$, $c = k_3 m$ e $d = k_4 m$. Daí, $a^2 + b^2 + c^2 + d^2 = m^2(k_1^2 + k_2^2 + k_3 2 + k_4^2)$, isto é, $m^2 \mid a^2 + b^2 + c^2 + d^2$ e implica em $m^2 \mid mp$ e $m \mid p$, o que é uma contradição, pois $p$ é primo e $1 \leq m < p$.

De (2) e (3), temos $mn = a_0^2 + b_0{}^2 + c_0^2 + d_0^2 < 4 \cdot \frac{m^2}{4} = m^2$, então $mn < m^2$, ou seja, $n < m$. Como $mn = a_0^2 + b_0{}^2 + c_0^2 + d_0^2$ e $mp = a^2 + b^2 + c^2 + d^2$, o produto $m^2np = (mn)(mp)$ é uma soma de quadrados. Logo, pelo Lema (3.9), temos

$$m^2np = r^2 + s^2 + t^2 + u^2$$

com $r = aa_0 + bb_0 + cc_0 + dd_0$, $s = ab_0 - ba_0 + cd_0 - dc_0$, $t = ac_0 - bd_0 + ca_0 - db_0$ e $u = ad_0 + bc_0 - cb_0 - da_0$. Utilizando novamente as congruências em (2), podemos concluir que $r$, $s$, $t$, $u$ são divisíveis por $m$. Mostraremos apenas para o caso de $s$. Nesse caso, $s = ab_0 - ba_0 + cd_0 - dc_0 \equiv ab - ba + cd - dc \equiv 0 \ (mod\ m)$. Portanto, podemos dividir $m^2np$ por $m^2$ e obtemos

$$np = \left(\frac{r}{m}\right)^2 + \left(\frac{s}{m}\right)^2 + \left(\frac{t}{m}\right)^2 + \left(\frac{u}{m}\right)^2$$

com $0 < n < m$. Entretanto, $m$ é o menor inteiro tal que $mp$ é soma de quatro quadrados. Logo, isso é uma contradição e, portanto, $m = 1$, ou seja,

$$p = mp = a^2 + b^2 + c^2 + d^2$$

como queríamos demonstrar. ∎

**Exemplo 3.12.** *O número* 7 *é escrito como* $7 = 2^2 + 1^2 + 1^2 + 1^2$.

**Exemplo 3.13.** *O número* 55 *é escrito como* $55 = 5^2 + 5^2 + 2^2 + 1^2$.

O teorema dos Quatro Quadrados também pode ser demonstrado utilizando Álgebra Abstrata. O matemático Adolf Hurwitz, em 1896, apresentou uma demonstração para este teorema utilizando, principalmente, a álgebra $\mathbb{H}$ dos quatérnios. Esta pode ser encontrada em Samuel (1967).

## 4. Conclusões

Portanto, mostramos, no decorrer do trabalho, um dos teoremas clássicos da Teoria dos Números, conhecido como Teorema dos Quatro Quadrados, afirmando que todo número inteiro positivo pode ser representado como soma de quatro quadrados. Entretanto, esse problema pode ser estendido para o caso de polinômios e conseguimos, assim, questionar "todos os polinômios podem ser escritos como soma de quadrados de outros polinômios?"ou "quais as condições para que um polinômio possa ser escrito dessa forma?".

Um dos estudiosos que aprofundaram sobre esse assunto foi o alemão David Hilbert (1862-1943). Em uma conferência no Congresso Internacional de Matemáticos em 1900, ele propôs vinte e três problemas, no qual o décimo sétimo questiona se uma função racional positiva pode ser escrita como soma de quadrados de funções racionais. Depois de 27 anos, o austríaco Emil Artin exibe uma demonstração para essa conjectura. Dessa forma, esses questionamentos podem ser interessantes para o desenvolvimento de trabalhos futuros.

## Agradecimentos

Quero agradecer ao professor orientador e ao Programa de Educação Tutorial PET-Matemática e Estatística (UFCG).

## Referências

DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. São Paulo: Saraiva, 2018. Citado na página 2.

NETO, A. P. *Soma de Quadrados*. 2015. Https://im.ufal.br/evento/bsbm/download/minicurso/quadrados.pdf. Citado 2 vezes nas páginas 1 e 3.

SAMUEL, P. *Théorie Algebébrique des Nombres*. Paris: Hermann, 1967. Citado na página 5.

# UM ESTUDO SOBRE RAÍZES PRIMITIVAS E UMA CARACTERIZAÇÃO DOS NÚMEROS QUE AS POSSUEM

**Pedro Vítor dos Santos Barbosa**[1] **- pedrovt91@gmail.com**
**Josefa Itailma da Rocha**[1] **- itailma@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Proveniente das congruências entre números inteiros, a raíz primitiva de um número é um importante conceito para diversas áreas da matemática, desde o estudo da teoria de grupos até aplicações na criptografia. O estudo que resultou no presente resumo expandido objetivou uma compreensão geral sobre ordens de um número módulo $m$, raízes primitivas e suas principais propriedades. O principal resultado apresentado fornece uma caracterização dos números inteiros que possuem raízes primitivas. Este trabalho foi desenvolvido através de uma iniciação científica vinculada ao PET Matemática e Estatística - UFCG, onde encontros remotos semanais ocorreram para discutir o conteúdo..*
***Palavras-chave****: Congruências; Ordem; Raízes primitivas.*

## 1. Introdução

O conceito de raízes primitivas é de grande importância na Teoria dos Números, já que fornece aplicações na Teoria de Grupos e na criptografia. O presente artigo foi desenvolvido com a intenção de estabelecer resultados que possam auxiliar na categorização dos números inteiros que possuem raízes primitivas.

Para que o conteúdo seja compreendido, é necessário o conhecimento acerca da ordem de um número que é estabelecida através de congruências módulo $m$. Dessa forma, uma vez abordado o conteúdo prévio necessário, pode-se analisar a existência das raízes primitivas de números inteiros que foram primariamente divididos em números primos e compostos.

Ademais, o trabalho objetivou apresentar características gerais acerca das raízes primitivas, além de determinar quais tipos de números se adequavam às condições impostas para a existência de tais raízes.

## 2. Metodologia

O artigo proveniente de revisões bibliográficas foi desenvolvido por meio de uma iniciação científica atrelada ao PET Matemática e Estatística – UFCG com orientação da professora Josefa Itailma da Rocha. Após uma revisão sobre congruências, as definições de ordem e raízes primitivas, assim como suas propriedades mais detalhadas, foram discutidas em reuniões semanais realizadas entre o integrante da iniciação científica e a orientadora através de videochamadas realizadas no *Google meet*.

## 3. Resultado e discussão

Dentre todos os resultados e conceitos que serão abordados acerca das raízes primitivas de um número, devemos iniciar com a definição de ordem, já que esta será necessária para a compreensão do tema principal abordado. Diferente da definição de ordem presente na teoria de grupos, a ordem de um número $a$ módulo $m$, denotada por $ord_m(a)$, é igual ao menor número inteiro $k$ tal que

$$a^k \equiv 1 \pmod{m}.$$

Pelo Teorema de Euler, (VIEIRA, 2015), se $mdc(a,k) = 1$ então

$$a^{\phi(k)} \equiv 1 \pmod{m},$$

onde $\phi(k)$ denota o número de inteiros menores ou iguais a $m$ que são relativamente primos com $m$. Assim, temos $ord_m(a) \leq \phi(m)$.

Quando $ord_m(a) = \phi(m)$ dizemos que $a$ é uma raíz primitiva de $m$.

**Exemplo 1.** Para $a = 2$ e $m = 3$, temos $2^{\phi(3)} = 2^2 = 4 \equiv 1 \pmod 3$. Como $2^1 \equiv 2 \pmod 3$, então $ord_3(2) = 2 = \phi(3)$, assim 2 é uma raiz primitiva de 3. Considerando agora $a = 2$ e $m = 7$, temos $\phi(7) = 6$ e

$$2^1 \equiv 2 \pmod 7, \quad 2^2 \equiv 4 \pmod 7, \quad 2^3 \equiv 1 \pmod 7$$

assim $ord_7(2) = 3 \neq \phi(7)$. Logo 2 não é raíz primitiva de 7.

A seguir enunciaremos algumas propriedades que serão amplamente utilizadas nos principais resultados desse trabalho.

**Teorema 1.** Se $ord_m(a) = k$, então

**(1)** $a^t \equiv 1 \pmod m$ se, e somente se, $k|t$.

**(2)** $a^t \equiv a^h \pmod m$ se, e somente se, $t \equiv h \pmod k$.

**(3)** Os inteiros $a, a^2, ..., a^k$ são incongruentes dois a dois módulo $m$.

**Teorema 2.** Se $ord_m(a) = k$ e $t > 0$, então

$$ord_m(a^t) = \frac{k}{d}$$

em que $d = mdc(t, k)$. Em particular, $ord_m(a^t) = k$, se, e somente se, $mdc(t.k) = 1$.

As demonstrações de tais resultados podem ser encontradas em (VIEIRA, 2015).

**Exemplo 2.** Sabendo que $ord_{10}(7) = 4$, então $ord_{10}(7^k) = 4$ quando $mdc(k, 10) = 1$. Por exemplo, $ord_{10}(7) = ord_{10}(7^3) = ord_{10}(7^7) = ord_{10}(7^9) = 4$.

Os resultados a seguir mostram que as raízes primitivas de um número, quando existem, são incongruentes duas a duas módulo $m$.

**Teorema 3.** Dado $g \in \mathbb{Z}$ tal que $mdc(g, m) = 1$ e sejam $a_1, a_2, ..., a_{\phi(m)}$ os números menores do que $m$ que são relativamente primos com este. Então, $g$ é uma raiz primitiva de $m$, se e somente se,

$$g, g^2, ..., g^{\phi(m)}$$

são congruentes módulo $m$, em alguma ordem, a $a_1, a_2, ..., a_{\phi(m)}$.
**Demonstração:** Supondo inicialmente que $g$ seja uma raiz primitiva de $m$, então sendo $mdc(g, m) = 1$, tem-se $mdc(g^k, m) = 1$, para todo $k = 1, 2, ..., \phi(m)$. Dessa foram, $g^k$ é congruente módulo $m$ a $a_i$ para algum $i = 1, 2, ..., \phi(m)$. Como, pelo item (3) do Teorema 1, os inteiros $g, g^2, ..., g^{\phi(m)}$ são incongruentes entre si módulo $m$, conclui-se que estes são congruentes, em alguma ordem, aos inteiros $a_1, a_2, ..., a_{\phi(m)}$.

Reciprocamente, suponhamos que os números $g, g^2, ..., g^{\phi(m)}$ são congruentes módulo $m$, em alguma ordem, a $a_1, a_2, ..., a_{\phi(m)}$. Dessa forma, digamos $g^k \equiv a_k \pmod m$ para $k = 1, 2, ..., \phi(m)$. Então, caso $g^k \equiv 1 \pmod m$, para algum $k < \phi(m)$, teríamos $g^k \equiv g^{\phi(m)} \pmod m$, o que é uma contradição. Logo, $g$ é uma raíz primitiva de $m$.

□

**Corolário 1:** Se $m$ tem raíz primitiva, então $m$ tem exatamente $\phi(\phi(m))$ raízes primitivas incongruentes duas a duas módulo $m$. Em particular, se $m$ é primo, então $m$ tem exatamente $\phi(m - 1)$ raízes primitivas.

A prova deste resultado pode ser encontrada em (BURTON, 2011).

**Exemplo 3.** Como $ord_{11}(2) = 10 = \phi(11)$, então 2 é uma raíz primitiva de 11. Pelo Corolário 1, temos que 11 possui $\phi(10) = 4$ raízes primitivas incongruentes módulo 11. Pelo Teorema 1, essas raízes pertencem ao conjunto

$$\{2^1, 2^2, ..., 2^{10}\}.$$

Porém, pelo Teorema 2, basta considerar os elementos $2^n$ onde $mdc(n, 10) = 1$, ou seja, $2^1, 2^3, 2^7$ e $2^9$. Como

$$2^1 \equiv 2 \pmod{11}, \quad 2^3 \equiv 8 \pmod{11}, \quad 2^7 \equiv 7 \pmod{11}, \quad 2^9 \equiv 6 \pmod{11},$$

então as raízes primitivas de 11, incongruentes módulo 11, são 2, 6, 7 e 8.

Estas e diversas outras propriedades inerentes às raízes primitivas só poderão ser exploradas em números que apresentem tais raízes, o que não acontece em todos os casos. Por exemplo, caso tomemos $m = 8$, temos

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1.$$

Ou seja, todos os números menores que 8 que são relativamente primos com ele têm ordem igual a 2, logo 8 não possui raíz primitiva.

Sendo assim, vamos caracterizar os números que possuem raízes primitivas. Para isso, dividiremos o estudo em 2 casos: números primos e números compostos.

### 3.1 Raízes Primitivas de Primos

Como visto no Corolário 1, basta que haja uma raíz primitiva de um número inteiro $p$ para que hajam $\phi(p-1)$ raízes primitivas incongruentes módulo $p$ duas a duas. Então basta exibirmos que um número primo contém uma raíz primitiva. Dessa forma, como demonstrado em (MARTINEZ et al., 2018), temos

**Teorema 4.** Se $p$ é um inteiro primo, então existe uma raíz primitiva módulo $p$.

Ademais, mesmo sabendo que todo primo ímpar tem raíz primitiva, ainda não é possível calculá-la de forma rápida e sem cálculos extensos quando tratarmos de números muito grandes. Apesar disso, os resultados apresentados até aqui podem assegurar sua existência e reduzir as etapas para encontrarmos tais raízes.

### 3.2 Raízes Primitivas de Números Compostos

Diferente dos números primos, nem todo número composto tem raíz primitiva(como o 8, que já foi citado). Neste tópico, procuramos caracterizar os números compostos que possuem raízes primitivas.

Para iniciar, vamos citar uma dois resultados técnicos que serão usados nas demonstrações dos principais resultados da seção, estes estão detalhados em (VIEIRA, 2015).

**Lema 1.** Se $k$ é um inteiro ímpar e $k \geq 3$, então $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.

**Lema 2.** Se $p$ é um primo ímpar, então existe uma raíz primitiva $g$ de $p$ tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$. Além disso,

$$g^{\phi(p^{k-1})} = g^{p-1} \not\equiv 1 \pmod{p^k}.$$

Inicialmente vamos caracterizar os números que não têm raízes primitivas.

**Teorema 5.** Os inteiros da forma $2^k$, para $k \geq 3$, não têm raíz primitiva.

**Demonstração:** Os inteiros que são relativamente primos com $2^k$ são todos os números ímpares. Como $\phi(2^k) = 2^{k-1}$, temos

$$\frac{\phi(2^k)}{2} = 2^{k-2}.$$

Logo, pelo Lema 1, se $a$ é ímpar, então

$$a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}.$$

Ou seja, $ord_{2^k}(a)$ é no máximo $\phi(2^k)/2$ que é menor que $\phi(2^k)$, chegando ao resultado de que $2^k$ não possui raiz quando $k \geq 3$.

□

Perceba que a condição imposta de que $k \geq 3$ é necessária, pois encontram-se 1 e 3, respectivamente, como raízes primitivas de 2 e 4.

**Teorema 6.** Sejam $m$ e $n$ inteiros tais que $m > 2, n > 2$ e $mdc(m,n) = 1$, então o inteiro $mn$ não tem raíz primitiva.

**Demonstração:** Escolhendo um inteiro $a$ tal que $mdc(a, mn) = 1$, então $mdc(a,m) = mdc(a,n) = 1$. Considere $d = mdc(\phi(m), \phi(n))$ e $\lambda = mmc(\phi(m), \phi(n))$. Como $m, n > 2$, de acordo com Burton (2011), $\phi(m)$ e $\phi(n)$ são pares e, consequentemente, $d \geq 2$, de modo que

$$\lambda = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}.$$

Pelo Teorema de Euler, $a^{\phi(m)} \equiv 1 \pmod{m}$. Agora elevando ambos os lados da congruência por $\phi(n)/d$, temos

$$a^{\lambda} = a^{\phi(m)\phi(n)/d} \equiv 1 \pmod{m}$$

Analogamente, temos $a^{\lambda} \equiv 1 \pmod{n}$. Então como $mdc(m,n) = 1, m|a^{\lambda} - 1$ e $n|a^{\lambda} - 1$, então $mn|a^{\lambda} - 1$, o que implica em $a^{\lambda} \equiv 1 \pmod{mn}$. Portanto, como $\lambda \leq \phi(mn)/2 < \phi(mn)$, então $ord_{mn}(a)$ é no máximo $\lambda$. Ou seja, $mn$ não tem raíz primitiva.

□

Pelos Teoremas 5 e 6 podemos concluir que um número inteiro $m$ não possui raízes primitivas quando $m$ é divisível por $pq$, em que $p$ e $q$ são primos ímpares distintos ou quando $m$ é da forma $2^{\lambda}p^k$, onde $p$ é um primo ímpar e $\lambda \geq 2$.

Com essas restrições, os números inteiros que são possíveis de possuírem raízes primitivas são os da forma $p^k$ e $2p^k$. Portanto, os próximos resultados serão focados nesses números.

**Teorema 7.** Se $p$ é um primo ímpar e $k \geq 1$, então $p^k$ tem raiz primitiva.

**Demonstração:** Pelo Lema 2, existe uma raíz primitiva $g$ de $p$ tal que

$$g^{\phi(p^{k-1})} \not\equiv 1 \pmod{p^k} \tag{1}$$

Dessa forma, tomemos $r$ a ordem de $g$ módulo $p^k$, então

$$g^r \equiv 1 \pmod{p^k}.$$

Como $mdc(g, p^k) = 1$, então, pelo Teorema de Euler, temos que $g^{\phi(p^k)} \equiv 1 \pmod{p^k}$. Logo, do item (1) do Teorema 1, $r|\phi(p^k) = p^{k-1}(p-1)$. Como $g^r \equiv 1 \pmod{p^k}$ e $p|p^k$, então $g^r \equiv 1 \pmod{p}$. Novamente pelo item (1) do Teorema 1, podemos concluir que $p - 1|r$, uma vez que $ord_p(g) = p - 1$. Portanto,

$$p^{k-1}(p-1) = r\lambda_1 \text{ e } r = (p-1)\lambda_2.$$

Substituindo o valor de $r$ na primeira igualdade, obtemos $p^{k-1} = \lambda_1\lambda_2$, Logo, $\lambda_2 = p^t$ com $1 \leq t \leq k-1$. Por isso, $r = p^t(p-1)$. Se $r \neq p^{k-1}(p-1)$, então $r|p^{k-2}(p-1)$ e do item (1) do Teorema 1, tem-se

$$g^{\phi(p^{k-1})} = g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}.$$

O que contradiz o que foi expresso em (2) e, consequentemente, prova que

$$r = p^{k-1}(p-1) = \phi(p^k).$$

Ou seja, $g$ é uma raiz primitiva de $p^k$.

□

**Corolário 2.** Se $p$ é um primo ímpar, então $2p^k$ tem raiz primitiva quando $k \geq 1$.

**Demonstração:** Seja $g$ uma raíz primitiva de $p^k$ que tem sua existência garantida pelo Teorema 7, podemos supor que $g$ seja ímpar sem perda de generalidade, pois caso contrário, bataria adotar $g + p^k$ que também é raíz primitiva de $p^k$ e tem paridade contrária. Dessa forma, como $2p^k$ é par e $g \nmid p$, então $mdc(g, 2p^k) = 1$ e do Teorema de Euler, temos

$$g^{\phi(2p^k)} \equiv 1 \pmod{2p^k}.$$

Dessa forma, seja $r$ a ordem de $g$ módulo $2p^k$, então $r|\phi(2p^k) = \phi(p^k)$. Porém, se $g^r \equiv 1 \pmod{2p^k}$, então $g^r \equiv 1 \pmod{p^k}$, e como $ord_{p^k}(g) = \phi(p^k)$, temos que $\phi(p^k)|r$. Mas como $r|\phi(p^k)$, segue que $r = \phi(2p^k)$. Portando $g$ é também raiz primitiva de de $2p^k$.

□

Para reunir todos os resultados obtidos até agora, podemos enunciar o seguinte teorema:

**Teorema 8.** Um número inteiro $m > 1$ tem raíz primitiva se, e somente se,

$$m = 2, 4, p^k \text{ou } 2p^k$$

onde $p$ é um primo ímpar.

**Demonstração:** Os Teoremas 5 e 6 já restringiram as possibilidades de números inteiros que possuem raízes primitivas a $m = 2, 4, p^k$ou $2p^k$. Por outro lado, vimos que 1 é raiz primitiva de 2, assim como 3 é raíz primitiva de 4. Por fim, o Teorema 7 e o Corolário 2 atestaram que dado um número $p$ primo ímpar, então $p^k$ e $2p^k$ tem raízes primitivas.

## 4. Conclusões

De forma geral, os objetivos da pesquisa foram alcançados uma vez que os resultados necessários para atestar a existência de raízes primitivas de um número inteiro foram estudados e todos os conceitos utilizados foram definidos.

Para artigos futuros, é viável o estudo de aplicações das raízes primitivas na criptografia, já que, a partir do presente estudo, diversas características já são conhecidas.

## Agradecimentos

Agradeço especialmente ao grupo PET Matemática e Estatística - UFCG e em geral ao PET/FNDE/MEC por proporcionar os recursos que possibilitaram a realização desse projeto.

## Referências

BURTON, D. M. *ELEMENTARY NUMBER THEORY*. 7. ed. New York: The McGraw-Hill, 2011. Citado 2 vezes nas páginas 2 e 4.

MARTINEZ, F. B. et al. *Teoria do Números: um passeio com primos e outros números familiares*. 7. ed. Rio de Janeiro: IMPA, 2018. Citado na página 3.

VIEIRA, V. L. *Um Curso Básico em Teoria dos Números*. Campina Grande: eduepb, 2015. Citado 3 vezes nas páginas 1, 2 e 3.

# Funções diferenciáveis e polinômio de Taylor

**Glêison Correia de Lima**[1] **- gleisoncorreialima14@gmail.com**
**José Lindomberg Possiano Barreiro**[1] **lindomberg@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Neste trabalho estudamos alguns conceitos de análise real, e aplicamos tais conceitos para estudar o polinômio de Taylor. Como manipular polinômio é mais simples do que certas funções, então veremos que o polinômio de Taylor é importante para a aproximar uma dada função em uma vizinhança de um ponto.*
***Palavras-chave****: Aproximação; Função; Polinômio de Taylor*

## 1. Introdução

A utilização da matemática pelas primeiras civilizações pode ser justificada por ser ela uma ciência que facilite o cotidiano das pessoas. Uma das maneiras que a matemática contribui para o nosso dia a dia é a criação de fórmulas para auxiliar em cálculos de algumas funções que são complicadas de serem resolvidas. Neste trabalho, comentaremos sobre uma dessas ferramentas, que é o polinômio de Taylor, este tem o intuito de auxiliar na aproximação de uma função $f$ que seja derivável em um ponto. E de acordo com Bartle e Sherbert (2000) podemos ver o polinômio de Taylor com uma extensão do Teorema do Valor Médio, pois este relaciona os valores de uma função e sua primeira derivada, e o polinômio de Taylor fornece uma relação entre os valores de uma função e suas derivadas de ordem superior. As demonstrações dos resultados desta seção serão omitidos, caso contrário, estenderia o trabalho, mas as mesma são encontradas em Bartle e Sherbert (2000).

**Definição 1.** *Seja $I \subseteq \mathbb{R}$ um intervalo, $f : I \to \mathbb{R}$ e um ponto $c \in I$. Dizemos que um número real $L$ é a derivada de $f$ em $c$, quando dado $\epsilon > 0$, existe $\delta(\epsilon) > 0$ tal que $x \in I$ satisfaz $0 < |x - c| < \delta(\epsilon)$, então*

$$\left| \frac{f(x) - f(c)}{x - c} - L \right| < \epsilon.$$

Em outras palavras, a derivada de $f$ em $c$ é dado como

$$\lim_{x \to c} \frac{f(x) - f(c)}{x - c}$$

se este limite existe.

**Teorema 1.** *Se $f : I \to \mathbb{R}$ é derivável em $c \in I$, então $f$ é continua em $c$.*

**Teorema 2** (Teorema de Carathéodory)**.** *Seja a função $f$ definida em um intervalo $I$, que contém o ponto $c$. Então, $f$ é diferenciável em $c$ se, e somente se, existe uma função $\varphi$ em $I$, tal que é contínua em $c$, e satisfaz*

$$f(x) - f(c) = \varphi(x)(x - c)$$

*Neste caso, temos que $\varphi(c) = f'(c)$.*

**Teorema 3** (Regra da cadeia)**.** *Sejam $f : I \to \mathbb{R}$ e $g : J \to \mathbb{R}$ duas funções reais definidas em intervalos $I$ e $J$, respectivamente, tais que $f(I) \subseteq J$ e $f(c)$ é um ponto interior de $J$. Suponhamos que $f$ seja derivável em $c$ e $g$ derivável em $f(c)$. Então, a função composta $g \circ f : I \to \mathbb{R}$ é derivável em $c$ e vale a fórmula:*

$$(g \circ f)'(c) = g'(f(c))f'(c).$$

**Teorema 4** (Rolle). *Seja $f : I \to \mathbb{R}$ uma função contínua definida em um intervalo $I = [a, b]$. Suponha que $f$ seja derivável no intervalo aberto $(a, b)$, e que $f(a) = f(b) = 0$. Então, $c \in (a, b)$ tal que $f^{'}(c) = 0$.*

**Teorema 5** (Teorema do valor médio). *Seja $f : I \to \mathbb{R}$ uma função contínua definida em um intervalo fechado $I = [a, b]$. Suponha que $f$ seja derivável no intervalo aberto $(a, b)$. Então, existe $c \in (a, b)$ tal que*

$$f(b) - f(a) = f^{'}(c)(b - a).$$

## 2. Metodologia

### 2.1 Polinômio de Taylor

Segundo Boye e Merzbach (1974), Brook Taylor (1683-1731), graduado de Cambridge, entusiástico admirador de Newton e secretário da Royal Society, publicou em 1715 em seu *Metrus incrementarum directa et inversa* uma técnica em que seu nome hoje é lebrado exclusivamente em conexão, que é o polinômio de Taylor. Além disso, o polinômio de Taylor já era conhecida já por James Gregory (1638-1675) muita antes de Taylor publicar em seu livro, e em essência também conhecida por Bernoulli (1700-1782), porém Taylor não sabia.

Seja $f : I \to \mathbb{R}$ uma função definida em um intervalo fechado $I = [a, b]$. Na seção 1 foi definida a função derivada, $f^{'} : I \to \mathbb{R}$, da função $f$. Essa derivada é denotada por derivada primeira. A derivada segunda de $f$ é a derivada da derivada primeira e usamos o símbolo $f^{''}$, em que a derivada segunda é também uma função $f^{''} : I \to \mathbb{R}$. Assim, por diante, definimos a derivada terceira $f^{'''}$, a derivada quarta $f^4$, ..., a derivada $n$-ésima $f^n$.

Se uma função $f$ tem n-ésima derivada em um ponto $x_0$, não é difícel construir um polinômio de grau $n$ tal que $P_n(x_0) = f(x_0)$ e $P_n^{(k)} = f^k(x_0)$ para $k = 1, 2, ..., n$.

De fato, paro o polinômio de Taylor de grau 2, consideremos um polinômio do segundo grau da forma:

$$P_2(x) = A + B(x - x_0) + C(x - x_0)^2$$

com $A, B$ e $C$ coeficientes reais. Temos $P_2(x_0) = A$ e, com isto, $f(x_0) = P_2(x_0) = A$

Além disso, $P_2^{'} = B + 2C(x - x_0)$ e $P_2^{''} = 2C$, assim

$$f^{'}(x_0) = P_2^{'} = B + 2C(x_0 - x_0) = B$$

$$f^{'}(x_0) = P_2^{''}(x_0) = 2C \Longrightarrow C = \frac{f^{''}(x_0)}{2}$$

Portanto, o polinômio de grau 2 de $f$ em volta de $x_0$ é dado por:

$$P_2(x) = f(x_0) + f'(x_0)(x - x_0) + \frac{f^{''}(x_0)}{2}(x - x_0)^2.$$

Esse procedimento para obter um polinômio de grau 2 pode ser generalizado para obtermos um polinômio de ordem $n$, com $n \in \mathbb{N}$, que aproxime o valores de $f$ em ponto $x$ em uma vizinhança de $x_0$. Assim, obtemos o polinômio:

$$P_n(x) = f(x_0) + f^{'}(x_0)(x - x_0) + \frac{f^{''}(x_0)}{2!}(x - x_0)^2 + ... + \frac{f^n(x_0)}{n!}(x - x_0)$$

que chamamos de *n-ésimo polinômio de Taylor.*

É natural esperar que esse polinômio forneça uma aproximação razoável próximo de $x_0$, mas para avaliar a qualidade da aproximação, é necessário ter informações sobre o erro cometido ao aproximar os valores, $f(x)$ por $P(x)$, ou ainda, $R_n = f - P_n$. O próximo resultado abaixo fornece essa informação.

**Teorema 6** (Fórmula de Taylor com resto de Lagrange)**.** *Seja $f : I \to \mathbb{R}$ uma função definida em um intervalo $I = [a, b]$. Suponha que as derivadas $f', ..., f^n$ existam e sejam continuas em $[a, b]$, e que $f^{n+1}$ exista em $(a, b)$. Se $x_0 \in I$, então para cada $x \in I$, existe um ponto $c$ entre $x$ e $x_0$ tal que*

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + ... + \frac{f^n(x_0)}{n!}(x - x_0) + R_{n+1}(x)$$

*onde*

$$R_{n+1}(x) = \frac{f^{n+1}(c)}{(n+1)!}(x - x_0)^{n+1}$$

*Demonstração.* Considerando o intervalo $J = [x_0, x]$. Definimos a função $F$ em $J$ como

$$F(t) = f(x) - f(t) - f'(t)(x - t) - \frac{f''(t)}{2!}(x - t)^2 - ... - \frac{f^{n+1}(c)}{(n+1)!}(x - t)^{n+1}$$

para $t \in J$. Então, com um cálculo simples encontramos que

$$F'(t) = -\frac{(x - t)^n}{n!} f^{n+1}(t).$$

Agora definimos $G$ em $J$ como

$$G(t) = F(t) - \left(\frac{x - t}{x - x_0}\right)^{n+1} F(x_0)$$

para $t \in J$, então $G(x_0) = G(x) = 0$.
Desta forma, aplicaremos o teorema de Rolle, assim existe $c$ entre $x$ e $x_0$ tal que

$$0 = G(c) = F'(c) + (n + 1)\frac{(x - c)^c}{(x - x_0)^{n+1}} F(x_0)$$

Logo, obtemos

$$F(x_0) = \frac{-1}{n+1}\frac{(x - x_0)^{n+1}}{(x - c)^n} F'(c) = \frac{1}{n+1}\frac{(x - x_0)^{n+1}}{(x - c)^n}\frac{(x - c)^n}{n!} f^{n+1}(c) = \frac{f^{n+1}(c)}{(n+1)!}(x - x_0)^{n+1}.$$

□

Mostra-se que $\lim_{x \to x_0} \frac{R_n(x)}{x - {x_0}^n} = 0$ , ou seja, quando $x$ tente a $x_0$, o erro $R_n(x)$ tente a zero mais rapidamente que $(x - x_0)^n$.

## 3. Resultado e discussão

Vamos determinar o polinômio de Taylor de ordem 2 em torno de $x_0$ da função $f(x) = \sqrt[3]{1 + x}$, com $x > -1$.

Notamos inicialmente que $f'(x) = \frac{1}{3}(1 + x)^{\frac{-2}{3}}$ e $f''(x) = -\frac{2}{9}(1 + x)^{-\frac{5}{3}}$, assim $f'(0) = \frac{1}{3}$ e $f''(0) = -\frac{2}{9}$.

Logo, obtemos:

$$f(x) = P_2(x) + R_2(x) = 1 + \frac{1}{3}x - \frac{1}{9}x^2 + R_2(x)$$

Assim, $R_2(x) = \frac{f'''(c)}{3!}x^3 = \frac{5}{81}(1 + c)^{\frac{-8}{3}}x^3$ para $c$ entre 0 e $x$.

No caso de escolhermos $x = 0,3$, temos que $P_2(0,3) = 1,09$ para $\sqrt[3]{1,3}$.

Como $c > 0$, temos que $(1+c)^{-\frac{8}{3}} < 1$ e o erro estimado é:

$$R_2(0,3) = \frac{5}{81}(1+c)^{-\frac{8}{3}}(0,3)^3 \leq \frac{5}{81}(0,3)^3 = \frac{1}{600} < 0,17.10^{-2}$$

Portanto, com essa estimativa garantimos a precisão de duas casas decimais.

Vemos no gráfico abaixo a função $f$ e o polinômio $P_2$ o quanto estão próximo na vizinhança de $x = 0,3$.

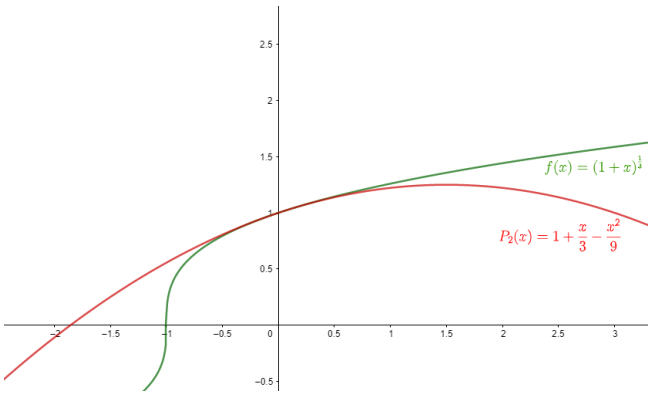



Figura 1: Elaborada pelo autor

## 4. Conclusões

A utilização do polinômio de Taylor para a aproximação de uma função derivável em um ponto é algo técnico e de fácil compreensão. Além disso, o método é bastante poderoso e há diversas aplicações utilizando o mesmo. Como também, é possível estimar o erro da aproximação o que torna bastante eficiente.

## Agradecimentos

Agradeço ao PET Matemática e Estatística, pois possibilitou a minha participação neste projeto de pesquisa. Agradeço ao FNDE pelo suporte financeiro.

## Referências

BARTLE, R. G.; SHERBERT, D. R. *Introduction to Real Analysis*. New York: John Wiley e Sons, 2000. 157-183 p. Citado na página 1.

BOYE, C. B.; MERZBACH, U. C. *História da Matemática*. São Paulo: E. Blucher, 1974. 306-307 p. Citado na página 2.

# UNIDADE DO ANEL DOS INTEIROS QUADRÁTICOS

**Matheus Pereira Amorim**[1] **- pereiramatheus742@gmail.com**
**Josefa Itailma da Rocha**[1] **- itailma@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Dizemos que um elemento $\alpha \in \mathbb{C}$ é dito um inteiro quadrático se $\alpha$ é um inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$, ou equivalente, se $T(\alpha) = 2a$ e $N(\alpha) = \alpha\overline{\alpha}$ são números inteiros. Ao conjunto dos inteiros quadráticos chamamos de anel dos inteiros quadráticos e denotamos por $O(m)$. Os elementos $u \in O(m)$ tal que existe $u' \in O(m)$ com $uu' = 1$ são denominados de unidade, e são esses que buscaremos estudar. Este trabalho tem como objetivo estudar o anel $O(m)$ e caracterizar o subanel $O(m)^*$ formado pela as unidades de $O(m)$. O estudo está separa no caso real ($m > 0$) e no complexo ($m < 0$). Para $m < 0$ apontamos precisamente quais são as unidades de $O(m)$. Já no real, existe uma única unidade $u_0$ tal que toda unidade é da forma $\pm u_0^n$ com $n \in \mathbb{Z}$.*
***Palavras-chave****: Inteiros; Quadráticos; Unidade*

## 1. Introdução

Um número complexo $\alpha$ é dito *algébrico* se existe um polinômio não nulo $f(x) \in \mathbb{Q}[x]$ que anula $\alpha$, ou seja, tal que $f(\alpha) = 0$. Se $\alpha \in \mathbb{C}$ é algébrico, dizemos que $\mathbb{Q}[\alpha] = \{f(\alpha), f(x) \in \mathbb{Q}[x]\}$ é um corpo algébrico. Em particular, se $\alpha \notin \mathbb{Q}$ anula um polinômio de grau 2, então $\mathbb{Q}[\alpha]$ é chamado de *corpo quadrático* e $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$, onde $\alpha = \dfrac{a + b\sqrt{m}}{c}$, em $a, b, c \in \mathbb{Z}$ e $m$ livre de quadrados.

Dado $\alpha \in \mathbb{C}$, dizemos que $\alpha$ é um inteiro algébrico se o mesmo anula um polinômio mônico em $\mathbb{Z}[x]$. Denotaremos por $O(m)$ o conjunto dos inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$. O conjunto $O(m)$ é um subanel de $\mathbb{Q}[\sqrt{m}]$ chamado de anel dos inteiros quadráticos.

Usando a norma e o traço dos elementos de $\mathbb{Q}[\sqrt{m}]$ podemos caracterizar os elementos de $O(m)$. Vamos também apresentar uma forma de escrever os seus elementos, o que sera usado para mostrar que $O(m)$ é de fato um anel. O objetivo principal desse trabalho é descrever o conjunto $O(m)^*$ formado pela as unidades de $O(m)$.

## 2. Metodologia

Este trabalho foi feito a partir de iniciação científica desenvolvido junto ao PET- Matemática e Estatística, bolsa fornecida pelo CNPq. Foi desenvolvido por meio de encontros semanais remotos, via Google Meet, pra discussão do referencial predefinido com a orientadora.

## 3. Resultado e discussão

Durante esse trabalho estaremos considerando o subconjunto dos números complexos dado por $\mathbb{Q}[\sqrt{m}] = \{a+b\sqrt{m} | a, b \in \mathbb{Q}\}$ onde $m$ é um inteiro livre de quadrados, isto é, que não é divisíveis por quadrados diferente de 1. Em vista disso, vamos introduzir alguns conceitos sobre $\mathbb{Q}[\sqrt{m}]$ que serão necessários para o desenvolvimento de nosso trabalho.

**Definição 1.** *Dado um elemento $\alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ chamamos de:*

**(i)** *Conjugado de $\alpha$, denotado por $\overline{\alpha}$, ao elemento $\overline{\alpha} = a - b\sqrt{m}$.*

**(ii)** *Traço de $\alpha$, denotado por $T(\alpha) = \alpha + \overline{\alpha} = 2a$.*

**(iii)** *Norma de $\alpha$, denotado por $N(\alpha) = \alpha\overline{\alpha} = a^2 - mb^2$.*

Observe que $T(\alpha)$ e $N(\alpha)$ são elementos de $\mathbb{Q}$. O próximo resultado apresenta algumas propriedades importantes de $T(\alpha)$ e $N(\alpha)$.

**Proposição 2.** *Dados $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$ temos:*

**(a)** $\overline{\alpha} + \overline{\beta} = \overline{\alpha+\beta}$, $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$ *e* $\overline{\alpha} = \alpha$ *se, e somente se,* $\alpha \in \mathbb{Q}$.

**(b)** $T(\alpha+\beta) = T(\alpha) + T(\beta)$.

**(c)** $N(\alpha\beta) = N(\alpha)N(\beta)$ *e* $N(\alpha) = 0$ *se, e somente se,* $\alpha = 0$.

**(d)** *Se* $\alpha \neq 0$, $\alpha^{-1} = \overline{\alpha}[N(\alpha)]^{-1}$.

**Demonstração:** Sejam $\alpha = a + b\sqrt{m}$ e $\beta = c + d\sqrt{m}$, então

**(a)** $\overline{\alpha} + \overline{\beta} = a - b\sqrt{m} + c - d\sqrt{m} = (a+c) - (b+d)\sqrt{m} = \overline{\alpha+\beta}$.

$\overline{\alpha}\overline{\beta} = (a - b\sqrt{m})(c - d\sqrt{m}) = ac + bdm + (ad - bc)\sqrt{m}$, note que $\alpha\beta = ac + bdm + (ad+bc)\sqrt{m}$ então $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$.

Se $\overline{\alpha} = \alpha$ então $2b\sqrt{m} = 0 \Rightarrow b = 0$ e $\alpha \in \mathbb{Q}$. Por outro lado, se $\alpha \in \mathbb{Q}$ então $\alpha = a$ com $a \in \mathbb{Q}$ daí $\overline{\alpha} = a$, isto é, $\alpha = \overline{\alpha}$.

**(b)** $T(\alpha+\beta) = \alpha + \beta + \overline{\alpha+\beta} = \alpha + \overline{\alpha} + \beta + \overline{\beta} = T(\alpha) + T(\beta)$.

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

Se $N(\alpha) = 0$, então $\alpha\overline{\alpha} = 0$ daí $\alpha = 0$ ou $\overline{\alpha} = 0$. Se o primeiro acontecer está provado, já se $\overline{\alpha} = 0$ então $a = b\sqrt{m}$ e $\alpha \in \mathbb{Q} \Rightarrow \alpha = \overline{\alpha} = 0$. A recíproca é direta, pois se $\alpha = 0$ então $N(\alpha) = \alpha\overline{\alpha} = 0$.

**(d)** $\alpha^{-1} = \alpha^{-1}\overline{\alpha}^{-1}\overline{\alpha} = \overline{\alpha}(\alpha^{-1}\overline{\alpha}^{-1}) = \overline{\alpha}[N(\alpha)]^{-1}$.

□

**Proposição 3.** *Seja $\alpha \in \mathbb{Q}[\sqrt{m}]$. Então $\alpha$ é raíz do polinômio*

$$f_\alpha(x) = x^2 - T(\alpha)x + N(\alpha) \in \mathbb{Q}[x].$$

**Demonstração:** Seja $\alpha = a + b\sqrt{m}$, então:

$$\alpha^2 = (a + b\sqrt{m})(a + b\sqrt{m}) = a^2 + 2ab\sqrt{m} + bm^2.$$

Assim,

$$f_\alpha(\alpha) = a^2 + 2ab\sqrt{m} + b^2m - 2a(a + b\sqrt{m}) + a^2 - b^2m = 2a^2 + 2ab\sqrt{m} - 2a^2 - 2ab\sqrt{m} = 0$$

□

Pelo resultado acima, podemos caracterizar os elementos de $O(m)$ através de $T(\alpha)$ e $N(\alpha)$.

**Proposição 4.** *Seja $\alpha \in \mathbb{Q}[\sqrt{m}]$. Então $\alpha \in O(m)$ se, e somente se, $T(\alpha)$ e $N(\alpha)$ são inteiros*

Com essa caracterização podemos mostrar as seguintes propriedades de $O(m)$.

**Proposição 5.** **(a)** *$\alpha \in O(m)$ se, se somente se, $\overline{\alpha} \in O(m)$.*

**(b)** $\mathbb{Z} = O(m) \cap \mathbb{Q}$.

**Demonstração:** Seja $\alpha = a + b\sqrt{m} \in O(m)$, assim

**(a)** Note que $T(\overline{\alpha}) = \overline{\alpha} + \overline{\overline{\alpha}} = \overline{\alpha} + \alpha = T(\alpha)$ e $N(\overline{\alpha}) = \overline{\alpha}\overline{\overline{\alpha}} = \overline{\alpha}\alpha = N(\alpha)$. Assim $\overline{\alpha} \in O(m)$ se, e somente se, $\alpha \in O(m)$.

**(b)** A inclusão $\mathbb{Z} \subset O(m) \cap \mathbb{Q}$ é imediata. Por outro lado, seja $\alpha \in O(m) \cap \mathbb{Q}$ então $\alpha = a \in \mathbb{Q}$ e $N(\alpha) = a^2 \in \mathbb{Z}$, consequentemente $\alpha = a \in \mathbb{Z}$. Provamos assim a igualdade.

□

A partir de agora, vamos apresentar uma caracterização dos elementos de $O(m)$ a fim de mostrar que $O(m)$ é um subanel de $\mathbb{Q}(\sqrt{m})$. É fácil ver que $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} | a, b \in \mathbb{Z}\} \subset O(m)$, porém a inclusão contrária não é válida. De fato, seja $m = -3$ e $\xi = \dfrac{1+\sqrt{-3}}{2}$, vemos que $T(\xi) = 1$ e $N(\xi) = 1$ assim $\xi \in O(-3)$, mas $\xi \notin \mathbb{Z}[\sqrt{-3}]$.

Segundo ((ANDRADE, 2013)), se $m \not\equiv 1(mod4)$ então vale $O(m) = \mathbb{Z}[\sqrt{m}]$. Porém, se $m \equiv 1(mod4)$ os elemento de $O(m)$ são escritos como $\dfrac{a+b\sqrt{m}}{2}$, onde $a, b \in \mathbb{Z}$ e tem mesma paridade de modo geral, podemos escrever

$$O(m) = \{a + b\xi, \quad a, b \in \mathbb{Z}\}$$

onde

$$\xi = \begin{cases} \sqrt{m}, & \text{se } m \not\equiv 1(mod4) \\ \dfrac{1+\sqrt{m}}{2}, & \text{se } m \equiv 1(mod4) \end{cases}$$

**Corolário 6.** *$O(m)$ é um subanel de $\mathbb{Q}(\sqrt{m})$*

**Demonstração:** Sejam $\alpha = a + b\xi, \beta = c + d\xi \in O(m)$ com $\xi = \sqrt{m}$ se $m \not\equiv 1(mod4)$ ou $\xi = \dfrac{1+\sqrt{m}}{2}$ se $m \equiv 1(mod4)$. Então $\alpha + \beta = (a + c) + (b + d)\xi \in O(m)$ e $-\alpha = -a + (-b)\xi \in O(m)$, ou seja, $O(m)$ é fechado pra soma. Além disso, $\alpha\beta = (a + b\xi)(c + d\xi) = (ac + bd\xi^2) + (ad + bc)\xi$. Porém note que $\xi^2 = m$ se $m \not\equiv 1(mod4)$ e $\xi^2 = \dfrac{1+m-2\sqrt{m}}{4}$, ou seja, ambos os casos $\xi^2 \in O(m)$. Portanto, $\alpha\beta \in O(m)$ e $O(m)$ é fechado a multiplicação. Logo $O(m)$ é subanel de $\mathbb{Q}[\sqrt{m}]$.

□

Dados $\alpha, \beta \in O(m) - \{0\}$ dizemos que $\alpha$ divide $\beta$, e denotamos $\alpha \mid \beta$, se existe $\gamma \in O(m)$ tal que $\beta = \alpha\gamma$. Os elementos $\alpha$ e $\beta$ serão chamados associados se $\alpha \mid \beta$ e $\beta \mid \alpha$. Os elementos que são associados ao 1 são chamados unidades de $O(m)$. Vemos que $u \in O(m)$ é associado 1 quando existe $u' \in O(m)$ tal que $uu' = 1$, isto é, $u^{-1} = u' \in O(m)$. Vamos denotar por $O(m)^*$ ao conjunto das unidades de $O(m)$.

É fácil ver que o produto de duas unidades é ainda uma unidade e $O(m)^*$ é um subgrupo do grupo multiplicativo de $\mathbb{Q}[\sqrt{m}]$.

**Observação 7.** *Note que se $u \in O(m)^*$ então $N(u) = \pm 1$. De fato se $u$ é unidade então existe $u' \in O(m)$ tal que $uu' = 1$ daí $N(u)N(u') = 1$ como $N(u) \in \mathbb{Z}$, então $N(u) = N(u') = 1$ ou $N(u) = N(u') = -1$. Logo $N(u) = \pm 1$.*

Vamos classificar as unidades conforme o valor de sua norma. Dizemos que $u \in O(m)^*$ é *própria* se $N(u) = 1$ e que é *imprópria* se $N(u) = -1$. Como $N(-1) = N(1) = 1$ então 1 e $-1$ são unidades próprias e assim unidades próprias sempre existem. Já unidades impróprias podem não ocorrer, em particular se $m < 0$ não existem unidades impróprias.

**Exemplo 8.** *Tomando $m = 2$, temos que $N(1+\sqrt{2}) = 1^2 - 2 = -1$, assim $1+\sqrt{2}$ é uma unidade imprópria de $O(2)$. Por outro lado, tomando $m = 3$ vemos que $O(3)$ não tem unidades impróprias, isto porque $\alpha = a + b\sqrt{m}$ é uma unidade imprópria se, e somente se, $N(\alpha) = -1$, assim deveríamos ter $a^2 - 3b^2 = -1$ o que resulta em $a^2 \equiv -1(mod3)$, o que não poderia acontecer.*

A seguir vamos caracterizar as unidades de $O(m)$ com $m < 0$.

**Teorema 9.** **(a)** *Se $m = -1$, as unidades de $O(m)$ são $\pm 1$ e $\pm\sqrt{-1}$.*

**(b)** *Se $m = -3$, as unidades de $O(m)$ são $\pm 1$, $\pm\xi$ e $\pm\xi^2$, onde $\xi = \dfrac{1+\sqrt{m}}{2}$.*

**(c)** *Se $m < 0$ e $m \neq -1, -3$, as únicas unidades de $O(m) = \pm 1$.*

**Demonstração:** Seja $u = a + b\xi \in O(m)^*$

**(a)** Neste caso, $\xi = \sqrt{-1}$ (pois $m \not\equiv 1(mod4)$) e $N(u) = a^2 + b^2 = 1$. Portanto temos $a = \pm 1$ e $b = 0$ ou $a = 0$ e $b = \pm 1$, ou seja, $u = \pm 1$ ou $u = \pm\sqrt{-1}$.

**(b)** Como $-3 \equiv 1(mod4)$, então $u = a + b\left(\frac{1+\sqrt{-3}}{2}\right)$. Assim, $N(u) = ((2a+b)^2 + 3b^2)/4 = \pm 1$, daí $(2a+b)^2 + 3b^2 = 4$. Se $b \neq 0$, então $b = \pm 1$. Para $b = 1$, temos $a = 0$ ou $a = -1$ o que implica em $u = \xi^2$ ou $\xi$. Para $b = -1$, temos $a = 0$ ou $a = 1$ e daí $u = -\xi^2$ ou $u = -\xi$. Se $b = 0$, então $a = \pm 1$ o que implica em $u = \pm 1$.

**(c)** Para $m < -3$, se $b \neq 0$ então $N(u) = a^2 + 3b^2 > 1$, o que não pode acontecer pois $N(u) = \pm 1$. Logo as unidades de $O(m)$ são $\pm 1$, já que $a^2 = \pm 1$ daí $a = \pm 1$. Se $m = -2$ , $m \not\equiv 1(mod4)$ e assim a unidade $u$ é do tipo $u = a + b\sqrt{-2}$, portanto $N(u) = a^2 + 2b^2 \geq 2$ se $b \neq 0$. Analogamente, concluímos que $u = \pm 1$ e provamos o resultado.

□

O estudo das unidades para $m > 0$ é um pouco mais complicado e será tratado a partir de agora. Neste caso, vamos mostrar que se $m > 1$ então o conjunto $O(m)^*$ é infinito e que existe $u_0 \in O(m)^*$, chamada de *unidade fundamental*, tal que

$$O(m)^* = \{\pm u_0^n, n \in \mathbb{Z}\}$$

Seja $\alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ com $a > 0$ e $b > 0$, uma unidade de $O(m)$. Se $m \not\equiv 1(mod4)$, então $a, b \in \mathbb{Z}$ e claramente $\alpha > 1$. Para $m \equiv 1(mod4)$, $\alpha$ pode ser escrito da forma $\frac{c+d\sqrt{m}}{2}$, com $c, d \in \mathbb{Z}$ e de mesma paridade. Observe que o menor valor $m$ nesse caso será $m = 5$. Como $\sqrt{5} > 2$, então $\alpha > 1$. Em todo caso, temos que se $\alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ com $a > 0$ e $b > 0$ então $\alpha > 1$.

Considere $\alpha = a + b\sqrt{m} \in O(m)^*$, pela Proposição 2 e pela Observação 7, temos $\alpha^{-1} = \pm\overline{\alpha}$. Assim se $\alpha \neq \pm 1$, então $a \neq 0$ e $b \neq 0$ e $\pm a \pm b\sqrt{m}$ também são unidades. Podemos então garantir que no conjunto $\{\pm\alpha, \pm\overline{\alpha}\}$ temos uma unidade maior do que 1.

Por fim se $\alpha \in O(m)^*$, com $\alpha > 1$, então $O(m)^*$ é infinito, pois $\alpha^n \longrightarrow \infty$ quando $n \longrightarrow \infty$. Assim, para garantir $O(m)^*$ é infinito, basta mostrar que $O(m)^* \neq \{\pm 1\}$. Para isso, vamos precisar do seguinte resultado técnico cuja a demonstração pode encontrada em (BRUMATTI; ENGLER, 2001).

**Lema 10.** *Seja $\alpha > 0$ um número irracional. Existem infinitos pares de inteiros $(x, y)$ tais que $y \neq 0$ e $||x/y - \alpha|| < 1/y^2$.*

**Teorema 11.** *Existem inteiros $x$ e $y$, com $y \neq 0$, tais que $x^2 - my^2 = 1$. Ou equivalentemente $O(m)^* \cap \mathbb{Z}[\sqrt{m}] \neq \{\pm 1\}$.*

**Demonstração:** Vamos começar por encontrar $k \in \mathbb{Z}$ tal que $N(\alpha) = k$ para um número infinito de elementos $\alpha \in \mathbb{Z}[\sqrt{m}]$. Sejam $x, y \in \mathbb{Z}$ com $y \neq 0$ e

$$||x/y - \sqrt{m}|| < 1/y^2. \tag{1}$$

Temos então

$$\begin{aligned} ||N(x + y\sqrt{m})|| = ||x^2 - my^2|| = ||x - y\sqrt{m}||||x + y\sqrt{m}|| = \\ y^2||x/y - \sqrt{m}||||x/y + \sqrt{m}|| < ||x/y + \sqrt{m}|| = ||x/y - \sqrt{m} + 2\sqrt{m}|| \leq \\ ||x/y - \sqrt{m}|| + 2\sqrt{m} < 1/y^2 + 2\sqrt{m} \\ \Rightarrow ||N(x + y\sqrt{m})|| \leq 1 + 2\sqrt{m} \end{aligned}$$

Portanto $N(x+y\sqrt{m})$ é um inteiro entre $-1-2\sqrt{m}$ e $1+2\sqrt{m}$. Como, pelo Lema 10, existem infinitos pares $(x, y)$ que satisfazem (1) acima, temos que existe $x \in \mathbb{Z}$, $k \neq 0$, com $||k|| < 1+2\sqrt{m}$ e tal que $N_k = \{\alpha \in \mathbb{Z} | N(\alpha) = k\}$ é um conjunto infinito.

Sejam $\alpha, \beta \in N_k$ tais que $\alpha \neq \pm\beta$. Então $\alpha\beta^{-1} \neq \pm 1$ e $N(\alpha\beta^{-1}) = N(\alpha)/N(\beta) = k/k = 1$. Assim, se encontramos $\alpha, \beta$ nessas condições e tais que $\alpha\beta^{-1} \in \mathbb{Z}[\sqrt{m}]$ o teorema está demonstrado. Observemos que $\alpha\beta^{-1} = \alpha\overline{\beta}/N(\beta) = \alpha\overline{\beta}/k$. Estamos portanto procurando $\alpha, \beta \in N_k$ tais que $\alpha\overline{\beta} \in k\mathbb{Z}[\sqrt{m}]$ e $\alpha \neq \pm\beta$. Seja $S_k = \{(\overline{x}, \overline{y}) \in \mathbb{Z}_{||k||} \times \mathbb{Z}_{||k||} | \alpha = x + y\sqrt{m} \in N_k\}$, onde $\mathbb{Z}_{||k||}$ é o conjunto das classes dos inteiros módulo $||k||$. Como $S_k$ é finito e $N_k$ é infinito, existem $\alpha = x+y\sqrt{m}$ e $\beta = x'+y'\sqrt{m}$ em $N_k$ tais que $\alpha \neq \pm\beta$ e $(\overline{x}, \overline{y}) = (\overline{x'}, \overline{y'})$. Isto é, $k$ divide $x - x'$ e $y - y'$. Portanto $\alpha - \beta = k\gamma$ com $\gamma \in \mathbb{Z}[\sqrt{m}]$. Assim $k\gamma\overline{\beta} = (\alpha - \beta)\overline{\beta} = \alpha\overline{\beta} - k$. Logo $\alpha\overline{\beta} = k(\gamma\overline{\beta} + 1) \in k\mathbb{Z}[\sqrt{m}]$ e ainda $\alpha \neq \pm\beta$, como queríamos.

□

Pelo Teorema 11, e pelo observado anteriormente, podemos concluir que $O(m)^*$ é infinito, para $m > 1$. O próximo resultado garante a existência da unidade fundamental:

**Teorema 12.** *Existe uma única unidade $u_0 > 1$ em $O(m)$ tal que toda unidade de $O(m)$ é da forma $\pm u_0^n$ com $n \in \mathbb{Z}$.*

**Demonstração:** Usando o Teorema 11 podemos obter uma unidade $w = x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ com $w > 1$. Mais ainda existe apenas um número finito de unidades no intervalo $(1, w]$. Tome então $u_0 = \text{mínimo}\{u | u \in O(m)^* \ \ e \ \ u > 1\}$ e seja $v$ uma unidade de $O(m)$ com $v > 1$. Como $u_0^k \to \infty$ com $k \in \mathbb{N}$, temos que existe $n$ tal que $0 < u_0^{1-n} < v \leq u_0^n$ e pela escolha de $u_0, n \geq 1$. Assim $0 < 1 < vu_0^1 \leq u_0$. Novamente, pela escolha de $u_0$ temos $vu_0^{1-n} = u_0$ ou $v = u_0^n$. Seja agora $v \neq \pm 1$ uma unidade qualquer de $O(m)$. Como um dos elementos de $\{\pm v, \pm v^{-1}\}$ é maior do que 1, então $v = \pm u_0^n$, com $n \in \mathbb{Z}$. A unicidade de $u_0$ decorre de sua escolha. □

## 4. Conclusões

Concluímos que podemos determinar as unidades de $O(m)$ trabalhando em casos. Para $m < 0$, se $m = -1$ as unidades de $O(m)$ são $\pm 1$ e $\pm\sqrt{-1}$, se $m = -3$ as unidades são $\pm 1$, $\pm\xi$ e $\pm\xi^2$, onde $\xi = \dfrac{1+\sqrt{m}}{2}$, e se $m < 0$ (diferente dos valores anteriores) as unidades são $\pm 1$. Por outro lado, se $m > 0$ existe uma única unidade $u_0 > 1$ tal que toda unidade de $O(m)$ é da forma $\pm u_0^n$ com $n \in \mathbb{Z}$ e, neste caso, $O(m)^*$ é infinito. Logo conseguimos atingir os objetivos desejados.

## Agradecimentos

Gostaria de agradecer o CNPq por disponibilizar a bolsa, o PET - Matemática e Estatística por ajudar a desenvolver esse trabalho e a minha orientadora por me ajudar e guiar nesse estudo.

## Referências

ANDRADE, J. F. S. *Tópicos especiais em álgebra*. [S.l.]: Sociedade Brasileira de Matemática, 2013. Citado na página 3.

BRUMATTI, P.; ENGLER, A. J. Inteiros quadráticos e o grupo de classes. *23º COLÓQUIO BRASILEIRO DE MATEMÁTICA. Rio de Janeiro: IMPA*, 2001. Citado na página 4.

# O Problema Isoperimétrico

**Maria Débora de Oliveira Silva**[1] **- debora.oliveira@estudante.ufcg.edu.br**
**Alânnio Barbosa Nobrega**[1] **- alannio@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil. Parcialmente financiado pelo MEC/FNDE/PET.

***Resumo:*** *Qual curva engloba a maior área dentre todas as outras de mesmo perímetro? Essa é uma pergunta que os gregos no século II a.C. já imaginavam a resposta, mas que não conseguiram prová-la nos padrões atuais de rigor matemático. O Problema Isoperimétrico envolve a história da Rainha Dido de Cartago que teve de enfrentar um problema parecido para fundar seu próprio reino após um conflito familiar. Nesse trabalho, com auxílio de bibliografias clássicas sobre o assunto, exibiremos a demonstração apresentada pelo Matemático alemão Adolf Hurwitz (1859-1919) utilizando séries de Fourier.*
***Palavras-chave****: Problema de Dido; Desigualdade Isoperimétrica; Séries de Fourier.*

## 1. Introdução

Conta o poeta romano Públio Virgílio Maronis (70-19 a.C.) em um dos seus poemas épicos latinos intitulado de *Eneida* (MARONIS, 2005), a história da Rainha fenícia Dido que foi obrigada a fugir de sua cidade natal para o norte da África, após seu marido ser assassinato por seu irmão, o Rei Pigmalião de Tiro. Lá, desembarcando com todos os objetos de valor que conseguira reunir, Dido fez um acordo com um dos chefes locais: em troca de sua fortuna, ela receberia o máximo de terra que pudesse cercar com a pele de um único boi para viver com seus súditos. Os nativos ao escutar sua proposta, imaginaram que a Rainha conseguiria contornar apenas alguns metros de terra e não pensaram duas vezes antes de fechar o negócio. Entretanto, Dido decidiu cortar aquele couro em tiras extremamente finas, que quando amarradas, formaram um grande laço. A rainha muito esperta, viu que entre todas as outras curvas de mesmo perímetro, o círculo seria o que englobaria a maior área, e assim foi feito. Seus súditos construíram um enorme semicírculo que com a costa litorânea do local, acabou contornando uma área muito maior do que todos esperavam, fundando assim a cidade de Cartago.

Intuitivamente, A Rainha Dido recorreu à *Desigualdade Isoperimétrica*, ou ainda, *Problema Isoperimétrico*, que anos mais tarde, segundo Blåsjö (2005), Karl Weierstrass (1815-1897) daria as primeiras provas rigorosas da veracidade da desigualdade usando métodos embasados em Análise e Cálculo. No entanto, vale salientar que o matemático Pappus Alexandrinus (290-350) publicou no século IV provas puramente geométricas da validade da Desigualdade Isoperimétrica atribuídas ao Matemático Zenodorus (200-140 a.C), mas que não são aceitas, pois não se encaixam no padrão matemático atual (SIEGEL, 2003). Já existem outras diversas maneiras de resolver esse Problema, e nesse trabalho, apresentaremos a do matemático alemão Adolf Hurwitz (1859-1919) utilizando séries de Fourier.

## 2. Metodologia

Esse estudo foi realizado na atividade de Iniciação Científica do Grupo PET-Matemática-UFCG, sob a orientação do Professor Doutor Alânnio Barbosa Nobrega. A partir de bibliografias clássicas de *Análise e Séries de Fourier* como o livro *Análise de Fourier e Equações Diferenciais Parciais*, do Professor Djairo Guedes de Figueiredo, e o livro *Fourier Analysis and its Applications*, do Professor Gerald Budge Folland, foi feito uma pesquisa acerca da utilização das séries de Fourier que resultou no presente trabalho.

## 3. Resultado e discussão

Em 1811, o Matemático francês Jean-Baptiste Joseph Fourier (1768-1830) apresentava ao *Institut de France* o trabalho *Théorie Analytique de la Chaleur* (Teoria Matemática de Condução do Calor), no qual afirmava que toda função de uma variável podia ser expressa em uma série de senos e cossenos. Anos mais tarde, Lejeune Dirichlet(1805-1859) mostrou que nem toda função de uma variável pode ser representada de tal forma

e estabeleceu alguns critérios (BURTON, 2011). Atualmente, essas Séries Trigonométricas conhecidas como séries de Fourier desempenham um papel muito importante em diversas áreas da Física Moderna e abaixo, conforme Figueiredo (1977), exibiremos a definição.

**Definição 1.** *(Série de Fourier.) Dada uma função $f : \mathbb{R} \to \mathbb{R}$ periódica de período $2L$, integrável e absolutamente integrável, chamamos de Série de Fourier de $f$ a expressão*

$$\frac{1}{2}a_0 + \sum_{n=1}^{\infty}(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L}),$$

*onde os coeficientes de Fourier são dados por*

$$a_n = \frac{1}{L}\int_{-L}^{L} f(x)\cos\frac{n\pi x}{L}dx, \quad n \geq 0$$

*e*

$$b_n = \frac{1}{L}\int_{-L}^{L} f(x)\sin\frac{n\pi x}{L}dx, \quad n \geq 1.$$

### 3.1 Resultados Preliminares

Agora, apresentaremos alguns resultados importantes para a resolução do Problema Isoperimétrico utilizando séries de Fourier. As devidas demonstrações serão ocultadas por exigirem resultados avançados de *Análise de Fourier*, mas o detalhamento desses resultados podem ser encontrados em Figueiredo (1977).

**Teorema 1.** *(Teorema de Fourier.) Seja $f : \mathbb{R} \to \mathbb{R}$ uma função seccionalmente diferenciável e de período $2L$. Então a Série de Fourier da função $f$, converge, em cada ponto $a$, para $\frac{1}{2}[f(a+0) + f(a-0)]$, onde*

$$f(a+0) = \lim_{x\to a^+} f(x) \quad e \quad f(a-0) = \lim_{x\to a^-} f(x).$$

**Definição 2.** *Uma função $f : \mathbb{R} \to \mathbb{R}$ é de quadrado integrável quando $f$ e $|f|^2$ são integráveis.*

**Teorema 2.** *(Identidade de Parseval.) Dada uma função $f : \mathbb{R} \to \mathbb{R}$ periódica de período $2L$ e de quadrado integrável, então*

$$\frac{1}{2}{a_0}^2 + \sum_{n=1}^{\infty}({a_n}^2 + {b_n}^2) = \frac{1}{L}\int_{-L}^{L}|f(x)|^2 dx,$$

*onde $a_n$ e $b_n$ são os coeficientes de Fourier de $f$.*

**Corolário 2.1.** *Se $f$ e $g$ são funções periódicas de período $2L$ e seccionalmente contínuas, então*

$$\frac{1}{L}\int_{-L}^{L} f(x)g(x)dx = \frac{1}{2}a_0\alpha_0 + \sum_{n=1}^{\infty}(a_n\alpha_n + b_n\beta_n),$$

*onde $a_n$ e $b_n$ são os coeficientes de Fourier de $f$ e $\alpha_n$ e $\beta_n$ os de $g$.*

**Lema 3.** *Seja $C$ uma curva fechada simples e seccionalmente diferenciável, de comprimento $L$, com parametrização $\gamma = (x(t), y(t))$, $t \in [a, b]$. Então o comprimento $L$ e a área da curva $C$ são dados por*

$$L = \int_a^b \sqrt{x'(t)^2 + y'(t)^2}dt \quad e \quad A = \int_a^b x(t)y'(t)dt.$$

*Ademais, é possível parametrizar a curva $C$ pelo comprimento de arco $s$, definido por*

$$s(t) = \int_a^t \sqrt{x'(\tau)^2 + y'(\tau)^2}dt, \quad t \in [a, b],$$

*obtendo*

$$x'_*(s)^2 + y'_*(s)^2 = 1, \quad s \in [0, L],$$

*onde* $x_*(s(t)) = x(t)$ *e* $y_*(s(t)) = y(t)$.

### 3.2 Problema Isoperimétrico

**Teorema 4.** *(Desigualdade Isoperimétrica.) A área $A$ englobada por qualquer curva simples plana fechada retificável $C$, de comprimento $L$, satisfaz a desigualdade $A \leq \frac{L^2}{4\pi}$. Além disso, a igualdade ocorre, se e só se, $C$ for um círculo.*

*Demonstração.* Seja $C$ uma curva simples fechada retificável de comprimento $L$ que engloba uma área $A$. Sem perda de generalidade, como toda curva retificável pode ser aproximada por uma curva seccionalmente diferenciável (FIGUEIREDO, 1977), tomemos $C$ desta forma. Agora, consideremos $\gamma_1 = (x_1(s), y_1(s))$ a parametrização de $C$ usando o comprimento de arco $s$. Assim, pelo Lema 3, temos

$$x'_1(s)^2 + y'_1(s)^2 = 1, \quad s \in [0, L]. \tag{1}$$

Fazendo $t = s/L$, obtemos a parametrização $\gamma = (x(t), y(t))$ com $t \in [0, 1]$, onde $x(t) = x_1(tL)$ e $y(t) = y_1(tL)$. Logo,

$$x'(t) = x'_1(tL) \cdot L = x'_1(s) \cdot L \quad e \quad y'(t) = y'_1(tL) \cdot L = y'_1(s) \cdot L.$$

Dado isso, segue

$$x'(t)^2 + y'(t)^2 = x'_1(s)^2 \cdot L^2 + y'_1(s)^2 \cdot L^2 = (x'_1(s)^2 + y'_1(s)^2) \cdot L^2,$$

ou ainda, por (1),

$$x'(t)^2 + y'(t)^2 = L^2. \tag{2}$$

Como as funções $x(t)$ e $y(t)$ são periódicas de período 1 e seccionalmente diferenciáveis, pelo Teorema 1, podemos expressá-las pelas séries

$$x(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos 2n\pi t + b_n \sin 2n\pi t) \tag{3}$$

e

$$y(t) = \frac{\alpha_0}{2} + \sum_{n=1}^{\infty}(\alpha_n \cos 2n\pi t + \beta_n \sin 2n\pi t). \tag{4}$$

Daí, derivando as expressões (3) e (4), temos

$$x'(t) \sim \sum_{n=1}^{\infty} 2n\pi(-a_n \sin 2n\pi t + b_n \cos 2n\pi t)$$

e

$$y'(t) \sim \sum_{n=1}^{\infty} 2n\pi(-\alpha_n \sin 2n\pi t + \beta_n \cos 2n\pi t).$$

Visto que $x'(t)$ e $y'(t)$ são periódicas de período $2L = 1$ e de quadrado integrável, utilizando o Teorema 2, obtemos

$$\sum_{n=1}^{\infty}[(-2n\pi a_n)^2 + (2n\pi b_n)^2] = \frac{1}{1/2}\int_{-1/2}^{1/2} |x'(t)|^2 dt$$

e

$$\sum_{n=1}^{\infty}[(-2n\pi\alpha_n)^2+(2n\pi\beta_n)^2]=\frac{1}{1/2}\int_{-1/2}^{1/2}|y'(t)|^2dt.$$

.

Ademais, simplificando as expressões acima, chegamos a

$$\int_0^1|x'(t)|^2dt=\sum_{n=1}^{\infty}2n^2\pi^2({a_n}^2+{b_n}^2)$$

e

$$\int_0^1|y'(t)|^2dt=\sum_{n=1}^{\infty}2n^2\pi^2({\alpha_n}^2+{\beta_n}^2).$$

Agora, observe que

$$\int_0^1|y'(t)|^2dt+\int_0^1|x'(t)|^2dt=2\pi^2\sum_{n=1}^{\infty}n^2({a_n}^2+{b_n}^2+{\alpha_n}^2+{\beta_n}^2),$$

portanto, de (2), segue

$$\int_0^1|y'(t)|^2dt+\int_0^1|x'(t)|^2dt=\int_0^1L^2dt\Rightarrow$$

$$L^2=2\pi^2\sum_{n=1}^{\infty}n^2({a_n}^2+{b_n}^2+{\alpha_n}^2+{\beta_n}^2). \tag{5}$$

Por outro lado, do Corolário 2.1, tiramos que

$$2\int_0^1x(t)y'(t)dt=\sum_{n=1}^{\infty}(a_n[2n\pi\beta_n]-b_n[2n\pi\alpha_n])=\sum_{n=1}^{\infty}2n\pi(a_n\beta_n-b_n\alpha_n),$$

e assim, pelo Lema 3, chegamos a

$$A=\sum_{n=1}^{\infty}n\pi(a_n\beta_n-b_n\alpha_n). \tag{6}$$

Como consequência de (5) e (6), obtemos

$$\begin{aligned}L^2-4\pi A&=2\pi^2\sum_{n=1}^{\infty}n^2({a_n}^2+{b_n}^2+{\alpha_n}^2+{\beta_n}^2)-\sum_{n=1}^{\infty}4n\pi^2(a_n\beta_n-b_n\alpha_n)\\&=2\pi^2\sum_{n=1}^{\infty}[(n^2{a_n}^2-2na_n\beta_n+\beta_n^2)+(n^2{b_n}^2+2nb_n\alpha_n+\alpha_n^2)+\alpha_n^2(n^2-1)+\beta_n^2(n^2-1)]\\&=2\pi^2\sum_{n=1}^{\infty}[(na_n-\beta_n)^2+(nb_n+\alpha_n)^2+(n^2-1)(\alpha_n^2+\beta_n^2)].\end{aligned}$$

O que implica na Desigualdade Isoperimétrica procurada $L^2-4\pi A\geq 0$.

Veja que quando $L^2-4\pi A=0$, teremos a curva C com a área máxima do perímetro dado. Agora, basta mostrarmos que, para este caso, C é um círculo. Note que os valores que satisfazem a igualdade são exatamente

$$a_1=\beta_1, b_1=-\alpha_1\quad e\quad \alpha_n=\beta_n=a_n=b_n=0\quad para\quad n>1.$$

Daí, voltando nas expressões (3) e (4), chegamos em

$$x(t) = \frac{a_0}{2} + a_1 \cos 2\pi t - \alpha_1 \sin 2\pi t \Leftrightarrow x(t) = \frac{a_0}{2} + \langle (a_1, -\alpha_1), (\cos 2\pi t, \sin 2\pi t) \rangle$$

e

$$y(t) = \frac{\alpha_0}{2} + \alpha_1 \cos 2\pi t + a_1 \sin 2\pi t \Leftrightarrow y(t) = \frac{\alpha_0}{2} + \langle (\alpha_1, a_1), (\cos 2\pi t, \sin 2\pi t) \rangle.$$

Da Álgebra Vetorial, sabemos que dados dois vetores $u$ e $v$, o produto escalar entre eles é dado por $\langle u, v \rangle = |u||v|cos(\theta)$, onde $\theta$ é o ângulo formado entre eles (WINTERLE, 2014). Assim,

$$x(\theta) = \frac{a_0}{2} + \sqrt{a_1^2 + \alpha_1^2} \cos\theta \quad e \quad y(\theta) = \frac{\alpha_0}{2} + \sqrt{a_1^2 + \alpha_1^2} \sin\theta,$$

pois chamando $c = \cos 2\pi t$ e $s = \sin 2\pi t$, temos

$$\langle (a_1, -\alpha_1), (c, s) \rangle^2 = (a_1^2 + \alpha_1^2)(c^2 + s^2) \cos^2\theta = a_1^2 c^2 - 2a_1 c\alpha_1 s + \alpha_1^2 s^2$$

e

$$\langle (\alpha_1, a_1), (c, s) \rangle^2 = (a_1^2 + \alpha_1^2)(c^2 + s^2) \cos^2\theta_* = \alpha_1^2 c^2 + 2a_1 c\alpha_1 s + a_1^2 s^2,$$

daí, somando as equações acima obtemos

$$\langle (a_1^2 + \alpha_1^2)(c^2 + s^2)(\cos^2\theta + \cos^2\theta_*) \rangle = (a_1^2 + \alpha_1^2)(c^2 + s^2) \Rightarrow \cos^2\theta + \cos^2\theta_* = 1 \Rightarrow \cos\theta_* = \sin\theta.$$

Portanto, concluímos que a curva $C$ é um círculo de centro $(\frac{a_0}{2}, \frac{\alpha_0}{2})$ e raio $\sqrt{a_1^2 + \alpha_1^2}$, o que encerra a demonstração. □

## 4. Conclusões

Nesse texto, pudemos verificar a aplicabilidade das séries de Fourier, uma ferramenta matemática que desempenha um papel excepcional para o estudo das equações diferenciais parciais, através do clássico Problema Isoperimétrico. Tal Problema instigou a curiosidade de matemáticos desde a Grécia antiga, e a sua abordagem utilizando séries de Fourier apresentada pelo alemão Adolf Hurwitz (1859-1919) em 1902 foi exibida neste trabalho.

## Agradecimentos

O presente trabalho foi realizado com apoio parcial do FNDE, Fundo Nacional de Desenvolvimento da Educação, através do Programa de Educação Tutorial (PET).

## Referências

BLåSJö, V. The evolution of the isoperimetric problem. *The American Mathematical Monthly*, v. 112, p. 526–566, 2005. Citado na página 1.

BURTON, D. M. *The History of Mathematics: an introduction*. New York: McGraw-Hill, 2011. 610-614 p. Citado na página 2.

FIGUEIREDO, D. G. *Análise de Fourier e Equações Diferenciais Parciais*. Rio de Janeiro: IMPA, 1977. 96-99 p. Citado 2 vezes nas páginas 2 e 3.

MARONIS, P. V. *Eneida*. eBooksBrasil, 2005. 14-44 p. Disponível em: ⟨https://www.ebooksbrasil.org/adobeebook/eneida.pdf⟩. Citado na página 1.

SIEGEL, A. A historical review of the isoperimetric theorem in 2-d, and its place in elementary plane geometry. *Courant Institute of Mathematical Sciences New York University*, p. 1–11, 2003. Citado na página 1.

WINTERLE, P. *Vetores e Geometria Analítica*. São Paulo: Pearson, 2014. 49-62 p. Citado na página 5.

# ATUAÇÕES DO PIBID DURANTE A PANDEMIA DO COVID-19 NA PREPARAÇÃO DE ALUNOS PARA O ENEM

**Diego Rawalyson Marques de Souza[1] - diego.rawalyson@estudante.ufcg.edu.br**
**Eliel Marques Brito[1] - eliel.marques@estudante.ufcg.edu.br**
**Joelson Joventino Santos[1] - joelson.joventino@estudante.ufcg.edu.br**
**Lívia Tito Ribeiro[1] - livia.tito@estudante.ufcg.edu.br**
**Rafael Alves Silva[1] - rafael.alves@estudante.ufcg.edu.br**
**Sérgio Victor de Melo Soares[1] - sergiovictor.svms@gmail.com**
**Wander Ícaro Guedes Medeiros[1] - wander.icaro@estudante.ufcg.edu.br**
**Wilton dos Santos[1] - wilton.santos@estudante.ufcg.edu.br**
**Jacqueline Félix de Brito Diniz[1] - jacqueline@mat.ufcg.edu.br**
**Larise Carmélia de França Silva[2] - larise.silva1@professor.pb.gov.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil
[2]Escola Cidadã Integral Itan Pereira - Campina Grande, PB, Brasil

***Resumo:*** *Neste relato será apresentado um projeto realizado pelo PIBID matemática da UFCG - Campus I, nas turmas do 3° ano do ensino médio da Escola Cidadã Integral Professor Itan Pereira, com o objetivo de preparar os estudantes para a prova de matemática do ENEM 2021. Essas atividades foram oferecidas durante o segundo semestre de 2021 e de forma remota devido à pandemia do Covid-19. O relato sugere que apesar do caráter emergencial forçado pela pandemia, as aulas foram bastante satisfatórias em termos de aprendizagem e participação dos alunos. Essas aulas remotas foram realizadas com uso de diversos recursos digitais. Além de descrever as dinâmicas usadas nas aulas, apresentaremos os princípios adotados e apontaremos acertos e dificuldades na implementação. Ao mesmo tempo, sugerimos características que poderão ser incorporadas nos próximos anos, inclusive com o retorno das atividades presenciais.*
***Palavras-chave****: Ensino remoto; Matemática; PIBID; ENEM.*

## 1. Introdução

Há quase dois anos o mundo inteiro vem sendo drasticamente afetado pela disseminação e todas as graves consequências do Novo Coronavírus. Nesta nova realidade fomos todos forçados a readequar as nossas rotinas. O que antes era normal já não era mais possível. O mundo mudou e juntamente com essas mudanças as salas de aula também se transformaram. O que antes era um quadro branco hoje é a tela de um computador ou celular, as canetas viraram teclas e os alunos se tornaram ícones definidos por letras ou fotos de personagens, a nossa interação nas aulas se prendeu a *chats*, mensagens curtas e a pouca participação dos alunos nas aulas.

A mudança também ocorreu nos horários, além de termos as aulas seriamente afetadas em seus formatos também tivemos sérias mudanças na carga horária. Nas escolas integrais do estado da Paraíba foi comum a prática de que as aulas ocorressem pela manhã e o turno da tarde fosse reservado para que os alunos realizassem as atividades previstas. Nesse formato, na ECI Professor Itan Pereira, o número de aulas de matemática no ensino médio que antes era de seis aulas por semana passou a ser de apenas duas aulas por semana. Mediante essa situação os professores viram a necessidade de se reinventar, buscando ao máximo capacitar os seus alunos que irão realizar o ENEM (Exame Nacional do Ensino Médio), que neste ano de 2021 acontecerá em Novembro, e posteriormente os demais vestibulares e concursos que desejarem.

Durante a pandemia, o Programa Institucional de Bolsa de Iniciação à Docência (PIBID), que é uma proposta de valorização dos futuros docentes durante seu processo de formação, e que tem como objetivo o aperfeiçoamento da formação de professores para a educação básica e a melhoria da qualidade da educação pública brasileira, buscou meios para ajudar os alunos do ECI Professor Itan Pereira nesse momento adverso enfrentado.

Através das oportunidades proporcionadas pelo projeto para a criação e participação em experiências me-

todológicas, tecnológicas e práticas docentes de caráter inovador e interdisciplinar, esses estudantes podem buscar a superação de problemas identificados no processo de ensino público. Os estudantes são inseridos no universo das escolas públicas desde o início da sua formação acadêmica para que desenvolvam atividades didático-pedagógicas sob orientação de um docente da licenciatura e de um professor da escola. Com isso, o programa está incentivando a formação de professores em nível superior para a educação básica e contribui para a valorização do magistério.

Devido a proximidade das provas e o pouco tempo para trabalhar com esses alunos, o PIBID/Matemática - UFCG preparou um material de apoio que foi apresentado aos alunos em aulas elaboradas e ministradas pelos próprios bolsistas do projeto. Trazendo assuntos específicos para cada aula e utilizando somente questões contextualizadas. O intuito do projeto era apresentar os assuntos mais abordados nas edições anteriores do ENEM. Estas aulas preparatórias foram realizadas dentro e fora do horário previsto de aulas da escola, sendo pela manhã no horário já previsto para as aulas de matemática e a tarde como aulas extras.

## 2. Metodologia

Desde 2020 o ensino remoto emergencial entrou em cena, em virtude da pandemia causada pelo Covid-19. Visando dar continuidade às aulas, por meio do ensino remoto, as escolas precisaram se adaptar às tecnologias digitais. Surgindo assim um verdadeiro mundo de novas possibilidades para professores e estudantes.

Uma das possibilidades foi a utilização de jogos e aplicativos *(google meet, google forms, geogebra, kahoot!*, entre outros) que se tornaram ferramentas de extrema importância no processo de ensino e aprendizagem. O projeto relatado neste trabalho teve como objetivo auxiliar os alunos na fixação de alguns conteúdos matemáticos necessários para realização do ENEM. As ações foram desenvolvidas pelos pibidianos com os alunos dos 3º anos do ensino médio da ECI Professor Itan Pereira.

Inicialmente, como forma de preparação para essas ações, foram realizadas revisões bibliográficas de conteúdos matemáticos e pesquisas relacionadas à funcionalidade de algumas plataformas digitais. O desenvolvimento das ações foi feito por meio de aulas voltadas para resolução de questões de provas de anos anteriores do ENEM. Os encontros foram ministrados por duplas ou trios de integrantes do PIBID e realizados através do aplicativo *Google Meet* utilizando apresentação de slides. Em alguns momentos, visando despertar maior interesse dos alunos, foi utilizado o recurso lúdico da plataforma *on-line* de quiz *Kahoot!*.

O planejamento das aulas foi realizado pelos pibidianos com supervisão e orientação da professora supervisora da ECI Itan Pereira e da professora coordenadora de área do PIBID. Os assuntos foram selecionados pela professora da turma (supervisora), levando em consideração as dificuldades dos alunos nas aulas. Dentre os conteúdos escolhidos destacamos: Estatística, Geometria Plana e Geometria Espacial.

Ao final do projeto foi enviado aos alunos um formulário qualitativo do *Google Forms* a respeito do aproveitamento do conteúdo das aulas visando o *feedback* dos alunos para possíveis melhorias na realização de futuras ações semelhantes.

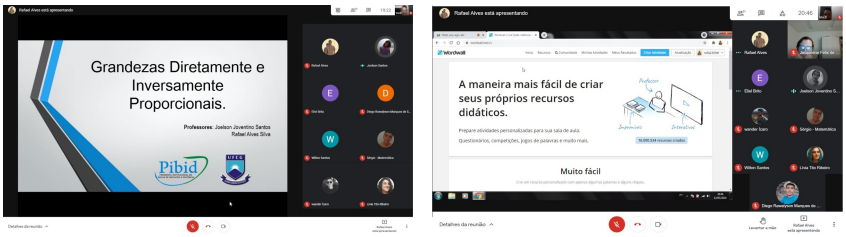
## 3. Resultado e discussão

A intenção do PIBID é unir as universidades públicas da educação básica e as salas de aula , a favor da melhoria do ensino nas escolas públicas. Pensando nisso, o trabalho intitulado "Acesso Domiciliar à Internet e Ensino Remoto Durante a Pandemia" (NASCIMENTO et al., 2020), nos levou a refletir sobre o grande número de estudantes das escolas públicas que não tem acesso às tecnologias da informação, e deste modo foram os mais afetados ao longo dos últimos dois anos em relação à aprendizagem escolar, e de que maneira poderíamos contribuir para diminuir essas perdas na formação desses estudantes.

Essa experiência, assim como todas as atividades oferecidas pelo PIBID, foi prontamente adaptada para o ensino remoto emergencial, e esse relato buscou evidenciar como isso foi realizado.

**1ª Etapa:**

Num primeiro momento, em reuniões realizadas com os integrantes do PIBID, decidimos realizar entre o grupo revisões bibliográficas de conteúdos matemáticos [Figura 1 (a)] com o propósito de trabalhar esses conteúdos com os alunos, além disse, pesquisamos a funcionalidade de algumas plataformas digitais [Figura 1 (b)], a fim de facilitar o processo de ensino e aprendizagem no momento pandêmico que estávamos vivendo.




(a) (b)

Figura 1: (a) Revisão bibliográfica e (b) Estudo da plataforma *Wordwall* (Fonte: registro dos autores)

| Conteúdos revisados | Aplicativos pesquisados | |
|---|---|---|
| Função | *Geoboard* | *Scratch* |
| Frações | *GeoGebra* | *Padlet* |
| Grandezas diretamente e inversamente proporcionais | Torre de Hanói (virtual) | *Wordwall* |
| Polígonos regulares inscritos na circunferência | *Desmos* | *Khan Academy - Goconqr* |
| Geometria Plana e Espacial | *Google Forms* | *Kahoot!* |

Tabela 1: Atividades formativas

Além disso, em paralelo a essas atividades formativas, os alunos do PIBID participaram como ouvintes das aulas de matemática da professora supervisora nas turmas do ensino médio, com o objetivo de observar e aprender como a docente ministrava e desenvolvia suas atividades.

**2ª Etapa:**

Com o intuito de revisar conteúdos de matemática que são abordados no ENEM, nessa etapa optou-se por adotar encontros quinzenais síncronos de 2h, preferencialmente, no contraturno das aulas regulares para não interferir no planejamento da professora titular. Essas aulas foram efetivadas no formato *on-line* através de um conjunto de itens multimídia variados, possibilitando diferentes formas de interação com os estudantes e uma experiência enriquecedora tanto para os estudantes da escola como para os discentes do PIBID. Em seguida apresentamos alguns registros dessas aulas de revisão para o ENEM, seguindo a ordem em que foram realizadas:


Figura 2: Aula de revisão para o ENEM. Conteúdo: Estatística

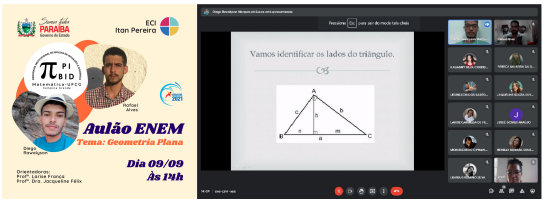



Figura 3: Aula de revisão para o ENEM. Conteúdo: Geometria Plana

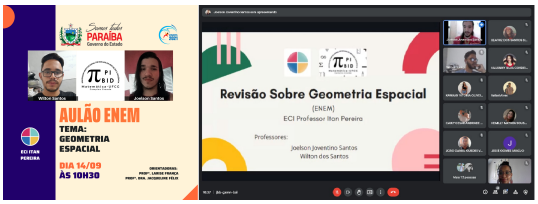



Figura 4: Aula de revisão para o ENEM. Conteúdo: Geometria Espacial

As aulas de preparação para o ENEM (Exame Nacional do Ensino Médio), foram de grande valia para os alunos da ECI Professor Itan Pereira. Nessas aulas procuramos desenvolver nos alunos o seu grande potencial matemático, resolvendo junto com eles exercícios de raciocínio lógico, dos quais a grande maioria foi retirado do próprio banco de questões do ENEM de anos anteriores.

Podemos afirmar que o ambiente que se instaurou durante os encontros síncronos foi muito produtivo, uma vez que a etapa inicial de revisão de conteúdos e aplicativos foi essencial para o bom planejamento e elaboração de aulas remotas criativas e dinâmicas. Isso permitiu que as aulas fossem mais concentradas em discussões entre os alunos e docentes sobre como resolver os problemas propostos.

Sempre nas aulas, após esclarecer algumas dúvidas sobre os conteúdos, era apresentada uma seleção de questões para os alunos responderem de forma coletiva. Durante essa apresentação, com incentivo dos integrantes do PIBID e da professora supervisora, os estudantes foram capazes de formular conjecturas e criar estratégias de resolução dos problemas propostos. Apesar de não ter sido possível atingir 100% dos alunos, os estudantes puderam vivenciar momentos de investigação onde era necessário ouvir e interpretar as hipóteses de um colega, fazer testes e verificações, avaliar observações e refinar as hipóteses.

Observamos que as atividades coletivas de resolução de problemas criaram a possibilidade de um grande engajamento entre os estudantes.

Um aspecto que chamou atenção foi o interesse dos alunos presentes nesses encontros *on-line*. Sempre ao final das aulas, eles perguntavam quando seria o próximo encontro, o que deixava o grupo bastante satisfeito com o resultado do trabalho. Por outro lado, dos 66 alunos matriculados nas turmas do 3° ano, em média 30 alunos participavam das aulas *on-line*, o que indicou uma participação mínima dos estudantes durante as aulas remotas. Esses números trazem a reflexão sobre umas das grandes barreiras enfrentadas pelos estudantes da rede pública durante esse período, a falta de acesso aos recursos tecnológicos. De onde concluímos que o ensino remoto serviu para acentuar ainda mais a desigualdade educacional no país.

**3ª Etapa:**

Após a realização das ações referentes às aulas preparatórias para o ENEM, enviamos para os alunos participantes um formulário com 5 (cinco) questões através do *Google Forms* com o objetivo de obter um *feedback* dos estudantes a respeito do trabalho realizado e com os dados obtidos foram criados os gráficos a seguir:

É importante ressaltar que dos alunos que participaram das aulas apenas 20 responderam o formulário. As questões aplicadas foram as seguintes:

Questão 1: Você achou que as aulas preparatórias ministradas pelos alunos do PIBID foram importantes?
Questão 2: Você se sente melhor preparado para o ENEM após as aulas preparatórias?
Questão 3: Você recomendaria que esse formato de aula se repetisse em outras escolas?
Questão 4: Você acha que esse tipo de aula ajuda os alunos a absorver os conteúdos?
Questão 5: Comente um pouco sobre o que você achou da experiência proporcionada com essas aulas.

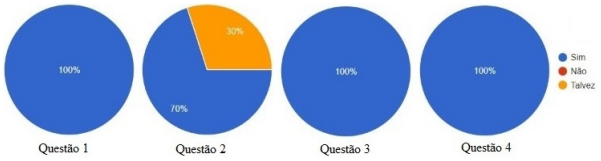



Figura 5: Gráficos referentes ao formulário

Algumas respostas da questão 5:
"Eu gosto muito da forma como foi trabalhadas as questões, proporcionando pra gente alunos um novo olhar para as questões como fazer elas rápido."
"as aulas preparadas e passadas para nós alunos foi de suma importância, pois além de revisar, nós também aprendemos a lidar com o tempo do enem e diversas maneiras de responder as questões."
"Eu como aluno prestes a fazer o Enem eu amei essa experiência proporcionadas pelo PIBID, por que foram demonstradas várias dicas de como resolver questões facilmente sem precisar perder tanto tempo lendo e relendo as questões pra pegar as informações necessárias"
"Me ajudou bastante a montar um plano de estudos, e me deu mais confiança."
"Foram momentos muito bons! Os professores souberam administrar as aulas com facilidade, ajudando-nos a compreender as questões referentes ao Enem."
"Foi muito boa e deu para entender os conteúdos que foram explicados."
"Eu aprendi bastante com as aulas, foram essenciais para a minha aprendizagem até o ENEM."

É importante observar que esses alunos foram prejudicados em relação à aprendizagem desde 2020 e hoje temos a consciência de que o ensino remoto não substitui o ensino presencial. No entanto, ficou evidente o papel fundamental da tecnologia para o processo de ensino e aprendizagem.

Por fim, no que diz respeito a experiência docente, sentimos o quão desafiador é manter os alunos motivados e engajados durante as aulas remotas.

## 4. Conclusões

Foi possível identificar por meio das aulas preparatórias o interesse e empenho dos estudantes. A partir das resoluções das questões tivemos a oportunidade de revisar alguns conteúdos, trabalhando com eles diversos pontos importantes visando um bom desempenho na prova de Matemática e Suas Tecnologias, como a interpretação das questões, ideias de passos a serem seguidos e conseguimos mostrar a diversidade nas maneiras de resolução.

Houve bastante interação dos estudantes com os professores através do *chat* e em alguns momentos pelo microfone, além disso ao final de cada aula houve uma procura dos estudantes por novas datas e também sugestões de conteúdos a serem abordados. Tudo isso mostra que o nosso objetivo inicial foi alcançado, conseguimos abordar tudo que estava planejado para o momento e de uma maneira clara e de fácil entendimento por parte dos alunos.

Pode-se perceber que apesar de todas as dificuldades e limitações impostas pela pandemia, é possível preparar os estudantes para o ENEM de uma forma leve e atrativa. Do ponto de vista educacional, além das aprendizagens acerca do formato remoto, as experiências vivenciadas pelo PIBID foram também fundamentais para a solidificação da formação docente dentro da Licenciatura em Matemática.

## Agradecimentos

Aos órgãos colaboradores CAPES, UAMat, UFCG e ECI Professor Itan Pereira pelo apoio ao projeto PIBID.

## Referências

NASCIMENTO, P. M. et al. *Acesso Domiciliar à Internet e Ensino Remoto Durante a Pandemia.* [S.l.]: IPEA, 2020. 16 p. Citado na página 2.

# Uma Proposta Histórico-Construtivista dos Logaritmos

**Daniel Cordeiro de Morais Filho**[1] **- demoraisfilho@gmail.com**
**Rayanne Dantas Maia**[2] **- rayanne-maia@hotmail.com**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Parcialmente financiado pelo PET/FNDE - Campina Grande, PB, Brasil

[2]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *O presente trabalho aborda um estudo para conceitualização dos logaritmos baseada no seu processo de construção histórica e no estudo dos métodos puramente algébricos, utilizados na construção das tábuas de logaritmos. Apresentamos uma proposta, até certo ponto, autoral, para a construção do conceito de logaritmo a partir do resgate histórico da ligação desse conceito com os de PAs e de PGs. Em consequência, discutiremos algumas limitações desse processo para definir o logaritmo de todo número real positivo, porém, contornaremos esses "obstáculos" usando importantes resultados da Análise Matemática na reta real. Intencionando levar, até certo ponto, nosso trabalho para uma sala de aula, encerramos com uma proposta de atividade construtivista, com o intuito de proporcionar ao professor uma sugestão de trabalho que possibilitará ao aluno uma aprendizagem histórica e significativa sobre os logaritmos, a partir da ideia de PAs e de PGs.*
***Palavras-chave****: Construtivismo; História da Matemática; Logaritmos*

## 1. Introdução

O ensino dos logaritmos, pode muitas vezes ser visto pelos alunos do Ensino Médio como um conteúdo de pouca importância para o conhecimento, e sem conexão com qualquer outro assunto que os alunos já viram. Um fator que contribui para essa ocorrência pode ser a forma como os logaritmos são abordados em sala de aula, por ser, quase sempre, consequência de processos pedagógicos focados na memorização da definição, nas propriedades e repetição dessas propriedades em exercícios manipulativos. Muitas vezes, não se exibe a necessidade da criação dos logaritmos, tampouco se faz um resgate dos processos históricos que levaram a sua construção, e nem se trabalham com os conhecimentos prévios dos alunos para facilitar a compreensão desse conceito. Para mudar essa realidade, faz-se necessário realizar um trabalho que conduza o aluno a um novo olhar para o estudo do tema, percebendo a importância dos logaritmos no contexto da História da Matemática, bem como para resolução de diversas situações-problemas.

Acreditamos ser indispensável que o professor desenvolva uma postura de pesquisador, e que agregue às suas aulas conhecimentos além dos livros didáticos, como uma forma de enriquecer seu trabalho. Nesse sentido, pode acrescentar questionamentos e debates que levem o aluno a agir, a pensar e a ir de encontro às respostas, além de estimulá-lo na participação ativa do processo de construção do conhecimento, pois "aprende-se agindo sobre o conteúdo a ser aprendido e retirando das ações sobre esse conteúdo qualidades próprias dessas ações e não mais dos conteúdos apenas" (BECKER, 2012a, p.265).

Com esse intuito, encontramos na História da Matemática uma alternativa para realizar um estudo estimulador dos logaritmos, partindo da necessidade da sua engenhosa construção, associada aos conceitos de $PAs$ e de $PGs$, que proporcionaram aos pioneiros matemáticos dos séculos XVI e XVII pensar em maneiras para se chegar ao conceito dos logaritmos principiando-se com essas sequências numéricas. Empregando um processo construtivo, elaborado por questionamentos, construções de teoremas e discussões de exemplos, apresentaremos como garantir a existência do logaritmo de todo número real positivo, bem como encontrar boas aproximações para ele, a partir de $PAs$ e $PGs$, refazendo o verdadeiro processo histórico de criação dessas ideias.

Analisamos, também, livros didáticos atuais para verificar se encontramos algum resquício do elo histórico perdido entre o estudo dos logaritmos e as progressões aritméticas e geométricas. Tendo em vista o resgate histórico didático desse elo, e, propondo uma ressignificação para o estudo dos logaritmos, temos por objetivos:

### 1.1 Objetivo Geral

Desenvolver uma proposta de trabalho para o estudo dos logaritmos envolvendo a história da matemática sob uma perspectiva construtivista.

#### 1.1.1 Objetivos Específicos

- Analisar os processos históricos-algébricos usados na construção das tábuas de logaritmos;
- Discutir como os logaritmos apareciam nos livros didáticos antigos e atuais;
- Propor uma atividade histórica-construtivista para o estudo dos logaritmos.
- Disponibilizar uma proposta, para ser usada por professores em sala de aula, que forneça conhecimento histórico-construtivista dos logaritmos.

## 2. Metodologia

O presente trabalho foi motivado pela análise de um dos livros da coleção de livros didáticos da editora FTD, intitulada "ÁLGEBRA CURSO SUPERIOR: Para o ciclo Colegial e admissão às Escolas Superiores", publicado no ano de 1947 (PEDRO, 1947), que aborda a definição dos logaritmos associando-a às $PAs$ e $PGs$. Inspirados por esta apresentação e realizando um levantamento bibliográfico em livros de História da Matemática, e, até mesmo, na obra original de Henry Briggs (BRUCE, 2021), um dos criadores dos logaritmos, realizamos uma releitura, até certo ponto, autoral, para trazer a conceitualização dos logaritmos, para professores e alunos, sob uma nova perspectiva.

Adicionalmente ao nosso trabalho, analisamos livros didáticos atuais, (IEZZI et al., 2016), (SOUZA; GARCIA, 2016), para verificar como a relação entre logaritmos e $PAs$ e $PGs$ é abordada no Ensino Médio, e percebemos que essa relação não era enfatizada. Pensando na sala de aula, apresentamos uma proposta de atividade para o estudo do logaritmo, partindo da associação essas sequências numéricas e o logaritmo.

## 3. Resultado e discussão

Interessado em desenvolver uma ferramenta capaz de simplificar os longos e exaustivos cálculos de multiplicações, divisões e extrações de raízes − cada vez mais demandados pelo desenvolvimento da Ciência em sua época − o escocês, John Napier (1550-1617), criou os logaritmos. Sua ideia surgiu da observação de que, associando-se os termos de uma progressão geométrica

$$b, b^2, b^3, b^4, ..., b^m, ..., b^n, ...$$

com os termos da progressão aritmética

$$1, 2, 3, 4, ..., m, ..., n, ...,$$

o produto $b^m \cdot b^n = b^{m+n}$, de dois termos da primeira progressão, está associado à soma $m+n$ dos termos correspondentes da segunda progressão(EVES, 2011). Logo, seria possível simplificar a tarefa de multiplicar por somar.

No entanto, essa abordagem, que inspirou a construção do conceito do logaritmos, não consta, ou apresenta-se de forma bem oculta nos livros didáticos. O aluno do Ensino Médio, ao se deparar com um problema sobre logaritmos, não tem a percepção de que este conteúdo está associado às progressões aritméticas e geométricas.

Para a construção da definição dos logaritmos a partir da associação entre as $PAs$ e as $PGs$, abordamos as definições destas sequências com algumas peculiaridades inerentes aos nossos objetivos, como apresentaremos a seguir.

**Definição:** *Uma* ***progressão aritmética (PA)*** *é uma sequência infinita da forma* $(PA)_r = (..., -3r, -2r, -r, 0, r, 2r, 3r, ...)$, *onde* $r \in \mathbb{R}$, $r > 0$ *e a diferença entre cada termo da sequência e o termo anterior é constante, chamada de* ***razão****. Uma* ***progressão geométrica (PG)*** *é uma sequência infinita da forma* $(PG)_q = (..., q^{-3}, q^{-2}, q^{-1}, 1, q^1, q^2, q^3, ...)$, *onde* $q \in \mathbb{R}$, $q > 0$, $q \neq 1$ *e o quociente entre cada termo e o termo anterior é constante, chamado de* ***razão****.*

**Exemplo:** *A sequência infinita* $(..., -3\sqrt{2}, -2\sqrt{2}, -\sqrt{2}, 0, \sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, ...)$ *é uma PA de razão* $\sqrt{2}$. *A sequência infinita* $(..., \left(\frac{1}{3}\right)^{-3}, \left(\frac{1}{3}\right)^{-2}, \left(\frac{1}{3}\right)^{-1}, 1, \left(\frac{1}{3}\right)^{1}, \left(\frac{1}{3}\right)^{2}, \left(\frac{1}{3}\right)^{3}, ...)$ *é uma PG de razão* $\frac{1}{3}$.

Baseando-se no contexto histórico, associamos cada $q^n$ da $(PG)_q$, para $n \in \mathbb{Z}$, a um único termo $nr$ da $(PA)_r$, por exemplo, a $(PG)_{\frac{1}{3}}$ está associada a $(PA)_{\sqrt{2}}$, como mostra a tabela abaixo:

Tabela 1: $(PG)_{\frac{1}{3}}$ associada à $(PA)_{\sqrt{2}}$

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ... | $\left(\frac{1}{3}\right)^{-n}$ | ... | $\left(\frac{1}{3}\right)^{-2}$ | $\left(\frac{1}{3}\right)^{-1}$ | $\left(\frac{1}{3}\right)^{0}$ | $\left(\frac{1}{3}\right)^{1}$ | $\left(\frac{1}{3}\right)^{2}$ | ... | $\left(\frac{1}{3}\right)^{n}$ | ... |
| ... | $-n\sqrt{2}$ | ... | $-2\sqrt{2}$ | $-1\sqrt{2}$ | 0 | $1\sqrt{2}$ | $2\sqrt{2}$ | ... | $n\sqrt{2}$ | ... |

Definimos que o logaritmo do termo $q^n \in (PG)_q$ é o seu correspondente na $nr \in (PA)_r$, com $q, r \in \mathbb{R}_+^*$ e $q \neq 1$, ou seja, $log(q^n) = nr$. Mas, como determinar o logaritmo de um número que não pertence à $(PG)_q$? A ideia natural seria inserir termos entre cada dois termos consecutivos e gerar novas $PGs$, e, com isso, encontrar uma $PG$ que contivesse esse número. Com esses questionamentos, pensamos e chegamos a ideia de *refinamento* para $PAs$ e $PGs$:

**Definição:** *Sejam os números reais positivos* $r$ *e* $r'$. *A* $\boldsymbol{(PA)_{r'}}$ ***é um refinamento da*** $\boldsymbol{(PA)_r}$, *se* $(PA)_r \subset (PA)_{r'}$. *Sejam os números reais positivos* $q, q'$, *com* $q, q' \neq 1$. *A* $\boldsymbol{(PG)_{q'}}$ ***é um refinamento da*** $\boldsymbol{(PG)_q}$, *se* $(PG)_q \subset (PG)_{q'}$.

Quando os respectivos refinamentos existem temos $r' = \frac{r}{m}$ e $q' = q^{\frac{1}{k}}$, para certos $m, k \in \mathbb{N}$.

### 3.1 Uma importante pergunta sobre refinamentos das PAs e das PGs

Diante da definição acima, ficam as perguntas:

Dados $x \in \mathbb{R}$ e uma $(PA)_r$, com $r \in \mathbb{R}$ e $r > 0$, tal que $x \notin (PA)_r$, é possível encontrar um refinamento

$(PA)_{r'}$ de $(PA)_r$ de modo que $x \in (PA)_{r'}$?

Dados $x \in \mathbb{R}$ e uma $(PG)_q$ com $q \in \mathbb{R}$, tal que $q > 0$ e $q \neq 1$, é possível encontrar um refinamento $(PG)_{q'}$ de $(PG)_q$ de modo que $x \in (PG)_{q'}$?

As respostas estão nas Tabelas 2 e 3, encontradas mais adiante. Os resultados apresentados nas tabelas nos mostraram que nem sempre é possível determinar um refinamento dessas sequências, tal que todo número real positivo $x$ pertença a algum refinamento.

Tabela 2: Respostas às perguntas sobre refinamentos de PAs

| $x$ | $r$ | Resposta |
|---|---|---|
| $x \in \mathbb{Q}$ | $r \in \mathbb{Q}$ | Sim |
| $x \in \mathbb{R}\backslash\mathbb{Q}$ | $r \in \mathbb{Q}$ | Não |
| $x \in \mathbb{Q}$ | $r \in \mathbb{R}\backslash\mathbb{Q}$ | Não |
| $x \in \mathbb{R}\backslash\mathbb{Q}$ | $r \in \mathbb{R}\backslash\mathbb{Q}$ | Nem sempre |

Fonte: Elaborada pelos autores

Tabela 3: Resposta às perguntas sobre refinamentos de PGs

| $x$ | $q$ | Resposta |
|---|---|---|
| $x \in \mathbb{Q}$ | $q \in \mathbb{Q}$ | Não |
| $x \in \mathbb{R}\backslash\mathbb{Q}$ | $q \in \mathbb{Q}$ | Nem sempre |
| $x \in \mathbb{Q}$ | $q \in \mathbb{R}\backslash\mathbb{Q}$ | Nem sempre |
| $x \in \mathbb{R}\backslash\mathbb{Q}$ | $q \in \mathbb{R}\backslash\mathbb{Q}$ | Nem sempre |

Fonte: Elaborada pelos autores

### 3.2 Definição formal dos logaritmos

Até este ponto relacionamos os termos de uma $(PG)_q$ aos termos de uma $(PA)_r$ para definir logaritmo de um número que está na $(PG)_q$ ou em algum refinamento de $(PG)_q$. Na seção anterior, mesmo com refinamentos de $PAs$ e $PGs$, vimos nem sempre ser possível determinar o logaritmo de um número positivo qualquer, mesmo inserindo uma quantidade tão grande, quanto se queira, de termos entre termos da $PGs$.

Então, como determinar o logaritmo de um número que não pertence ao refinamento? Para responder a essa pergunta, montamos um resultado de suma importância nessa construção, que culminou na definição formal dos logaritmos

**Teorema:** *Dados uma progressão geométrica de razão $q$, com $q > 0$ e $q \neq 1$, e um número real positivo $b$, existe um único número real $c$, tal que $q^c = b$.*

Para demonstração deste Teorema, utilizamos resultados muito importantes na formação de um professor de Matemática, como o Teorema dos Intervalos Encaixantes (OLIVEIRA, 2017), o Axioma de Dedekind (NETO, 2015) e o Teorema de Bolzano-Weierstrass (LIMA, 2006). Isso comprova a grande contribuição da Análise Matemática para compreender em profundidade ideias de temas do Ensino Médio.

Posteriormente vimos que nossas ideias de refinamento de progressões coincidem com as ideias do matemático Henry Briggs(1561-1631), que calculou o logaritmo apenas com sucessivas raízes quadradas, ou seja, a média geométrica, que equivale ao refinamento para $m = 2$. Com o resultado anterior, formalizamos a definição dos logaritmos:

**Definição** *Dados os números reais positivos $q$ e $b$, com $q \neq 1$. Chamamos de logaritmo de $b$ na base $q$, o número real $c$ tal que $q^c = b$, ou seja,*

$$\log_q b = c \Leftrightarrow q^c = b.$$

## 4. Conclusões

Partindo da necessidade histórica da engenhosa criação dos logaritmos, até o ponto de conceituá-los, resgatamos o elo perdido dessa criação, partindo de $PAs$, $PGs$, bem como de seus refinamentos, para a definição forma de logaritmo. Tentamos convencer de que, para obter o logaritmo de qualquer número positivo, necessita-se de uma argumentação mais elaborada, fundamentada na Análise Real.

## Agradecimentos

A CAPES por oferecer esse curso para uma melhor qualificação dos professores. A todo corpo docente da UFCG, pelo compromisso e dedicação com a formação profissional dos seus discentes, de modo especial ao meu orientador, Daniel Cordeiro de Morais Filho, por todos as horas de estudos, ideias e ensinamentos para construção deste trabalho.

## Referências

BECKER, F. *A epistemologia do professor: O cotidiano da escola.* [S.l.]: Vozes, 2012a. Citado na página 1.

BRUCE, I. *Briggs' ARITHMETICA LOGARITHMICA*. 2021. Disponível em: ⟨http://www.17centurymaths.com/contents/albriggs.html⟩. Citado na página 2.

EVES, H. *Introdução à História da Matemática; tradução Hygino H. Domingues*. 5ª. ed. [S.l.]: Unicamp, 2011. Citado na página 3.

IEZZI, G. et al. *MATEMÁTICA: ciência e aplicações*. [S.l.]: Saraiva, 2016. Citado na página 2.

LIMA, E. L. *Análise Real*. [S.l.]: IMPA, 2006. v. 1. Citado na página 4.

NETO, A. C. M. *Fundamentos de Cálculo*. [S.l.]: Coleção PROFMAT, 2015. Citado na página 4.

OLIVEIRA, M. M. de. *Conceitos de Análise na Reta para bem compreender os Números Reais no Ensino Médio*. [S.l.]: Dissertação (Mestrado) — PROFMAT/UFCG, 2017. Citado na página 4.

PEDRO, I. I. *ÁLGEBRA: CURSO SUPERIOR*. [S.l.]: Paulo de Azevedo LTDA, 1947. Citado na página 2.

SOUZA, J.; GARCIA, J. *Contato Matemática*. 1º. ed. [S.l.]: FTD, 2016. Citado na página 2.

# Uma estratégia para resolver questões de Análise Combinatória no ENEM.

**Jaldir de Oliveira Costa** [1] **- jaldir.matematica@gmail.com**
**Romildo Nascimento de Lima**[1] **- romildo@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Neste trabalho, destacamos a grande relevância que o Exame Nacional do Ensino Médio (ENEM) tem para educação brasileira. Iniciamos por um breve histórico do ENEM, destacando a sua Matriz de Referência e a abordagem dada às questões de Análise Combinatória. Pois identificamos a incidência de 26 questões que exigem o domínio das diferentes técnicas de contagem, conforme o levantamento realizado nas provas aplicadas a partir de 2009. Além disso, apresentamos e aplicamos uma estratégia para resolver problemas combinatórios, em duas questões.*
***Palavras-chave****: Análise Combinatória; ENEM; Resolução de Problemas.*

## 1. Introdução

O Exame Nacional do Ensino Médio (ENEM) é, certamente, o principal instrumento avaliativo da etapa final da Educação Básica. Esta avaliação foi instituída através da Portaria MEC nº 438, de 28 de maio de 1998, cumprindo com a atribuição da União de realizar o processo de avaliação nacional para os estudantes do Ensino Médio, conforme o previsto no Artigo 9º da LDB (BRASIL, 1996), Inciso VI: "Assegurar processo nacional de avaliação do rendimento escolar no ensino fundamental, médio e superior, em colaboração com os sistemas de ensino, objetivando a definição de prioridades e a melhoria da qualidade do ensino".

A relevância deste exame é comprovada não somente pela quantidade de inscritos (Tabela 1), mas, principalmente, pela importante atribuição de selecionar candidatos para o ingresso no Ensino Superior.

Tabela 1: Quantidade de inscritos no ENEM: 1998 a 2019

| Ano | Quantidade de Inscritos | Ano | Quantidade de Inscritos |
|---|---|---|---|
| 1998 | 157.221 | 2009 | 4.148.721 |
| 1999 | 346.819 | 2010 | 4.626.094 |
| 2000 | 390.180 | 2011 | 5.380.857 |
| 2001 | 1.624.131 | 2012 | 5.791.332 |
| 2002 | 1.829.170 | 2013 | 7.173.574 |
| 2003 | 1.882.393 | 2014 | 8.722.290 |
| 2004 | 1.552.316 | 2015 | 7.792.025 |
| 2005 | 3.004.491 | 2016 | 8.627.371 |
| 2006 | 3.742.827 | 2017 | 6.731.186 |
| 2007 | 3.568.592 | 2018 | 5.513.662 |
| 2008 | 4.018.070 | 2019 | 5.095.308 |

Fonte dos dados: ⟨https://www.gov.br/inep⟩ Acesso 01/06/2021, às 00:09.

Nesta tabela, também observamos que o ENEM registrava os menores quantitativos de inscritos nas primeiras edições, visto que a participação dos estudantes era voluntária, conforme expresso no Artigo 5º da Portaria supracitada. Mas, nos anos seguintes, quando a nota obtida no ENEM passou a ser utilizada como meio de seleção para o ingresso nas instituições privadas, através do Programa Universidade Para Todos - PROUNI (2004) e do Fundo de Financiamento Estudantil - FIES (2010), o número de inscrições aumentou consideravelmente.

Em 2012, a criação do Sistema de Selecão Unificada - SISU possibilitou o credenciamento das Instituições Públicas de Ensino Superior (IES) para utilizarem também as notas do ENEM como critério de seleção, em substituição parcial/total aos vestibulares.

As questões do ENEM são elaboradas seguindo as orientações da Matriz de Referência, reformulada em 2009, que norteia sobre os conteúdos, competências e habilidades requeridas dos canditatos.

Assim, objetivamos realizar um levantamento nas avaliações anteriores e identificarmos a ocorrência de questões relacionadas aos princiais conceitos da Análise Combinatória: Princípio Fundamental da Contagem, Permutação Simples (ou Com Repetição), Arranjo, Combinação Simples (ou Com Repetição), entre outras.

Por fim, apresentamos uma estratégia que auxilia na resolução de problemas combinatórios. E, selecionamos duas questões com as respectivas propostas de solução, segundo a estratégia que fora indicada.

## 2. Metodologia

Este trabalho foi desenvolvido, principalmente, a partir de uma pesquisa documental, consulta ao acervo de provas do ENEM e bibliografias relacionadas ao conteúdo de Análise Combinatória. Motivados pela dissertação do Mestrado Profissional em Matemática, elaborada por COSTA (2021), que apresenta uma proposta de ensino para o conteúdo Análise Combinatória no Ensino Médio e dedicou um capítulo à discussão desse conteúdo no ENEM.

Também analisamos alguns documentos da legislação educacional brasileira. Dentre estes, destacamos a Portaria MEC nº438/1998, que criou o ENEM, e a Portaria Normativa Nº18/2012, que instituiu o SISU. Além da Matriz de Referência, vigente desde 2009, que é o principal instrumento norteador sobre os conteúdos, competências e habilidades exigidos no exame, itens que estão organizados em quatro áreas do conhecimento e uma produção do genêro dissertativo-argumentativo. Neste caso, a área de Matemática e Suas Tecnologias contempla 45 questões, que corresponde a 20% da nota final do candidato.

Na Matriz de Referência (BRASIL, 2009), também identificamos que o conteúdo de Análise Combinatória é mencionado na Competência 1, através da Habilidade 2: *"H2 - Identificar padrões numéricos ou* ***princípios de contagem****"*. Mas, esta é uma descrição abrangente, que deixa implícito quais tópicos atendem aos "Princípios de Contagem". Mais adiante, o texto cita, novamente, os princípios de contagem, ao tratar dos Conhecimentos Numéricos: *"(...) operações em conjuntos numéricos (naturais, inteiros, racionais e reais), desigualdades, divisibilidade, fatoração, razões e proporções, porcentagem e juros, relações de dependência entre grandezas, sequências e progressões,* ***princípios de contagem****."*

Como os Princípios de Contagem são aplicáveis em diferentes contextos, principalmente, em situações-problemas do cotidiano, o estudo da Análise Combinatória é dividido em subtópicos que possibilitam compreender as tópicos derivados do Princípio Fundamental de Contagem, e estes subtópicos denominamos técnicas de contagem.

Para o estudo de cada uma dessas técnicas e como, referências desse trabalho, destacamos MORGADO; CARVALHO, HAZZAN e PEREIRA; CAMPOS, pois, reunem as principais teorias e apresentam exemplos que permitem aprofundar os conhecimentos sobre o Princípio Fundamental da Contagem, Permutação, Arranjo, Combinação, para o tratamento de agrupamentos simples ou com repetição de elementos. Neste resumo, não revisaremos tais conteúdos, pois pressupomos que estes tenham sido previamente estudados.

Assim, destacamos a estratégia de resolução apresentada por MORGADO e CARVALHO (2015, p. 108-109) para atacar e resolver problemas de contagem:

> **1) Postura.** Devemos sempre nos colocar no papel da pessoa que deve fazer a ação solicitada pelo problema e ver que decisões devemos tomar. (...)
> **2) Divisão.** Devemos, sempre que possível, dividir as decisões a serem tomadas em decisões mais simples. (...)
> **3) Não adiar as dificuldades.** Pequenas dificuldades adiadas costumam se transformar em imensas dificuldades. Se uma das decisões a serem tomadas for mais restrita que as demais, essa é a decisão que deve ser tomada em primeiro lugar.

E, também as recomendações de PEREIRA e CAMPOS (2012, p. 16) que apresentam uma estratégia semelhante para chegar a solução de problemas combinatórios, que consiste em dividir a decisão em subdecisões e aplicar o Princípio da Multiplicação.

O **Princípio da Multiplicação** pode ser utilizado também quando a decisão é dividida em mais que duas subdecisões. Por exemplo, suponha que a decisão tenha que ser tomada e que tal decisão seja dividida em três subdecisões $d_1$,$d_2$,$d_3$ que deverão ser tomadas uma após a outra e numa seqüência. Em outras palavras, para tomarmos a decisão $d$, primeiro uma decisão $d_1$ tem que ser tomada, depois de $d_1$ uma decisão $d_2$ tem que ser tomada, depois de tomadas as decisões $d_1$ e $d_2$, uma decisão $d_3$ tem que ser tomada.

Ambas estratégias indicam a necessidade prévia de organizar as ideias e, em seguida, aplicar o conhecimento matemático correspondente, ter uma postura ativa para buscar soluções e aprender com os próprios erros. Adquirindo, neste processo, uma base de conteúdos que permita-o solucionar situações mais complexas que venham a surgir, inclusive para os desafios do Ensino Superior.

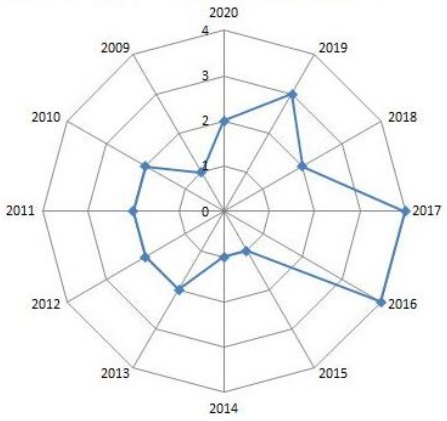
Assim, a próxima etapa é identificar e resolver questões em que possam ser aplicadas estas estratégias. Por isso, prosseguimos com um levantamento das questões do ENEM, identificando, dentre estas, quais contemplam o conteúdo de Análise Combinatória.

## 3. Resultado e discussão

O Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira - INEP é responsável pela elaboração e aplicação do ENEM, mantendo, em seu site, o banco de provas e gabaritos de todos os exames aplicados, desde o primeiro realizado em 1998 até o ano de 2020.

Analisamos cada prova e cada questão com respectivo gabarito, com a finalidade de constatar a incidência das questões cujo conteúdo é Análise Combinatória, a partir de 2009. O resultado está ilustrado no Gráfico Figura 1, onde é possível observar o quantitativo anual, variando de 1 a 4 questões, e o total de 26 questões aplicadas nas doze últimas edições.

Figura 1: Questões de Análise Combinatória no ENEM - 2009 a 2020

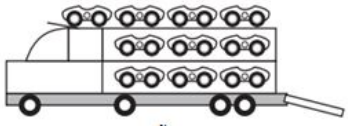



Fonte: Autoral utilizando os dados do (INEP, 2021)

Depois que as questões foram identificadas e catalogadas, somos motivados a resolver algumas dessas para compreensão da estratégia de resolução apresentada na metodologia. O trabalho de COSTA (2021) sugere as resoluções para dez questões aplicadas no ENEM, referentes ao mesmo conteúdo. Mas, aqui, detalharemos a solução para duas questões, que foram aplicadas nos exames de 2017 e 2018, respectivamente.

Estas questões exemplificam bem o modelo de questão aplicado no exame e podem, claramente, serem resolvidas segundo a estratégia de MORGADO e CARVALHO (2015). Além disso, as resoluções são interessantes porque demonstram a variabilidade de técnicas que são exigidas.

**(ENEM 2017)** Um brinquedo infantil caminhão-cegonha é formado por uma carreta e dez carrinhos nela transportados, conforme a figura.



No setor de produção da empresa que fabrica esse brinquedo, é feita a pintura de todos os carrinhos para que o aspecto do brinquedo fique mais atraente. São utilizadas as cores amarelo, branco, laranja e verde, e cada carrinho é pintado apenas com uma cor. O caminhão-cegonha tem uma cor fixa. A empresa determinou que em todo caminhão-cegonha deve haver pelo menos um carrinho de cada uma das quatro cores disponíveis. Mudança de posição dos carrinhos no caminhão-cegonha não gera um novo modelo do brinquedo.
Com base nessas informações, quantos são os modelos distintos do brinquedo caminhão-cegonha que essa empresa poderá produzir?
A) $C_{6,4}$ B) $C_{9,3}$ C) $C_{10,4}$ D) $6^4$ E) $4^6$

***Solução:*** Existem 10 carrinhos a serem coloridos, utilizando-se quatro cores, onde cada cor deve ser utilizada pelo menos uma vez. Sigamos as seguintes etapas:

1ª) Tomando as 4 cores disponíveis e colorindo um carrinho com cada uma delas, garantimos que todas as cores serão utilizadas, e, teremos $10 - 4 = 6$ carrinhos restantes;

2ª) Para colorir os 6 carros, teremos 4 cores à disposição, que podem repetir-se ou não. Por isso, utilizamos o conceito de Combinação com repetição: $C_{n-1+p,p} = C_{4-1+6,6} = C_{9,6}$;

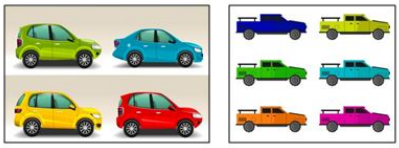
Depois disso, é necessário aplicar a propriedade de Combinação, onde $C_{n,p} = C_{n,n-p}$, temos que $C_{9,6} = C_{9,9-6} = C_{9,3}$. Portanto, a quantidade de modelos distintos do brinquedo caminhão-cegonha é $B)$ $C_{9,3}$. □

**(ENEM 2018)** O Salão do Automóvel de São Paulo é um evento no qual vários fabricantes expõem seus modelos mais recentes de veículos, mostrando, principalmente, suas inovações em design e tecnologia. **Disponível em: http://g1.globo.com. Acesso em: 4 fev. 2015 (adaptado).**

Uma montadora pretende participar desse evento com dois estandes, um na entrada e outro na região central do salão, expondo, em cada um deles, um carro compacto e uma caminhonete. Para compor os estandes, foram disponibilizados pela montadora quatro carros compactos, de modelos distintos, e seis caminhonetes de diferentes cores para serem escolhidos aqueles que serão expostos. A posição dos carros dentro de cada estande é irrelevante.
Uma expressão que fornece a quantidade de maneiras diferentes que os estandes podem ser compostos é:
A) $A_{10}^4$ B) $C_{10}^4$ C) $C_4^2 \times C_6^2 \times 2 \times 2$ D) $A_4^2 \times A_6^2 \times 2 \times 2$ E) $C_4^2 \times C_6^2$

***Solução:*** Existem 4 carros compactos e 6 caminhotes à disposição (Figura 2), dos quais serão selecionados 2 de cada, sob as condições dadas. Assim, dividimos a solução em três etapas:

Figura 2: Ilustração das Opções de Carros



Fonte: Google Imagens.

1ª) Existem 4 carros compactos à disposição, dos quais serão selecionados apenas 2, isto é, $C_4^2$. Uma vez escolhidos os dois carros compactos, existem duas possibilidades para posicioná-los: entrada ou dentro do salão, o que resulta em $C_4^2 \times 2$.

2ª) De modo análogo, existem 6 caminhonetes à disposição, das quais serão selecionados 2, isto é, $C_6^2$. Após a escolha, teremos duas maneiras para posicioná-las: $C_6^2 \times 2$.

Como a escolha do carro compacto não interfere na escolha da caminhonete, e vice-versa. Pelo Princípio Fundamental da Contagem, a quantidade de maneiras para organizar o estande será: $C_4^2 \times C_6^2 \times 2 \times 2$. Portanto, a alternativa correta é $C$. □

Vale salietar que, estas soluções não são exclusivas, pois existem outros meios e técnicas de contagem que permitem chegar ao mesmo resultado, por um raciocínio análogo. Ou seja, a utilização da estratégia proposta por (MORGADO; CARVALHO, 2015) auxilia na resolução dessas questões, pois determina uma sequência de ações a serem seguidas: Postura, Divisão e Não adiar dificuldades.

Primeiramente, assuminos o papel de quem deseja resolver o problema, que, na primeira questão consiste em colorir os carros sob as condições dadas. E, na segunda questão, somos os responsáveis pela organização do estande.

Em seguida, dividimos a decisão principal em duas subdecisões mais simples. No primeiro caso, é necessário colorir um carro de cada cor e, com isso, cumprir uma das exigências, para finalmente poder aplicar corretamente o conceito de Combinação para elementos repetidos, e colorir os seis carros restantes. Já na situação dos estandes, primeiro selecionamos os dois carros compactos e suas possíveis posições e, em seguida, as duas caminhonetes e suas respectivas posições.

O último passo é não adiar as dificuldades, por esta razão fomos tomando as decisões mais restritas em primeiro lugar, para consequentemente se chegar à solução completa.

Deste modo, entendemos que a estratégia apresentada, de fato, auxilia na resolução de probemas de contagem, mas ela por si só não garante o êxito da resposta correta. Por isso, ressaltamos, mais uma vez, que é de fundamental importância a aprendizagem prévia dos conceitos pertinentes à Análise Combinatória, que devem ser previamente estudados e exercitados. E como sugestão para estudo indicamos o trabalho de (COSTA, 2021).

## 4. Conclusões

Ao concluirmos este resumo, certificamos que o ENEM é uma importante avalição do sistema educacional brasileiro e, talvez, a mais decisiva da Educação Básica, pois possibilita o acesso para o Ensino Superior.

O exame foi reformulado em 2009 e, atualmente, as questões são elaboradas em consonância com a Matriz de Referência. Em relação ao conteúdo de Análise Combinatória, constatamos que o documento aponta para o domínio dos princípios de contagem. Por isso, o exame exige a habilidade de compreender as diferentes técnicas de contagem e a capacidade de distingui-las e aplicando-as, corretamente, em diferentes contextos.

Além disso, constatamos a inserção deste conteúdo em todas as edições, através do levantamento realizado no acervo de provas. E, ao examinar as soluções de duas questões, compreendemos que além do domínio das diferentes técnicas é, também, conveniente ter uma boa estratégia para resolver os problemas combinatórios. Por isso, recomendamos as estratégias de MORGADO e CARVALHO (2015) e PEREIRA e CAMPOS (2012).

Portanto, dentro do conteúdo programático para o Ensino de Matemática na Educação Básica, destacamos que a Análise Combinatória deverá contemplar o maior número possível de técnicas, teoria e exemplos, que permitam reconhecer e resolver os diversos problemas de contagem.

## Referências

BRASIL. *Lei de Diretrizes e Bases da Educação Nacional.* Brasília: Diário Oficial da União, 1996. Citado na página 1.

BRASIL. *Matriz de referência do ENEM.* Brasília: MEC, 2009. Citado na página 2.

COSTA, J. O. *Guia de ensino para análise combinatória a partir dos livros didáticos, ENEM e BNCC.* Campina Grande: UFCG, 2021. Citado 3 vezes nas páginas 2, 3 e 5.

HAZZAN, S. *Fundamentos de matemática elementar: Combinatória, Probabilidade. Vol. 5. 8. ed.* São Paulo: Atual, 2013. Citado na página 2.

INEP. *Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira.* 2021. Disponível em: ⟨https://www.gov.br/inep/pt-br/areas-de-atuacao/avaliacao-e-exames-educacionais/enem⟩. Citado na página 3.

MORGADO, A. C.; CARVALHO, P. *Matemática Discreta.* Rio de Janeiro: SBM, 2015. Citado 3 vezes nas páginas 2, 3 e 5.

PEREIRA, A. G. C.; CAMPOS, V. S. M. *Análise Combinatória e Probabiliade. 2. ed.* Natal: EDUFRN, 2012. Citado 2 vezes nas páginas 2 e 5.

# CÁLCULO DE ÁREA
# RESUMO EXPANDIDO

**Edvenilson Venâncio Dantas Farias[1] - edvenilsondantas@gmail.com**
**Dr. Romildo Nascimento de Lima[2] - romildo@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil
[2]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *Neste trabalho, apresentaremos uma análise de como os documentos norteadores da Educação brasileira expõe os conceitos de Área e Cálculo de Área, considerando como base para esse momento a Base Nacional Comum Curricular (BNCC). Por fim, apresentaremos uma proposta de atividade que melhore o processo de Ensino e Aprendizagem desse conceito dos alunos do Ensino Básico, usando como ferramenta motivadora a História da Matemática e como ferramenta pedagógica auxiliar software.*
***Palavras-chave****: Área; Cálculo de Área; Documentos Norteadores; Ensino e Aprendizagem.*

## 1. Introdução

Nos documentos norteadores da Educação brasileira, encontramos definições ou introduções aos conceitos pertinentes à Geometria e à Matemática como um todo. Pensando em analisar o ensino de Áreas de figuras, e questionar formas de aperfeiçoar o ensino, é essencial a análise de como o tema é inserido nesses documentos oficiais, como BNCC e PCN's, pois nesses documentos fica descrito e determinado que habilidades os alunos devem adquirir e dominar.

Por fim, com o intuito de contribuir no processo de Ensino e Aprendizagem dos nossos discentes do Ensino Básico, faremos algumas propostas de atividades para uma melhor difusão do ensino do Cálculo de Áreas.

Nessas propostas, apresentaremos as atividades levando em consideração algumas metodologias, não só a aula expositiva, mas trazer algo que atraia ainda mais a atenção dos discentes e, assim, fazer a aula mais produtiva para docentes e discentes.

### 1.1 Objetivos

#### 1.1.1 Objetivo Geral

Nosso trabalho tem como objetivo geral contribuir com processo de ensino e aprendizagem, fazendo uma análise de como está inserido o conceito de Cálculo de Área nos documentos oficiais, além de fazer sugestões de atividades para melhorar o processo já existente.

#### 1.1.2 Objetivos Específicos

• Analisar como o tema está inserido nos Documentos Oficiais;
• Enriquecer o conhecimento do professor, contribuindo com a sua docência no que faz relação com o Cálculo de Área;
• Colaborar com o processo ensino-aprendizagem da Matemática relativo ao Cálculo de Área de figuras planas.

## 2. Documentos Norteadores da Educação e o Cálculo de Área

Para começarmos a falar dos Documentos Norteadores da Educação, vamos as leis consideradas maiores, e seguindo uma ordem de leis, chegaremos a BNCC. Assim, apresentaremos o contexto da Educação, bem como do Cálculo de Área começando pela Constituição da República Federativa do Brasil de 1988 (Constituição Federal), logo após teremos à Lei de Diretrizes e Bases da Educação Nacional (LDB), Plano Nacional de Educação (PNE), Diretrizes Curriculares Nacionais da Educação Básica (DCN's), Parâmetros Curriculares Nacionais (PCN's) e

Base Nacional Comum Curricular (BNCC).

Na nossa Constituição, podemos ter uma rápida noção dos princípios de uma Educação de qualidade, bem como mostrar que a Educação não é de responsabilidade única das escolas, e sim uma parceria entre escola e família.

A Lei n° 9.394, de 20 de Dezembro de 1996, conhecida com Lei de Diretrizes e Bases da Educação Nacional (LDB), ou popularmente chamada de LDB, é considerada por muitos estudiosos da área, a lei mais importante no que se refere à Educação. Ela é composta por 92 artigos que abordam temas diversos sobre a educação do nosso País. Nesses artigos, encontramos a primeira divisão nas etapas de ensino, dividido em Educação Básica e Educação Superior, e depois realiza uma nova subdividida nessas etapas, apresentando que a Educação Básica é subdivisão em Ensino Infantil, Ensino Fundamental e Ensino Médio.

O Plano Nacional de Educação (PNE) foi aprovado através da Lei N° 13.005/2014 na data de 25 de Junho de 2014, a qual apresenta, em resumo, um total de 20 metas a serem alcançadas pelo sistema educacional em todo territórios nacional. Analisando as metas, prazos e estudos realizados posteriormente, vemos que ainda estamos longe do ideal. Em 2019 foi realizado um estudo, sob a responsabilidade de Andressa Pellanda (Coordenadora Executiva da Campanha Nacional pelo Direito à Educação), onde ficou claro que 16 das 20 metas não foram cumpridas dentro do prazo, e as outras 4 foram cumpridas parcialmente.

As Diretrizes Curriculares Nacionais (DCN's) para a Educação Nacional são diretrizes que estabelecem a base nacional comum, a qual é "responsável por orientar a organização, articulação, o desenvolvimento e a avaliação das propostas pedagógicas de todas as redes de ensino brasileiras. " (BRASIL, 2013, p. 04). Nesse mesmo documento, encontramos, de forma bem clara, uma das funções da educação, que é de "proporcionar o desenvolvimento humano na sua plenitude, em condições de liberdade e dignidade, respeitando e valorizando as diferenças. " (BRASIL, 2013, p. 04).

Os Parâmetros Curriculares Nacionais (PCN's), são uma coleção de documentos que abordam a estrutura curricular de uma instituição educativa, bem como apresentam o ponto de partida para o trabalho docente, dando direcionamentos para a realização de atividades em sala de aula. Essa coleção de documentos é dividida por etapas de Ensino e por componente curricular.

### 2.1 BNCC

Para começarmos a falar da Base Nacional Comum Curricular (BNCC), encontramos primeiro uma definição do que é Geometria e também de como ela é tratada por alguns docentes e discentes na Educação Básica. Ela diz que "a Geometria envolve o estudo de um amplo conjunto de conceitos e procedimentos necessários para resolver problemas do mundo físico e de diferentes áreas do conhecimento. " (BRASIL, 2018, p. 271). Em resposta a esse fato, a BNCC nos apresenta um detalhe muito importante, que é o fato de como muitos tratam a geometria. Ela descreve que "a Geometria não pode ficar reduzida a mera aplicação de fórmulas de cálculo de área e de volume nem a aplicações numéricas imediatas de teoremas sobre relações de proporcionalidade em situações relativas a feixes de retas paralelas cortadas por retas secantes ou do Teorema de Pitágoras."(BRASIL, 2018, p. 272)

Com isso, podemos ver que ainda temos muito a avançar no Ensino de Geometria no Ensino Básico e a BNCC veio para nos dar um norte melhor e mais efetivo nesses pontos, pois esse documento traz as competências (Gerais e Específicas), as habilidades e as aprendizagens essencias que todos os alunos, em cada etapa da Educação Básica (Educação Infantil, Ensino Fundamental e Ensino Médio), precisam desenvolver. Ela também frisa que todas as competências, habilidades e conteúdos devem ser os mesmos para todas as crianças, os adolescentes e os jovens, independentemente de onde estudam ou moram.

Com relação ao conceito de Área, a BNCC nos apresenta que, já no Ensino Fundamental – Anos Iniciais, os alunos devem desenvolver algumas habilidades em Geometria, uma delas é que eles reconheçam que medir é realizar uma comparação entre uma grandeza e uma unidade, bem como apresentar essa comparação por meio de um número. Ela também apresenta que os alunos nessa fase devem conseguir resolver problemas em situações cotidianas que envolvem algumas grandezas "como comprimento, massa, tempo, temperatura, área (de triângulos e retângulos) [...], sem uso de fórmulas, recorrendo, quando necessário, a transformações entre unidades de medida padronizadas mais usuais." (BRASIL, 2018, p. 273). Logo, podemos concluir que, desde o berço da educação, o conceito de Área deve estar incluído dentro da Matemática apresentada a nossos estudantes, pois esses contextos são importante para o desenvolvimento e aperfeiçoamento do pensamento matemático deles

e, assim, se convertendo em objetos de conhecimento.

O primeiro objeto de conhecimento que a BNCC nos apresenta o conceito de Área está no 3° Ano do Ensino Fundamental, dentro da Unidade Temática: Grandezas e Medida; Objeto do Conhecimento: Comparação de Área por superposição; Habilidade: (EF03MA21)[1] Comparar, visualmente ou por superposição, áreas de faces de objetos, de figuras planas ou de desenhos; na qual os estudantes já começam a se deparar com a tentativa de Cálculo de Área através da comparação com outras figuras, mas nessa fase não usa-se ainda conceito numéricos, e sim só as comparações; e, a partir dessa, vai fazendo a interligação entre as próximas etapas até se desenvolver por completo no Ensino Médio com a Habilidade: (EM13MAT307) Empregar diferentes métodos para a obtenção da medida da área de uma superfície (reconfigurações, aproximação por cortes etc.) e deduzir expressões de cálculo para aplicá-las em situações reais (como o remanejamento e a distribuição de plantações, entre outros), com ou sem apoio de tecnologias digitais.

Podemos citar também como exemplo dessas habilidades, a habilidade EF06MA24 - Resolver e elaborar problemas que envolvam as grandezas comprimento, massa, tempo, temperatura, área (triângulos e retângulos), capacidade e volume (sólidos formados por blocos retangulares), sem uso de fórmulas, inseridos, sempre que possível em contextos oriundos de situações reais e/ou relacionadas às outras áreas do conhecimento, que está interligada ao Objeto de Conhecimento Problemas sobre medidas envolvendo grandezas como comprimento, massa, tempo, temperatura, área, capacidade e volume. Essa Habilidade e esse Objeto de Conhecimento já nos mostram que os documentos oficiais estão se preocupando desde o início do Ensino Fundamental II com temas bem relevantes para nosso prosseguimento escolar, fazendo, assim, as boas interligações também entre as Unidades de Conhecimento.

## 3. Atividade 01: Habilidade EF09MA16 (BRASIL, 2018, p. 319)

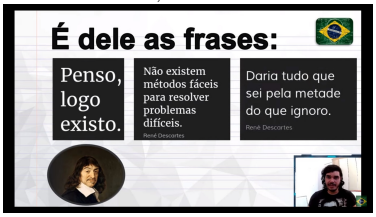
### 3.1 Objetivos

- Retomar o conceito de plano cartesiano e os elementos nele;
- Compreender o conceito de medida da distância entre 2 pontos no plano cartesiano;
- Usar o conceito de medida de distância entre 2 pontos no plano cartesiano para calcular a medida da Área de polígonos;
- Compreender o conceito de ponto médio de um segmento de reta.

### 3.2 Metodologia

Para iniciarmos nossa proposta, sugerimos que seja reproduzido o vídeo "René Descartes - Sua história, o Plano Cartesiano e a Geometria Analítica"[2] (Figura 1), pois nesse vídeo é tratado um pouco da história de René Descarte, que foi o matemático que sintetizou e desenvolveu o plano cartesiano que usamos hoje, que é a base para a obtenção da habilidade dessa etapa de ensino. Além de falar da história de René no vídeo, ele apresenta como foi pensado por ele inicialmente o plano cartesiano, faz alguns exemplos para encontrar pontos no plano cartesiano, e ainda dá uma introdução à Geometria Analítica, apresentando as contribuições de René.

Figura 1: René Descartes - Sua história, o Plano Cartesiano e a Geometria Analítica




Fonte: ⟨https://www.youtube.com/watch?v=M6BEWnLKECE⟩

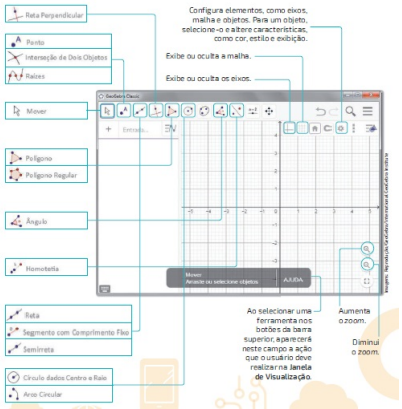
[1] O Primeiro par de letras indica a etapa de Ensino Fundamental; O primeiro par de números indica o ano a que se refere a habilidade; O segundo par de letras indica a componente curricular e o último par de números indica a posição da habilidade na numeração sequencial do ano

[2] Disponível de forma gratuita no Youtube, através do link: ⟨https://youtu.be/M6BEWnLKECE⟩

Após término do vídeo, o professor pode gerar um pequeno debate para ver o que eles lembram de plano cartesiano e também vê-lo em situações do dia-a-dia. Como no vídeo já mostra o básico deste conteúdo, que é traçar pontos, o docente pode fazer a ponte e já mostrar que também podemos analisar essa distância entre eles, podendo usar como exemplo o GPS, pois o globo terrestre é um grande plano cartesiano. Dando continuidade, o docente vai mostrar que, usando os pontos do plano cartesiano, conseguimos construir vários polígonos e, usando o conceito de distância entre pontos e de ponto médio de um segmento, calcular a Área desses polígonos. As atividades propostas aqui, serviram de base para treino e observação se os discentes conseguiram obter a habilidade dessa etapa do ensino.

Outro mecanismo que pode ser utilizado para potencializar o ensino do docente e a aprendizagem do discente é o GeoGebra[3]. Com essa ferramenta, o docente pode explorar desde as construções mais simples até as construções mais complexas, podendo, assim, ativar mais uma vez a curiosidade do discente em buscar o novo, e cada vez mais aprender novas coisas para testar no GeoGebra e ver os novos resultados obtidos. A Figura 2 apresenta um resumo das configurações básica do GeoGebra.

Figura 2: GeoGebra

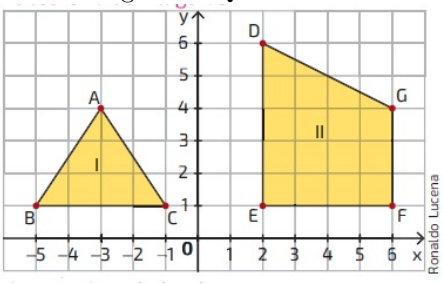



Fonte: (BALESTRI; PATARO, 2019)

## 4. Exercícios

Questão 1.1 – (BALESTRI; PATARO, 2019) Calcule a medida da Área e a medida do perímetro de cada uma das figuras representadas no plano cartesiano.

Figura 3: Questão 1.1




Fonte: (BALESTRI; PATARO, 2019)

[3]GeoGebra é um programa para computadores, ele é gratuito e apresenta várias ferramentas para ajudar no ensino do plano cartesiano, como: Construções geométrica, algébricas, gráficos, tabelas e cálculos. Podemos encontrar ele para *download* no link: ⟨https://www.geogebra.org/⟩

Questão 1.2 – (DANTE, 2019) Em uma malha quadriculada em centímetros, desenhe um sistema de eixos cartesianos e uma região retangular com medida de perímetro de 20 cm e medida de Área de 24 $cm^2$.

Ao propormos a Questão 1.1 tão direta, pretendemos deixar o caminho livre para o discente pensar e refletir seus conhecimentos e, assim, analisar se eles conseguem assimilar o caminho mais viável, que é usando a distância entre dois pontos e o ponto médio de um segmento, se ele conseguir realizar essa assimilação, podemos considerar que ele está bem encaminhado no que se diz respeito à habilidade dessa etapa. Ao propormos a Questão 1.2, queremos verificar se eles entenderam o suficiente dos conceitos estudados, para também realizar o processo inverso, isto é, dado a Área, encontrar a figura no plano cartesiano. E, para um melhor aproveitamento de material, o docente pode sugerir o uso do GeoGebra nessa questão, pois, com este *software*, eles terão a oportunidade de fazer vários testes e, em seguida, comparar com seus colegas. Para finalizar, o docente poderá comparar as figuras também, mostrando para o Cálculo de Área de figuras planas no plano cartesiano, não depende da posição da figura, ou seja, ela pode estar em qualquer dos quadrantes do planos, inclusive em mais de um, o que vai influenciar mesmo é a distância entre os pontos (vértice) da figura.

## 5. Conclusões

Diante do exposto, apresentamos uma análise da versão histórica do surgimento do Cálculo de Área proveniente da necessidade humana. Também apresentamos uma proposta didática baseada nas orientações didáticas da BNCC. Ressaltamos ainda, que na dissertação (FARIAS, 2021) apresentamos em detalhes esses materiais, como também diversos exemplos de outros exercícios que podem ser utilizados em sala de aula.

## Referências

BALESTRI, R.; PATARO, P. M. *Matemática Essencial 9°: Ensino Fundamental, Anos finais*. São Paulo: Editora Scipione, 2019. Citado na página 4.

BRASIL. *Diretrizes Curriculares Nacionais da Educação Básica*. Brasília,DF: MEC, SEB, DICEI, 2013. Citado na página 2.

BRASIL. *Base Nacional Curricular Comum*. [S.l.]: MEC/SEB, 2018. Citado 2 vezes nas páginas 2 e 3.

DANTE, L. R. *Teláris Matemática, 9°: Ensino Fundamental, Anos finais*. São Paulo: Editora Ática, 2019. Citado na página 5.

FARIAS, E. V. D. *Cálculo de Área: Da História à Prática Didática*. Dissertação (Mestrado Profissional em Matemática - PROFMAT): Universidade Federal de Campina Grande. Campina Grande, p. 114, 2021. Citado na página 5.

# PESQUISAS COM SALA DE AULA INVERTIDA E INSTRUÇÃO POR PARES NA MATEMÁTICA DO ENSINO MÉDIO

**Me. Suênia da Silva Rodrigues[1] - sueniaproinfo2012@gmail.com**
**Dr. Luiz Antônio da Silva Medeiros[2] - luiz.silva@professor.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil
[2]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil

***Resumo:*** *O presente trabalho tem por objetivo apresentar a análise de pesquisas desenvolvidas com a utilização de metodologias ativas no ensino médio, particularmente, na sala de aula invertida e a instrução por pares nos processos de ensino e de aprendizagem da Matemática . Para tal, a metodologia consistiu na busca das produções científicas disponibilizadas na Biblioteca Digital Brasileira de Teses e Dissertações - BDTD e, também, no Banco de Dissertações do PROFMAT. Os dados analisados revelaram diversas estratégias, públicos e conteúdos matemáticos aplicados na implementação das metodologias citadas. Além disso, os resultados apontam para o fato das metodologias ativas terem um efeito significativo na aprendizagem, no qual os alunos são estimulados a participar do processo de forma mais engajada, com mudanças de comportamentos e atitudes, concentração e motivação. Os resultados apontam ainda quebra nas abordagens tradicionais de ensino, proporcionando o um maior acompanhamento das aprendizagens e atribuição de novos papéis aos alunos e professores.*
***Palavras-chave****: Sala de Aula Invertida; Instrução por pares; Ensino de Matemática*

## 1. Introdução

Um dos grandes desafios dos professores de Matemática é despertar, nos alunos, o interesse em construir conhecimentos matemáticos. Para muitos teóricos, essa motivação inicial para aprender é uma condição necessária à ocorrência da aprendizagem, porém a aversão da matemática parece ser senso comum, provocada, na maioria das vezes, por uma abordagem mecânica que limita o processo cognitivo do aluno em relação à disciplina. Sendo assim, torna-se necessário que o professor tenha concepção da importância de refletir, sempre que preciso, sobre suas metodologias e práticas pedagógicas. A reflexão contribui para uma prática docente engajada com o processo educativo, que permite aprimorar as ações pedagógicas, identificar as técnicas e recursos que podem ser utilizados com maior eficiência em algum momento do planejamento. Para tal, o profissional de educação deve estar atento aos novos modelos educacionais e aos novos recursos que estão sendo empregados com sucesso, isso faz parte natural de uma qualificação que evolui com a sociedade e deve ser incorporada quando for conveniente.

Nesse sentido, as metodologias ativas são bastante adequadas, uma vez que permitem maior autonomia para a realização das atividades escolares em outros ambientes e horários e com isso, assegurar a rotina escolar e possibilitar o desenvolvimento de habilidades importantes para formação, protagonismo e engajamento do aluno. A partir desse pressuposto, nossa proposta de pesquisa apresenta o seguinte objetivo:

- Apresentar a análise de algumas produções científicas sobre como as Metodologias Ativas, Sala de Aula Invertida e Peer Instruction (tradução livre, Instruções por pares), estão sendo utilizadas nos processos de ensino e de aprendizagem da Matemática do ensino Médio.

A sala de aula invertida é uma modalidade do ensino híbrido, onde sua estratégia sugere inverter o ensino tradicional para construir um ambiente de aprendizagem ativa em que os alunos sejam incentivados a participar de discussões e atividades práticas (EDUCAUSE, 2012), ou seja, o conceito é basicamente "[...] fazer em casa o que tradicionalmente era feito em aula e em aula o trabalho que era feito em casa" (BERGMANN; SAMS, 2019, p. 11). Esta estratégia de ensino pode ser organizada por meio de diferentes aulas e atividades remotas, e os alunos podem usar

> [...] material antes de ele frequentar a sala de aula, que passa a ser o lugar de aprender ativamente, realizando atividades de resolução de problemas ou projetos, discussões, laboratórios etc., com o apoio do professor e colaborativamente dos colegas (VALENTE, 2014, p. 79).

A metodologia pedagógica *Peer Instruction*, também denominada instrução por pares ou aprendizagem por pares, caracteriza-se como uma ferramenta ativa, cujo objetivo é envolver os alunos em atividades cooperativas de discussão de conteúdos para efetiva aprendizagem. Conforme Araujo e Mazur (2013), o *Peer Instruction* pode ser definido como um método que baseia-se no estudo prévio dos materiais fornecidos pelo professor e na apresentação de questões conceituais em sala de aula para que os alunos possam discutir entre si. Tem como objetivo promover a aprendizagem dos conceitos básicos dos conteúdos a serem estudados através da colaboração entre alunos.

Portanto, ao realizar a busca pelas produções científicas, procuramos destacar a relevância de trazer à tona um levantamento das investigações realizadas acerca das Metodologias Ativas, Sala de Aula Invertida e Peer Instruction, além de proporcionar a ampliação teórica acerca das temáticas, que têm produzido bons resultados do ponto de vista do aproveitamento dos alunos(VALENTE, 2018).

## 2. Metodologia

Como mencionado anteriormente, a busca das produções científicas consistiu em consulta na Biblioteca Digital Brasileira de Teses e Dissertações - BDTD e, também, no Banco de Dissertações do PROFMAT. Dessa forma, visando atende o nosso objetivo, estabelecemos algumas etapas:

- 1) levantamento de dados
- 2) organização e tratamento dos dados

Inicialmente, fizemos uma busca utilizando o descritor "sala de aula invertida" no título foram encontrados 55 trabalhos, e numa outra busca com o descritor *Peer Instruction*, 16 trabalhos (dados coletados até dezembro de 2020). Na sequência, filtramos cada descritor por área de matemática, conforme apresentamos na Tabela 1.

Tabela 1: Pesquisas que consideraram o(s) descritor(es) Sala de Aula Invertida e/ou *Peer Instruction* no Ensino de Matemática- Dados da BDTD/PROFMAT. Elaborado pelo próprio autor.

| DESCRITOR | TOTAL |
|---|---|
| Sala de Aula Invertida | 20 |
| Peer Instruction | 1 |
| Sala de Aula Invertida e Peer Instruction | 1 |

Por fim, concentramos-nos em publicações implementadas e direcionadas ao Ensino de Matemática dos alunos do Ensino Médio, como evidenciamos na Tabela 2.

Tabela 2: Trabalhos que consideraram o(s) descritor(es) Sala de Aula Invertida e/ou *Peer Instruction* no Ensino Médio - Dados da BDTD/PROFMAT. Elaborado pelo próprio autor.

| DESCRITOR | PESQUISAS |
|---|---|
| Sala de Aula Invertida | 5 |
| Peer Instruction | 0 |
| Sala de Aula Invertida e Peer Instruction | 1 |

A seguir, as pesquisas encontradas são apresentadas destacando os seus objetivos, qual o tipo de pesquisa, as atividades propostas para o público alvo, o conteúdo abordado, o desenvolvimento do planejamento, os principais resultados e as conclusões.

## 3. Resultado e discussão

### METODOLOGIAS ATIVAS: O ENSINO APRENDIZAGEM DE MATEMÁTICA NO ENSINO MÉDIO NA PERSPECTIVA DA SALA DE AULA INVERTIDA

O trabalho do autor Joelson Magno Dias teve por objetivo geral projetar e testar uma proposta metodológica baseada no modelo de Sala de Aula Invertida, utilizando os meios tecnológicos disponíveis pelos estudantes do 1º ano do Ensino Médio da rede pública estadual da cidade de Santarém-PA (DIAS, 2019, p. 27).

A pesquisa classificada como exploratória foi desenvolvida por meio de três sequências didáticas envolvendo os conteúdos: revisão de radiciação; funções e equações exponenciais; definição de logaritmo e suas consequências; e um projeto construído, executado e apresentado na III Jornada Científica da escola (DIAS, 2019, p. 44).

O autor destaca que a sala de aula ultrapassa o espaço físico, uma vez que se pode construir espaços digitais de aprendizagem, compartilhamento de informações e construção do conhecimento fora do ambiente escolar e ressalta também que a criação do Google sala de aula e do *WhatsApp* para compartilhamento das informações com as turmas foram espaços fundamentais na organização das atividades da SAI. Para o autor, houve algumas dificuldades apresentadas pelos estudantes quanto ao acesso as TDIC, no entanto, a maioria possuía um aparelho celular que comportava as atividades metodológicas (DIAS, 2019, p. 96).

### O ENSINO DE CILINDRO E DA PIRÂMIDE ATRAVÉS DA SALA DE AULA INVERTIDA

O trabalho de autoria de Anselmo Luís Corrêa da Silva teve o objetivo de analisar o ensino de cilindro e da pirâmide através da aplicação da metodologia Sala de Aula Invertida na 3ª série do Ensino Médio, utilizando recursos tecnológicos para despertar o interesse e realizar atividades para que o estudante se torne o protagonista de sua aprendizagem (SILVA et al., 2019, p. 1).

Durante a implementação da proposta, o autor utilizou em suas aulas alguns recursos tecnológicos para visualização dos sólidos em 3D, como, por exemplo, o *software* educativo GeoGebra, voltado para o ensino da matemática e o ambiente virtual de aprendizagem *Moodle* para disponibilizar listas de exercícios, slides e as videoaulas. Para o autor, a pesquisa foi satisfatória e alcançou os objetivos esperados, tendo em vista que houve uma evolução na aprendizagem. No entanto, uma das dificuldades encontradas foi o curto período de aplicação da proposta, em virtude do pesquisador não ser professor da turma e não disponibilizar de mais tempo (SILVA et al., 2019, p. 43).

### SALA DE AULA INVERTIDA: UM EXPERIMENTO NO ENSINO DE MATEMÁTICA

O trabalho realizado por Neylane Lobato dos Santos trouxe como objetivo "investigar a utilização da abordagem pedagógica Sala de Aula Invertida no ensino de Matemática, com apoio de tecnologia, em uma escola estadual da rede pública, com alunos do 2º ano do Ensino Médio" (SANTOS, 2019b, p. 19).

A pesquisa, de cunho qualitativo, foi desenvolvida por meio de atividades envolvendo o conteúdo Trigonometria, onde foram utilizados os recursos de videoaulas e a ferramenta Google Classroom, além da formação de grupos com 4 alunos, em momentos presenciais, para resolução de questões contextualizadas envolvendo o assunto estudado.

A autora destaca que a implementação da metodologia Sala de Aula Invertida apoiada a utilização das TDIC motivou grande parte dos alunos, uma vez que mostraram interesse pelas aulas de Matemática, refletindo no desempenho alcançado por cada um, com resultados positivos para aqueles que se dedicaram. "O grande desafio encontrado foi a questão da conectividade, que muitos alunos não possuem regularmente e a escola também não disponibiliza para eles" (SANTOS, 2019b, p. 86).

### SALA DE AULA INVERTIDA: UMA PROPOSTA PARA O ENSINO DE PROBABILIDADE

De autoria de Josie Pacheco de Vasconcellos Souza, o trabalho teve como objetivo a implementação da metodologia Sala de Aula Invertida em uma turma da 3ª série do Ensino Médio do Colégio Estadual Doutor Olímpio Saturnino de Brito, localizado no município de São João da Barra – RJ, com suporte nas tecnologias educacionais e nas ferramentas colaborativas para o ensino de Probabilidade (SOUZA, 2019, p. 19).

A pesquisa é de caráter exploratório, utilizando uma abordagem qualitativa por meio de intervenção pedagógica, onde buscou-se verificar como a modalidade de ensino denominada Ensino Híbrido, em particular a Sala de aula Invertida, pode auxiliar no processo de ensino e aprendizagem (SOUZA, 2019, p. 63).

Segundo a autora, durante a experimentação das atividades, os alunos contribuíram de forma valorosa para o andamento do trabalho, onde todos demonstraram grande interesse, realizam com entusiasmo e participaram ativamente. Houve boa aceitação das videoaulas, uma vez que foram assistidas com agrado e quase sempre com facilidade, informações obtidas através dos relatos pelos próprios alunos (SOUZA, 2019, p. 131).

### SALA DE AULA INVERTIDA: REVOLUCIONANDO A FORMA DE ENSINAR E DE APRENDER MATEMÁTICA

O trabalho do autor Edmilson Chaves dos Santos teve por objetivo analisar os resultados obtidos na implementação da metodologia da Sala de Aula Invertida em uma turma da 1ª série do Ensino Médio Regular, numa Instituição de Ensino Estadual – Almakazir Gally Galvão – localizada no Estado da Bahia, na cidade de Coaraci, e comparar com os resultados obtidos em outra turma (grupo de controle) da mesma série, do mesmo colégio e do mesmo professor, na qual foi mantida a metodologia tradicional de ensino. Ambas as turmas estavam estudando exatamente o mesmo conteúdo, Função Quadrática, durante o mesmo período de tempo (SANTOS, 2019a, p. 2).

Os dados coletados a partir da aplicação da proposta "foram base de uma minuciosa análise tanto quantitativa como qualitativa do desempenho e opiniões dos alunos acerca da participação na execução da referida proposta" (SANTOS, 2019a, p. 2).

Para o autor, "este trabalho mostrou como uma mudança do modelo de ensino tradicional para o invertido pode alterar o humor tanto do professor como de uma classe inteira, proporcionando-lhes uma nova visão sobre o ensino e a aprendizagem da matemática" (SANTOS, 2019a, p. 59).

### MÉTODOS COMBINADOS: SALA DE AULA INVERTIDA E PEER INSTRUCTION COMO FACILITADORES DO ENSINO DE MATEMÁTICA

A pesquisa foi desenvolvida por Helio Valdemar Damião Freire durante o 2º bimestre (maio e junho) dos anos de 2017 e 2018 em turmas diversificas do 2º ano do Ensino Médio e teve como "objetivo verificar se a utilização de métodos combinados, como Sala de Aula Invertida e *Peer Instruction* (Instrução por Pares), pode contribuir positivamente para o processo de ensino e aprendizagem de Matemática" (FREIRE, 2019, p. 12). O conteúdo matemático abordado durante a aplicação dos métodos foi Matrizes.

Dentre os principais resultados apontados pelo autor estão a assiduidade, os métodos que implicaram na diminuição da evasão escolar e no excesso de faltas. Quanto a postura dos alunos, estes se mostraram mais motivados e encorajados para participar das aulas, além do respeito mútuo entre eles. Também foi notória a melhoria no desempenho nas avaliações formal e tradicional solicitadas pela escola (FREIRE, 2019, p. 64). O autor concluiu que os métodos combinados proporcionaram aprendizagens significativas (FREIRE, 2019, p. 74).

## 4. Conclusões

A educação é imprescindível ao desenvolvimento humano. Enxergar o aluno como protagonista é dar a ele a capacidade de desempenhar um papel ativo na construção do seu aprendizado, tomando decisões mais claras e acertadas para além da escola. Diante do supradito, esta pesquisa teve como objetivo geral apresentar uma análise de como as Metodologias Ativas, Sala de Aula Invertida e *Peer Instruction*, podem contribuir no processo de ensino e aprendizagem da Matemática dos alunos do Ensino Médio. Tal objetivo foi alcançado visto que o trabalho conseguiu verificar que professores e pesquisadores têm estudado melhorias para o processo de ensino-aprendizagem de Matemática e as Metodologias Ativas integrada as novas tecnologias são alternativas para este progresso.

**Agradecimentos**

A UFCG por todo ambiente inspirador e pela oportunidade de concluir este curso. Aos professores do PROFMAT-UFCG, pela dedicação, competência, apoio e todo conhecimento compartilhado, especialmente, ao meu orientador, Prof. Drº. Luiz Antônio da Silva Medeiros.

**Referências**

ARAUJO, I. S.; MAZUR, E. Instrução pelos colegas e ensino sob medida: uma proposta para o engajamento dos alunos no processo de ensino-aprendizagem de física. *Caderno brasileiro de ensino de física. Florianópolis Vol. 30, n. 2 (ago. 2013), p. 362-384*, 2013. Citado na página 2.

BERGMANN, J.; SAMS, A. *Sala de aula invertida: uma metodologia ativa de aprendizagem*. [S.l.]: Rio de Janeiro: LTC, 2019. Citado na página 1.

DIAS, J. M. *Metodologias ativas: o ensino aprendizagem de matemática no ensino médio na perspectiva da sala de aula invertida*. Tese (Doutorado) — Universidade Federal do Oeste do Pará, 2019. Acesso em, 10 Mai. de 2021. Disponível em: ⟨https://repositorio.ufopa.edu.br/jspui/handle/123456789/294⟩. Citado na página 3.

EDUCAUSE, C. Things you should know about flipped classrooms. *Retrieved from*, 2012. Acesso em, 25 Out. 2020. Disponível em: ⟨https://library.educause.edu/resources/2012/2/7-things-you-should-know-about-flipped-classrooms⟩. Citado na página 1.

FREIRE, H. V. D. a. *Métodos combinados: Sala de Aula Invertida e Peer Instruction como facilitadores do ensino da matemática*. Tese (Doutorado) — Universidade de São Paulo, 2019. Acesso em, 10 Mai. de 2021. Disponível em: ⟨https://www.teses.usp.br/teses/disponiveis/97/97138/tde-06112019-162934/pt-br.php⟩. Citado na página 4.

SANTOS, E. C. d. *Sala de Aula Invertida: revolucionando a forma de ensinar e de aprender matemática*. Tese (Doutorado) — Universidade Estadual de Santa Cruz, 2019. Acesso em, 10 Mai. de 2021. Disponível em: ⟨https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?cpf=99400316534&d=20200116074854&h=f5d02318301a3e5950cd03e79946582e84eb0569⟩. Citado na página 4.

SANTOS, N. L. d. *Sala de aula invertida: um experimento no ensino de Matemática*. Tese (Doutorado) — Universidade Federal do Oeste do Pará, 2019. Acesso em, 10 Mai. de 2021. Disponível em: ⟨https://repositorio.ufopa.edu.br/jspui/handle/123456789/296⟩. Citado na página 3.

SILVA, A. L. C. d. et al. *O ensino do cilindro e da pirâmide através da sala de aula invertida*. Tese (Doutorado) — Universidade Federal do Amazonas, 2019. Acesso em, 10 Mai. de 2021. Disponível em: ⟨https://tede.ufam.edu.br/handle/tede/7538⟩. Citado na página 3.

SOUZA, J. P. d. V. *Sala de Aula Invertida: uma proposta para o ensino de probabilidade*. Tese (Doutorado) — Universidade Estadual do Norte Darcy Ribeiro, 2019. Acesso em, 10 Mai. de 2021. Disponível em: ⟨https://uenf.br/posgraduacao/matematica/wp-content/uploads/sites/14/2020/02/170460031_JOSIE_PACHECO_DE_VASCONCELLOS_SOUZA.pdf⟩. Citado na página 4.

VALENTE, J. A. Blended learning e as mudanças no ensino superior: a proposta da sala de aula invertida. *Educar em revista*, SciELO Brasil, n. 4, p. 79–97, 2014. Acesso em, 04 Jan. de 2021. Disponível em: ⟨https://www.scielo.br/pdf/er/nspe4/0101-4358-er-esp-04-00079⟩. Citado na página 2.

VALENTE, J. A. A sala de aula invertida e a possibilidade do ensino personalizado: uma experiência com a graduação em midialogia. *Metodologias ativas para uma educação inovadora: uma abordagem teórico-prática. Porto Alegre: Penso*, p. 26–44, 2018. Citado na página 2.