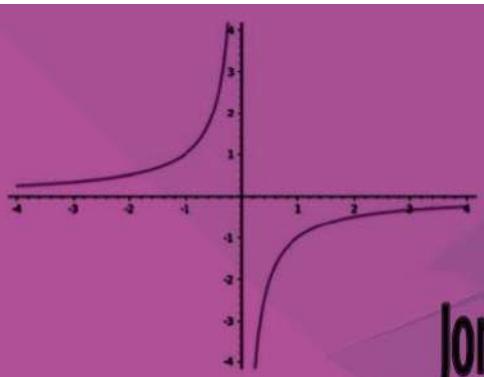
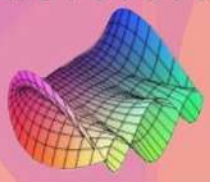


JEEPEMA

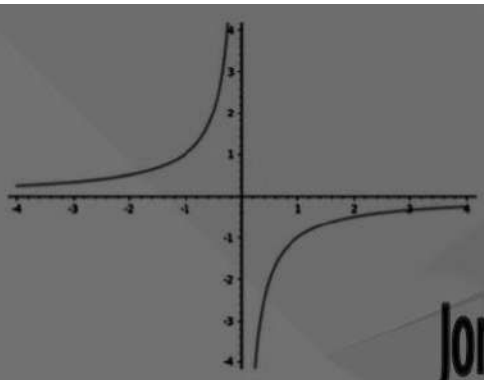
Jornal eletrônico de Ensino e Pesquisa de matemática

Cálculo Diferencial e Integral:

Exercícios • Apostilas • Resoluções • Vídeos Aulas •



um kit de sobrevivência!

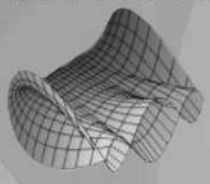


JEEPEMA

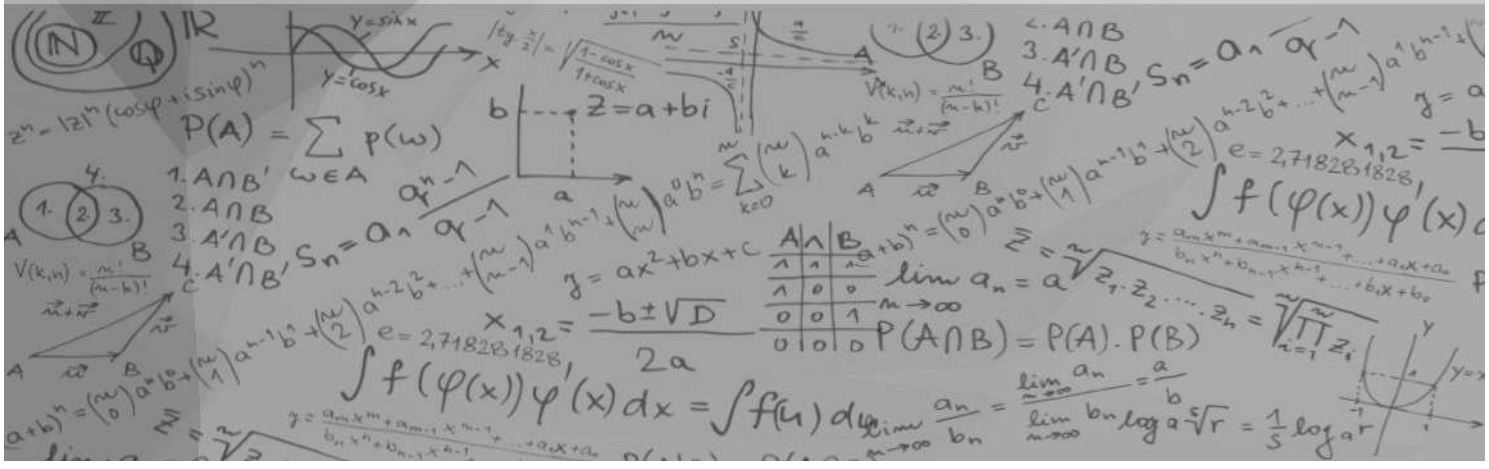
Jornal eletrônico de Ensino e Pesquisa de matemática

Cálculo Diferencial e INTEGRAL:

Exercícios • Apostilas • Resoluções • Vídeos Aulas •



um kit de sobrevivência!



Jornal Eletrônico de Ensino de Matemática - JEEPEMA
Universidade Estadual de Maringá, Maringá-PR - Brasil
ISSN: 2594-6323
DOI: 10.4025/jeepema

Vol. 5 N° 1 / 53 páginas - Julho/2021

Palavras-chave: Conjuntos, Análise Real, Física Quântica, Taxa de Variação, Polinômios Ortogonais, SageMath, Cálculo Diferencial, Criptografia, Curvas Elípticas.

Índice

Volume 5 - N° 1

Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v.5** 1 (2021): 1–15. ©Jeepema–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Conjuntos infinitos enumeráveis e não-enumeráveis: Aplicações na física quântica

Gabriel Costa Vieira Arantes – Email: gabriel.prof.exatas@gmail.com, Clóves Gonçalves Rodrigues – Email: cloves@pucgoias.edu.br
Escola de Formação de Professores e Humanidades, Pontifícia Universidade Católica de Goiás, 74605-010, CP 86, Goiânia, Goiás, Brazil

Resumo: O enfoque principal deste trabalho é o estudo dos conjuntos infinitos sob a ótica da Análise Real. São apresentados teoremas e definições importantes sobre o tema, com algumas aplicações concretas no campo da física quântica.
Palavras-chave: Conjuntos infinitos, conjuntos enumeráveis, conjuntos não-enumeráveis, análise real, física quântica.

1. Introdução

Conjuntos infinitos podem ser classificados em enumeráveis e não-enumeráveis, de acordo com a sua natureza. O matemático Georg Cantor foi o primeiro a constatar que existem diferentes tipos de conjuntos infinitos, fato este que culminou na sua teoria dos números cardinais. Apesar de ser um tema abstrato, a noção de enumerabilidade dos conjuntos infinitos é valiosa para a Física Estatística, especialmente no que diz respeito aos fenômenos de caráter aleatório e/ou probabilístico. Veremos que uma das hipóteses acerca da Equação de Onda na Mecânica Quântica assegura que o conjunto de soluções para $\Psi(x,t)$ é infinito e não-enumerável, onde $\Psi(x,t)$ é a função de onda associada. Um argumento para convencer o leitor da importância deste tema é o fato que diversos problemas físicos apresentam conjuntos de soluções infinitos, onde surge o interesse em saber se estes são enumeráveis ou não. Além disso, todo fenômeno físico é modelado em um espaço métrico, cuja estrutura topológica está fundamentada numa métrica estabelecida sobre um conjunto infinito. Algumas definições e teoremas importantes sobre o tema são apresentados na Seção 2, e aplicações práticas no estudo de fenômenos físicos são apresentados na Seção 3. A Seção 4 se reserva às conclusões e comentários finais.

2. Enumerabilidade em Análise Real

O ponto de partida para o estudo da enumerabilidade em Análise Real (Lima, 2017a, 2017b) é o conjunto dos números naturais ($\mathbb{N}$), que é definido por meio dos Axiomas de Peano:

(1) Existe uma função injetiva $s : \mathbb{N} \to \mathbb{N}$ tal que, para todo $n \in \mathbb{N}$, dizemos que $s(n)$ é o sucessor de n, onde $s(n) \in \mathbb{N}$. Nota: $s(n) = n + 1$.

(2) Existe um único número natural $1 \in \mathbb{N}$ que não é sucessor de nenhum outro número natural pela função $s : \mathbb{N} \to \mathbb{N}$. Em símbolos: $\exists! 1 \in \mathbb{N}; 1 \notin s(\mathbb{N})$. Isto significa que a função sucessor $s : \mathbb{N} \to \mathbb{N}$ não é sobrejetiva, pois $s(\mathbb{N}) = \mathbb{N} - \{1\}$, logo tem-se $s(\mathbb{N}) \neq \mathbb{N}$.

(3) (Princípio da Indução) Dado $X \subset \mathbb{N}$, se $1 \in X$ e $s(X) \subset X$, então $X = \mathbb{N}$. Nota: $s(X) \subset X$ significa dizer que $s(n) \in X$, para todo $n \in X$. Noutras palavras, dado $X \subset \mathbb{N}$, se o natural 1 pertence a X e, para cada elemento n de X, o seu sucessor $s(n)$ também pertence a X, então X é o próprio conjunto dos números naturais ($X = \mathbb{N}$).

O Axioma (3) de Peano recebe o nome de Princípio da Indução em $\mathbb{N}$. Ele será utilizado em diversas demonstrações dos teoremas que vêm a seguir. Basicamente, a fim de provar que determinada propriedade P é válida para todo número natural $n \in \mathbb{N}$, devemos mostrar que P vale para $n = 1$, e, posteriormente, devemos provar que P vale para $s(n) = n + 1$, admitindo, pela hipótese de indução, que P vale para n. Em valores lógicos, demonstrar que uma propriedade P vale para todo número natural $n \in \mathbb{N}$ significa provar que:

$$P(1) \text{ é verdadeira e } P(n) \Rightarrow P(s(n)), \forall n \in \mathbb{N},$$

então $P(n)$ é verdadeira $\forall n \in \mathbb{N}$, onde $P(n)$ ser verdadeira é a hipótese de indução.

Faz-se necessário apresentar o Princípio da Boa-Ordenação em $\mathbb{N}$, que será muito útil na demonstração do Teorema 2.1 adiante. Trata-se do 2º Princípio da Indução. O Princípio da Boa-Ordenação afirma que todo subconjunto não-vazio $A \subset \mathbb{N}$ possui um menor elemento.

Prosseguimos para a definição formal de conjunto infinito. Vamos admitir, sem maiores detalhes, que o conjunto $\mathbb{N}$ dos números naturais é infinito. O leitor interessado pode consultar a demonstração em (Lima, 2017a, 2017b). Assim, dizemos que o conjunto X é infinito quando existe uma função injetiva $f : \mathbb{N} \to X$. Isto significa que, se X é infinito, então $card(X) \geq card(\mathbb{N})$, onde $card(\ )$ indica a cardinalidade, que é uma função que associa a cada conjunto o número natural que corresponde à quantidade de elementos pertencentes a este conjunto. Vale salientar que a função injetiva $f : \mathbb{N} \to X$ é definida por indução

em $n \in \mathbb{N}$. Para isso, tomamos inicialmente $f(1) \in X$. Então, para cada $k \in \mathbb{N}$, escolhemos $f(k) \in A_k = X - \{f(1), f(2), ..., f(k-1)\}$. Pela hipótese de indução, supomos definidos $f(1), f(2), ..., f(n)$ e escrevemos $A_{n+1} = X - \{f(1), f(2), ..., f(n)\}$, onde $A_{n+1} \subset X$ é não-vazio, pois X é infinito. Assim, basta tomar $f(n+1) \in A_{n+1}$. Isto completa a definição de $f : \mathbb{N} \to X$. A injetividade de f decorre do fato que, dados $m, n \in \mathbb{N}$, digamos com $m < n$, tem-se $f(m) \in \{f(1), f(2), ..., f(n-1)\}$ e $f(n) \in X - \{f(1), f(2), ..., f(n-1)\}$, logo $f(m) \neq f(n)$.

Conjuntos infinitos podem ser classificados em enumeráveis ou não-enumeráveis. Por definição, todo conjunto finito é enumerável. Porém, como o foco principal deste trabalho são os conjuntos infinitos, daremos atenção especial ao que torna um conjunto infinito enumerável. Dizemos que um conjunto infinito X é enumerável quando existe uma bijeção $f : \mathbb{N} \to X$. Isto significa que, se X é infinito e enumerável, então $card(X) = card(\mathbb{N})$. Noutras palavras, podemos afirmar que os conjuntos infinitos enumeráveis são, de certa forma, os "menores infinitos"que existem. Em matemática e em física, existem infinitos maiores que outros. Por conseguinte, dizemos que um conjunto infinito X é não-enumerável quando não existe sobrejeção $f : \mathbb{N} \to X$, ou seja, $f(\mathbb{N}) \neq X$ para toda função $f : \mathbb{N} \to X$. Isto significa que, se X é infinito e não-enumerável, então $card(X) > card(\mathbb{N})$.

Portanto, todo conjunto enumerável possui uma enumeração do tipo $X = \{x_1, x_2, ..., x_n, ...\}$. Basta definir $f(1) = x_1, f(2) = x_2, ..., f(n) = x_n, ...$ a partir da bijeção $f : \mathbb{N} \to X$. Resumidamente, um conjunto infinito X é enumerável quando x_{k+1} está bem definido para todo elemento $x_k \in X$ arbitrário. Dizemos que x_{k+1} é o próximo elemento de X após x_k. Esta noção nos permite verificar intuitivamente que o conjunto $\mathbb{R}$ dos números reais é não-enumerável, pois dado qualquer número real $x \in \mathbb{R}$, é impossível afirmar qual é o próximo número real. Para entender este fato, pense no seguinte exemplo: dado $1,001 \in \mathbb{R}$, qual é o próximo número real? $1,00101$? $1,001001$? $1,0010001$? ...? $1,001000...0001$? Não há como dizer. Pensando no conjunto dos números naturais, temos que $\mathbb{N}$ é obviamente enumerável, pois existe pelo menos a bijeção trivial $f : \mathbb{N} \to \mathbb{N}$, dada por $f(n) = n$ para todo $n \in \mathbb{N}$, que é a função identidade. Por outro lado, podemos verificar intuitivamente que $\mathbb{N}$ é enumerável pensando no seguinte fato: para todo $n \in \mathbb{N}$, o Axioma (3) de Peano assegura que $s(n) = n + 1 \in \mathbb{N}$, onde $s(n)$ é o sucessor de n pela função injetiva $s : \mathbb{N} \to \mathbb{N}$. Logo, o número natural $s(n) \in \mathbb{N}$ está bem definido para todo $n \in \mathbb{N}$, onde $s(n)$ é o próximo natural após n. Isto permite definir uma enumeração do conjunto dos números naturais, pondo $\mathbb{N} = \{n_1, n_2, ..., n_k, ...\} = \{1, s(1), s(s(1)), ..., s^k(1), ...\}$. De maneira simplificada, dizemos que o conjunto $\mathbb{N}$ dos números naturais é enumerável porque podemos contar os seus elementos. O mesmo não pode ser dito para $\mathbb{R}$.

Prosseguiremos para os teoremas referentes aos conjuntos infinitos enumeráveis. Estes

teoremas serão de grande valor para os estudos da Física Estatística e da Mecânica Quântica, bem como das suas particularidades, onde estão envolvidas variáveis aleatórias e condições probabilísticas em meio aos fenômenos físicos investigados.

Teorema 2.1 *Todo subconjunto infinito $X \subset \mathbb{N}$ é enumerável.*

Demonstração: Definiremos uma enumeração do subconjunto infinito $X \subset \mathbb{N}$ por indução. Usaremos aqui o Princípio da Boa-Ordenação em $\mathbb{N}$. Começamos tomando $x_1 = minX$. Daí, definimos $A_1 \subset X$ tal que $A_1 = X - \{x_1\}$. Tomamos então $x_2 = minA_1$ e definimos $A_2 \subset X$ tal que $A_2 = X - \{x_1, x_2\}$. Prosseguindo indutivamente, supomos definido $A_n \subset X$ tal que $A_n = X - \{x_1, x_2, ..., x_n\}$. Daí, basta tomar $x_{n+1} = minA_n$. Obtemos desta maneira uma enumeração do subconjunto infinito $X \subset \mathbb{N}$ dada por $X = \{x_1, x_2, ..., x_n, \ldots\}$, com $x_1 = minX$ e $x_{k+1} = minA_k$ para todo $k \in \mathbb{N}$, onde $A_k = X - \{x_1, x_2, ..., x_k\}$. ◥

Teorema 2.2 *Sejam X, Y conjuntos infinitos e $f : X \to Y$ uma função injetiva. Se Y é enumerável, então X também é.*

Demonstração: Se Y é infinito e enumerável, então existe uma bijeção $g : \mathbb{N} \to Y$. Além disso, se $f : X \to Y$ é injetiva, então $f(X) \subset Y$. Daí, podemos obter uma bijeção $f|_{f(X)} : X \to f(X)$ restringindo o contradomínio da função original $f : X \to Y$ ao subconjunto $f(X) \subset Y$. Mais ainda, como $g : \mathbb{N} \to Y$ é bijetiva, deve existir $A \subset \mathbb{N}$ tal que $g|_{f(X)} : A \to f(X)$ também é bijeção. Pelo Teorema 2.1, temos que $A \subset \mathbb{N}$ é enumerável, donde $g|_{f(X)} : A \to f(X)$ bijeção implica em $f(X)$ enumerável. Por sua vez, $f|_{f(X)} : X \to f(X)$ bijeção implica em X enumerável. ◥

Teorema 2.3 *Sejam X, Y conjuntos infinitos e $f : X \to Y$ uma função sobrejetiva. Se X é enumerável, então Y também é.*

Demonstração: Com efeito, basta tomar para cada $y \in Y$ um elemento $g(y) \in X$ e definir a partir daí uma função $g : Y \to X$ tal que $f(g(y)) = y$ para todo $y \in Y$. A nova função $g : Y \to X$ assim definida é injetiva. Para verificar este fato, basta tomar $g(y_1) \neq g(y_2) \in X$ genéricos, donde obtemos que $f(g(y_1)) \neq f(g(y_2)) \Rightarrow y_1 \neq y_2$. A função g é a inversa à direita de f. Pelo Teorema 2.2, se $g : Y \to X$ é injetiva e X é enumerável por hipótese, então Y também é enumerável. ◥

Teorema 2.4 *Sejam X, Y conjuntos infinitos e enumeráveis. O produto cartesiano $X \times Y$ também é enumerável.*

Demonstração: Sejam X, Y conjuntos infinitos e enumeráveis. Por definição, temos que existem bijeções $f : \mathbb{N} \to X$ e $g : \mathbb{N} \to Y$. Em particular, podemos considerar que existem sobrejeções $f : \mathbb{N} \to X$ e $g : \mathbb{N} \to Y$. Definimos a partir daí uma função sobrejetiva $F : \mathbb{N} \times \mathbb{N} \to X \times Y$ pondo $F(m, n) = (f(m), g(n))$ para todo $m, n \in \mathbb{N}$. Pelo Teorema 2.3, basta provar que $\mathbb{N} \times \mathbb{N}$ é enumerável. Com efeito, tomando a função $\Psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $\Psi(m, n) = 2^m.3^n$, temos que Ψ é injetiva, devido à unicidade da decomposição de números naturais em fatores primos, assegurada pelo Teorema Fundamental da Aritmética. Pelo Teorema 2.2, como a função $\Psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ é injetiva e $\mathbb{N}$ é enumerável, então $\mathbb{N} \times \mathbb{N}$ é enumerável.

◥

Teorema 2.5 *A reunião de uma família enumerável de conjuntos enumeráveis é enumerável. Em outra notação, se $(X_\lambda)_{\lambda \in L}$ é uma família enumerável cujos elementos são conjuntos enumeráveis, então a reunião $\bigcup_{\lambda \in L} X_\lambda$ também é enumerável.*

Demonstração: Consideremos uma família enumerável $(X_\lambda)_{\lambda \in L}$ cujos elementos são conjuntos enumeráveis $X_1, X_2, ..., X_n, \ldots$. Por definição, temos que existem bijeções $f_1 : \mathbb{N} \to X_1$, $f_2 : \mathbb{N} \to X_2, \ldots, f_n : \mathbb{N} \to X_n, \ldots$. Em particular, podemos considerar que existem sobrejeções $f_1 : \mathbb{N} \to X_1, f_2 : \mathbb{N} \to X_2, \ldots, f_n : \mathbb{N} \to X_n, \ldots$. Seja $\bigcup_{n=1}^{\infty} X_n$ a reunião de todos os elementos de $(X_\lambda)_{\lambda \in L}$. Definimos a partir daí uma função sobrejetiva $F : \mathbb{N} \times \mathbb{N} \to \bigcup_{n=1}^{\infty} X_n$ pondo $F(m, n) = f_n(m)$ para todo $m, n \in \mathbb{N}$, isto é, pondo $F(m, n)$ igual à n-ésima função, f_n, aplicada ao natural m. Como já foi provado no Teorema 2.4 que $\mathbb{N} \times \mathbb{N}$ é enumerável, segue do Teorema 2.3 que se $F : \mathbb{N} \times \mathbb{N} \to \bigcup_{n=1}^{\infty} X_n$ é sobrejetiva, então a reunião $\bigcup_{n=1}^{\infty} X_n = \bigcup_{\lambda \in L} X_\lambda$ (a igualdade anterior induz a concluir que L é infinito excluindo-se o caso em que L é finito, esta é a intenção?) é enumerável.

◥

É importante ressaltar que a notação $A \equiv B$ significa que os conjuntos A e B são equipotentes, isto é, que A e B possuem o mesmo número de elementos. Portanto, afirmar que $A \equiv B$ equivale a escrever $card(A) = card(B)$, ou seja, dois conjuntos são equipotentes se, e somente se, possuem a mesma cardinalidade. Mais precisamente, se os conjuntos A e B são equipotentes, então existe uma relação biunívoca entre eles, dada pela função bijetiva $f : A \to B$.

Teorema 2.6 *Todo conjunto infinito contém um subconjunto infinito enumerável.*

Demonstração: Seja X um conjunto infinito. Consideremos inicialmente que X é enumerável. Neste caso, basta considerar $A = X$. Temos que A é um subconjunto de X e A é infinito enumerável.

Consideremos agora que X é não-enumerável. Logo, não existe sobrejeção $\mathbb{N} \to X$. Por definição, se X é infinito, então deve existir uma função injetiva $h : \mathbb{N} \to X$. Segue-se daí que $card(X) > card(\mathbb{N})$ e $h(\mathbb{N}) \subset X$. Além disso, podemos obter uma bijeção $h|_{h(N)} : \mathbb{N} \to h(\mathbb{N})$ restringindo o contradomínio da função original $h : \mathbb{N} \to X$ ao subconjunto $h(\mathbb{N}) \subset X$. Portanto, se $h|_{h(N)} : \mathbb{N} \to h(\mathbb{N})$ é uma bijeção, então $card(\mathbb{N}) = cardh(\mathbb{N})$, isto é, $N \equiv h(\mathbb{N})$. Consequentemente, $h(\mathbb{N}) \subset X$ é infinito enumerável. ◥

O resultado do Teorema 2.6 é de importância para o estudo dos fenômenos físicos probabilísticos, cujos domínios geralmente são conjuntos infinitos não-enumeráveis de variáveis aleatórias. A fim de estabelecer uma lei matemática para essas variáveis, de modo que se obtenha uma solução determinística para o fenômeno físico estudado, é interessante analisar um subconjunto infinito de variáveis do domínio original que seja enumerável, cuja existência é assegurada pelo Teorema 2.6. Por exemplo, pensando na Física Estatística, imagine a seguinte situação: o pesquisador está modelando um fenômeno puramente probabilístico, cujo domínio de variáveis aleatórias é caracterizado por um conjunto infinito não-enumerável. Considere ainda que o conjunto de soluções do problema não pode ser determinado analiticamente, mas apenas numericamente. O pesquisador conseguirá encontrar as soluções do problema através de métodos numéricos, mas não será capaz de estabelecer uma lei matemática que rege o fenômeno estudado para todo o domínio. Um fator problemático neste cenário pode ser justamente a não-enumerabilidade do domínio de variáveis aleatórias que descrevem os parâmetros do fenômeno investigado.

Diante desta situação, é importante destacar a relevância dos estudos matemáticos referentes à perturbação de domínios dos fenômenos físicos. De maneira simplificada, perturbação de domínio é a alteração intencional realizada sobre o corpo de elementos que constituem o domínio do fenômeno estudado. Por exemplo, o ato de restringir uma função genérica $f : X \to Y$ a um subconjunto $X' \subset X$ do seu domínio original, consequentemente obtendo a restrição $f|_{X'} : X' \to Y$, implica uma perturbação do domínio da função $f : X \to Y$. Retomando o cenário descrito anteriormente, se o pesquisador está interessado em resolver analiticamente um problema físico de caráter aleatório e/ou probabilístico, ainda que isto seja impossível para todo o conjunto de variáveis do problema original, ele pode investigar se há uma perturbação do domínio que permita determinar uma lei matemática capaz de modelar o fenômeno físico restrito às variáveis do novo subconjunto obtido após a perturbação. Explorando mais a fundo, seja $f : X \to Y$ a função genérica que modela determinado fenômeno físico. Consideremos que o domínio X desta função é um conjunto infinito não-enumerável. O pesquisador pode investigar uma possível perturbação do domínio de $f : X \to Y$ que resulte num subconjunto infinito $A \subset X$, de tal modo que A seja enumerável. O subconjunto $A \subset X$ do domínio de $f : X \to Y$ munido destas características certamente existe, devido ao

resultado provado no Teorema 2.6. Assim, o problema do pesquisador se reduz a descobrir como perturbar o domínio original do fenômeno físico estudado, de tal modo que se obtenha um subconjunto enumerável deste.

Resumindo, é mais fácil estabelecer um padrão matemático para um conjunto infinito enumerável que para um conjunto infinito não-enumerável, mesmo que isto resulte em uma lei que modele apenas parte do fenômeno físico estudado, isto é, uma lei que valha apenas para uma restrição do seu domínio. Isto porque um conjunto infinito enumerável possui, por definição, uma bijeção com o conjunto $\mathbb{N}$ dos números naturais, ou seja, ele pode ser enumerado, o que por si só resulta em um padrão matemático que permite saber, a partir de qualquer elemento deste conjunto, quem é o seu próximo elemento (reveja a definição de enumerabilidade apresentada previamente, onde utilizou-se a notação em símbolos). Além disso, a obtenção de uma solução analítica para o fenômeno físico estudado, restringindo-o a um certo subconjunto enumerável de variáveis, mesmo que não seja uma solução forte, já é algo de grande valor.

Em algumas situações, o método descrito nos parágrafos anteriores, cuja validade é assegurada pelo Teorema 2.6, pode não ser suficiente para estabelecer uma lei matemática capaz de fornecer soluções analíticas, mesmo que de maneira restrita. Nestes casos, o pesquisador ainda dispõe de outra ferramenta. é possível fracionar o subconjunto infinito enumerável $A \subset X$ do domínio de $f : X \to Y$, obtido a partir do método anterior, em partes enumeráveis $A_n \subset A, n \in \mathbb{N}$, originando cisões. Então, o subconjunto $A \subset X$ passa a ser analisado como a reunião de uma família enumerável de partes enumeráveis $A_n \subset A, n \in \mathbb{N}$. Em outra notação, temos $(A_n)_{n\in\mathbb{N}}$, onde $\bigcup_{n=1}^{\infty} A_n = A$. Deste modo, o pesquisador limita seu problema à investigação de leis matemáticas que expliquem o fenômeno físico estudado para cada parte enumerável $A_n \subset A, n \in \mathbb{N}$. A partir daí, é possível descartar as partes de $(A_n)_{n\in\mathbb{N}}$ indesejadas, restando apenas aquelas que podem ser modeladas analiticamente. As partes enumeráveis $A_\lambda \subset A, \lambda \in L$ de interesse do pesquisador, isto é, aquelas que de fato apresentam soluções analíticas, podem ser reunidas novamente, obtendo um novo subconjunto $\bigcup_{\lambda\in L} A_\lambda = \bar{A}$, onde $\bar{A} \subset A$. Pelo Teorema 2.5, temos que a reunião $\bigcup_{\lambda\in L} A_\lambda = \bar{A}$ é enumerável, pois $(A_\lambda)_{\lambda\in L}$ é uma família enumerável de partes enumeráveis $A_\lambda \subset A$, $\lambda \in L$.

Os fenômenos de perturbação de domínios constituem um dos principais objetos de estudo dos Sistemas Dinâmicos, um campo da física matemática destinado à investigação de funções que descrevem a evolução ao longo do tempo de sistemas definidos em espaços topológicos (Brin, 2015). Portanto, as noções de conjunto infinito e de enumerabilidade são de grande valor para o estudo dos sistemas que evoluem com o tempo. Estes sistemas são geralmente descritos por meio de Equações Diferenciais Parciais, onde podemos destacar os fenômenos físicos da Mecânica Celeste moderna, principalmente os estudos sobre a evolução de galáxias,

que podem ser interpretadas matematicamente como sistemas dinâmicos.

Vejamos a seguir alguns exemplos concretos e aplicações práticas.

3. Aplicações e Exemplos

3.1. Método da Diagonal de Georg Cantor

Discutimos na Seção 2 um método que possibilita a obtenção de subconjuntos infinitos enumeráveis a partir de qualquer conjunto não-enumerável, com base nos resultados demonstrados no Teorema 2.5 e no Teorema 2.6. Veremos neste exemplo um método que propõe o caminho inverso. Estamos falando do Método da Diagonal, um raciocínio desenvolvido pelo matemático alemão Georg Cantor em 1891, visando a obtenção de conjuntos não-enumeráveis a partir de conjuntos infinitos enumeráveis (Lima, 2017a). Foi com base neste método que Cantor comprovou a existência de conjuntos infinitos com naturezas distintas. Seja X um conjunto infinito enumerável e Y um conjunto arbitrário contendo pelo menos dois elementos. Consideremos que o símbolo $F(X;Y)$ representa o conjunto $F(X;Y) = \{X, Y \subset \mathbb{R};$ existe $f : X \to Y\}$ cujos elementos são todas as funções $f : X \to Y$ possíveis. O raciocínio de Cantor afirma que nenhuma função $\varphi : X \to F(X;Y)$ é sobrejetiva. Inicialmente, o argumento do Método da Diagonal, devido a Georg Cantor, foi enunciado para o caso particular da função $\varphi : \mathbb{N} \to F(\mathbb{N};\{0,1\})$, onde $X = \mathbb{N}$ e $Y = \{0,1\}$. Somente depois este raciocínio foi demonstrado para o caso mais geral, com base no mesmo argumento, consolidando-se como teorema. Veremos somente a demonstração do caso particular, visando a definição do nosso método de interesse. A fim de verificar que $\mathbb{N} \to F(\mathbb{N};\{0,1\})$ não é sobrejetiva, basta definir indutivamente $\varphi(1) = s_1$, $\varphi(2) = s_2$, ..., $\varphi(n) = s_n, \ldots$, onde s_1, s_2, ..., s_n, ... são sequências cujos termos são elementos do conjunto $\{0,1\}$. Seja s_{m_n} o n-ésimo termo da sequência s_m. Então, sempre será possível obter uma nova sequência s^* diferente de todas as anteriores, simplesmente tomando $s^*_n = 0$ se for $s_{m_n} = 1$ ou então $s^*_n = 1$ se for $s_{m_n} = 0$. Isto significa que nenhuma lista enumerável pode esgotar todas as funções do conjunto $F(\mathbb{N};\{0,1\})$. Este resultado será fundamental para a demonstração a seguir. Seja $X \subset \mathbb{R}$ um conjunto infinito e enumerável. Consideremos o conjunto $P(X) = \{A \subset \mathbb{R};$ A é subconjunto de $X\}$ das partes de X. Tomando novamente $Y = \{0,1\}$ no Método da Diagonal de Cantor, vamos provar que existe uma função $\xi : P(X) \to F(X;\{0,1\})$ bijetiva. Para cada subconjunto $A \subset X$, isto é, para cada elemento de $P(X)$, definimos uma função restrita $\xi|_A : X \to \{0,1\}$ tal que, para todo $x \in X$, tem-se $\xi|_A(x) = 1$ se $x \in A$ e $\xi|_A(x) = 0$ se $x \notin A$. Portanto, obtemos a bijeção $\xi : P(X) \to F(X;\{0,1\})$ que relaciona $A \mapsto \xi|_A$ para todo $A \in P(X)$. Vimos que a função $\varphi : X \to F(X;\{0,1\})$ não pode ser sobrejetiva. Então, certamente a composta $\xi^{-1} \circ \varphi : X \to P(X)$ não é sobrejetiva. No entanto,

existe uma injetividade trivial $\psi : X \to P(X)$ dada por $\psi(x) = \{x\}$ para todo $x \in X$. Resulta daí que $card(X) < cardP(X)$. Por hipótese, tomamos um conjunto infinito arbitrário $X \subset \mathbb{R}$ de natureza enumerável, logo temos $card(X) = card(\mathbb{N})$. Consequentemente, obtemos $card(\mathbb{N}) < cardP(X)$. Por definição, isto significa que o conjunto das partes de X dado por $P(X) = \{A \subset \mathbb{R}; A \text{ é subconjunto de } X\}$ é não-enumerável, seja qual for o conjunto infinito enumerável $X \subset \mathbb{R}$ considerado. Em resumo, o Método da Diagonal de Georg Cantor nos permite obter um conjunto não-enumerável $P(X)$ a partir de qualquer conjunto infinito enumerável $X \subset \mathbb{R}$ que tivermos. Para isso, basta definir $P(X)$ como sendo o conjunto das partes de X. O raciocínio que acabamos de examinar é muito simples e poderoso, apesar do teor abstrato da sua demonstração. O Método da Diagonal de Cantor será contextualizado no Exemplo 3.4 mais adiante para provar um resultado muito interessante da Física Teórica: todo fenômeno físico cuja natureza é discreta pode ser extrapolado de modo a obter uma interpretação contínua do seu conjunto de soluções, que pode ter validade prática ou não.

3.2. Hipótese da Linearidade de $\Psi(x,t)$ na Equação de Onda da Mecânica Quântica

A equação fundamental da mecânica quântica foi apresentada pelo físico austríaco Erwin Schrödinger em 1925. Estamos falando da equação de onda de Schrödinger, um marco na história da ciência moderna. Ela é uma equação diferencial parcial (EDP) de 2ª ordem cujas soluções são chamadas de funções de onda e simbolizadas por $\Psi(x,t)$ (Eisberg, 1974). Estas funções, por sua vez, descrevem o comportamento das partículas subatômicas, portanto, constituem a base do conhecimento quântico. A equação de onda unidimensional, devida a Schrödinger, é dada pela seguinte expressão:

$$-\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2} + V(x,t)\Psi(x,t) = i\hbar\frac{\partial\Psi(x,t)}{\partial t}$$

onde m é a massa da partícula, $\hbar$ é a constante de Planck reduzida, $i = \sqrt{-1}$ é o número imaginário e $V(x,t)$ é a energia potencial da partícula. A principal motivação de Schrödinger para obter esta equação foi a hipótese de De Broglie sobre a natureza dual da matéria. Também é possível obter a equação de onda de Schrödinger a partir de quatro hipóteses, ou axiomas, que justificam a validade desta equação. Uma delas é a hipótese da linearidade de $\Psi(x,t)$. Esta hipótese afirma que a Equação de Onda deve ser linear em $\Psi(x,t)$. Isto significa que se $\Psi_1(x,t)$ e $\Psi_2(x,t)$ são duas soluções distintas da Equação de Onda para uma dada energia potencial $V(x,t)$ da partícula, então qualquer combinação linear arbitrária $\Psi(x,t) = \alpha_1\Psi_1(x,t) + \alpha_2\Psi_2(x,t)$ também é solução, onde α_1, α_2 são constantes.

Obviamente, o conjunto de soluções da Equação de Onda proposta por Schrödinger é

infinito, em virtude da arbitrariedade das combinações lineares. Noutras palavras, existem infinitas Funções de Onda $\Psi(x,t)$ que satisfazem esta equação. Seja Ω o conjunto de todas essas funções $\Psi(x,t)$. Vamos provar que Ω é não-enumerável. Fixando duas soluções $\Psi_1(x,t)$ e $\Psi_2(x,t)$ da Equação de Schrödinger, podemos definir o subconjunto $\Omega' \subset \Omega$ dado por $\Omega' = \{\Psi(x,t) \in \Omega; \Psi(x,t) = \alpha_1\Psi_1(x,t) + \alpha_2\Psi_2(x,t) \wedge \alpha_1, \alpha_2 \in \mathbb{R}\}$. O símbolo $\wedge$ representa o operador lógico da conjunção, que equivale ao conectivo "e"da gramática. Como $\Omega' \subset \Omega$, temos que $card(\Omega') \leq card(\Omega)$. Logo, basta mostrar que Ω' é não-enumerável. Para isso, definimos a bijeção $\mathcal{F} : \mathbb{R} \times \mathbb{R} \to \Omega'$ dada por $\mathcal{F}(\alpha_1, \alpha_2) = \alpha_1\Psi_1(x,t) + \alpha_2\Psi_2(x,t)$. Sabemos que o conjunto $\mathbb{R}$ dos números reais é não-enumerável. Além disso, vale $card(\mathbb{R}) \leq card(\mathbb{R} \times \mathbb{R})$. Por definição, resulta daí que $\mathbb{R} \times \mathbb{R}$ também é não-enumerável. Finalmente, como $\mathcal{F}$ é uma bijeção entre $\mathbb{R} \times \mathbb{R}$ e Ω', então o subconjunto $\Omega' \subset \Omega$ é não-enumerável. Em suma, acabamos de provar que o conjunto de soluções $\Omega(\Psi)$ da Equação de Onda proposta por Schrödinger é não-enumerável. Em virtude deste fato, valem as seguintes conclusões:

1. O conjunto Ω não possui bijeção com $\mathbb{N}$. Consequentemente, card $\Omega > card(\mathbb{N})$.

2. Todos os fenômenos da Mecânica Quântica que cumprem a Equação de Schrödinger são contínuos, pois a natureza não-enumerável do conjunto Ω assegura que é impossível quantizá-los para todo o espectro das Funções de Onda $\Psi(x,t) \in \Omega$.

3. De acordo com o resultado demonstrado no Teorema 2.6, existe pelo menos um subconjunto infinito de Ω que é enumerável. Seja $\Omega'' \subset \Omega$ este subconjunto. Podemos definí-lo facilmente a partir do conjunto auxiliar Ω' utilizado na prova anterior. Basta limitar os coeficientes das combinações lineares de Ω' apenas aos números naturais. Deste modo, obtemos o subconjunto $\Omega'' = \{\Psi(x,t) \in \Omega; \Psi(x,t) = n_1\Psi_1(x,t) + n_2\Psi_2(x,t) \wedge n_1, n_2 \in \mathbb{N}\}$. A fim de verificar que $\Omega'' \subset \Omega$ é enumerável, consideramos a bijeção $\mathcal{F} : \mathbb{N} \times \mathbb{N} \to \Omega''$ dada por $\mathcal{F}(n_1, n_2) = n_1\Psi_1(x,t) + n_2\Psi_2(x,t)$. Vimos na demonstração do Teorema 2.4 que $\mathbb{N} \times \mathbb{N}$ é enumerável. Portanto, o subconjunto $\Omega'' \subset \Omega$ também o é.

4. Uma interpretação muito interessante da conclusão anterior pode ser enunciada da seguinte maneira: todo fenômeno quântico que cumpre a Equação de Onda proposta por Schrödinger é quantizável numa dada restrição do seu domínio. Para isso, basta limitar a hipótese da linearidade da Equação de Onda em $\Psi(x,t)$ de modo que os coeficientes permitidos para as combinações lineares sejam números naturais. Em geral, todos os conjuntos de soluções não-enumeráveis que descrevem fenômenos físicos de natureza contínua possuem subconjuntos infinitos enumeráveis que satisfazem os casos particulares quantizáveis destes fenômenos. Estes casos particulares, por sua vez, possuem

natureza discreta. Esta afirmação também é sustentada pelo Teorema 2.6.

3.3. Quantização da Energia, Fótons de Luz e Equação de Planck (1900)

No ano de 1900, o físico alemão Max Planck publicou sua teoria sobre a quantização da energia luminosa, numa tentativa de explicar o problema da Radiação do Corpo Negro, que estava em aberto desde 1860 devido às observações experimentais realizadas principalmente por Gustav Kirchhoff. A famosa Equação de Planck foi capaz de descrever, com êxito, o fenômeno da emissão do Corpo Negro, através de uma teoria completamente inovadora (Eisberg, 1974). Planck sugeriu que a energia E das ondas eletromagnéticas estacionárias, oscilando senoidalmente com o tempo, seria uma grandeza discreta em vez de contínua. Assim, Planck sugere que

$$E = n(h\nu), n \in \mathbb{N}$$

onde h é uma constante (denominada posteriormente de constante de Planck) e ν a frequência da onda eletromagnética correspondente. Fixando a frequência ν, consideremos o conjunto $\Gamma = \{E = n(h\nu); n \in \mathbb{N}\}$ de todas as energias permitidas para as ondas eletromagnéticas desta radiação. Evidentemente, este conjunto é infinito, pois para cada múltiplo natural $n = 1, 2, 3, ...$ associa-se um valor de energia. A fim de provar que o conjunto $\Gamma(E)$ é enumerável, basta definir a bijeção $\mathcal{F} : \mathbb{N} \to \Gamma(E)$ dada por $\mathcal{F}(n) = n(h\nu)$ para todo $n \in \mathbb{N}$. Isto demonstra matematicamente que os fenômenos quânticos que cumprem a Equação de Planck são discretos. É interessante notar que, no campo de estudo da Física, os fenômenos contínuos sempre são associados a conjuntos não-enumeráveis, enquanto que os fenômenos discretos são associados a conjuntos infinitos enumeráveis. Isto decorre diretamente da existência (ou não) de uma restrição destes fenômenos ao conjunto $\mathbb{N}$ dos números naturais, ou a qualquer outro conjunto equipotente a ele, por exemplo, $\mathbb{N} \times \mathbb{N}$.

3.4. As Relações entre o Discreto e o Contínuo na Física

Realizamos uma discussão geral sobre os fenômenos físicos de natureza contínua e mostramos que eles estão associados a conjuntos não-enumeráveis. Neste contexto, destacamos como exemplo a Equação de Onda da Mecânica Quântica. Em virtude do resultado demonstrado no Teorema 2.6, vimos que existem casos particulares destes fenômenos contínuos que são descritos por conjuntos enumeráveis. Isto define uma condição quantizável do fenômeno original para uma dada restrição do seu domínio, conferindo a ele uma interpretação discreta. Este resultado, é claro, permanece no campo da Física Teórica. Não obstante, a existência de uma relação entre a natureza dos fenômenos físicos e a natureza dos conjuntos infinitos é um fato no mínimo curioso.

Neste ponto, sabemos que é possível obter o discreto a partir do contínuo. Discutimos bastante sobre o significado físico desta restrição, que caracteriza uma perturbação do domínio que rege o fenômeno estudado. No entanto, ainda não analisamos o caminho inverso. Eis que levantamos o seguinte questionamento: podemos definir um fenômeno físico de natureza contínua a partir de um caso discreto, ou seja, quantizável? O Método da Diagonal de Georg Cantor, discutido na Seção 1, nos dá a resposta. Vamos provar que, de fato, é possível obter o contínuo a partir do discreto. Para isso, consideremos novamente o caso da Equação de Planck. Dada uma radiação qualquer de frequência ν do espectro eletromagnético, seja o conjunto $\Gamma = \{E = n(h\nu); n \in \mathbb{N}\}$ de todas as energias permitidas para as ondas eletromagnéticas. Conforme a análise realizada na Seção 3.3, vimos que o conjunto Γ é infinito e enumerável. Por conseguinte, o Método da Diagonal nos permite obter facilmente o conjunto não-enumerável $P(\Gamma) = \{A \subset \mathbb{R}; A \text{ é subconjunto de } \Gamma\}$ cujos elementos são as partes de Γ. Este conjunto pode ser interpretado, em termos físicos, como a reunião de todos os eventos da natureza em que a Equação de Planck faz sentido, para alguma restrição dos múltiplos naturais de $h\nu$ a um subconjunto de $\mathbb{N}$. Procedendo desta maneira, obtemos um caso contínuo, isto é, não-enumerável, a partir dos fenômenos quânticos discretos que obedecem a Equação de Planck.

O conjunto $\Gamma = \{E = n(h\nu); n \in \mathbb{N}\}$ é enumerável porque descreve as energias permitidas para as ondas de uma radiação eletromagnética específica, cuja frequência ν é fixa. Se, por outro lado, considerarmos o conjunto $\Upsilon = \{E = n(h\nu); n \in \mathbb{N}, \nu \in \mathbb{R}\}$ de todas as energias permitidas para as ondas de qualquer radiação do espectro eletromagnético, então temos que Υ é um conjunto não-enumerável, pois existe uma bijeção clara $\mathcal{F} : \mathbb{N} \times \mathbb{R} \to \Upsilon$ dada por $\mathcal{F}(n, \nu) = n(h\nu)$ para todo $n \in \mathbb{N}$ e $\nu \in \mathbb{R}$, onde o produto cartesiano $\mathbb{N} \times \mathbb{R}$ é evidentemente não-enumerável. Portanto, a natureza não-enumerável do conjunto Υ nos permite inferir que o espectro eletromagnético em sua totalidade é contínuo, o que condiz com a teoria da Física sobre as ondas eletromagnéticas.

3.5. O Princípio da Indução e a Hipótese da Linearidade da Equação de Schrödinger

Foi comentado na Seção 3.2 que foram admitidas quatro hipóteses, ou axiomas, em relação à equação de onda da mecânica quântica (também conhecida por equação de Schrödinger). Estas hipóteses justificam a sua validade e fundamentam uma possível demonstração da mesma. Na Seção 3.2, investigamos a hipótese da linearidade da Equação de Schrödinger em $\Psi(x, t)$, a partir da qual provamos a natureza não-enumerável do conjunto de soluções Ω. Esta hipótese afirma que, se $\Psi_1(x, t)$ e $\Psi_2(x, t)$ são duas soluções distintas da Equação de Onda para uma dada energia potencial $V(x, t)$ da partícula, então qualquer combinação

linear arbitrária $\Psi(x,t) = \alpha_1\Psi_1(x,t) + \alpha_2\Psi_2(x,t)$ também é solução, onde $\alpha_1, \alpha_2 \in \mathbb{R}$. Sejam $\Psi_1(x,t)$, $\Psi_2(x,t)$,..., $\Psi_n(x,t)$,... soluções da Equação de Schrödinger. Por conseguinte, temos:

$$-\frac{\hbar^2}{2m}\frac{\partial^2\Psi_1(x,t)}{\partial x^2} + V(x,t)\Psi_1(x,t) - i\hbar\frac{\partial\Psi_1(x,t)}{\partial t} = 0$$

$$-\frac{\hbar^2}{2m}\frac{\partial^2\Psi_2(x,t)}{\partial x^2} + V(x,t)\Psi_2(x,t) - i\hbar\frac{\partial\Psi_2(x,t)}{\partial t} = 0$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

$$-\frac{\hbar^2}{2m}\frac{\partial^2\Psi_n(x,t)}{\partial x^2} + V(x,t)\Psi_n(x,t) - i\hbar\frac{\partial\Psi_n(x,t)}{\partial t} = 0$$

Pode ser provado, por indução em $n \in \mathbb{N}$, que a hipótese da linearidade é válida para toda combinação linear arbitrária destas soluções. Para $n = 1$, temos $\Psi^{(1)} = \alpha_1\Psi_1(x,t)$. Segue-se daí que:

$$\begin{aligned}
-\frac{\hbar^2}{2m}\frac{\partial^2\Psi^{(1)}}{\partial x^2} + V\Psi^{(1)} - i\hbar\frac{\partial\Psi^{(1)}}{\partial t} &= -\frac{\hbar^2}{2m}\frac{\partial^2(\alpha_1\Psi_1)}{\partial x^2} + V(\alpha_1\Psi_1) - i\hbar\frac{\partial(\alpha_1\Psi_1)}{\partial t} \\
&= \alpha_1\left(-\frac{\hbar^2}{2m}\frac{\partial^2\Psi_1}{\partial x^2}\right) + \alpha_1(V\Psi_1) - \alpha_1\left(i\hbar\frac{\partial\Psi_1}{\partial t}\right) \\
&= \alpha_1\left(-\frac{\hbar^2}{2m}\frac{\partial^2\Psi_1}{\partial x^2} + V\Psi_1 - i\hbar\frac{\partial\Psi_1}{\partial t}\right) \\
&= \alpha_1 \cdot (0) = 0.
\end{aligned}$$

Portanto, a combinação linear $\Psi^{(1)} = \alpha_1\Psi_1(x,t)$ é solução da Equação de Schrödinger. Prosseguindo com a demonstração, devemos admitir a hipótese de indução para $n \in \mathbb{N}$ e mostrar que a propriedade também vale para $n+1$. Sejam $\Psi_1(x,t)$, $\Psi_2(x,t)$,..., $\Psi_n(x,t)$, $\Psi_{n+1}(x,t)$ soluções da Equação de Schrödinger. A hipótese de indução consiste em admitir que a combinação linear

$$\Psi^{(n)}(x,t) = \alpha_1\Psi_1(x,t) + \alpha_2\Psi_2(x,t) + ... + \alpha_n\Psi_n(x,t)$$

é uma solução desta equação. Com base na hipótese de indução, devemos mostrar que

$$\Psi^{(n+1)} = \alpha_1\Psi_1(x,t) + \alpha_2\Psi_2(x,t) + ... + \alpha_n\Psi_n(x,t) + \alpha_{n+1}\Psi_{n+1}(x,t),$$

também satisfaz à Equação de Schrödinger. A fim de simplificar a notação, definimos

$$\Psi^{(n+1)} = \Psi^{(n)} + \alpha_{n+1}\Psi_{n+1}(x,t).$$

Assim, obtemos:

$$\begin{aligned}
-\frac{\hbar^2}{2m}\frac{\partial^2\Psi^{(n+1)}}{\partial x^2} + V\Psi^{(n+1)} - i\hbar\frac{\partial\Psi^{(n+1)}}{\partial t} &= -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}(\Psi^{(n)} + \alpha_{n+1}\Psi_{n+1}) \\
&\quad +V(\Psi^{(n)} + \alpha_{n+1}\Psi_{n+1}) - i\hbar\frac{\partial}{\partial t}(\Psi^{(n)} + \alpha_{n+1}\Psi_{n+1}) \\
&= -\frac{\hbar^2}{2m}\frac{\partial^2\Psi^{(n)}}{\partial x^2} - \frac{\hbar^2}{2m}\frac{\partial^2(\alpha_{n+1}\Psi_{n+1})}{\partial x^2} + V\Psi^{(n)} + V(\alpha_{n+1}\Psi_{n+1}) \\
&\quad -i\hbar\frac{\partial\Psi^{(n)}}{\partial t} - i\hbar\frac{\partial(\alpha_{n+1}\Psi_{n+1})}{\partial t} \\
&= \left(-\frac{\hbar^2}{2m}\frac{\partial^2\Psi^{(n)}}{\partial x^2} + V\Psi^{(n)} - i\hbar\frac{\partial\Psi^{(n)}}{\partial t}\right) + \\
&\quad \left(-\frac{\hbar^2}{2m}\frac{\partial^2(\alpha_{n+1}\Psi_{n+1})}{\partial x^2} + V(\alpha_{n+1}\Psi_{n+1}) - i\hbar\frac{\partial(\alpha_{n+1}\Psi_{n+1})}{\partial t}\right) \\
&= \left(-\frac{\hbar^2}{2m}\frac{\partial^2\Psi^{(n)}}{\partial x^2} + V\Psi^{(n)} - i\hbar\frac{\partial\Psi^{(n)}}{\partial t}\right) + \\
&\quad \alpha_{n+1}\left(-\frac{\hbar^2}{2m}\frac{\partial^2\Psi_{n+1}}{\partial x^2} + V\Psi_{n+1} - i\hbar\frac{\partial\Psi_{n+1}}{\partial t}\right) \\
&= (0) + \alpha_{n+1}(0) = 0,
\end{aligned}$$

ou seja, a combinação linear $\Psi^{(n+1)} = \Psi^{(n)} + \alpha_{n+1}\Psi_{n+1}(x,t)$ também é solução da Equação de Schrödinger. Isto completa a nossa demonstração. Portanto, acabamos de provar por indução que a hipótese da linearidade da Equação de Schrödinger é válida para quaisquer soluções $\Psi_1(x,t)$, $\Psi_2(x,t)$,..., $\Psi_n(x,t)$,... desta equação.

4. Comentários finais

Neste artigo, exploramos as relações entre o discreto e o contínuo com ênfase na Física Quântica. Mostramos que a hipótese da linearidade das funções de onda $\Psi(x,t)$ na Equação de Schrödinger pode ser provada através do Princípio da Indução, que é o 3º Axioma de Peano. Este princípio só vale para eventos matemáticos que possuem bijeção com o conjunto dos número naturais, isto é, fenômenos enumeráveis. Por outro lado, foi demonstrado que o conjunto Ω de todas as funções de onda permitidas pela Equação de Schrödinger é não-enumerável, o que significa que não existe uma bijeção entre $\mathbb{N}$ e Ω. Isto se deve ao princípio da superposição, que garante que se $\Psi_n(x,t)$ é uma sequência enumerável de funções de onda que solucionam a equação de Schrödinger para $n \in \mathbb{N}$, então a combinação linear $\sum\alpha_n\Psi_n(x,t)$ também é solução, onde $\alpha_n \in \mathbb{R}$. Portanto, podemos concluir que as funções de

onda $\Psi_n(x,t)$ da Mecânica Quântica possuem características discretas, isto é, enumeráveis, quando analisadas isoladamente. No entanto, o conjunto das possibilidades para $\Psi_n(x,t)$ é contínuo, isto é, não-enumerável. Isto reflete um fato muito intrigante do mundo quântico: dependendo da maneira como analisamos os fenômenos neste domínio, podemos observar comportamentos tanto discretos como contínuos. Neste artigo, também demonstramos algo similar para o caso da quantização da energia das ondas eletromagnéticas, em virtude da equação de Planck. Mostramos que cada faixa de frequência do espectro eletromagnético possui um conjunto infinito e enumerável da energia permitida para a onda eletromagnética, onde a frequência da onda permanece fixa. Este conjunto é dado por $\Gamma = \{E = n(h\nu); n \in \mathbb{N}\}$ e possui uma bijeção com $\mathbb{N}$. Isto significa que a energia da onda eletromagnética de cada faixa de frequência do espectro eletromagnético formam um conjunto discreto, ou seja, quantizado. Por outro lado, analisando o espectro eletromagnético em sua totalidade, onde a frequência das radiações $\nu \in \mathbb{R}$ é variável, provamos que o conjunto de todos os níveis de energia permitidos para as ondas eletromagnéticas destas radiações é não-enumerável. Este conjunto é dado por $\Upsilon = \{E = n(h\nu); n \in \mathbb{N}, \nu \in \mathbb{R}\}$ e não possui bijeção com $\mathbb{N}$. Em suma, concluímos que cada faixa de frequência do espectro eletromagnético apresenta um conjunto enumerável de níveis de energia, isto é, estes níveis são discretos. Por outro lado, o espectro eletromagnético em sua totalidade, com todas as suas possibilidades de feixes de radiações, apresenta um conjunto não-enumerável de níveis de energia, isto é, a energia total do espectro eletromagnético é contínua, apesar da mesma ser constituída por infinitos conjuntos discretos de níveis de energia. Desta forma, este artigo nos permite enfatizar de maneira analítica e matemática que os principais paradigmas e contradições da Mecânica Quântica são de fato originados pela dualidade entre o discreto e o contínuo.

Referências

1 BRIN, Michael; STUCK, Garrett. **Introduction to dynamical systems**. Cambridge: Cambridge university press, 2002.

2 LIMA, Elon Lages. **Análise Real**. 12. ed. Rio de Janeiro: IMPA–Projeto Euclides, 2017. v. 1.

3 _____. **Curso de Análise**. 14. ed. Rio de Janeiro: IMPA–Projeto Euclides, 2017. v. 1.

4 RESNICK, Robert; EISBERG, Robert et al. **Quantum physics of atoms, molecules, solids, nuclei, and particles**. New York: Wiley, 1974.

Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 5** 1 (2021): 16–21. ©Jeepema–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Taxa de variação de casos de COVID-19 com e sem vacinação

Marcelo Osnar Rodrigues de Abreu – Email: osnar@outlook.com

Resumo: O foco deste trabalho é apresentar como ferramentas de cálculo tais como polinômios ortogonais, ajuste de curvas e taxa de variação podem ser uteis na análise de dados.
Palavras-chave: taxa de variação, polinômios ortogonais, COVID-19.

1. Introdução

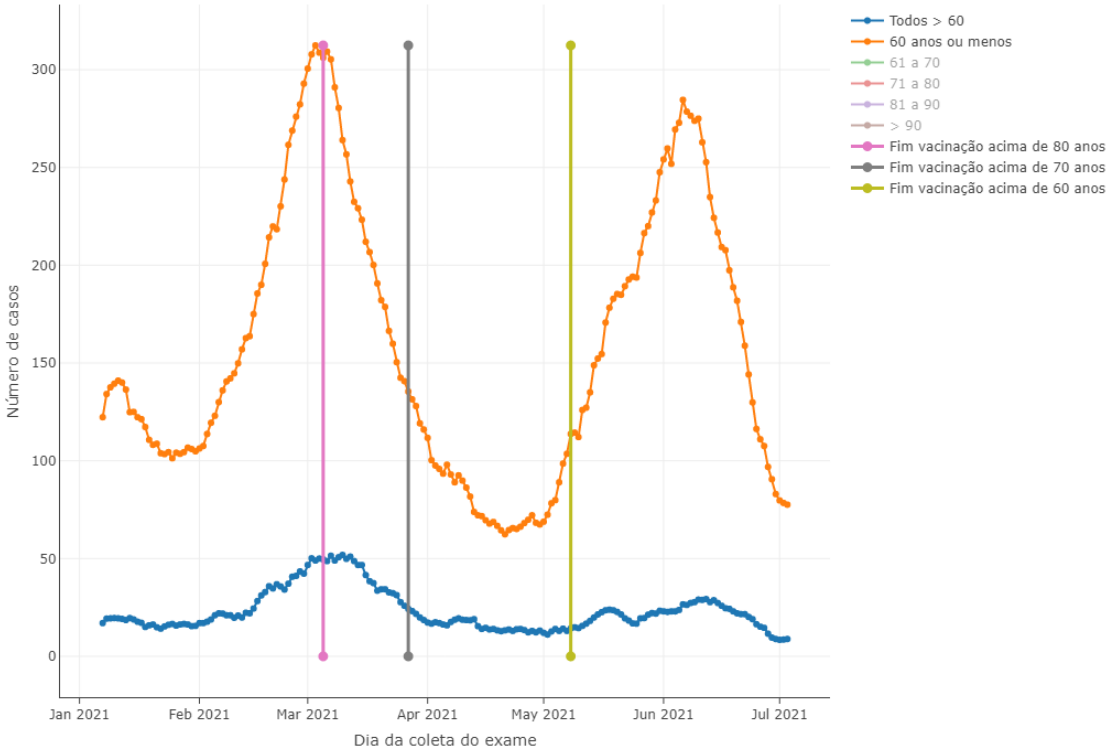
A vacinação tem avançado na cidade de Maringá e uma importante pergunta surge: está sendo eficaz? Os idosos, pessoas acima de 60 anos de idade, já iniciaram a vacinação há alguns meses e neste período tivemos uma nova "onda"[1] de COVID-19 onde podemos analisar o aumento no número de casos entre idosos e não idosos. Claramente, uma maneira mais precisa de se avaliar seria cruzar as informações de vacinados com casos positivos e ter uma informação precisa. No entanto pela não publicidade de informações das pessoas vacinadas este artigo tenta avaliar a eficácia da vacinação apenas com base nas informações sobre os casos positivos de COVID-19 na cidade de Maringá.

2. Dados do problema

Os dados analisados são da cidade de Maringá desde o início de 2021 até julho de 2021, que foram suavizados com uma média móvel semanal, a fim de que os comportamentos mais gerais da série temporal fossem evidenciados. A fim de compreender as tendências da série no grupo que recebeu e que não recebeu a vacina, os dados foram separados em duas curvas, sendo elas a representação dos casos no grupo de pessoas com 60 anos ou menos e outro grupo formado pelas pessoas com mais de 60 anos, conforme ilustrado a seguir:

[1] atualmente chama-se de onda um grande aumento na média de casos de COVID-19 em um curto período de tempo

Figura 1 – Medias móveis de 7 dias dos casos positivos de COVID-19 em Maringá



Fonte: Elaborada pelo autor

No início do ano, mais precisamente no dia 25/01/2021, quando ocorreu a menor média de casos antes de um novo pico, observou-se que a média de casos em pessoas com mais de 60 anos era de aproximadamente 16 casos, enquanto a média de casos em pessoas com menos de 60 anos era de aproximadamente 101 casos. Na sequência houve um aumento dos casos, que teve seu pico no mês de março. Neste período observou-se que a média de casos nas pessoas com menos de 60 anos triplicou atingindo 312 em 03/03/2021. O mesmo comportamento ocorreu no grupo acima de 60 anos, de 16 casos em média atingiu o pico de 51 casos em 07/03/2021. Entre março e abril ao mesmo tempo em que avançava a vacinação houve uma redução no número de casos que acreditamos ser devido às diversas medidas que foram tomadas na época. Entre as pessoas com 60 anos ou menos a média de casos foi reduzindo até atingir 62 casos em 21/04/2021. Na sequência observa-se um novo aumento expressivo no número de casos, atingindo a média de 284 casos em 06/06/2021. O pico da média atingiu 4.58 vezes a média antes do aumento. Já entre o grupo de pessoas acima de 60, a média atingiu seu pico de 29 em 10/06/2021, apenas 2.6 vezes o valor mínimo de 11 que ocorreu em 02/05/2021.

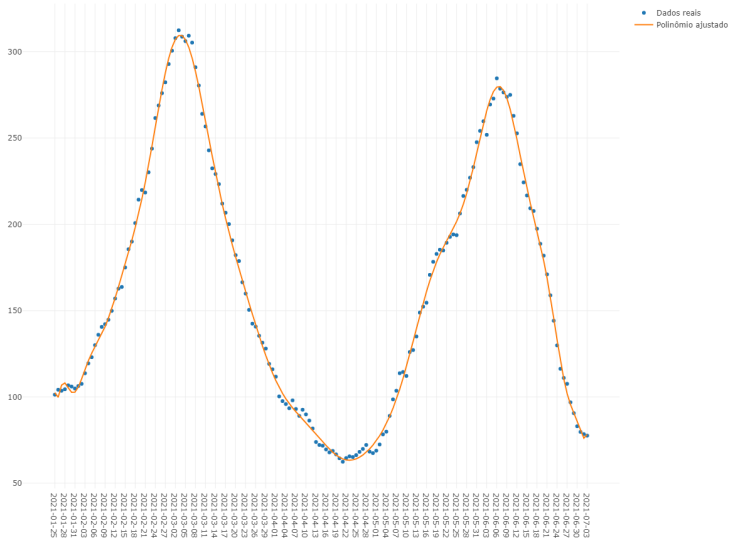
3. Taxa de variação

Na seção anterior vimos que tanto visualmente quanto uma verificação numérica dos pontos de máximo e mínimo local do gráfico apresentado na Figura 1 nos levam a acreditar que houve um menor crescimento nos casos entre pessoas com mais de 60 anos na segunda onda, em relação à primeira onda. No entanto, esta análise está sujeita ao viés do observador e não dá uma dimensão de quanto isto é expressivo ou não.

A fim de comparação, vamos dividir os dados em duas partes, sendo a primeira compreendendo o período de 25/01/2021 a 21/04/2021 (87 dias) e a segunda parte de 22/04/2021 a 03/07/2021 (73 dias). O ponto de corte foi escolhido como sendo 21/04/2021 pelo fato de que este é o ponto de mínimo local no gráfico dos casos em pessoas com 60 anos ou menos (que passaremos a chamar de *não idosos* para facilitar a escrita) e separa as duas "ondas".

Para suavizar os dados e facilitar o cálculo e a interpretação da taxa de variação, usamos um modelo de regressão polinomial. Dentre as diversas maneiras de se fazer isto optamos por utilizar a função **poly** da linguagem R. O ajuste consiste em determinar os coeficientes de um polinômio de grau n que melhor descreve o comportamento dos dados. Após realizar a modelagem dos dados concluiu-se que $n = 25$ é o mais apropriado. Para $n = 25$, a função descreve o polinômio ajustado a partir da base usual de polinômios $\{1, x, x^2, x^3, \ldots, x^{25}\}$. Outra abordagem, disponível pela função, é usar uma base de polinômios ortogonais descrita em Chambers e Hastie (1992). A Figura 2 apresenta o ajuste usando polinômios ortogonais, que apresentou um menor erro quadrático médio em relação à base usual.

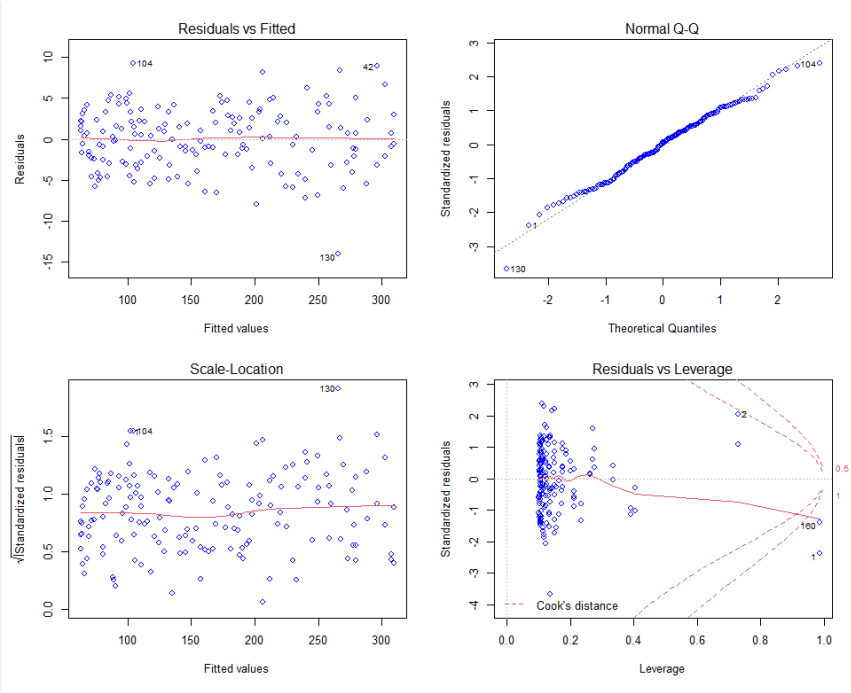
Figura 2 – Ajuste polinômio ortogonal de grau 25 aos dados dos *não idosos*



Fonte: Elaborada pelo autor

A além da inspeção visual empregou-se a análise dos resíduos para avaliar o ajuste.

Figura 3 – Análise de resíduos ajuste polinomial aos dados dos *não idosos*

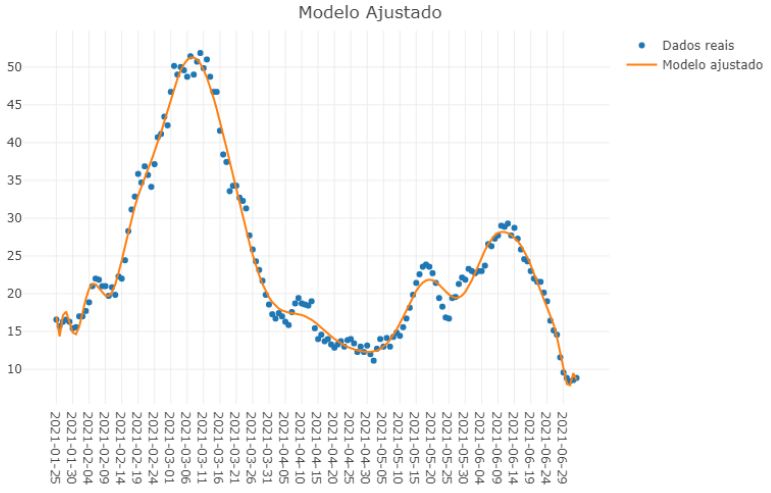


Fonte: Elaborada pelo autor

Apesar da existência de alguns pontos influentes, como o teor desta análise é apenas descritivo, pode-se considerar um ajuste apropriado.

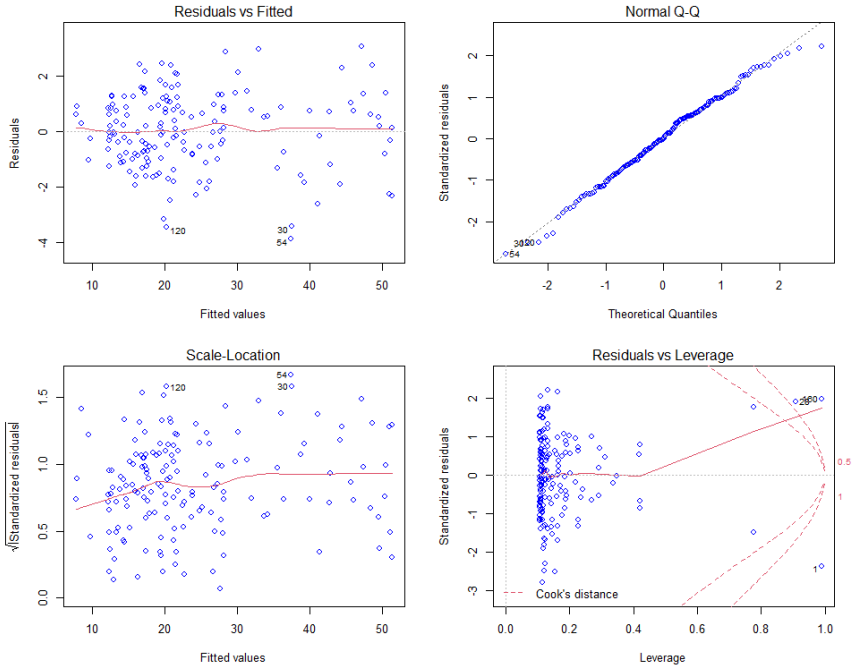
A Figura 4 apresenta o ajuste usando polinômios ortogonais aos casos em idosos.

Figura 4 – Ajuste polinômio ortogonal de grau 25 aos dados dos idosos



Fonte: Elaborada pelo autor

Figura 5 – Análise de resíduos ajuste polinomial aos dados dos idosos

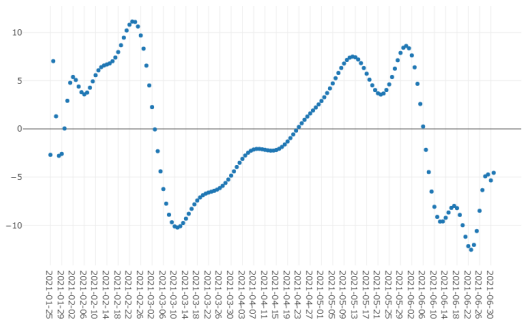


Fonte: Elaborada pelo autor

Analogamente ao caso dos não idosos, pode-se considerar o ajuste descrito na Figura 4 como adequado.

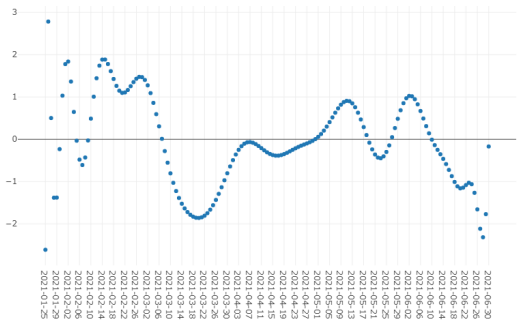
Em posse do polinômio ajustado pode-se calcular a taxa de variação. Uma abordagem possível seria determinar a equação algébrica do polinômio e posteriormente calcular a derivada analítica. No entanto, optou-se por utilizar um método de derivação numérica haja visto a complexidade de determinar algebricamente a base de polinômios ortogonais utilizada pela função **poly**.

Figura 6 – Taxa de variação *não idosos*



Fonte: Elaborada pelo autor

Figura 7 – Taxa de variação *idosos*



Fonte: Elaborada pelo autor

Analisando ambas as taxas de variação observa-se uma similaridade no comportamento

das curvas ao longo do tempo. No período em que ocorre a segunda onda, ficou evidente que houve uma redução na taxa de variação nos casos de COVID-19 no grupo de *não idosos*, porém mantendo-se elevada e com média de casos crescente, ao passo que entre os idosos esta taxa de variação atingiu valores negativos, o que corresponde a uma redução na média de casos, o que indica que neste período a média de casos não manteve um padrão de crescimento como na primeira onda na qual manteve-se a maior parte do tempo acima de 1 que foi a taxa de variação máxima na segunda onda.

4. Conclusões

Houve uma redução na média de casos em pessoas acima de 60 anos na segunda onda em relação à primeira de forma mais acentuada do que no grupo de não idosos, em um período em que os casos aumentaram expressivamente. Esta análise não garante que esta redução deva-se exclusivamente à vacinação, mas do exposto neste estudo e levando em consideração as datas que marcam o fim da vacinação em pessoas acima de 60 anos, há indícios da existência de uma redução nos casos de contágio no grupo de idosos, que representam a maior parte dos vacinados.

Sabe-se da viabilidade do uso das vacinas o qual foi testado clinicamente pelos laboratórios, contudo as vacinas de COVID-19 são muito recentes e seu comportamento em massa ainda não foi totalmente explorado. Um resultado positivo na cidade de Maringá foi saber que mesmo com alta exposição à doença quando houve os picos no grupo de não idosos a vacina cumpriu com o seu papel.

Referências

1 ABREU, Marcelo Osnar Rodrigues de. **Dashboard COVID-19**. 2020. Disponível em: <https://mlealserver.shinyapps.io/covid19-15RS>. Acesso em: 10 jul. 2021.

2 CHAMBERS, JM; HASTIE, TJ. Statistical Models in S., Wadsworth & Brooks/Cole. **Pacific Grove, CA**, 1992.

Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 5** 1 (2021): 22–34. ©JEEPEMA–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Uma experiência na produção de materiais didáticos para a utilização do *software* SageMath.

Ester H. Bento[1], Vitoria V. Gongora[2], Rodrigo Martins[3], Mariana Moran[4]

1 Acadêmica do curso de Matemática, DMA/UEM, ra114099@uem.br

2 Bolsista FA-SETI/PIBEX-2020/21-UEM, ra114100@uem.br

3 Departamento de Matemática - UEM, rmartins@uem.br

4 Departamento de Matemática - UEM, mmbarroso@uem.br

Resumo: Nesse texto aborda-se aspectos gerais da produção e publicação de materiais e recursos didáticos, para a utilização do *software* SageMath no aprendizado de Cálculo Diferencial e Integral. Tais materiais foram produzidos no âmbito de um projeto de extensão intitulado "Cálculo Diferencial e Integral: um kit de sobrevivência (KIT)" desenvolvido no Departamento de Matemática (DMA) da Universidade Estadual de Maringá (UEM). O objetivo destes materiais didáticos consiste em possibilitar um aprendizado do Cálculo Diferencial e Integral por meio de um *software* computacional, com teorias e exemplos dos assuntos estudados. O desenvolvimento deste projeto proporcionou: oportunidades para acadêmicos compreenderem o Cálculo por meio de uma ferramenta diferente do convencional; produção de um material didático que pode ser utilizado por professores e acadêmicos para o ensino e a aprendizagem do Cálculo; fácil acesso aos assuntos propostos; maior conhecimento das participantes do projeto sobre os assuntos abordados; dentre outras características.

Palavras-chave: SageMath, cálculo diferencial, matemática básica.

1. Introdução.

Esse trabalho é fruto do desenvolvimento de um projeto de extensão intitulado "Cálculo Diferencial e Integral: um kit de sobrevivência (KIT)", pertencente ao Departamento de Matemática (DMA) da Universidade Estadual de Maringá (UEM). O objetivo principal do projeto é a produção de materiais didáticos que auxiliem na utilização do *software* SageMath para a aprendizagem de assuntos relacionados ao Cálculo Diferencial e Integral. O SageMath é um *software* gratuito que possibilita a resolução de cálculos (simples ou complexos) por meio de linguagens de diferentes programas sendo acessível a públicos de faixas etárias variadas.

Com o intuito de situar o leitor a respeito do *software* e das atividades desenvolvidas durante a execução e implementação do projeto, será descrito neste texto as experiências

vivenciadas por 2 acadêmicas do 2° ano de Licenciatura em Matemática sob a orientação de um professor coordenador do KIT e docente do DMA da UEM. Os materiais produzidos no contexto do KIT visam orientar e direcionar os estudantes das disciplinas decorrentes do Cálculo Diferencial e Integral em como utilizar o SageMath para resolverem listas de exercícios e problemas, que envolvam conteúdos relacionados ao Cálculo. Os estudantes inserem as informações no *software* por meio da linguagem de programação determinada pelo SageMath, e este último retorna com o resultado correto do problema e, desse modo, os estudantes podem conferir se seus raciocínios e suas resoluções estão corretos.

Portanto, o presente texto apresenta-se como uma forma de: registrar a história do projeto KIT, o modo como ocorreu e ainda ocorre a sua execução, bem como o papel do *software* SageMath e suas potencialidades na aprendizagem de assuntos relacionados ao Cálculo Diferencial e Integral.

A seguir, será descrita uma breve história do projeto de extensão "Cálculo Diferencial e Integral: um kit de sobrevivência (KIT)".

2. O Projeto KIT: sua história.

Na intenção de descrever o processo de fundação e implementação do projeto de extensão KIT, destaca-se neste texto a importância de uma conversa de viés histórico com o Prof. Dr. Doherty Andrade, professor aposentado do Departamento de Matemática da Universidade Estadual de Maringá e ex-coordenador e co-fundador do projeto de extensão. Durante essa entrevista, o professor relatou que esse projeto teve início na década de 1990, com a ajuda dos professores doutores Ma To Fu, Nelson Martins Garcia e Jorge Lacerda, todos, na época, pertencentes ao Departamento de Matemática da UEM. Segundo o professor Doherty, o KIT foi o primeiro projeto de matemática do Brasil que disponibilizou os materiais didáticos produzidos, por meio da internet.

A idealização do projeto surgiu em 1996, durante as aulas de "Cálculo de Várias Variáveis" que eram ministradas pelo professor Doherty. Ao lecionar essa disciplina, o professor observou uma certa dificuldade nos alunos durante o estudo e a aprendizagem de gráficos de superfícies, principalmente no que dizia respeito a visualizar as regiões de integração. Nessa época, o recurso mais recente e mais utilizado para enfrentar os desafios de desenhar e interpretar os gráficos de superfícies, era o *software* Maple, considerado uma revolução na computação. Este *software* é um sistema computacional que permite o registro de expressões algébricas possibilitando o desenho de gráficos de duas ou três dimensões, e pode auxiliar no trabalho com as disciplinas do Cálculo. Desse modo, como o professor possuía conhecimento da implementação deste *software*, decidiu organizar um material de modo que pudesse utilizar

essa ferramenta em suas aulas e depois disponibilizar esse conteúdo pelo Laboratório de Informática da Matemática na rede interna do DMA.

Essa prática se tornou recorrente, e de 1996 a 1998, permaneceu exclusiva para alunos do DMA da UEM, porém o KIT ainda não era um projeto reconhecido e regulamentado pelo DMA e pela Universidade. Quando o departamento se conectou com o *world wide web* (www), todo o material produzido pela equipe do KIT tornou-se disponível na internet [1], porém ainda de modo não oficial. Apenas no dia 06 de setembro de 1999, o projeto "Cálculo Diferencial e Integral: um kit de sobrevivência (KIT)" foi aprovado pelo DMA como um projeto de extensão, passando a existir e a ser executado oficialmente.

Com o passar do tempo, Andrade notou um aumento no número de acesso ao material, possuindo acessos e comentários de estudantes de outros estados. Além disso, alguns estudantes que acessavam o material disponível na internet, enviavam e-mails para o professor comentando sobre a utilização de seus textos como material de estudo para aprender a calcular com o Maple, bem como para contribuir no aprendizado de outras matérias. Tais situações demonstraram o interesse por parte de alguns estudantes pelos sistemas de Matemática Simbólica, o que gerou mais motivação para a produção de materiais e minicursos que abordassem o uso e a exploração do Maple. No contexto do projeto de extensão KIT, seus integrantes também promoveram minicursos de *softwares* como Geogebra, MatLab, LaTeX, Cinderella, Mupad, dentre outros.

Infelizmente o *software* Maple tornou-se um *software* pago e com o passar dos anos a Universidade não pode mais pagar por sua licença e isso dificultou o acesso dos seus próprios acadêmicos. Assim, nos últimos anos, procurando por uma alternativa adequada, o projeto migrou para o *software* SageMath, uma vez que este funciona de modo semelhante ao Maple, porém é um *software* de código aberto e gratuito.

3. O *software* SageMath.

O SageMath é um *software* gratuito que possibilita a resolução de cálculos (simples ou complexos) por meio de linguagens de diferentes programas sendo acessível a públicos de diferentes faixas etárias. Este *software* é uma alternativa viável de código aberto para programas como Magma, Maple, Mathematica e MatLab (2021).

> **SageMath** é um sistema de software de matemática de código aberto gratuito licenciado sob a GPL. Ele se baseia em muitos pacotes de código aberto existentes: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R e muitos mais. Acesse seu poder combinado por meio de uma linguagem

[1] O link disponível para o acesso ao material produzido pelo KIT é: http://www.dma.uem.br/kit/ .

> comum baseada em Python ou diretamente por meio de interfaces ou wrappers.(SAGE. (s.d.), 2021)

A escolha desse *software* foi feita por sua grande lista de vantagens, dentre elas: a multiplataforma que possibilita o seu uso em diversas plataformas existentes, o acesso gratuito que pode ser feito de modo *online* ou realizando o *download* do aplicativo, e além disso, a possibilidade de trabalhar linguagens de diferentes programas anteriores. O SageMath é útil para a resolução de cálculos que vão dos mais simples até os mais complexos, alcançando um público amplo, com usuários de diferentes níveis de ensino e conhecimento. Este proporciona aos seus usuários uma experiência de desenvolvimento de grande escala que contou com a contribuição de muitos líderes de matemática, bem como profissionais da informática, alunos de graduação e pós-graduação.

Assim, com base na ferramenta SageMath - utilizada para o desenvolvimento e a prática do projeto KIT - é possível observar que este projeto poderia ser realizado com diferentes faixas etárias, e expandir-se para outras áreas além do Cálculo, alcançando um público maior, uma vez que seu objetivo é a produção de materiais didáticos para a utilização do SageMath.

Portanto, como uma forma de tornar compreensível o que tem se entendido por material didático no contexto do projeto KIT, a seguir serão descritas noções sobre essa abordagem de acordo com alguns pesquisadores, bem como o uso das tecnologias no ensino.

4. A elaboração de materiais didáticos.

Conforme citado anteriormente, o objetivo do projeto KIT é a criação de materiais didáticos que auxiliem na utilização do *software* SageMath para a aprendizagem de assuntos relacionados ao Cálculo Diferencial e Integral. Contudo, nesta seção será esclarecida a compreensão de alguns termos, ressaltando a reflexão e exemplificação de estudiosos da área a respeito.

Dois termos utilizados no contexto da escrita e descrição dessa pesquisa são: materiais didáticos e recursos didáticos. O pesquisador e educador matemático Sergio Lorenzato, em seu livro *"O Laboratório de Ensino de Matemática na Formação de Professores"* apresenta uma definição de material didático como:

> Material Didático (MD) é qualquer instrumento útil ao processo de ensino e aprendizagem. Portanto MD pode ser giz, uma calculadora, um filme, um livro, um quebra-cabeça, um jogo, uma embalagem, uma transparência, entre outros. (Lorenzato (2012), p.18)

Porém, ao fazer uma leitura do documento norteador do ensino da Educação Básica Brasileira - *Base Nacional Comum Curricular (BNCC, 2018)* -, encontrou-se uma definição

para o termo recursos didáticos que se adequa a definição de materiais didáticos proposta por Lorenzato (2012). Entende-se

> [...] recursos didáticos como malhas quadriculadas, ábacos, jogos, calculadoras, planilhas eletrônicas e softwares de geometria dinâmica, é importante incluir a história da Matemática como recurso que pode despertar interesse a representar um contexto significativo para aprender e ensinar Matemática. Entretanto, esses recursos e materiais precisam estar integrados a situações que propiciem a reflexão, contribuindo para a sistematização e a formação dos conceitos matemáticos. (BNCC (2018))

Logo, é possível observar que o entendimento do termo "recursos didáticos"é muito próximo do termo "materiais didáticos", portanto para esse texto ambos os conceitos serão utilizados como sinônimos.

Os materiais didáticos, na maioria das áreas do conhecimento, possuem grande importância no processo de ensino e aprendizagem, pois possibilitam o despertar da curiosidade e o interesse dos estudantes pelos assuntos abordados. Em relação ao ensino da matemática, Bezerra (1962) destaca em seu livro "*O material didático no ensino da matemática*" a principal função da utilização desses recursos nas salas de aula

> i) auxiliar o professor a tornar o ensino da matemática mais atraente e acessível,
> ii) acabar com o medo da matemática que, criado por alguns professores e alimentado pelos pais e pelos que não gostam da matemática, está aumentando cada vez mais a dificuldade do ensino dessa matéria e
> iii) interessar maior número de alunos no estudo dessa ciência.
> (BEZERRA (1962),p.10-13)

No mesmo sentido, França e Felisberto (2017), relatam uma pesquisa realizada em uma Escola Normal Primária de Ponta Grossa, em que foram encontrados registros de fotografias de uma aula de Metodologia e uma aula de Desenho.

Na primeira, há poucos alunos, muitas carteiras vazias e algo escrito na lousa, que, infelizmente, não foi possível ler. Já na aula de Desenho é possível observar que o conteúdo abordado é de Noções de Perspectiva. Nesta fotografia, o professor e uma aluna estão à frente de uma turma, ela encontra-se com um esquadro na mão fazendo uma construção no quadro, enquanto o professor a observa, e seus colegas de turma tomam nota em seus cadernos. Neste caso, o esquadro foi utilizado pela estudante e pelo professor com um recurso didático para auxiliar na aula em questão. Ainda, atualmente, observa-se, conforme Fiorentini e Miorim (1990), que a cada dia mais professores buscam cursos, palestras e conferências que incentivam o uso de recursos e materiais didáticos alternativos para contribuírem no ensino

da matemática. É importante destacar que a simples presença desses objetos em sala de aula não é o que o torna a ferramenta útil na aprendizagem, mas sim a maneira como ela é utilizada pelo professor que conduz o trabalho em sala de aula.

Com o passar do tempo, o acesso a esses materiais foi sendo facilitado, principalmente com os avanços tecnológicos. Os alunos e professores, não dependem mais completamente das escolas, eles podem encontrar materiais manipuláveis, gizes, compassos, material dourado, etc. vendidos em papelarias, procurar em livrarias revistas, apostilas e livros publicados por editoras ou revistas, ou até mesmo encontrar esses materiais publicados em páginas da internet, blogs, bibliotecas virtuais, fóruns de discussão, entre outros.

Para a disponibilização desses materiais didáticos se tornar possível, é necessário o investimento na produção. Como já visto, materiais didáticos são instrumentos úteis para o processo de aprendizagem, assim, a produção de cada tipo é diferente e varia desde artesãos e fábricas que produzem material dourado, compasso, transferidor, por exemplo, passando por livros e apostilas que, em sua maioria, são produzidos por especialistas, professores ou estudantes da área, chegando a sites e plataformas *online* como o Geogebra, Khan Academy, Scratch, SageMath, entre outros.

Até esse momento foram discutidos sobre os materiais didáticos em geral, porém é necessário destacar a importância do uso das Tecnologias da Informação e Comunicação (TIC), em sua maior parte representada por computadores, celulares, calculadoras e outras tecnologias. Carneiro e Passos (2014) comentam sobre o início da utilização dos computadores nas escolas e a reação de medo dos professores, que temiam ser substituídos por esses novos recursos, mas "a máquina precisa do pensamento humano para se tornar auxiliar no processo de aprendizado" (RIBEIRO (2005), p. 94).

Os autores ainda abordam pontos positivos sobre a utilização das TIC's em sala de aula, como, além de aprender os conteúdos específicos de cada matéria que serão abordados, também se capacitam na utilização de softwares, computadores e desenvolvem uma alfabetização tecnológica, o que auxiliará no futuro mercado de trabalho, já que grande parte das empresas demandam algum conhecimento tecnológico.

Além disso, um outro ponto positivo da utilização das TIC's em sala de aula é que as tecnologias se tornaram parte da vida da maioria dos estudantes, e por isso, ao invés de encará-la como algo negativo, que desprende a atenção do aluno, sua utilização em sala de aula, como instrumento de ensino para acesso a materiais didáticos, pode trazer benefícios diversos. No início de sua implementação, a utilização desses eletrônicos gerava um certo receio aos professores e estudantes, mas ao reconhecer as suas potencialidades para o ensino e ao utilizá-las como aliadas nas salas de aula, o professor e o aluno conseguem sentir uma sensação de prazer e liberdade.

A seguir, descreveremos as experiências realizadas no contexto do projeto KIT, bem como algumas atividades desenvolvidas durante os últimos 6 meses de projeto, como forma de relatar as atividades desenvolvidas.

5. Sobre a experiência.

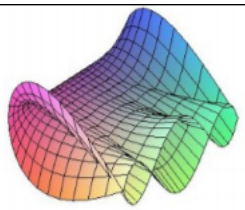
O projeto "Cálculo Diferencial e Integral: um kit de sobrevivência (KIT)" contou com a participação de 2 acadêmicas, todas do curso de Licenciatura em Matemática. No período de setembro de 2020 a janeiro de 2021, com o trabalho de uma nova coordenação, o foco do projeto, além da exploração do *software*, foi a produção de textos curtos de acesso rápido, para orientar a utilização do SageMath relacionado aos conteúdos de Cálculo Diferencial e Integral. Na primeira reunião discutiu-se o *software* SageMath, demonstrando como a instalação do *software* deveria ser realizada e alguns de seus comandos básicos. Foi também discutido a estrutura e os conteúdos a serem abordados nos textos para os seminários das próximas semanas e acordando que o *software* de edição de texto que deveria ser utilizado por todos para uma padronização seria o Latex.

Uma semana após a primeira reunião, uma das participantes fez a primeira apresentação com o texto sobre o assunto "Limites de funções", onde foi discutido como poderiam melhorar a estrutura dos textos para que ficassem mais acessíveis ao entendimento do leitor. Após uma quinzena, a outra estudante apresentou também seu primeiro texto sobre "Funções", já com as estruturas de acordo com o que havia sido discutido anteriormente.

Foi-se decidido que os textos produzidos deveriam conter em média três páginas e possuir a seguinte estrutura: inicia-se com o cabeçalho contendo o nome do projeto, da autora, do orientador e, logo abaixo, o tópico abordado naquela publicação seguido de um resumo da parte teórica contendo as principais definições, teoremas ou propriedades, como pode ser visto, de forma breve, na Figura 1.

Logo depois, encontra-se uma forma genérica de como o código deve ser escrito no SageMath e este acompanha a função *copy paste* onde os usuários podem apenas copiar os comandos, colá-los no SageMath e alterar os dados conforme suas necessidades, podemos ver um exemplo na Figura 2.

Figura 1: Polinômio de Taylor.



Cálculo Diferencial e Integral:
um kit de sobrevivência
"SageMath"

Vitória Vendramini Gongora.
Orientador: Prof. Dr. Rodrigo Martins.

Polinômio de Taylor:

Uma das aplicações de derivada é o Polinômio de Taylor, que nos permite aproximar uma função por um polinômio, estimando um erro. A única condição é que a função seja derivável.

Teorema: Fórmula de Taylor com resto de Lagrange: Seja f derivável até a ordem $n+1$ no intervalo I e sejam $x_o, x \in I$.Então, existe pelo menos um $\overline{x}$ no intervalo aberto de extremos x_0 e x tal que:

$$f(x) = P(x) + \frac{f^{n+1}(\overline{x})}{(n+1)!}(x-x_0)^{n+1}$$

onde: $P(x) = f(x_0) + f'(x_0)(x-x_0) + \frac{f''(x_0)}{2}(x-x_0)^2 + ... + \frac{f^n(x_0)}{n!}(x-x_0)^n$.

Fonte: autores.

Figura 2: Polinômio de Taylor no SageMath.

Polinômio de Taylor no SageMath:

Para facilitar, você pode copiar as áreas em azul e verde, colar no SageMath e substituir as verdes pelas informações que você tem, como a função, o ponto, o intervalo etc.

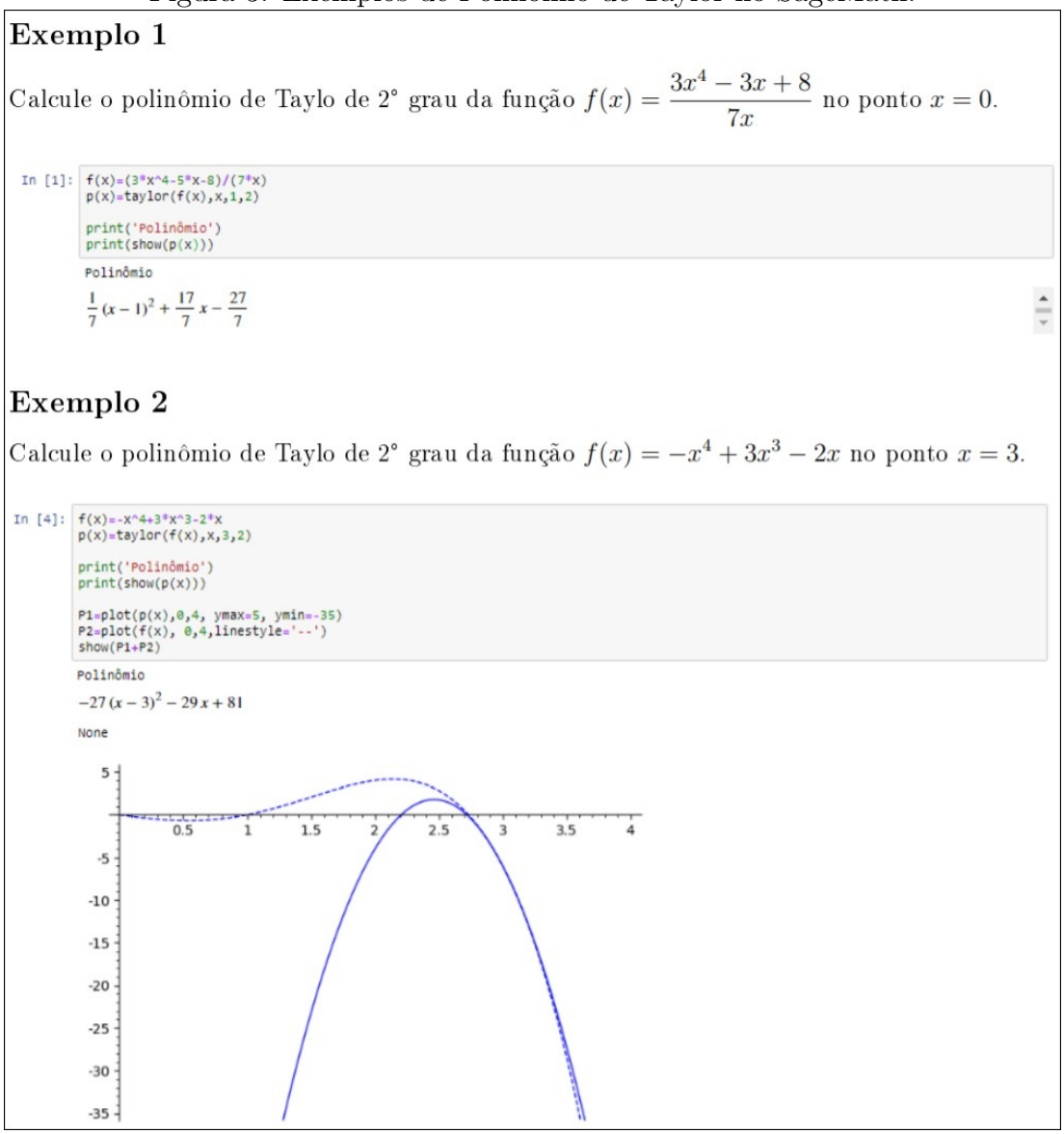
Para calcular o Polinômio de Taylor de uma função devemos:
$f(x)$ = defina $f(x)$
$p(x)$= taylor ($f(x)$, x,ponto que desejamos calcular, grau do polinômio)
print('Polinômio')
print(show($p(x)$))

Podemos plotar o gráfico de $f(x)$ e de $p(x)$ juntos, para isso devemos escrever:
plot($p(x)$, intervalo de visão em x) + plot($f(x)$, intervalo de visão em x, linestyle=':')
ou
P1 = plot($p(x)$, intervalo de visão em x)
P2 = plot($f(x)$, intervalo de visão em x, linestyle=':')
show(P1 + P2)

Fonte: autores.

Ao final destes textos curtos, são apresentados em média dois exemplos da aplicação do código em problemas matemáticos e suas referências, contendo o manual disponível em inglês ou espanhol na página do SageMath, fóruns *online* e livros de cálculo como os de James Stuart, Guidorizzi e outros. Esse trecho pode ser observado nas Figuras 3 e 4.

Figura 3: Exemplos de Polinômio de Taylor no SageMath.



Fonte: autores.

Figura 4: Referências do texto de Polinômio de Taylor no SageMath.

Exemplo 3

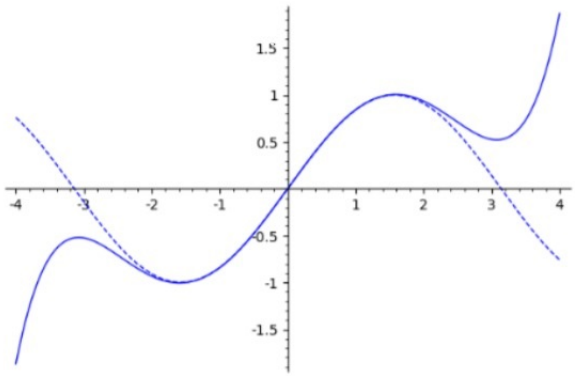
Calcule o polinômio de Taylor de 6° grau da função $f(x) = sen(x)$ no ponto $x = 0$ e plote o gráfico.

```
In [2]: f(x)=sin(x)
        p(x)=taylor(f(x),x,0,6)

        print('Polinômio')
        print(show(p(x)))

        P1=plot(p(x),-4,4)
        P2=plot(f(x), -4,4,linestyle='--')
        show(P1+P2)
```

Polinômio

$$\frac{1}{120}x^5 - \frac{1}{6}x^3 + x$$

None



Referências

[1] GUIDORIZZI, H. L. Um curso de cálculo. 5. ed. Rio de Janeiro: Ltc, 2001. 1 v.

[2] BARD,G. V. Sage para Estudiantes de Pregrado. Cochabamba: Sagemath, 2014. Tradução de: Diego Sejas Viscarra. Disponível em < http://www.sage-para-estudiantes.com/ >. Acesso: 17/08/2020.

[3] SANTOS, E. I. do. O Polinômio e Série de Taylor: Um estudo com aplicações. João Pessoa, 2017. Disponível em: < https://repositorio.ufpb.br/jspui/bitstream/tede/9833/4/Arquivototal.pdf >. Acesso em 07/08/2020.

Fonte: autores.

O *software* SageMath é simples de ser utilizado, e após algumas semanas as graduandas já apresentaram habilidade em manuseá-lo. Como citado anteriormente, as alunas estavam no 2° ano do curso de Licenciatura em Matemática e já haviam cursado a disciplina de Cálculo Diferencial e Integral 1 durante o 1° ano, o qual contém os conteúdos relacionados a funções, limites, derivadas e integrais, por isso os primeiros textos abordaram esses assuntos.

As reuniões eram feitas semanalmente onde as graduandas se alternavam para apresentar o texto produzido naquela quinzena. Na maioria destas, os tópicos eram corrigidos e aperfeiçoados, além da resolução de dúvidas a respeito da utilização do SageMath, do Latex, dos

conteúdos abordados e sobre a graduação.

Esses textos auxiliaram as alunas a retomar alguns conteúdos de Cálculo 1, tornando mais acessível à compreensão, e diante da construção desses materiais, as alunas realizaram uma revisão dos conteúdos a serem abordados. Além desses, sob a orientação do prof. coordenador do projeto, expandiu-se os textos para conteúdos de Cálculo 2, abordando assuntos como: Multiplicadores de Lagrange, Integrais Múltiplas e Objetos Paramétricos, direcionando as alunas a adquirirem um novo conhecimento, entendimento e curiosidade sobre a matemática.

Durante o período de produção foram produzidos 15 manuais, incluindo versões 1 e 2, de alguns temas, uma vez que esses continham várias opções de códigos. As publicações incluem:

- Funções;
- Gráficos de funções 1 (comando plot);
- Gráficos de funções 2 (mais opções do comando plot);
- Solução de equações;
- Funções contínuas;
- Máximo e mínimo de funções;
- Limite de funções;
- Derivada 1 (derivada por definição e o problema da tangente);
- Derivada 2 (derivada de graus superiores);
- Derivadas Parciais;
- Soma de Riemann;
- Integrais;
- Integrais Múltiplas;
- Série de Taylor;
- Objetos Paramétricos.

Por ser um *software* aberto, o SageMath permite que diversas pessoas implementem diferentes métodos de resolução para um mesmo problema. Em razão disso, algumas funções não são encontradas no manual disponibilizado no site. Assim como ocorreram em alguns casos em que as graduandas não encontraram maneiras de implementar o conteúdo abordado no manual, então, após pesquisas, foram encontrados fóruns e páginas da internet que discutiam sobre o *software* e outros problemas matemáticos os quais ajudaram na produção dos textos.

6. Reflexões finais.

A proposta deste texto versou sobre a disseminação de um projeto de extensão intitulado "Cálculo Diferencial e Integral: um kit de sobrevivência (KIT)", pertencente ao Departamento de Matemática (DMA) da Universidade Estadual de Maringá (UEM).

O objetivo principal do projeto é a produção de materiais didáticos que auxiliem na utilização do *software* SageMath para a aprendizagem de assuntos relacionados ao Cálculo Diferencial e Integral. Desse modo, com o conteúdo e as referências expostas no quadro teórico deste texto, foi possível observar a importância de sempre manter atualizados os métodos de ensino-aprendizagem e os materiais didáticos utilizados, e como essa prática leva a melhorias, avanços, e construção do conhecimento durante os estudos dos alunos.

Desde a criação do projeto, o professor Dr. Doherty Andrade tinha como objetivo auxiliar os estudantes na aprendizagem de assuntos de Cálculo. Os manuais produzidos de como utilizar o SageMath continuam com o mesmo intuito e por isso são textos curtos, de rápido acesso e que podem auxiliar os estudantes na hora de resolver listas, exercícios e problemas que envolvam conteúdos, mais especificamente, de Cálculo Diferencial e Integral I, utilizando o software SageMath.

Além de auxiliar alunos externos ao projeto, este acabou agregando muito para as graduandas que os produziram, pois com a produção desses manuais foi possível rever, revisar e fixar melhor os conteúdos, para compreenderem algumas partes que promoviam dúvidas, o que fez com que o entendimento sobre a disciplina melhorasse.

Apesar de ser uma fase nova, a ideia do projeto foi apresentada no evento "III Encontro Anual de Extensão da Universidade Estadual de Maringá de 2020 (EAEX)". Além disso, foi bem recebido pelos alunos de estatística e matemática, que ouviram falar do KIT e por curiosidade utilizaram os textos para aprender a usar o SageMath o que auxiliou nos estudos.

Esperamos que com esse texto, possamos divulgar o projeto KIT para que acadêmicos e professores, tenham conhecimento do trabalho executado no seu contexto e que os estudantes possam reconhecê-lo como uma possibilidade de aprender assuntos relacionados ao Cálculo Diferencial e Integral.

Referências

1 BEZERRA, M.J. **O material didático no ensino da matemática**. Rio de Janeiro: MEC/ caderno CEDES, 1962. p. 10–13.

2 CARNEIRO R.F.; PASSOS, C. L. B. A utilização das Tecnologias da Informação e Comunicação nas aulas de Matemática: Limites e possibilidades. **Revista Eletrónica de Educação**, v. 8, n. 2, p. 101–119, 2014. Disponível em: ¡http://www.reveduc.ufscar.br/index.php/reveduc/article/view/729/328¿.

3 FIORENTINI D.; MIORIM, M. A. Uma reflexão sobre o uso de materiais concretos e jogos no ensino da matemática. **Boletim SBEM-SP**, v. 4, n. 7, 1990.

4 FRANÇA, I. S.; FELISBERTO L. G. S. Usos dos materiais para ensinar matemática (1920 - 1930). In: ENCONTRO PARANAENSE DE EDUCAÇÃO MATEMÁTICA, 2017, Unioeste.

5 GREGORY, V. B. **Sage para Estudiantes de Pregrado.** Tradução: Diego Sejas Viscarra. Cochabamba, Bolivia, 2014. p. 330. Disponível em: ¡http://www.dma.uem.br/kit/apostilas-software/sage-para-estudiantes.pdf¿.

6 LORENZATO, Sergio. Laboratório de ensino da matemática e materiais didáticos e manipuláveis. In: O Laboratório de Ensino de Matemática na Formação de Proofessores. 3. ed. Campinas, SP: Autores Associados, 2012. cap. 1, p. 3–37.

7 MARTINS, R. **Cálculo Diferencial e Integral: um KIT de Sobrevivência.** Maringá, Brasil, 2020. Disponível em: ¡http://www.dma.uem.br/kit/sobre¿.

8 MINISTÉRIO DA EDUCAÇÃO, Brasil. **Base Nacional Comum Curricular**. edicao. Brasilia, 2018. p. 600. Disponível em: ¡http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf¿.

9 RIBEIRO, O. J. Educação e novas tecnologias: um olhar para além das técnicas. **Letramento digital: aspectos sociais e possibilidades pedagógicas**, Belo Horizonte, Brasil, p. 86–97, 2005.

10 SAGE. **Sage Mathematical Software**. [S.l.]. Disponível em: ¡https://www.sagemath.org/index.html¿.

11 SILVA R. S. DA; NOVELLO, T. P. O Uso das Tecnologias Digitais no Ensinar Matemática: Recursos, Percepções e Desafios. **Revista Educacional de Educação Superior**, Campinas, SP, v. 6, p. 1–15, 2020. Disponível em: ¡https://periodicos.sbu.unicamp.br/ojs/index.php/riesup/article/view/8655884/21478¿.

12 SOUZA, R. F. **Templos de civilização: a implantação da escola primária graduada no Estado de São Paulo, 1890-1910**. São Paulo, SP: Fundação Editora da Unesp, 1998.

Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 5** 1 (2021): 35–48. ©JEEPEMA–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Exemplo de cálculo com chaves criptografadas com curvas elípticas

Ana Carolina Sakurai Ferreira – Email: carolynasf@msn.com

Resumo: Este artigo é um fragmento da dissertação de mestrado apresentado no Programa de Mestrado Profissional em Rede Nacional - Profmat e nele mostramos as curvas elípticas a partir de uma adaptação do Problema do Logaritmo Discreto. São apresentados alguns embasamentos teóricos de aritmética e apresentamos um exemplo de uma mensagem/palavra criptografada utilizando o método estudado.
Palavras-chave: Criptografia, Curvas Elípticas, ElGamal.

1. Introdução

Falaremos sobre a criptografia com uso de curvas elípticas. Essa técnica foi, inicialmente, introduzida em 1985 por Victor Miller e Neal Koblitz e foi abordada no uso de curvas elípticas como uma nova forma de implementação a um sistema de chave pública em algumas das aplicações já existentes.

Esse método criptográfico tem tido uma relevância nas últimas décadas pois está associado a crescente necessidade de segurança nos modernos meios de comunicação, fundamentado em computadores onde a eficiência de processamento tem evoluído a cada instante.

Apresentamos os conceitos matemáticos usados no sistema de criptografia desenvolvido a partir das curvas elípticas definidas sobre corpos finitos. Para tal, assumiremos que o leitor tenha conhecimento de alguns conceitos apresentados em disciplinas do curso de graduação em matemática tais como grupos, anéis, corpos, etc. O referencial teórico empregado neste texto pode ser averiguado nas obras de (OLIVEIRA, 2009), (ANDRADE, 2016), (CORREIA, 2013) e (F. B. LARA, 2010).

2. Curvas Elípticas

Curvas elípticas são definidas a partir da Equação de Weierstrass sobre um corpo $\mathbf{K}$:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

com $a, b, c, d, e \in \mathbf{K}$ mais, um ponto chamado de ponto no infinito (representaremos esse ponto por ∞). Neste trabalho, trabalharemos com curvas elípticas simétricas em relação ao

eixo das abcissas e sem singularidades. Assim, trabalharemos com uma versão simplificada da Equação de Weierstrass.

Definição 2.1 *Seja* $\mathbf{K}$ *um corpo. Uma curva elíptica* E *sobre* $\mathbf{K}$*, denotada por* $E(\mathbf{K})$*, é o lugar geométrico dos pontos* $(x, y) \in \mathbf{K} \times \mathbf{K}$ *tais que* x *e* y *são soluções da equação*

$$y^2 = x^3 + Ax + B$$

com $A, B \in \mathbf{K}$ *e* $4A^3 + 27B^2 \neq 0$.

Esta curva não possui raízes múltiplas, ou seja, deve ser uma curva não-singular, por isso devemos ter $\Delta = 4A^3 + 27B^2 \neq 0$.

Abaixo estão alguns gráficos de curvas elípticas.

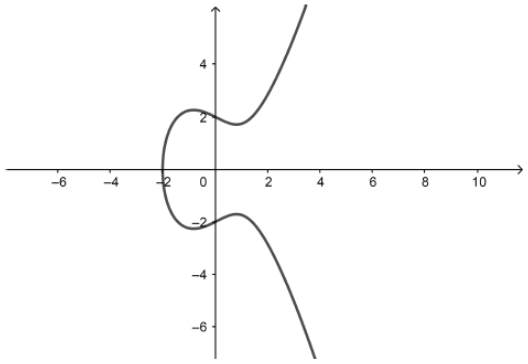


Figura 1: Gráfico da curva $y^2 = x^3 - 2x + 4$

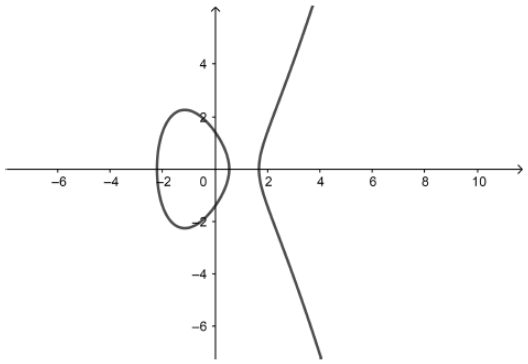


Figura 2: Gráfico da curva $y^2 = x^3 - 4x + 2$

Esses gráficos são de curvas definidas para os reais, ou seja, os valores das variáveis x e y na equação são reais e os valores dos parâmetros A e B são números reais. Porém uma curva

elíptica pode ser definida em qualquer corpo. Aqui, estamos interessados no caso onde elas estão definidas sobre corpos finitos.

Queremos definir uma estrutura de grupo no conjunto das curvas elípticas, para isso vamos definir a "soma"entre dois pontos. Essa soma pode ser tratada tanto de forma geométrica ou algébrica, iremos, inicialmente, analisar a forma geométrica.

O ponto infinito ∞ será o nosso elemento neutro da operação. Assim, se Ω é uma curva elíptica sobre um corpo K, e temos $P \in \Omega$, então:

$$P + \infty = P = \infty + P.$$

Consideremos o simétrico de um ponto $P = (x, y)$ sendo o ponto $-P = (x, -y)$, se somarmos um ponto $P \in \Omega$ com o ponto simétrico $-P$, obtemos o ponto infinito, logo:

$$P + (-P) = \infty = (-P) + P.$$

Tome dois pontos P e Q distintos de uma curva elíptica sobre o corpo $\mathbb{R}$ dos números reais, seja PQ o segmento de reta que interceptará a curva em um terceiro ponto que chamaremos de R' (estamos considerando o caso em que a reta não seja vertical). Assim, o reflexo do ponto R' em relação ao eixo horizontal, que é dado por R, será a soma de P e Q. Logo:

$$R = P + Q.$$

O gráfico abaixo, representa graficamente a soma entre dois pontos distintos $P, Q \in \Omega$ em uma curva elíptica sobre o corpo $\mathbb{R}$.

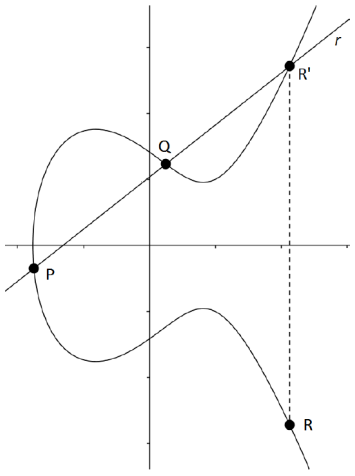


Figura 3: Soma de dois pontos em uma curva $E(\mathbb{R}) : R = P + Q$.

Agora vamos definir a soma $P + P$, para isso trassemos a reta tangente ao ponto P, de tal modo que a reta tangente em P intersecta a curva em um segundo ponto R' e tomamos

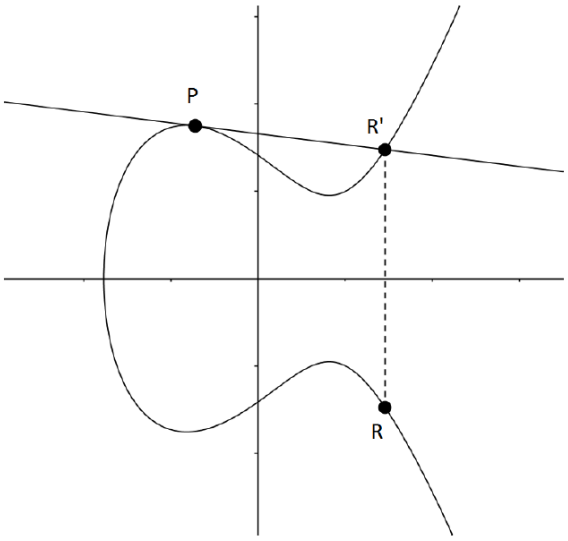


Figura 4: $R = P + P$ ou $R = 2P$.

a reflexão R em relação ao eixo horizontal, ou seja $P + P = R$. Podemos representar a soma de $P + P$ por $2P$.

Um caso particular é disposto se tivermos $P = (x, 0)$, pois, neste caso, a reta tangente à curva no ponto P será vertical e não interceptará a curva em um outro ponto. Neste caso teremos:

$$P + P = 2P = \infty.$$

Veremos agora a soma de dois pontos utilizando a soma algébrica. Para tal iremos trabalhar com as coordenadas dos pontos em uma curva elíptica.

Sejam $P = (x_p, y_p)$ e $Q = (x_q, y_q)$ dois pontos em uma curva elíptica Ω de equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$ e $P \neq \infty$ e $Q \neq \infty$, vamos analisar o caso $P \neq Q$. Seja r a reta que passa pelos pontos P e Q, que intersecta a curva Ω em um terceiro ponto que chamaremos de $R' = (x'_r, y'_r)$ e agora chamaremos de R a reflexão de R'. Assim, pela fórmula da inclinação da reta, conclui-se que a inclinação da reta r é:

$$m = \frac{y_q - y_p}{x_q - x_p},$$

com $x_p \neq x_q$.

Logo a equação da reta r é:

$$y = m(x - x_p) + y_p$$

pois r passa pelo ponto P. Para obter as intersecções entre a reta r e a curva Ω iremos substituir a equação da reta na equação da curva, ou seja,

$$(m(x - x_p) + y_p)^2 = x^3 + ax + b$$

o que nos dá,

$$x^3 + ax + b = m^2x^2 - 2m^2x_px + m^2x_p^2 + 2my_px - 2mx_py_p + y_p^2.$$

Portanto,

$$x^3 - m^2x^2 + (a + 2m^2x_p - 2my_p)x + (b - m^2x_p^2 + 2mx_py_p - y_p^2) = 0.$$

$$\text{Tomando } a' = -m^2, b' = a + 2m^2x_p - 2my_p \text{ e } c' = -m^2x_p^2 + 2mx_py_p - y_p^2$$

teremos:

$$x^3 + a'x^2 + b'x + c' = 0.$$

Sabemos que P, Q e $R^{'}$ são as intersecções da reta r com a curva Ω, então x_p, x_q e $x_r^{'}$ são as raízes da equação. Aplicando as Relações de Girard, temos que a soma das raízes é:

$$-a' = x_p + x_q + x_r^{'}.$$

Como $a = -m^2$ temos que :

$$m^2 = x_p + x_q + x_r^{'};$$

$$x_r^{'} = m^2 - x_p - x_q. \tag{1}$$

Como $R^{'} \in r$, podemos substituir suas coordenadas na equação da reta r, assim:

$$y_r^{'} = m(x_r^{'} - x_p) + y_p. \tag{2}$$

Como $R = P+Q$, $R = (x_r, y_r)$ é a reflexão de $R^{'}$ em relação ao eixo horizontal, assim $x_r = x_r^{'}$ e $y_r = -y_r^{'}$. Substituindo nas equações (1) e (2) temos :

$$x_r = m^2 - x_p - x_q$$

e

$$y_r = m(x_p - x_r) - y_p.$$

Vamos analisar o caso que em $P = Q$, nesse caso temos que a reta r é tangente à curva no ponto P. Assim, a inclinação da reta será a derivada no ponto P em relação a x. Logo,

podemos concluir que:

$$m = \frac{3x_p^2 + a}{2y_p},$$

com $y_p \neq 0$, pois caso contrario a reta seria vertical e teríamos $P + P = \infty$. Logo, a reta r que passa por P com inclinação m tem a mesma forma da equação $y = m(x - x_p) + y_p$. Observe que se realizarmos a interseção desta reta com a curva Ω, obteremos a equação $x^3 + ax^2 + bx + c = 0$, porem agora as raízes não são todas distintas, pois x_p é uma raiz dupla. Assim, aplicando as Relações de Girard, temos que:

$$m^2 = x_p + x_p + x_r^{'};$$

$$x_r = x_r^{'} = m^2 - 2x_p.$$

Agora, para determinar y_r seguimos o mesmo procedimento para o caso $P \neq Q$ e temos

$$y_r = m(x_p - x_r) - y_p.$$

O caso em que $P = \infty$, teremos $x_r = x_p$ e $y_r = y_p$ e no caso $Q = \infty$, teremos $x_r x_q$ e $y_r = y_q$, pois ∞ é o elemento neutro da operação.

Podemos, agora, padronizar a definição de soma entre dois pontos de uma curva elíptica em termos algébricos.

Definição 2.2 *(Soma de dois pontos de uma curva elíptica em termos algébricos) Seja Ω uma curva elíptica de equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$ e sejam $P = (x_p, y_p), Q = (x_q, y_q)$ e $R = (x_r, y_r)$ pontos da curva Ω tais que $R = P + Q$.*

- *Se $P = \infty$, então $R = Q$;*
- *Se $Q = \infty$, então $R = P$;*
- *Se $P = -Q$ então $R = \infty$;*

Nos demais casos, defina

$$m = \begin{cases} \dfrac{y_q - y_p}{x_q - x_p}, & \text{se } P \neq Q; \\ \\ \dfrac{3x_p^2 + a}{2y_p}, & \text{se } P = Q. \end{cases}$$

Em termos de coordenadas, temos:

$$x_r = \begin{cases} m^2 - x_p - x_q, & se\ P \neq Q; \\ \\ m^2 - 2x_p, & se\ P = Q; \end{cases}$$

e

$$y_r = m(x_p - x_r) - y_p$$

Proposição 2.3 $(E(\mathbf{K}), +)$[1]*, onde* $+$ *é a operação de soma entre dois pontos de* $\mathbf{K}$*, é um grupo abeliano.*

A demonstração pode ser encontrada em (WASHINGTON, 2008), página 20.

A operação de soma é válida para qualquer corpo K, assim podemos trabalhar com curvas sobre corpos finitos. Neste trabalho, trabalharemos com curvas sobre o corpo $\mathbb{Z}_p$.

3. Curvas elípticas sobre o corpo $\mathbb{Z}_p$

Definição 3.1 *Uma curva elíptica sobre o corpo* $\mathbb{Z}_p$*, é o conjunto de pontos* (x, y) *com* $x, y \in \mathbb{Z}_p$*, tais que* $y^2 = x^3 + ax + b$*, com* $a, b \in \mathbb{Z}_p$ *e* $4a^3 + 27b^2 \neq 0$ *mod p incluindo o ponto no infinito* ∞*.*

A curva $\mathbb{Z}_p$ possui um número finito de pontos, pois existem p possibilidades para a coordenada x e, para cada valor de x, existem dois valores possíveis para y. Assim, acrescentando o ponto infinito, uma curva no ponto $\mathbb{Z}_p$, terá, no máximo, $2p + 1$ pontos.

A curva E($\mathbf{K}$) é um conjunto finito de pontos. No exemplo abaixo iremos determinar todos os pontos de uma equação cúbica.

Exemplo 3.2 *Determine todos os pontos da curva* $E(\mathbb{Z}_{11})$ *de equação* $y^2 = x^3 - x + 3$*.*

Solução:

Para descobrirmos se um ponto pertence à curva, pegamos cada valor de x*, substituímos em* $(x^3 - x + 3)$ *mod* 11 *e averiguamos se este resultado é o quadrado módulo* 11 *de algum* y*. A tabela abaixo apresenta todos os valores possíveis de* x *e* y*.*

[1]Um grupo $(G, *)$ é um conjunto G com uma operação binária $*$ definida sobre G, de tal forma que as seguintes propriedades sejam válidas:

- A operação * é associativa, isto é, $\forall a, b, c \in G$ temos $a * (b * c) = (a * b) * c$.
- Existe um elemento $e \in G$, chamado elemento neutro, tal que $\forall a \in G$ temos $a * e = e * a = a$.
- Para cada elemento $a \in G$ existe um elemento $a^{-1} \in G$, chamado elemento inverso, tal que $a * a^{-1} = a^{-1} * a = e$.

Se a operação $*$ for comutativa, o grupo é chamado grupo comutativo ou grupo abeliano.

y	y^2 *mod 11*	x	$x^3 - x + 3$ *mod 11*
0	*0*	*0*	*3*
1	*1*	*1*	*3*
2	*4*	*2*	*9*
3	*9*	*3*	*5*
4	*5*	*4*	*8*
5	*3*	*5*	*2*
6	*3*	*6*	*4*
7	*5*	*7*	*9*
8	*9*	*8*	*1*
9	*4*	*9*	*8*
10	*1*	*10*	*3*

Na tabela podemos observar, por exemplo, que para $x = 3$*, temos* $x^3 - x + 3 \equiv 5$ *mod* 11*, que por sua vez é quadrado módulo* 11 *de* $y = 4$ *e* $y = 7$*. Assim, os pontos* $(3, 4)$ *e* $(3, 7)$ *pertencem a curva. Note que para* $x = 5$ *temos* $x^3 - x + 3 \equiv 2$ *mod* 11*, mas não há nenhum valor de* y *cujo quadrado seja congruente a* 2 *módulo* 11*, ou seja, nenhum ponto da curva tem coordenada* $x = 5$*.*

Logo, os pontos da curva são:

$$(0,5), (0,6), (1,5), (1,6), (2,3), (2,8), (3,3), (3,7), (6,2), (6,9), (7,3), (7,8), (8,1), (8,10), (10,5)$$

$$e\ (10,6).$$

Podemos observar que quanto maior o número primo p, mais inacessível se torna determinar todos os pontos de $E(\mathbb{Z}_p)$.

Na curva $E(\mathbb{Z}_p)$, queremos calcular a soma entre dois pontos na forma algébrica. Vejamos o exemplo abaixo:

Exemplo 3.3 *Seja a curva* $E(\mathbb{Z}_{11})$ *de equação* $y^2 = x^3 - x + 3$ *e os pontos* $P = (1, 5)$ *e* $Q = (2, 8)$ *pertencentes a curva. Calcule as coordenadas do ponto* $R = P + Q$*.*

Solução:

Como $P \neq Q$ *e* $x_p \neq x_q$*, então*

$$m = \frac{y_q - y_p}{x_q - x_p} = 3.$$

Estamos trabalhando em $\mathbb{Z}_{11}$*, isto significa que* m *é o inteiro tal que* $1m \equiv 3$ *mod* 11*, logo,* $m = 3$*, pois* $1.3 = 3 \equiv 3$ *mod* 11*.*

Calculando a coordenada x_r:

$$x_r = (m^2 - x_p - x_q) \ mod \ 11$$

$$x_r = ((3)^2 - 1 - 2) \ mod \ 11$$

$$x_r = 6 \ mod \ 11.$$

Para y_r:

$$y_r = (m(x_p - x_r) - y_p) \ mod \ 11$$

$$y_r = (3(1 - 6) - 5) \ mod \ 11$$

$$y_r = -20 \equiv -9 \equiv 2 \ mod \ 11.$$

Logo, $R = (6, 2)$ e, pelo exemplo anterior, $R \in \mathbb{Z}_{11}$.

4. Logaritmo discreto elíptico

Já vimos que se realizarmos a soma $P + P$ temos como resultado $2P$, que é múltiplo de P. Realizando o mesmo procedimento e somando P novamente, teremos $2P + P$ e o seu resultado será $3P$, fazendo esse procedimento n vezes, com $n \in \mathbb{N}$, temos:

$$P + P + P + \cdots + P = nP.$$

Assim, dado um ponto $P \in E(\mathbb{Z}_p)$, podemos determinar os múltiplos $2P, 3P, \cdots, nP$ deste ponto P.

Exemplo 4.1 *Considere a curva $E(\mathbb{Z}_{13})$ de equação $y^2 = x^3 + 2x - 1$. Verifique se o ponto $P = (5, 2)$ pertence à curva e, em caso positivo, determine seus múltiplos.*

Solução: Encontrando os pontos da curva, que são: $(0, 5), (0, 8), (5, 2), (5, 11), (11, 0)$, $(12, 3)$ e $(12, 10)$. Temos que $P \in E(\mathbb{Z}_{13})$.

Iremos, agora, determinar os múltiplos de P pela definição da soma algébrica.

$$2P = P + P = (5; 2) + (5; 2) = (12, 3);$$

$$3P = 2P + P = (12; 3) + (5; 2) = (0, 8);$$

$$4P = 3P + P = (0; 8) + (5; 2) = (11, 0);$$

$$5P = 4P + P = (11; 0) + (5; 2) = (0, 5);$$

$$6P = 5P + P = (0; 5) + (5; 2) = (12, 10);$$

$$7P = 6P + P = (12; 10) + (5; 2) = (5, 11);$$

$$8P = 7P + P = (5; 11) + (5; 2) = \infty.$$

Observe que estes são os únicos múltiplos de P, pois como $8P = \infty$, a partir de $9P$ os resultados seriam repetidos.

Observe que, no exemplo anterior, todos os pontos da curva são múltiplos de $P = (5, 2)$, como $E(\mathbb{Z}_{13})$ com a operação de adição entre dois pontos é um grupo abeliano, dizemos que P é um gerador do grupo.

Podemos reescrever o Problema do Logaritmo Discreto em relação à operação de soma entre dois pontos de uma curva sobre $\mathbb{Z}_p$. Considere um ponto $P \in E(\mathbb{Z}_p)$ tal que P seja um gerador de $E(\mathbb{Z}_p)$. Assim, para cada $Q \in E(\mathbb{Z}_p)$, existe $n \in (\mathbb{Z}_p)$ tal que

$$Q = nP,$$

onde n é o Logaritmo Discreto Elíptico de Q em relação a P, representado por $n = \log_p(Q)$. O Problema do Logaritmo Discreto Elíptico baseia-se em determinar n para cada ponto Q.

5. Criptografia com Curvas Elípticas

O referencial teórico empregado nesta seção é averiguado na obra de (R.C.COMPUTADOR, 2019), (NO, 2019) e (F. B. LARA, 2010).

5.1. Protocolo Diffie-Hellman aplicado a curvas elípticas sobre $\mathbb{Z}_p$

Vamos supor que duas pessoas, Maria e João desejam criar e compartilhar uma chave de codificação segura. Neste protocolo, além do número primo p e do gerador P, a equação da curva $E(\mathbb{Z}_p)$ é pública, pois Maria e João precisam calcular os pontos usando a mesma curva. Abaixo está descrito a metodologia do Protocolo Diffie-Hellman :

- Maria e João escolhem um primo p, uma curva $E(\mathbb{Z}_p)$ de equação $y^2 = x^3 + Ax + B$ com $\Delta = 4A^3 + 27B^2 \neq 0$, e um ponto $P \in E(\mathbb{Z}_p)$ gerador do grupo.
- Maria escolhe um inteiro $n_A \in \mathbb{Z}_p$, mantem secreto, e calcula $Q_A = n_A P$ e envia Q_A para João.
- João escolhe um inteiro n_B, mantem secreto, calcula $Q_B = n_B P$ e envia Q_B para Maria.
- Maria calcula $R_A = n_A Q_B$, que equivale a

$$R_A = n_A(n_B P) = (n_A n_B)P.$$

- João calcula $R_B = n_B Q_A$, que equivale a

$$R_B = n_B(n_A P) = (n_A n_B)P.$$

- Logo a chave secreta é $R_{AB} = R_A = R_B$.

Podemos observar que o método para criar e compartilhar a chave secreta é o mesmo. Logo, a comunicação pode ser realizada por um criptossistema qualquer. Caso um terceiro consiga capturar a comunicação, deverá calcular o Logaritmo Discreto Elíptico de Q_A e Q_B para alcançar os dados iniciais.

Vejamos um exemplo:

Exemplo 5.1 *Considere a curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$ e o ponto $P = (1, 5)$ seu gerador.*

- *Suponhamos que Maria escolha $n_A = 3$, e calcule $Q_A = n_A P$, ou seja,*

$$P = (1, 5),$$

$$2P = (2, 8),$$

$$3P = (6, 2) = Q_A$$

e envia Q_A para João.

- *Suponhamos que João escolha $n_B = 2$, e calcule $Q_B = n_B P$, ou seja,*

$$P = (1, 5),$$

$$2P = (2, 8)$$

e envia Q_B para Maria.

- *Maria então calcula $R_A = n_A Q_B$, ou seja,*

$$R_A = 3.(2, 8) = (3, 4).$$

- *João calcula $R_B = n_B Q_A$. Temos:*

$$R_B = 2.(6, 2) = (3, 4).$$

Logo a chave secreta é $R_{AB} = R_A = R_B = (3, 4)$.

5.2. Criptossistema ElGamal

Iremos exemplificar o criptossistema de chave pública ElGamal utilizando, novamente, o caso Maria e João.

Mais uma vez, o primo p, a curva $E(\mathbb{Z}_p)$ da equação $y^2 = x^3 + ax + b$, com $4a^3 + 27b^2 \neq 0$, e o ponto $p \in E(\mathbb{Z}_p)$, gerador do grupo, são abertos para o público. Para iniciar o processo de encriptação João, que irá enviar uma mensagem a Maria, deve transformar a mensagem, que chamaremos de M, em um ponto $P_M \in E(\mathbb{Z}_p)$. Essa transformação pode ser realizada de várias maneiras, por exemplo, converter a mensagem por um inteiro utilizando a Tabela 1, onde cada letra do alfabeto, a partir de A recebe um valor numérico iniciado em 1.

Tabela 1: Tabela de conversão ElGamal

Letra	Valor	Letra	Valor	Letra	Valor
A	01	J	10	S	19
B	02	K	11	T	20
C	03	L	12	U	21
D	04	M	13	V	22
E	05	N	14	W	23
F	06	O	15	X	24
G	07	P	16	Y	25
H	08	Q	17	Z	26
I	09	R	18		

Fonte: A autora.

Feito isso, separamos esse inteiro em duas coordenadas de um ponto, de maneira que este ponto pertença à curva $E(\mathbb{Z}_p)$. Caso o ponto gerado não pertença à curva, habitualmente acrescenta-se zero, ou outro algarismo ajustado entre as partes, no caso João e Maria, até que as coordenadas encontradas formem um ponto de $E(\mathbb{Z}_p)$.

Realizada esta transformação podemos iniciar a codificação.

Abaixo está descrito a metodologia do Criptossistema ElGgamal:

1. Maria escolhe um inteiro secreto $n_A \in \mathbb{Z}_p$, calcula $Q_A = n_A P$ e envia Q_A para João.

2. João escolhe um inteiro aleatório k e calcula

$$R = kP \text{ e } S = P_M + kQ_A$$

3. João envia para Maria o par de pontos (R, S).

Para Maria decifrar a mensagem, basta calcular $S - n_A R$:

$$S - n_A R = P_M + kQ_A - n_A.kP = P_M + k.n_A P - k.n_A P = P_M.$$

Vejamos um exemplo:

Exemplo 5.2 *Considere a curva $E(\mathbb{Z}_{11})$ de equação $y^2 = x^3 - x + 3$ e o ponto $P = (1, 5)$ gerador de $E(\mathbb{Z}_{11})$ com a operação de soma entre dois pontos. Transforme a mensagem M em um ponto P_M da curva.*

Solução:

Utilizando a tabela de conversão ELGamal temos que a mensagem M = FI, em termos numéricos, corresponde ao inteiro 0609*, pois F*=06 *e I*=09*. Desmembrando este inteiro em duas coordenadas, encontramos o ponto $(06, 09) = (6, 9)$, vamos verificar se este ponto pertence a curva:*

$$y^2 = 9^2 = 81 \equiv 4 \ mod\ 11$$

$$x^3 - x + 3 = (6)^3 - 6 + 3 \equiv 216 - 6 + 3 = 213 \equiv 4 \ mod\ 11$$

Logo, a mensagem M é transformada no ponto $P_M = (6, 9)$.

Exemplo 5.3 *Agora, vamos supor, que João deseja enviar a mensagem M para Maria empregando o primo, a curva e o ponto gerador do exemplo anterior. Faça a codificação e decodificação da mensagem M utilizando o criptossistema ElGamal.*

Solução:

Usando os dados do exemplo anterior temos que $P_M = (6, 9)$. Vejamos os passos do ElGamal:

1. *Suponhamos que Maria escolha $nA = 3$. Temos:*

$$P = (1, 5)$$

$$2P = (2, 8)$$

$$3P = (6, 2) = Q_A$$

e envia para João.

2. *Suponhamos que João escolha $k = 2$, temos:*

$$R = kP = 2(1, 5) = (2, 8)$$

e

$$S = P_M = (6, 9) + KQ_A = (6, 9) + 2(6, 2) = (6, 9) + (3, 4) = (6, 2).$$

3. *João envia para Maria p par de pontos* (R, S)

   Para decodificar a mensagem, basta Maria calcular

$$S - n_A R = (6,2) - 3(2,8) = (6,2) - (3,4) = (6,2) + (3,4 = (6,2) + (3,7) = (6,9) = P_M.$$

Assim, Maria consegue ler a mensagem.

Referências

1 ANDRADE, E. G. **Criptografia com curvas elipticas**. 2016. f. 78. Mestrado Profissional em Matemática - PROFMAT – Universidade Federal do Pará Instituto de Ciências Exatas e Naturais, Belém/AM.

2 CONHECIMENTO COMPUTADOR, Rede de. **Quais são as vantagens e desvantagens de Elliptic Curve Cryptography para segurança sem fio**. edicao. Internet, 2019. p. 1. Disponível em: ¡ptcomputador.com/Networking/wireless-networking/81737.html¿.

3 CORREIA, S. S. J. **Criptografia via curvas elípticas**. 2013. f. 87. Mestrado Profissional em Matemática - PROFMAT – Universidade Federal do Estado do Rio de Janeiro - UNIRIO, Rio de Janeiro/RJ.

4 DESCONHECIDO. **Segurança Lógica de Software**. edicao. Internet, 2019. p. 1. Disponível em: ¡segurancalogica01.blogspot.com/2008/04/criptografia-com-o-usode-%20curvas.html¿.

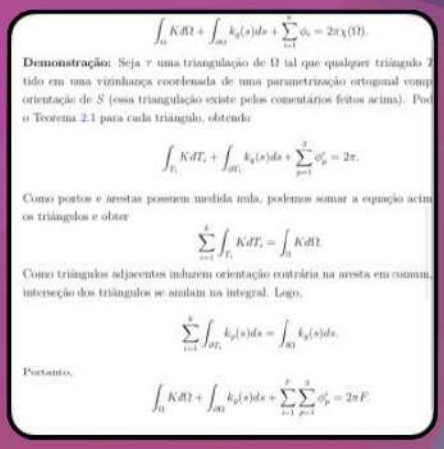
5 F. B. LARA, P. C. S; Oliveira. **Curvas Elípticas: Aplicação em Criptografia Assimétrica.** Petrópolis/RJ: [s.n.], 2010.

6 OLIVEIRA, J. G. Curvas Elípticas sobre Corpos Finitos e Criptografia de Chave. In: COLÓQUIO DE MATEMÁTICA DA REGIÃO CENTRO-OESTE, I., 2009, Universidade Federal do Mato Grosso do Sul. CADERNO do Minicurso. Campo Grande/MS: SBM, 2009. p. 1–12.

7 WASHINGTON, L. C. **Elliptic Curves: number theory and criptography**. 2nd edition. Boca Raton: Chapman e Hall, 2008. p. 531.

UEM Universidade Estadual de Maringá

Cálculo Diferencial e Integral:
um kit de sobrevivência



$$\int_\Omega K d\Omega + \int_{\partial\Omega} k_g(s)ds + \sum_{i=1}^{k} \phi_i = 2\pi\chi(\Omega).$$

Demonstração: Seja τ uma triangulação de Ω tal que qualquer triângulo T tido em uma vizinhança coordenada de uma parametrização ortogonal comp orientação de S (essa triangulação existe pelos comentários feitos acima). Poc o Teorema 2.1 para cada triângulo, obtendo

$$\int_{T_i} K dT_i + \int_{\partial T_i} k_g(s)ds + \sum_{p=1}^{3} \phi_p^i = 2\pi.$$

Como pontos e arestas possuem medida nula, podemos somar a equação acim os triângulos e obter

$$\sum_{i=1}^{k} \int_{T_i} K dT_i = \int_\Omega K d\Omega.$$

Como triângulos adjacentes induzem orientação contrária na aresta em comum, interseção dos triângulos se anulam na integral. Logo,

$$\sum_{i=1}^{k} \int_{\partial T_i} k_g(s)ds = \int_{\partial\Omega} k_g(s)ds.$$

Portanto,

$$\int_\Omega K d\Omega + \int_{\partial\Omega} k_g(s)ds + \sum_{i=1}^{k}\sum_{p=1}^{3} \phi_p^i = 2\pi F.$$

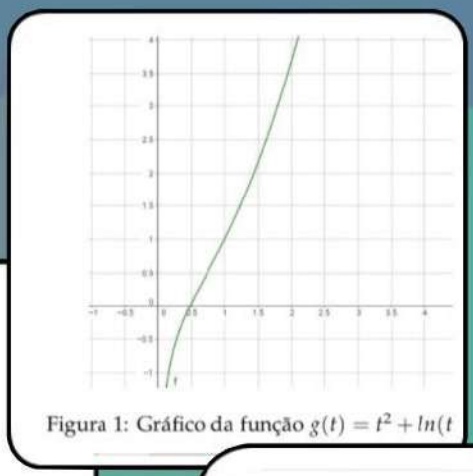
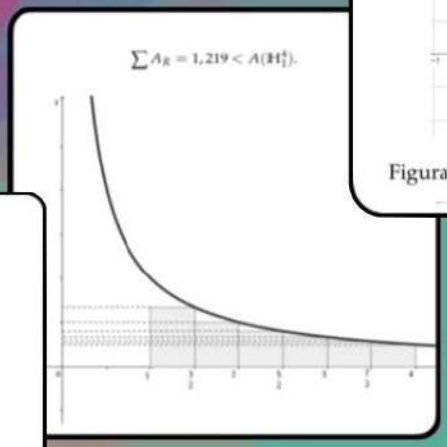


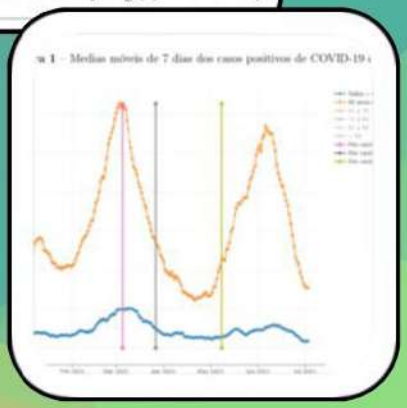
Figura 1: Gráfico da função $g(t) = t^2 + ln(t$



$$\sum A_R = 1,219 < A(\mathbb{H}^4_1).$$

O volume da esfera

Figura 8: Cone com área da base igual a πr^2 e altura $4r$.



Esta revista é responsável pela formulação de textos autorais desenvolvido pelo projeto de extensão "Kit". Neste projeto, contamos com alunos graduandos e demais interessados em matemática aplicada.
Entre seus textos, podemos encontrar, curiosidades, resoluções, demonstrações , fatos relevantes , ideais para IC, entre outros!