PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.5, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo841

A problemática do quadrado perdido e sua relação geométrica com a sequência de Fibonacci

Luana Paula Goulart de Menezes Vitor Marques Pereira

Abstract

Neste artigo investigaremos o enigma do quadrado perdido (*puzzle missing square*) e sua relação com a sequência de Fibonacci. Acreditamos que a exploração do problema tem o potencial de relacionar diversos conteúdos dentro da própria matemática e, consequentemente, pode ser um meio profícuo para o processo de ensino e aprendizagem nos mais diferentes níveis.

Palavras-chave: O quadrado perdido; Paradoxo de Curry; Identidade de Cassini; Geometria.

Abstract

In this article we will investigate the missing square puzzle and its relation to the Fibonacci sequence. We believe that the exploration of the problem has the potential to relate different contents within mathematics itself and, consequently, can be a useful means for the teaching and learning process at the most different levels.

Keywords: The lost square; Curry Paradox; Cassini's identity; Geometry.

1. Introdução

O *puzzle missing square* conhecido como paradoxo de Curry (que não é o paradoxo de Curry da teoria dos conjuntos) é um tipo de charada geométrica que consiste em observarmos duas organizações com 4 peças geométricas planas que estão ilustradas na Figura 1 .

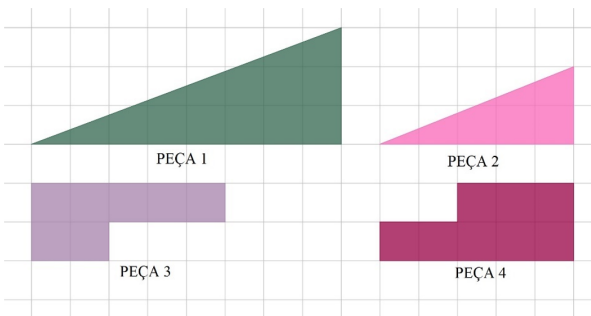


Figura 1: As 4 peças do *puzzle missing square*. Imagem reconstruída a partir de [2].

Usando as peças ilustradas acima, vamos organizá-las de modo a obter a Figura 2 que reproduzimos abaixo:

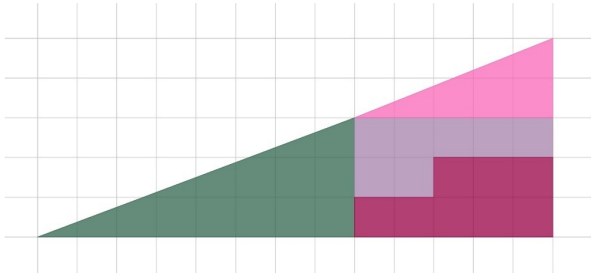


Figura 2: Organização das peças. Imagem reconstruída a partir de [2].

Observe que a figura obtida parece se ajustar ao triângulo retângulo com dimensões 13×5 . Note ainda que podemos reorganizar as posições das peças como mostra a Figura 3:

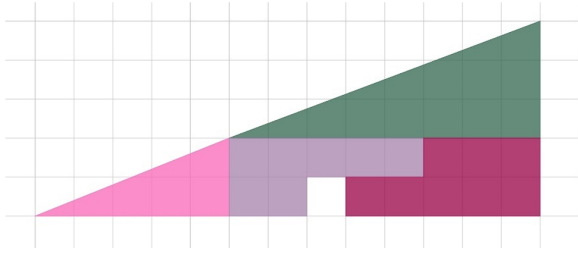


Figura 3: O quadrado perdido. Imagem reconstruída a partir de [2].

Perceba que tal disposição das peças também parece se ajustar em um triângulo retângulo com dimensões 13×5, com uma diferença: falta um quadrado! Como usamos as mesmas peças, deveríamos ter a conservação da área em ambas as disposições. Então, como isso é possível? Onde está o quadrado? O objetivo de apresentarmos o *puzzle* é responder essas perguntas.

2. A Área das peças e a área do "triângulo" construído

Com o objetivo de explicar o que aconteceu com o quadrado, vamos começar verificando a área de cada peça, encontrando, assim:

Peça 1: $\dfrac{8 \cdot 3}{2} = 12$u.a.

Peça 2: $\dfrac{5 \cdot 2}{2} = 5$u.a.

Peça 3: $1 \cdot 5 + 1 \cdot 2 = 7$u.a.

Peça 3: $1 \cdot 3 + 1 \cdot 5 = 8$u.a.

Desse modo, temos que área total ocupada pelas peças é:

$$A = 12 + 5 + 7 + 8 = 32\text{u.a.}$$

Mas como em ambas as Figuras 2 e 3 formamos um triângulo retângulo de dimensões 13×5, temos que área do mesmo pode ser obtida fazendo:

$$A = \frac{13 \cdot 5}{2} = 32,5\text{u.a.}$$

Logo, as peças 1, 2, 3 e 4 não cobrem todo o triângulo retângulo, pois não preenchem meio quadrado. Contudo, note que estamos observando a falta de meio quadrado e não 1 quadrado. Para explicarmos qual o segredo da disposição das peças, vamos calcular o ângulo θ entre a hipotenusa e o cateto adjacente das peças 1 e 2 e do triângulo obtido com a arrumação das peças que chamaremos de T (com catetos 13 e 5):

Peça 1: $\theta = \arctan\left(\frac{3}{8}\right) \approx 20,56^\circ$

Peça 1: $\theta = \arctan\left(\frac{2}{5}\right) \approx 21,8^\circ$

T: $\theta = \arctan\left(\frac{5}{13}\right) \approx 21,04^\circ$

Disso, obtemos que a hipotenusa não é uma reta, pois da construção realizada deveríamos obter o mesmo valor para o ângulo θ. Portanto, as figuras obtidas não são triângulos retângulos e sim quadriláteros. Mas como não notamos isso nas duas imagens? Uma explicação plausível está na diferença pequena entre os declives das peças 1 e 2:

$$\frac{2}{5} - \frac{3}{8} = \frac{1}{40}$$

Logo, a diferença ínfima não nos permite visualizá-la. As figuras 4 e 5 fora de escala ilustram o detalhe de falta e sobra nas áreas:

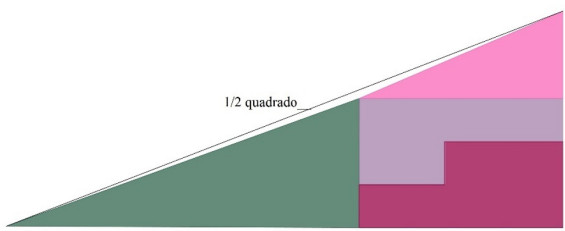


Figura 4: O quadrado perdido. Imagem reconstruída a partir de [2].

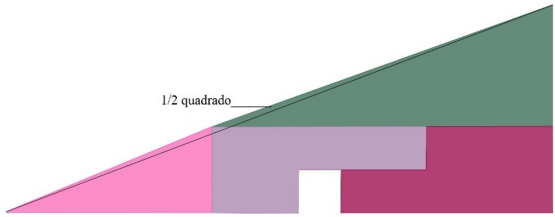


Figura 5: Visualizando a diferença. Imagem reconstruída a partir de [2].

Assim, o quadrado perdido está na metade de um quadrado que falta na Figura 4 e na metade do quadrado que sobra na Figura 5

2.1. A identidade de Cassini

Vamos observar ainda algo interessante: as dimensões inteiras dos lados das peças são 1, 2, 3, 5, 8 e 13, termos consecutivos da sequência de Fibonacci, isto é, $8n \geq 3$, $f_n = f_{n-1} + f_{n-2}$, com $f_1 = 1$ e $f_2 = 1$ (ver [3]).

Para efeito de curiosidade, aqui cabe um pequeno parêntese sobre Fibonacci (c.1175-c.1240): sabemos que nasceu em Pisa, Itália, e que "[...] viveu parte de sua juventude no norte da África, onde aprendeu o idioma e familiarizou-se com os costumes e a cultura árabes" (Santos, 2018, p. 20). Além disso, "Viajou extensamente pelo Mediterrâneo durante grande parte de sua vida, o que lhe rendeu o apelido Leonardo Bigollo (Leonardo Viajante). De volta à Itália, em torno de 1200, publicou o *Liber Abaci* (Livro do Ábaco ou Livro de Cálculo) em 1202" (Santos, 2018, p. 20). Em tal livro ele apresentou uma situação hipotética acerca da reprodução de coelhos, que é amplamente conhecido (veja mais em [3]).

No mais, vejamos que é uma propriedade da sequência citada acima que o produto de dois termos alternados da sucessão difere de uma unidade do quadrado do termo intermediário, isto é,

$$f_{n-1} \cdot f_{n+1} = f_n^2 + (-1)^n, 8n \in \mathbb{N}. \tag{1}$$

Exemplo 1: Para visualizarmos a relação escolhemos como exemplo os números consecutivos da sequência: 2, 3 e 5. Dessa forma: $2 \cdot 5 = 10$ e $3^2 = 9$, que satisfaz (1) com a adição do número 1 no segundo membro.

Exemplo 2: Do mesmo modo, se escolhermos os números 3, 5 e 8, obteremos $3 \cdot 8 = 24$ e $5^2 = 25$, que também satisfaz (1), agora com a subtração do número 1 no segundo membro.

Tal propriedade é conhecida como *identidade de Cassini*. Para demonstrá-la vamos considerar a matriz $F = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ e $f_{n+2} = f_{n+1} + f_n$, com $f_0 = 0$ e $f_1 = 1$ a sequência de Fibonacci.

Note que estamos considerando o primeiro termo como sendo zero, mas isso não altera a sequência e suas propriedades.

Assim, temos que se $F = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$:

$$F^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

$$F^3 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}$$

$$F^4 = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

$$\vdots$$

$$F^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}.$$

Para provarmos a última igualdade, vamos usar o Princípio de Indução Finita; mostrando que a igualdade é válida para n = 1, e, supondo que é válida para n = k, iremos mostrar que vale para n = k + 1:

i) F é válida para n = 1, pois:

$$F^1 = \begin{bmatrix} f_2 & f_1 \\ f_1 & f_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

ii) Suponha que F é válida para n = k, então:

$$F^k = \begin{bmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{bmatrix}. \tag{2}$$

Multiplicando ambos os membros da Equação (2) por F, temos:

$$F^k \cdot F = \begin{bmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \Leftrightarrow F^{k+1} = \begin{bmatrix} f_{k+1} + f_k & f_{k+1} \\ f_k + f_{k-1} & f_k \end{bmatrix} = \begin{bmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{bmatrix}.$$

Logo, F vale para n = k + 1. Portanto:

$$F^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}.$$

Voltando na identidade de Cassini, temos $f_{n-1} \cdot f_{n+1} = f_n^2 + (-1)^n$. Como $\det(F^n) = f_{n+1} \cdot f_{n-1} - f_n^2$, devemos mostrar que $\det(F^n) = (-1)^n$.

E, de fato, é propriedade dos determinantes que:

$$\det(F^n) = [\det(F)]^n. \tag{3}$$

Como $\det(F) = -1$, podemos substituir na Equação (3) e obtermos que $\det(F^n) = (-1)^n$.

Logo, $\det(F^n) = f_{n+1} \cdot f_{n-1} - f_n^2$, ou seja, $(-1)^n = f_{n+1} \cdot f_{n-1} - f_n^2$. Portanto:

$$f_{n-1} \cdot f_{n+1} = f_n^2 + (-1)^n$$

,

como queríamos demonstrar.

3. Identidade de Cassini e a relação geométrica com a construção

Como vimos, existe uma relação entre os três termos da sequência de Fibonacci. Todavia, como isso se relaciona com nossa problemática?

Para responder essa questão, iremos usar as notações de [1]:

$$\begin{cases} A + B = C \\ B^2 = A \cdot C \pm X, \end{cases}$$

em que A, B e C, no sistema, são consecutivos da sequência de Fibonacci, e, como vimos, temos que $\pm X$ na identidade de Cassini é ± 1 (a segunda equação do sistema). Notamos então, que temos a área de um quadrado de lado B que ao compararmos com o lado de um retângulo com lados A e C, deveremos acrescentar ou retirar uma unidade.

No exemplo que estamos considerando desde o início deste artigo podemos dobrar as peças que estão na Figura 1 para termos um quadrado com A = 64u.a.. Assim, uma possível organização é ilustrada na Figura 6.

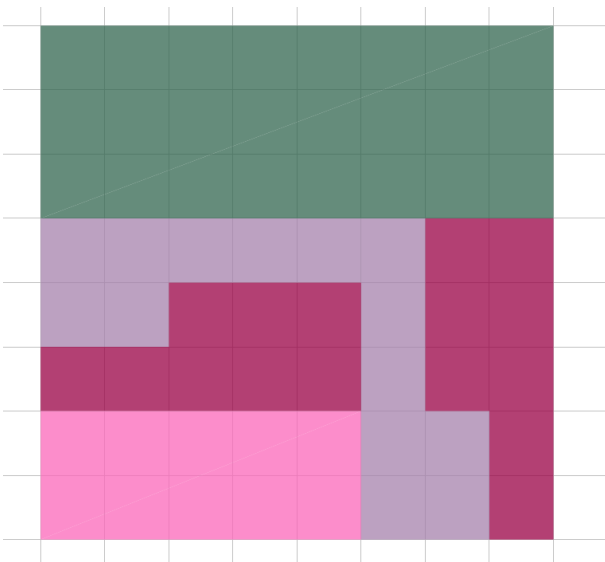


Figura 6: Uma organização quadrada das peças.

Note agora que usando as mesmas peças teremos a falta de um quadrado (Figura 7):

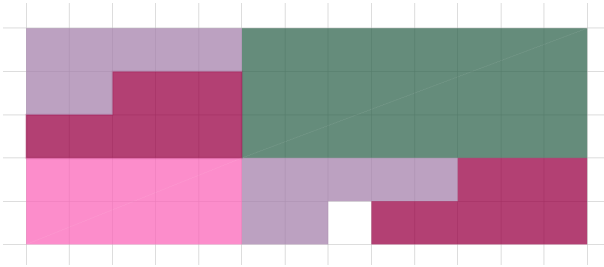


Figura 7: Uma organização retangular das peças.

Isso já era esperado, uma vez que a equação $8^2 = 5 \cdot 13 + X$ é válida com $X = -1$. Isso significa que um quadrado é perdido de uma organização para outra.

4. Considerações Finais

Da identidade de Cassini temos que outras figuras que apresentam o mesmo fenômeno podem ser obtidas com termos consecutivos da sequência de Fibonacci, como o *puzzle* de Carroll que não foi apresentado neste artigo.

Ademais, com a motivação do enigma do quadrado perdido, podem ser ensinados vários conceitos, por exemplo, área, declive, o princípio de indução finita, determinantes, sequência de Fibonacci e propriedades. Não podemos deixar de mencionar ainda que sua construção tem a vantagem de visualização e manipulação de material concreto, sendo assim um interessante instrumento para o processo de ensino-aprendizagem. Tal problemática pode ser explorada tanto em níveis básicos como em nível superior considerando-se diversos níveis de complexidade.

Referências

[1] Gardner, *M. Mathematics, magic and mystery*. Dover, New York, 1956.

[2] Santos, C. P.; NETO, J. P.; SILVA, J. N. *Sucessão de Fibonacci + 'Missing Square'*. Lisboa: Público-Visão, 2007.

[3] Santos, F. H. *Funções de Fibonacci:Um estudo sobre a razão áurea e a sequência de Fibonacci*. 2018. 51 f. Dissertação (Mestrado) -Profmat, Universidade Federal de Alagoas, Maceió, 2018.

Luana Paula Goulart de Menezes
Universidade Estadual de Maringá
<lluanagoulart@gmail.com>

Vitor Marques Pereira
Universidade Estadual do Oeste do Paraná
<vitormarques@yahoo.com>

Recebido: 21/09/2020
Publicado: 25/11/2020

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.5, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo842

Torres de Hanói de 3 e 4 pinos: abordagens para o Ensino Básico

Débora Borges Ferreira Edvan Pontes de Oliveira [1] Francisco Quaranta Neto

Resumo

Este trabalho mostra como explorar diversos conceitos matemáticos usando o jogo clássico Torres de Hanói com 3 pinos, e também como encontrar a solução para uma de suas variantes com 4 pinos. Para o caso clássico de 3 pinos, investigamos uma fórmula matemática que expressa a quantidade mínima de jogadas necessárias para vencer o jogo em função da quantidade de discos usando recorrências/recursividade, modelagem matemática e progressões geométricas. Apresentamos também fórmulas para o número de vezes que um disco ocupa cada um dos pinos durante a solução ideal do quebra-cabeça, ou seja, a que utiliza a menor quantidade de jogadas possíveis. Para a variante do jogo com 4 pinos, conhecida como quebra-cabeça de Reve, encontraremos uma fórmula fechada que expressa a quantidade mínima de jogadas para vencer o jogo em função do número de discos.

Palavras-chave: Torre de Hanói com 3 pinos; Torre de Hanói com 4 pinos; Recorrência; Quantidade Mínima de Movimentos; Modelagem Matemática.

Abstract

In this work we show how to explore mathematical concepts using the classical puzzle Tower of Hanói with 3 pegs, and how to find the solution for one of the variations with 4 pegs. For the classical case with 3 pegs, we investigated a mathematical formula that express the minimum amount of moves required to win the game based on the number of disks, we use recurrences, mathematical modeling and geometric progressions. We also present formulas for the number of times a disc occupies each one of the pegs during the ideal puzzle solution, that is, the one that uses the least amount of moves possible. For the variation with 4 pegs, known Reve´s puzzle, we find a closed formulae that express the minimum quantity of moves to win the game.

Keywords: Tower of Hanói with 3 pegs; Tower of Hanói with 4 pegs; Recurrences; Minimum Amount of Moves; Mathematical Modeling.

1. Introdução

O quebra cabeça as Torres de Hanói ficou famoso por meio do matemático francês Édouard Lucas no ano de 1893, na obra *Récréations Mathématiques*, volume III, [6]. Lucas conheceu-o através do

[1]Parcialmente apoiada pela Capes

amigo e professor N. Claus (do Sião), que fora apresentado ao quebra-cabeça em uma das suas viagens ao Vietnã, especificamente na região de Tonkin.

Figura 1: Édouard Lucas.

Lucas estimou o tempo necessário para resolver o jogo considerando um movimento por segundo. Com 64 discos, seriam necessários 18.446.744.073.709.551.615 movimentos, o que equivale a bilhões de séculos para resolver sem pausas. Além disso, Lucas comparou a solução matemática com um quebra-cabeça muito famoso da China, o Baguenaudier, que é um quebra-cabeça de desemaranhamento de anéis.

Logo após a descoberta do jogo, surgiram outras variações de desafios no início do século XX, sendo a mais famosa as Torres de Hanói com 4 pinos citada na obra *The Canterbury Puzzle* do especialista em quebra-cabeças e matemático Henry Ernest Dudeney, [2]. 87

Há muitas curiosidades envolvidas nesse jogo, por exemplo: a semelhança entre o Triângulo de Sierpinsk e um grafo representando os possíveis movimentos dos discos da Torre, ver em [9]. Para o caso clássico, em uma solução para o jogo utilizando a menor quantidade de movimentos possível, suponha que essa seja interrompida em uma jogada i,; em [3] ou [8] é descrita a configuração da torre nesse instante, isto é, em qual pino cada um dos discos estará. Mais curiosidades e detalhes sobre o assunto no livro [4].

O quebra-cabeça Torres de Hanói é composto por uma base e três pinos; chamaremos esses de A, B e C. No pino A há discos empilhados com diferentes tamanhos, em sequência do maior para o menor, como mostra a figura a seguir:

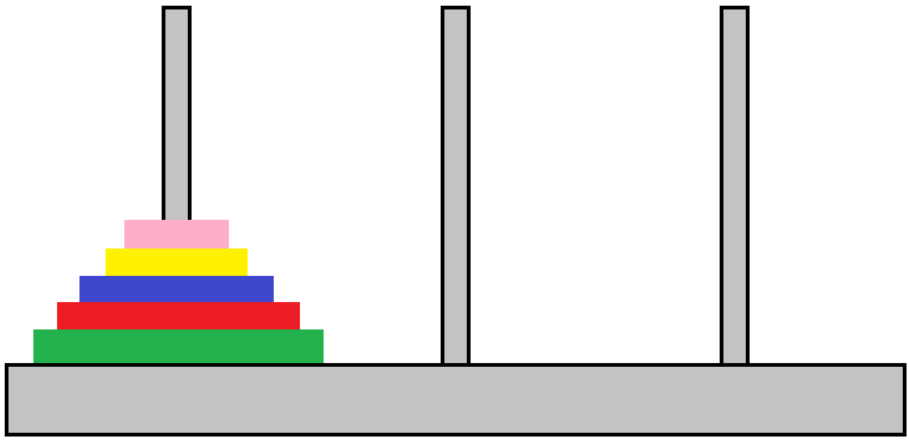


Figura 2: Torre de Hanói com 3 pinos.

O objetivo do jogo é transferir a pilha de discos do pino inicial A para o pino C, usando as regras a seguir:

- Apenas um disco pode ser movido por vez.
- Nenhum disco pode ficar em cima de um de raio menor.
- Apenas o disco do topo pode ser movido.

Nesse artigo, exploramos as ferramentas matemáticas no estudo da quantidade mínima de movimentos necessários para vencer o quebra-cabeça com n discos nos dois casos, com 3 e 4 pinos, e também quantas vezes cada disco se mover-se-á para os pinos A, B e C, caso clássico com 3 pinos. Consideramos as sequências numéricas $\{a_n\}$, onde a_n é a quantidade mínima de movimentos necessários para transferir os n discos de um pino A para C quando possuirmos 3 pinos e $\{b_n\}$, para 4 pinos. Estamos à procura de uma expressão para a_n e b_n.

2. Torre com 3 pinos

2.1. Recursão

Suponha que temos os n discos empilhados no pino A em forma de cone e desejamos transferi-los para o pino C. Observe que o último disco, ou seja, o maior de todos, será movido após retirarmos os $n-1$ discos que estão em cima dele, para isso usaremos a_{n-1} movimentos e os colocaremos no pino B. Então, transferimos o maior disco para o pino C usando 1 movimento, e para finalizar realocamos os $n-1$ discos no pino B para o pino C, usando mais a_{n-1} movimentos e concluímos o jogo. Para isso, efetuamos $a_{n-1} + 1 + a_{n-1}$ movimentos no total, ou seja,

$$a_n = 2a_{n-1} + 1 \text{ e } a_1 = 1, \tag{1}$$

pois com 1 disco temos apenas 1 movimento, que seria retirá-lo do pino A e colocá-lo do pino C. Acabamos de obter uma forma recursiva para a sequência (a_n) .

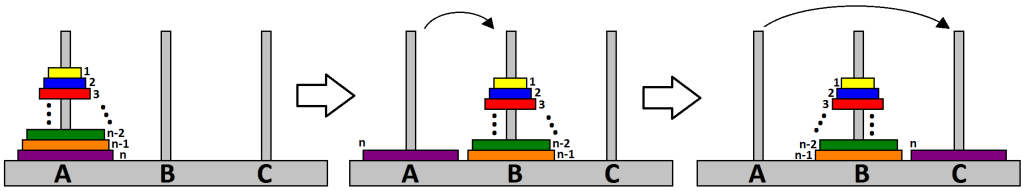


Figura 3: Solução com n discos.

Para uma torre com 1 disco é necessário 1 movimento apenas, daí $a_1 = 1$:

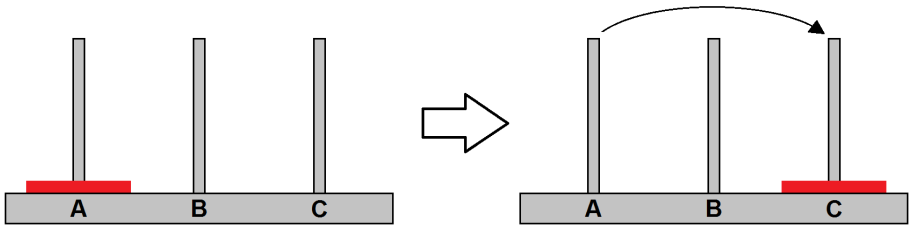


Figura 4: Solução com 1 disco.

Para uma torre com 2 discos são necessários 3 movimentos:

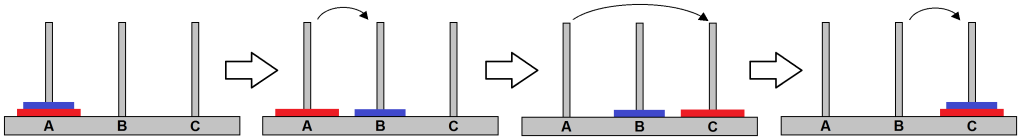


Figura 5: Solução com 3 discos.

Logo, $a_2 = 2a_1 + 1 = 2.1 + 1 = 3$. Com 3 discos, substituímos $a_3 = 2a_2 + 1 = 2.3 + 1 = 7$:

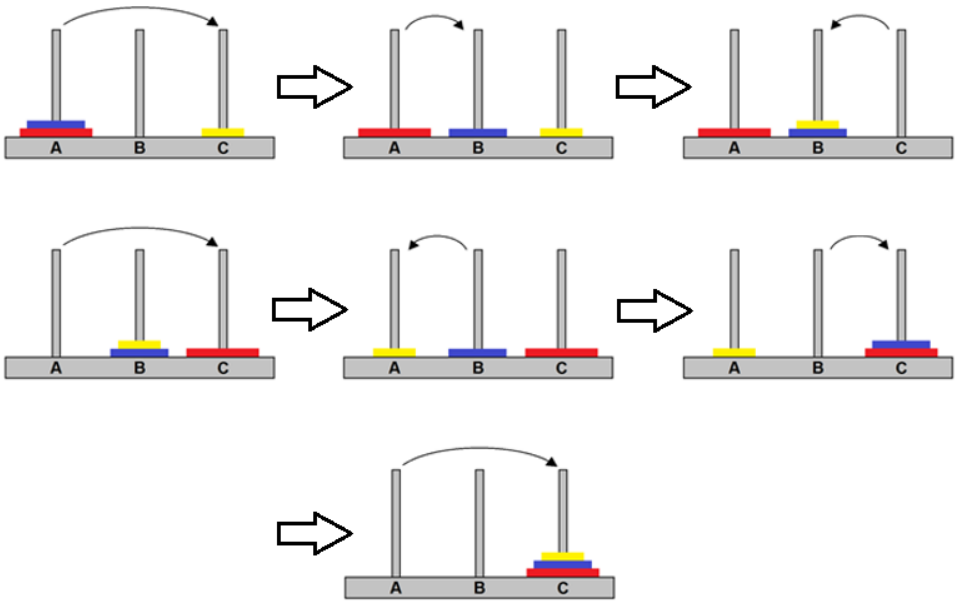


Figura 6: Solução com 3 discos.

Intuitivamente, percebemos que o maior disco move-se 1 vez, o segundo maior 2 vezes, o disco seguinte 4 vezes, ou seja, cada disco tem o dobro de movimentos do seu antecessor. Sendo assim, podemos escrever:

$$a_n = 2^{n-1} + 2^{n-2} + ... + 2 + 1,$$

que é a soma de uma Progressão Geométrica com n termos, primeiro termo 2^{n-1} e razão 2^{-1}.

Assim,

$$a_n = \frac{2^{n-1}(1-2^{-n})}{1-2^{-1}} \Rightarrow a_n = 2^n - 1 \qquad (2)$$

para todo n natural, obtemos uma expressão fechada para a_n.

2.2. Indução Matemática

Note que essa argumentação foi apenas intuitiva. Uma prova formal para esse fato pode ser obtida usando Indução Matemática, que é uma ferramenta poderosíssima em demonstrações de proposições no conjunto dos números naturais. Em resumo, seja uma proposição ou propriedade que desejamos mostrar ser satisfeita para todos os números naturais. Tal proposição é verdadeira para n = 1 . Se, por hipótese, a proposição for satisfeita para um certo n, e isso implicar em ser satisfeita para n + 1, então a proposição é válida para todo n natural.

Queremos provar que $a_n = 2^n - 1$ para todo n natural. Para n=1, temos $a_1 = 1 = 2^1 - 1$; logo, a proposição é verdadeira para n=1. Suponha, por hipótese de indução, que $a_n = 2^n - 1$ para algum

natural n. Agora, suponha que temos n + 1 discos, e queremos saber quanto vale a_{n+1}. Vimos na fórmula recursiva que $a_{n+1} = 2a_n + 1$, e, então,

$$a_{n+1} = 2a_n + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 1.$$

Logo, se supusermos a proposição válida para n , então ela vale para n + 1 . Desse modo, por Indução Matemática, ela é válida para todo n natural.

2.3. Modelagem Matemática

Uma outra maneira de encontrar o termo geral de e ao mesmo tempo abordar o assunto funções é usar modelagem matemática, ou seja, estudar o comportamento da sequência e encontrar uma função elementar que a descreva. De modo geral, toda sequência numérica (a_n) é uma função com domínio nos naturais e imagem nos reais. Procuramos $f : \mathbb{R} \to \mathbb{R}$ dentre as funções estudadas no ensino básico (polinomial, trigonométrica, logaritmica e exponencial), uma que coincida com a sequência, isto é, $a_n = f(n)$. Para facilitar, a partir de agora chamamos a_n de f(n). Considere a tabela abaixo, que representa as quantidades mínimas de movimentos necessários para vencer o jogo de acordo com a quantidade de discos:

Número de discos	**Quant. movimentos**
1	1
2	3
3	7
4	15
5	31
6	63
7	127

Tabela 1: Número mínimo de jogadas em função do número de discos.

A partir dela, traçamos o gráfico de pontos cujo eixo das abscissas corresponde ao número de discos e o eixo das ordenadas à quantidade mínima de movimentos.

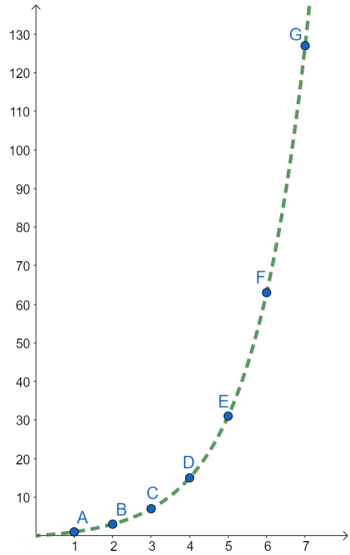


Figura 7: Gráfico ajustado.

Observando o gráfico, desconfiamos que seja uma polinomial ou função com crescimento exponencial. Primeiramente, observe, intuitivamente, que é crescente e injetiva pois quanto mais discos o jogo possui, maior a quantidade de movimentos necessária para vencer o jogo. Mostraremos agora que f não é do tipo polinomial.

Proposição 1. *A função* f(n)*, número mínimo de movimentos em função do número de discos* n*, não é polinomial.*

Demonstração. Suponha por contradição que $f(n) = \sum_{p=0}^{k} b_p n^p$ é um polinômio de grau k, com $b_k \neq 0$. Então:

$$f(n+1) = \sum_{p=0}^{k} b_p (n+1)^p. \tag{3}$$

Subtraindo de (3) f(n), obtemos:

$$\begin{aligned}
f(n+1)-f(n) &= \sum_{p=0}^{k} b_p(n+1)^p - \sum_{p=0}^{k} b_p n^p \\
&= \sum_{p=0}^{k} b_p\left((n+1)^p - n^p\right) \\
&= b_k\left((n+1)^k - n^k\right) + \sum_{p=0}^{k-1} b_p\left((n+1)^p - n^p\right) \\
&= b_k\left(n^k + \sum_{p=0}^{k-1}\binom{k-1}{p} n^{k-1-p} - n^k\right) + \sum_{p=0}^{k-1} b_p\left((n+1)^p - n^p\right) \\
&= b_k\left(\sum_{p=0}^{k-1}\binom{k-1}{p} n^{k-1-p}\right) + \sum_{p=0}^{k-1} b_p\left((n+1)^p - n^p\right),
\end{aligned}$$

que é um polinômio de grau $k-1$. Por recorrência, vimos que $f(n) = 2\cdot f(n-1)+1$; logo, $f(n+1) = 2\cdot f(n)+1$. Assim, $f(n+1)-f(n) = f(n)+1$. Se f fosse uma polinomial de grau k, então o grau de $f(n+1)-f(n)$ teria o mesmo grau de $f(n)+1$, que é k. O que não ocorre em polinômios. Logo, f **não** é uma função polinomial.

□

Uma outra demonstração da Proposição 1 é por meio de derivadas de ordem superior. Vejamos a seguir.

Demonstração. Seja $f(n) = \sum_{p=0}^{k} b_p n^p$ um polinômio de grau k, com $b_k \neq 0$.

Sabendo que $f(n) = 2\cdot f(n-1)+1$ e derivando k vezes f, obtemos:

$$f^{(k)}(n) = k!\cdot b_k.$$

Assim, temos:

$$\begin{aligned}
f^{(k)}(n) &= 2\cdot f^{(k)}(n-1) \\
\Rightarrow k!\cdot b_k &= 2\cdot k!\cdot b_k \\
\Rightarrow b_k &= 2\cdot b_k.
\end{aligned}$$

Essa igualdade só é verdadeira se $b_k = 0$, o que contraria a nossa hipótese. Portanto, função f não pode ser um polinômio. □

Proposição 2. *A função* f(n)*, número mínimo de movimentos em função do número* n *discos, não é logarítmica.*

Demonstração. Seja $f(n) = \log_a(bn+c)+d$, $8a,b,c,d \in \mathbb{R}$, onde $a \neq 1$ e $a > 0$.

Utilizando a relação da recorrência (1), temos:

$$\begin{aligned}
f(n+1) &= 2\cdot f(n)+1\\
\Rightarrow \log_a(b(n+1)+c)+d &= 2\cdot(\log_a(bn+c)+d)+1\\
\Rightarrow \log_a(b(n+1)+c)+d &= 2\cdot\log_a(bn+c)+2d+1\\
\Rightarrow \log_a(b(n+1)+c) &= \log_a(bn+c)^2+d+1\\
\Rightarrow \log_a(b(n+1)+c)-\log_a(bn+c)^2 &= d+1\\
\Rightarrow \log_a\left(\frac{(b(n+1)+c}{(bn+c)^2}\right) &= d+1\\
\Rightarrow a^{d+1} &= \frac{b(n+1)+c}{(bn+c)^2}\\
\Rightarrow a^{d+1}\cdot(bn+c)^2 &= b(n+1)+c\\
\Rightarrow a^{d+1}b^2n^2+2a^{d+1}bcn+c^2a^{d+1} &= bn+b+c.
\end{aligned}$$

Igualando os coeficientes de mesma potência temos:

$$a^{d+1}b^2 = 0, \tag{4}$$
$$2a^{d+1}bc = b \quad e \tag{5}$$
$$c^2a^{d+1} = b+c. \tag{6}$$

De (4), temos que $a=0$ ou $b=0$. Não é possível $a=0$, pois contraria a definição de logaritmo; logo, $b=0$. Assim, $f(n)=\log_a(c)+d$ é constante, mas f não é constante, logo, não pode ser desse tipo. □

Continuando a nossa análise, vamos verificar se f é exponencial. Analisando o comportamento das derivadas de ordem superior da função polinomial $f^{(k)}(n)=2\cdot f^{(k)}(n-1)$, vemos que a função relacionada ao jogo é uma função de crescimento exponencial. Logo, a função $f(n)=k\cdot a^n+b$, tal que k, b e $a\in\mathbb{R}$ constantes, com $a\neq 1$, é a função candidata que procuramos.

Proposição 3. *A função* $f(n)$*, número mínimo de movimentos em função do número* n *de discos não é exponencial, isto é, não tem a forma* $f(x)=b^x, 0<b\neq 1$*, e sim de crescimento exponencial.*

Demonstração. De acordo com [5], as funções exponenciais têm, exclusivamente, as seguintes propriedades:

1. $f(x)\cdot f(y)=f(x+y)$
2. $f(x)=b^x$, $8x\in\mathbb{R}$, onde $f(1)=b$
3. $f(nx)=f(x)^n$
4. $x<y\Rightarrow f(x)<f(y)$, $b>1$
   $x<y\Rightarrow f(y)<f(x)$, $0<b<1$

Sabemos que para vencer o jogo com 1 disco é necessário apenas 1 movimento, ou seja, $f(1)=1$. Com 2 discos, são necessários 3 movimentos então, $f(2)=3$. Com 3 discos, são necessários 7 movimentos, ou seja, $f(3)=7$.

Observando as características da definição de função exponencial, vemos que obedece apenas uma das propriedades:

1. $f(1) \cdot f(2) = 1 \cdot 3 = f(1+2) = 7$ (falso)

2. $f(x) = b^x$, $8x \in \mathbb{N}$, onde $f(1) = b = 1$ (falso)

3. $f(2 \cdot 1) = f(1)^2$ (falso)

4. $1 < 2 \Rightarrow f(1) < f(2)$, $b > 1$ (verdadeiro)

O que mostra claramente que a função não é do tipo $f(n) = b^n$. Resta-nos analisar a função da família da exponencial mais geral, a do tipo $f(n) = k \cdot b^n + c$, $a > 0, b \neq 1, k \neq 0, b, c, k \in \mathbb{R}$.

Pela relação da recorrência (1) sabemos que $f(n) = 2 \cdot f(n-1) + 1$, daí obtemos:

$$\begin{aligned} f(n) &= 2 \cdot f(n-1) + 1 \\ \Rightarrow k \cdot a^n + b &= 2 \cdot (k \cdot a^{n-1} + b) + 1 \\ \Rightarrow k \cdot a^n + b &= 2 \cdot k \cdot a^{n-1} + 2 \cdot b + 1 \\ \Rightarrow k \cdot a^n &= 2 \cdot k \cdot a^{n-1} + b + 1 \\ \Rightarrow k \cdot a \cdot a^{n-1} &= 2 \cdot k \cdot a^{n-1} + b + 1. \end{aligned} \tag{7}$$

Da equação (7), vamos igualar os coeficiente dos dois lados. Temos que $2 \cdot k = k \cdot a \Rightarrow a = 2$ e $b + 1 = 0 \Rightarrow b = -1$. Portanto, a função $f(n) = k \cdot 2^n - 1$ é a procurada. Resta saber o valor de k. Como $f(1) = 1$, então $f(1) = k \cdot 2^1 - 1 = 1$. Logo, $2k = 2$, implicando $k = 1$. Assim, a função que procuramos é

$$f(n) = 2^n - 1. \tag{8}$$

□

2.4. Progressão Geométrica

Para finalizar essa seção, encontraremos uma expressão para f(n) usando progressões geométricas e a quantidade total de movimento de cada disco na solução do jogo.

Suponha uma torre com n discos. Se observarmos o movimento de cada disco no jogo, vemos que o maior disco move-se uma única vez. O disco $n-1$ move-se duas vezes: uma vez para ir ao pino B, logo a seguir $n-2$ discos serão colocados em cima dele, o maior disco fará seu único movimento para o pino C, a seguir os $n-1$ discos retornam ao pino A, e o disco $n-1$ fará seu segundo movimento para o pino C, totalizando dois movimentos. O disco $n-2$ fará o dobro de movimentos do disco $n-1$, totalizando 4 movimentos. E assim sucessivamente. Considere a tabela a seguir onde a primeira coluna é a quantidade total de discos e a segunda descreve a soma dos movimentos de cada disco, do maior (sempre 1) até o menor.

Nº discos	Quant. movimentos
1	1
2	1 + 2
3	1 + 2 + 4
4	1 + 2 + 4 + 8
5	1 + 2 + 4 + 8 + 16

Tabela 2: Número mínimo de jogadas para 5 discos em função da soma dos movimentos de cada disco

A tabela anterior mostra que a quantidade de movimentos de cada disco é o dobro do anterior, em especial potências de base 2, sendo que o maior disco tem apenas 1 movimento.

Nº discos	Quant. movimentos
1	2^0
2	$2^1 + 2^0$
3	$2^2 + 2^1 + 2^0$
4	$2^3 + 2^2 + 2^1 + 2^0$
5	$2^4 + 2^3 + 2^2 + 2^1 + 2^0$

Tabela 3: Número mínimo de jogadas para 5 discos em função da soma dos movimentos de cada disco

Pra reforçar esse padrão, vamos utilizar novamente a Proposição , mostrando a quantidade mínima de movimentos para 6 discos:

$$\begin{aligned} a_n &= 2 \cdot a_{n-1} + 1 \\ \underbrace{2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0}_{6 \text{ discos}} &= 2 \cdot (\underbrace{2^0 + 2^1 + 2^2 + 2^3 + 2^4}_{5 \text{ discos}}) + 1 \end{aligned}$$

As tabelas anteriores mostram essa propriedade de uma maneira empírica. Vamos ver uma prova formal para um disco k. Intuímos que, para uma Torre de Hanói com n discos, a quantidade mínima de movimentos de um disco k será 2^{n-k}.

Teorema 1. *A quantidade de movimentos de um disco* k *em função de* n *discos no total é dada por* $d_{n,k} = 2^{n-k}$, $1 \leq k \leq n$.

Demonstração. Seja k fixado tal que $k \leq n$. Para $n = 1$, então $k = 1$ e $d_{1,1} = 2^{1-1} = 2^0 = 1$, que é verdadeiro, pois com 1 disco só ocorre 1 movimento. Suponha por hipótese que $d_{n,k} = 2^{n-k}$ para algum $k \leq n$. Provaremos que $d_{n+1,k} = 2^{n+1-k}$, para todo $k \leq n+1$. Se $k \leq n$, então, para movermos a torre com $n+1$ discos do pino A para o pino C, primeiro movemos a torre com n discos de A para B; realizando $d_{n,k}$ movimentos com o disco k, por hipótese movemos o disco $k+1$ para o pino C, e depois movemos a torre com n discos de B para C, realizando mais 2^{n-k} movimentos com o disco k. Totalizamos $2 \cdot 2^{n-k} = 2^{n+1-k}$.

Assim, $d_{n+1,k} = 2^{n+1-k}$ se $k \leq n$. Se $k = n+1$, então, $d_{n+1,n+1} = 2^{n+1-(n+1)} = 2^0 = 1$ que é a quantidade de movimentos do disco $n+1$.

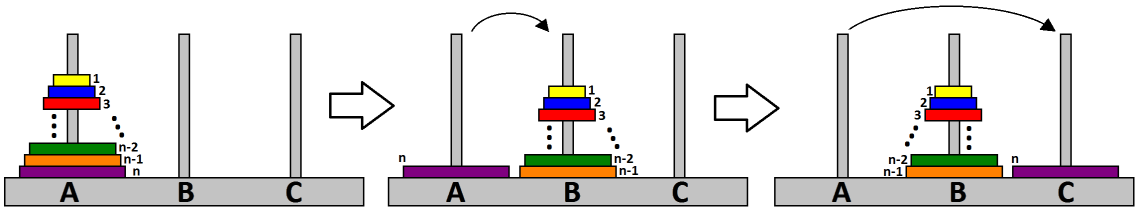


Figura 8: Solução da Torre com 3 pinos.

Agora que já sabemos que a quantidade de jogadas de cada disco é uma progressão geométrica de razão 2, com o primeiro elemento valendo 1, podemos encontrar a fórmula fechada da quantidade mínima de movimentos em função de n.

Aplicando a fórmula da soma S_n de n termos de uma progressão geométrica, de $d_{n,1} = 1$ e razão igual a 2, temos:

$$S_n = \frac{d_{n,1} \cdot (2^n - 1)}{2 - 1} = \frac{1 \cdot (2^n - 1)}{2 - 1} = 2^n - 1.$$

Logo, $a_n = S_n = 2^n - 1$.

□

2.5. Número de vezes que um disco k vai para os pinos A, B ou C

Nesta seção, iremos estudar, através de sequências e recorrências, o número de vezes que cada disco é movido para o pino inicial (A), o pino intermediário (B) e o pino final (C).

Sejam $A_{n,k}, B_{n,k}$ e $C_{n,k}$ a quantidade mínima de jogadas que um disco k vai para os pinos A, B e C, e $d_{n,k}$ a quantidade de movimentos que do disco k para um total de n discos.

Primeiramente, vamos observar o padrão com 1, 2, 3, 4 e 5 discos no total.

Disco k	A	B	C	Total
Disco 1	0	0	1	1

Tabela 4: Número de vezes que um disco vai para os pinos

Como temos apenas 1 disco, então esse só é movimentado uma vez para o pino C, ou seja, $A_{1,1} = 0$, $B_{1,1} = 0$ e $C_{1,1} = 1$. Para 2 discos temos a Tabela 5.

Disco k	A	B	C	Total
Disco 2	0	0	1	1
Disco 1	0	1	1	2

Tabela 5: Número de vezes que os discos 1 e 2 ocupam os pinos

O maior sempre vai primeiramente para o pino final C, enquanto o disco menor vai para o pino B e C, uma vez para cada. Usando a notação, teremos:

$$A_{2,2} = 0, B_{2,2} = 0 \text{ e } C_{2,2} = 1.$$
$$A_{2,1} = 0, B_{2,1} = 1 \text{ e } C_{2,2} = 1.$$

Vejamos agora uma tabela para 3 discos no total:

Disco k	A	B	C	Total
Disco 3	0	0	1	1
Disco 2	0	1	1	2
Disco 1	1	1	2	4

Tabela 6: Número de vezes que os discos 1, 2 e 3 ocupam os pinos

$$A_{3,3} = 0, B_{3,3} = 0 \text{ e } C_{3,3} = 1.$$
$$A_{3,2} = 0, B_{3,2} = 1 \text{ e } C_{3,2} = 1.$$
$$A_{3,1} = 1, B_{3,1} = 1 \text{ e } C_{3,1} = 2.$$

Observe que a soma das quantidades das jogadas do disco k em cada pino resulta na quantidade total de movimentos do disco k, que pelo Teorema 1 é 2^{n-k}, ou seja:

$$A_{n,k} + B_{n,k} + C_{n,k} = 2^{n-k}. \tag{9}$$

Teorema 2. *Considere o jogo com* n *discos. A quantidade de vezes que o disco k ocupa os pinos* A, B *e* C, *respectivamente, durante a solução do jogo é dada por:*

$$C_{n,k} = \frac{2^{n+1-k} + 3 + (-1)^{n+k}}{6}, \tag{10}$$
$$B_{n,k} = \frac{2^{n-k} + (-1)^{n+k+1}}{3} \quad \text{e} \tag{11}$$
$$A_{n,k} = \frac{2^{n+1-k} - 3 + (-1)^{n+k}}{6}. \tag{12}$$

Demonstração. Usaremos Indução Matemática, primeiro mostraremos que as três fórmulas anteriores são verdadeiras para n = 1; por hipótese de indução suporemos que são verdadeiras para um n qualquer, e mostraremos que valem para n + 1 discos, isto é,

$$A_{n+1,k} = \frac{2^{n+2-k} - 3 + (-1)^{n+k+1}}{6}$$
$$B_{n+1,k} = \frac{2^{n+1-k} + (-1)^{n+k+2}}{3} \quad \text{e}$$
$$C_{n+1,k} = \frac{2^{n+2-k} + 3 + (-1)^{n+k+1}}{6}.$$

Para n = 1, temos que k = 1, e

$$A_{1,1} = \frac{2^{1+1-1} - 3 + (-1)^{1+1}}{6} = 0$$
$$B_{1,1} = \frac{2^{1-1} + (-1)^{1+1+1}}{3} = 0$$
$$C_{1,1} = \frac{2^{1+1-1} + 3 + (-1)^{1+1}}{6} = 1.$$

Logo, as três fórmulas valem para $n = 1$.

Suponha que sejam válidas para n discos, e vamos provar que valem para $n+1$ discos. Para mover $n+1$ discos para o pino C, primeiro movemos os n discos menores para o pino B, o maior disco para o pino C, e por último os n discos que estão em B para C também.

Observe que $A_{n,k}$ é a quantidade de vezes que o disco k passa por A ao movermos a pilha de n discos de A para C. Assim, $A_{n,k}$ é também a quantidade de vezes que o disco k passa por B ao movermos a pilha de n discos de B para C. Como $B_{n,k}$ é a quantidade de vezes que o disco k passa por B ao mover a pilha de n discos de A para C, $B_{n,k}$ é também a quantidade de vezes que o disco k passa por C ao mover a pilha de n discos de A para B. Seguindo o raciocínio, $C_{n,k}$ é a quantidade de vezes que o disco k movimenta-se para o pino C ao transferirmos os n discos de A para C, e é também a quantidade de vezes que o mesmo disco k passa por B ao movermos os n discos de A para B.

Para sabermos quantas vezes um disco k se movimentar-se-á para o pino A durante esse processo de transferir $n+1$ discos de A para C, calculamos quantas vezes ele se move para A ao colocarmos os n discos em B, e somamos às quantidades de vezes que se move em A para transferir os n discos de B para C: $A_{n+1,k} = A_{n,k} + B_{n,k}$. Da mesma forma, $B_{n+1,k} = A_{n,k} + C_{n,k}$ e $C_{n+1,k} = B_{n,k} + C_{n,k}$.

Assim, se as fórmulas valem para n, podemos mostrar que valem para $n+1$.

$$\begin{aligned}
A_{n+1,k} &= A_{n,k} + B_{n,k} \\
&= \frac{2^{n+1-k} - 3 + (-1)^{n+k}}{6} + \frac{2^{n-k} + (-1)^{n+k+1}}{3} \\
&= \frac{2^{n+1-k} - 3 + (-1)^{n+k}}{6} + \frac{2 \cdot 2^{n-k} + 2 \cdot (-1)^{n+k+1}}{6} \\
&= \frac{2^{n+1-k} - 3 + (-1)^{n+k}}{6} + \frac{2^{n+1-k} + 2 \cdot (-1)^{n+k+1}}{6} \\
&= \frac{2 \cdot 2^{n+1-k} - 3 - (-1)^{n+k}}{6} \\
&= \frac{2^{n+2-k} - 3 - (-1)^{n+k+1}}{6}.
\end{aligned}$$

De modo análogo obtemos

$$\begin{aligned}
B_{n+1,k} &= A_{n,k} + C_{n,k} \\
&= \frac{2^{n+1-k} - 3 + (-1)^{n+k}}{6} + \frac{2^{n+1-k} + 3 + (-1)^{n+k}}{6} \\
&= \frac{2 \cdot 2^{n+1-k} + 2 \cdot (-1)^{n+k}}{6} \\
&= \frac{2^{n+1-k} + (-1)^{n+k}}{3}.
\end{aligned}$$

E também

$$\begin{aligned} C_{n+1,k} &= B_{n,k} + C_{n,k} \\ &= \frac{2^{n-k} + (-1)^{n+k+1}}{3} + \frac{2^{n+1-k} + 3 + (-1)^{n+k}}{6} \\ &= \frac{2 \cdot 2^{n-k} + 2 \cdot (-1)^{n+k+1}}{6} + \frac{2^{n+1-k} + 3 + (-1)^{n+k}}{6} \\ &= \frac{2^{n+2-k} + 3 + (-1)^{n+k+1}}{6}. \end{aligned}$$

Para concluir, vamos verificar que $A_{n,k} + B_{n,k} + C_{n,k} = 2^{n-k}$, pois essa soma corresponde ao total de vezes que o disco k passou pelos pinos A, B e C, respectivamente, logo, deverá valer 2^{n-k}.

$$\begin{aligned} A_{n,k} + B_{n,k} + C_{n,k} &= \frac{2^{n+1-k} - 3 + 2^{n+1-k} + 2^{n+1-k} + 3 + 2(-1)^{n+k} + 2(-1)^{n+k+1}}{6} \\ &= \frac{3 \cdot 2^{n+1-k} + 2(-1)^{n+k} + 2(-1)^{n+k+1}}{6} \\ &= \frac{3 \cdot 2^{n+1-k}}{6} \\ &= \frac{2^{n+1-k}}{2} \\ &= 2^{n-k}. \end{aligned}$$

□

Exemplo 1. Considerando o jogo das Torres de Hanói com 10 discos, quantas vezes o disco 1 foi movido para o pino C?

Solução. Aplicando a fórmula (10) obtemos:

$$\begin{aligned} C_{10,1} &= \frac{2^{10+1-1} + 3 + (-1)^{10+1}}{6} \\ &= \frac{1024 + 3 - 1}{6} \\ &= \frac{1026}{6} \\ &= 171. \end{aligned}$$

Logo, o disco 1 foi movido para o pino C 171 vezes.

Exemplo 2. Calcule quantas vezes o disco 4 foi movido para o pino B com um jogo de 6 discos.

Solução. Aplicando a fórmula (11) obtemos:

$$\begin{aligned} B_{6,4} &= \frac{2^{6-4} + (-1)^{6+4+1}}{3} \\ &= \frac{4 - 1}{3} \\ &= 1. \end{aligned}$$

Exemplo 3. Calcule quantas vezes o disco 4 foi movido para o pino A com um jogo de 6 discos.

Solução. Aplicando a fórmula (12) obtemos:

$$\begin{aligned} A_{6,4} &= \frac{2^{6+1-4} - 3 + (-1)^{6+4}}{6} \\ &= \frac{8 - 3 + 1}{6} \\ &= 1. \end{aligned}$$

3. Torre com 4 pinos - Número Mínimo de Movimentos

Suponha que temos os n discos empilhados no pino A em forma de cone e desejamos transferi-los para o pino D. Há várias formas de fazer essa transferência, mas estamos à procura da que minimiza a quantidade de movimentos. Denominaremos a quantidade mínima de movimentos necessária para mover os n discos de b_n.

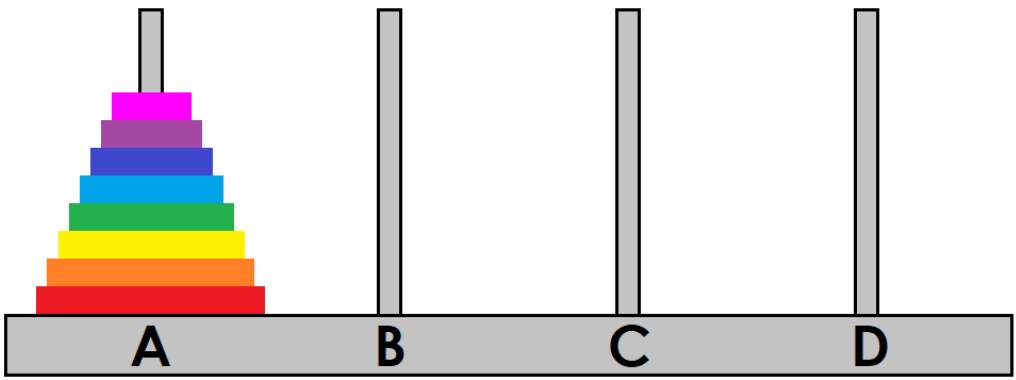


Figura 9: Torre de Hanói com 4 pinos.

De modo semelhante ao que foi feito no caso dos 3 pinos, observe que o último disco, ou seja, o maior de todos, será movido após retirarmos os $n-1$ discos que estão em cima dele e o distribuirmos nos pinos B e C. Ocorre que existem várias maneiras de tais discos estarem alocados nesses pinos B ou C, desse modo o caso da Torre com 4 pinos é distinto da Torre com 3 pinos, uma vez que nessa só há um modo dos pinos estarem distribuídos.

Vamos supor um método de solução e verificar se é o melhor. Para essse método, x_n será a quantidade de movimentos para mover n discos de um pino para outro usando os 4 pinos. Imagine que coloquemos todos os $n-1$ menores empilhados no pino B; para isso usaremos x_{n-1} movimentos. Então, transferimos o maior disco para o pino D usando 1 movimento, e para finalizar realocamos os $n-1$ discos no pino B para o pino D, usando mais x_{n-1} movimentos e concluímos o jogo. Para isso, efetuamos $x_{n-1} + 1 + x_{n-1}$ movimentos no total, ou seja,

$$x_n = 2x_{n-1} + 1 \text{ e } x_1 = 1, \tag{13}$$

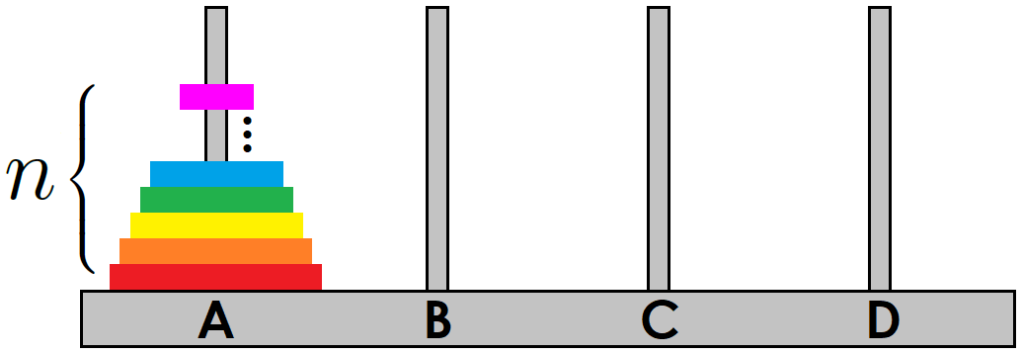


Figura 10: Torre de Hanói com 4 pinos.

pois com 1 disco, temos apenas 1 movimento que seria retirá-lo do pino A e colocá-lo do pino D, logo, $x_n = 2^n - 1$. Será que essa é a menor quantidade de movimentos possíveis? Ou seja, $x_n = b_n$?

Vejamos outra situação possível: nesse caso chamaremos de y_n a quantidade de movimentos para mover n discos. Imagine que transferimos os $n-2$ discos menores para B usando y_{n-2} movimentos, o segundo maior disco transferimos para C e o disco maior para D. Depois, transferimos o segundo disco maior para D, e para terminar os $n-2$ discos menores para D. Realizamos assim $y_{n-2} + 1 + 1 + 1 + y_{n-2}$ movimentos, logo,

$$y_n = 2y_{n-2} + 3 \text{ e } y_1 = 1, y_2 = 3 \tag{14}$$

uma recorrência diferente de (13). Vamos comparar os resultados para $n = 3$ discos. Como $y_1 = 1$ e $y_2 = 3$, então $y_3 = 2y_1 + 3 = 5$. Na solução do parágrafo anterior tínhamos $x_3 = 2^3 - 1 = 7$. Logo, a recorrência obtida dá-nos menos movimentos necessários que (13). Será que (14) é a recorrência procurada para 4 pinos? A resposta é não, vejamos por quê.

Para 6 discos, a solução de (14) será $y_6 = 2y_4 + 3 = 2.(2y_2 + 3) + 3 = 21$. Contudo, temos uma solução com menos movimentos: retirar os 3 menores discos de A e colocar em B usando z_3 movimentos, mover os 3 maiores discos de A para D usando os pinos A, C e D; logo, usamos $a_3 = 2^3 - 1 = 7$ movimentos. Por fim, movemos os 3 discos menores que estão em B para D usando z_3 movimentos, totalizando $5 + 7 + 5 = 17$ movimentos. Assim, (14) está descartada também.

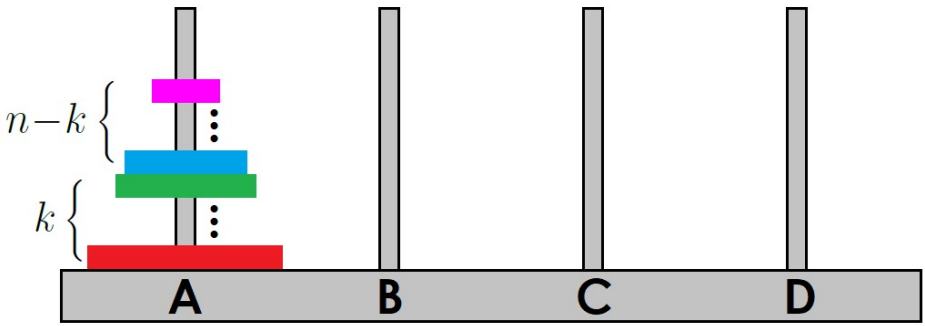


Figura 11: Torre de Hanói com 4 pinos.

Podemos concluir que o caso com 4 pinos é mais complexo do que o de 3 pinos, e a solução não é tão simples assim. Os resultados apresentados aqui estão em [1] com uma linguagem de programação.

Observe que queremos encontrar a quantidade mínima de movimentos e observamos que dado um certo valor k, $k < n$, usamos b_{n-k} movimentos para mover os $n-k$ discos menores para B; logo, a seguir movemos os discos restantes que são k para D, para isso poderemos usar apenas os pinos A, C e D, isto é, faremos a_k movimentos, e para finalizar movemos os discos menores que estavam em B para D, usando os 4 pinos, ou seja, b_{n-k} movimentos. Totalizando $b_n = 2b_{n-k} + a_k$ movimentos. Queremos encontrar o k que torna b_n mínimo. Assim, queremos

$$b_n = \min_{k\leq n}\{2b_{n-k} + a_k\} = \min_{k\leq n}\{2b_{n-k} + 2^k - 1\}. \tag{15}$$

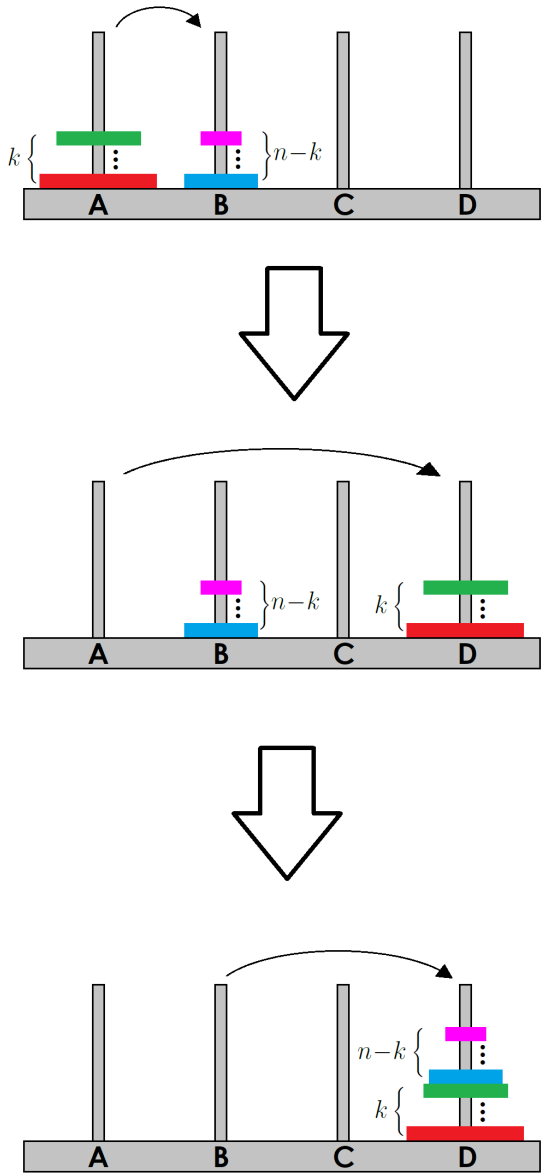


Figura 12: Torre de Hanói 4 pinos - Justificativa.

Analisando alguns casos: n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, observamos e levantaremos a hipótese de que os valores de k satisfazem a sequência

$$\{1, 1, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 5, 5, 5, 5, 5, 5, ...\}. \tag{16}$$

Se assim o for, dado n, precisamos saber sua posição na sequência, ou seja, o k_n. Sejam $\lfloor x \rfloor$ o maior inteiro menor ou igual a x, e $\lceil x \rceil$ o menor inteiro maior ou igual a x.

Proposição 4. *Seja a sequência* $\{k_n\} = \{1,1,2,2,2,3,3,3,3,4,4,4,4,4,5,5,5,5,5,5,..\}$, *então,*

$$k_n = \left\lfloor \frac{\sqrt{8n+1}-1}{2} \right\rfloor \tag{17}$$

Demonstração. Essa sequência é composta por blocos de repetição dos números naturais. O último número de cada bloco de repetição é igual à soma das quantidades de elementos de cada bloco anterior a ele, por exemplo,

$$k_2 = 1, 2 = 2 \;\; k_5 = 2,\; 5 = 3+2, \;\; k_9 = 3,\; 9 = 4+3+2. \tag{18}$$

Logo, a soma da quantidade de números de cada bloco resulta na última posição do bloco. Dado n, para sabermos o k_n correspondente a ele, resolvemos

$$\frac{k_n(k_n+1+2)}{2} = n. \tag{19}$$

Obviamente essa igualdade nem sempre é satisfeita; devemos resolver a equação do segundo grau

$$k_n^2 + 3k_n - 2n = 0 \Rightarrow k_n = \frac{-3+\sqrt{9+8n}}{2}. \tag{20}$$

Se o valor de k_n for inteiro, então o número mínimo de movimentos será $b_n = 2b_{n-k_n} + a_{k_n}$. Caso não seja inteiro, então,

$$k_n = \left\lfloor \frac{\sqrt{8n+9}-3}{2} \right\rfloor = \left\lfloor \frac{\sqrt{8n+1}-1}{2} \right\rfloor,$$

esse último valor é mais simplificado e $\frac{\sqrt{8n+1}-1}{2} - \frac{\sqrt{8n+9}-3}{2} < 1$ para todo n natural. □

Para provar o teorema principal dessa seção, precisamos do resultado a seguir.

Proposição 5. *A sequência* $\{b_n\}$ *satisfaz a recorrência*

$$b_{n+1} = b_n + 2^{k_n}. \tag{21}$$

Demonstração. Se temos n + 1 discos em A, devemos retirar os n discos menores usando a menor quantidade de movimentos e alocá-los em B e C.

Se $b_n = 2b_{n-k_n} + a_{k_n}$, a solução para n discos é transferir os $n - k_n$ discos menores para B usando os 4 pinos, depois os k_n restantes para C (em vez de D, caso convencional) usando os 3 pinos, e não faremos a última etapa, que é transferir os $n - k_n$ discos para C; assim usaremos $b_{n-k_n} + a_{k_n}$ movimentos.

Agora, transferiremos o disco n + 1 para D, os k_n que estão em C para D, e, para terminar, os $n-k_n$ que estão em B para D, usando $1 + a_{k_n} + b_{n-k_n}$. Logo, usamos $2b_{n-k_n} + 2a_{k_n} + 1$ movimentos.Assim, $b_{n+1} = 2b_{n-k_n} + 2a_{k_n} + 1 = 2b_{n-k_n} + a_{k_n} + a_{k_n} + 1 = b_n + a_{k_n} + 1 = b_n + 2^{k_n}$. □

O seguinte resultado dá-nos uma fórmula fechada para o número mínimo de movimentos da torre com n discos e 4 pinos.

Teorema 3. *Seja* n *o número de discos de um Torre de Hanói com 4 pinos. Se*

$$k_n = \left\lfloor \frac{\sqrt{8n+1}-1}{2} \right\rfloor,$$

então,

$$b_n = 2^{k_n}\left(n-1-\frac{k_n(k_n-1)}{2}\right)+1. \tag{22}$$

Demonstração. Suponha que o teorema é válido para n,, mostraremos por indução que ele é verdadeiro para n + 1. De acordo com a proposição anterior $b_{n+1} = b_n + 2^{k_n}$. Logo, por hipótese de indução, $b_{n+1} = 2^{k_n}\left(n-1-\frac{k_n(k_n-1)}{2}\right)+1+2^{k_n}$. Há 2 possibilidades $k_{n+1} = k_n$ ou $k_{n+1} = k_n + 1$. Se $k_{n+1} = k_n$, então,

$$b_{n+1} = 2^{k_n}\left(n-1-\frac{k_n(k_n-1)}{2}\right)+1+2^{k_n} = 2^{k_{n+1}}\left((n+1)-1-\frac{k_{n+1}(k_{n+1}-1)}{2}\right)+1.$$

logo, o teorema é válido. Caso $k_{n+1} = k_n + 1$, queremos mostrar que

$$b_{n+1} = 2^{k_n+1}\left((n+1)-1-\frac{(k_n+1)(k_n+1-1)}{2}\right)+1.$$

Simplificando,

$$b_{n+1} = 2^{k_n+1}\left(n-\frac{(k_n+1)(k_n)}{2}\right)+1. \tag{23}$$

Pela proposição anterior

$$b_{n+1} = 2^{k_n}\left(n-1-\frac{k_n(k_n-1)}{2}\right)+1+2^{k_n} = 2^{k_n}\left(n-\frac{k_n(k_n-1)}{2}\right)+1,$$

que será igual a (23) se, e somente se,

$$\begin{aligned}
&2n-(k_n+1)(k_n) = n-\frac{k_n(k_n-1)}{2}\\
\Rightarrow\ &4n-2(k_n+1)(k_n) = 2n-k_n(k_n-1)\\
\Rightarrow\ &2n-2(k_n+1)(k_n)+k_n(k_n-1) = 0\\
\Rightarrow\ &2(k_n)(k_n)-k_n(k_n-1)-2n =\\
\Rightarrow\ &k_n(2k_n-k_n+1)-2n = 0\\
\Rightarrow\ &k_n(k_n+1)-2n = 0\\
\Rightarrow\ &k_n = \frac{-1+\sqrt{8n+1}}{2}.
\end{aligned}$$

que comprova a veracidade do resultado. □

Exemplo 4. Quantos movimentos são minimamente necessários para resolver o quebra-cabeça Torre de Hanói com 4 pinos quando temos 40 discos?

Solução. Nesse caso, temos

$$k_{40} = \left\lfloor \frac{\sqrt{8.40+1}-1}{2} \right\rfloor = 8,$$

então

$$\begin{aligned} b_{40} &= 2^{k_{40}} \left(40 - 1 - \frac{k_{40}(k_{40}-1)}{2}\right) + 1 \\ b_{40} &= 2^{8} \left(39 - \frac{8(8-1)}{2}\right) + 1 \\ b_{40} &= 2^{8} \cdot 11 + 1 \\ b_{40} &= 2817. \end{aligned}$$

Referências

[1] Chu, I-P.; Johnsonbaugh, R. *The Four-Peg Tower of Hanoi Puzzle.* SIGCSE. Vol. 23. N° 3 Sept. 1991.

[2] Dudeney, H. E. *The Canterbury Puzzles*. New York: E. P. Dutton and co, 1908.

[3] Ferreira, D. B.; Oliveira, E. P. "A Matemática da Ordem das Movimentações das Peças da Torre de Hanói". *Gazeta de Matemática*, v. 1, N° 190, pp. 6-10, 2020.

[4] Hinz, A. M.; Klavža, S.; Milutinović, U.; Petr, C. *The Tower of Hanoi – Myths and Maths.* Birkhäuser Basel, Springer, 2013.

[5] Lima, E. L.; Carvalho, P. C. P.; Wagner E.; Morgado, A. C. *A Matemática do Ensino Médio.* SBM, V. 1, 2012.

[6] Lucas, É. *Récréations Mathématiques*. Paris: Albert Blanchard, 1893.

[7] Morgado, A. C.; Carvalho, P. C. P. *Matemática Discreta* - Coleção Profmat. Rio de Janeiro: SBM, 2015.

[8] Oliveira, E. P. *As Diversas Maneiras de Explorar a Matemática Através do Jogo Torres de Hanói.* - Dissertação de Mestrado do Profmat, 2018.

[9] Pereira, A.; Rodrigues, R. "O problema das torres de Hanoi: a lenda, algoritmos e generalizações". *Gazeta de Matemática*, V. 1, N° 144, pp. 10–11, 2003.

Débora Borges Ferreira
Universidade Federal do Rio Grande do Norte
<debora@ccet.ufrn.br>

Edvan Pontes de Oliveira
Escola Estadual em Tempo Integral Francisco de Assis Bittencourt
<edvan.pontes@hotmail.com>

Francisco Quaranta Neto
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
<francisco.quaranta@ifrn.edu.br>

Recebido: 27/04/2020
Publicado: 07/12/2020

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.5, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo843

Números de Stirling do primeiro tipo

Gabriel F. Pinheiro [1] Irene M. Craveiro Naiguiel A. da Silva [2]

Resumo

Neste trabalho investigamos as conexões existentes entre os números de Stirling do primeiro tipo e os grupos de permutações de n elementos. Apresentamos resultados conhecidos no intuito de elucidar a relação entre os números de Stirling e os conteúdos ensinados no Ensino Médio.

Palavras-chave: Números de Stirling; Ensino Médio.

Abstract

In this work we investigate the existing connections between the Stirling numbers of the first kind and the permutations groups on n *elements. We present known results order to elucidate the relationship between Stirling numbers and contents taught in High School.*

Keywords: Stirling numbers; High School.

1. Introdução

Números de Stirling demonstram ser uma ferramenta útil para lidar com diversos problemas combinatórios. Dessa forma, desenvolvemos diversas propriedades para os números de Stirling do primeiro tipo, apresentando uma prova algébrica ou combinatória. Os números de Stirling do primeiro tipo podem ser definidos por meio de permutações de um conjunto de n objetos, $I_n = \{c_1, c_2, \dots, c_n\}$. Sem perda de generalidade vamos supor que $I_n = \{1, 2, \dots, n\}$. Em seguida, estabelecemos uma recorrência para os números de Stirling do primeiro tipo. A partir dessa relação de recorrência instituimos a função geradora ordinária, ou seja, um polinômio na indeterminada x, cujos coeficientes das potências de x são números de Stirling do primeiro tipo.

A recorrência dos números de Stirling do primeiro tipo também permite dispor esses números na forma triangular; esse triângulo formado é similar ao Triângulo de Pascal formado pelos coeficientes binomiais. Os coeficientes binomiais podem ser interpretados combinatoriamente como o número de subconjuntos com k elementos de um conjunto com n objetos, enquanto que o número de Stirling do primeiro tipo pode ser interpretado como a quantidade de permutações de um conjunto de n elementos que se decompõe em k ciclos.

[1] Agradeço à UFGD pela concessão de bolsa de Iniciação Científica.
[2] Apoio Capes.

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

2. O Grupo de Permutações de n objetos

Nesta seção apresentamos diversos conceitos e resultados referentes ao grupo de permutações de n objetos. Os resultados que validamos agora seguem de [5].

Definição 1. Um grupo consiste de um conjunto não vazio G munido de uma operação indicada por $*$ (isto é, uma regra em que cada par (x, y) de G associa um terceiro elemento de G, indicado por $x * y$) satisfazendo as seguintes propriedades:

- **associatividade**: dados $x, y, z \in G$ vale $x * (y * z) = (x * y) * z$;
- **existência do elemento neutro**: para todo $x \in G$, existe $e \in G$ tal que $x * e = x$;
- **existência do elemento inverso**: para cada $x \in G$, existe $y \in G$ tal que $x * y = e$.

Se a operação $*$ satisfaz a propriedade comutativa (isto é, para todos $x, y \in G$ vale $x * y = y * x$) dizemos que G é um grupo comutativo ou abeliano.

Observação 1. Os elementos neutro e inverso são únicos.

Exemplo 1. Considere o conjunto dos números inteiros $\mathbb{Z}$ com a operação usual de adição. Sabemos que dados $x, y \in \mathbb{Z}$ temos que $x + y \in \mathbb{Z}$, logo, a operação de adição é fechada em $\mathbb{Z}$. Segue assim que, em $\mathbb{Z}$, vale a associatividade. Além disso, $e = 0$ é o elemento neutro da adição; de fato, dado $x \in \mathbb{Z}$ temos que $x + 0 = x$. Por fim, para cada $x \in \mathbb{Z}$ existe $-x \in \mathbb{Z}$ tal que $x + (-x) = 0$. Conclui-se dessa forma que $\mathbb{Z}$ com a operação de adição usual é um grupo.

Definição 2. Uma permutação de um conjunto não vazio X é uma bijeção de X em X. Denotamos por S(X) o conjunto de todas as permutações de X.

Exemplo 2. Considere X o conjunto formado pelos quatro ases de um baralho comum, disposto em qualquer ordem, como mostra a figura abaixo:

Figura 1: Sequência de ases

É natural supor que a ordem estabelecida para se dispor as cartas é arbitrária e que, além disso, a sequência dada na Figura 1 não é a única iniciada pelo ás de espadas. Assim caso se deseje começar a sequência pelo ás de ouros em vez de iniciar pelo ás de espadas, bastaria posicionar a carta citada na primeira posição e dispor as demais em uma ordem qualquer. Desse modo, se quisermos obter uma certa sequência dos quatro ases a partir do embaralhamento de uma sequência previamente estipulada, já não poderemos arbitrar a ordem em que colocaremos cada carta, uma vez que, a partir da sequência inicial, cada embaralhamento corresponderá a uma determinada ordem das cartas

Exemplo 3. Considere $X = \mathbb{R}$ o conjunto dos números reais. Observe que a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x$, para todo $x \in \mathbb{R}$, é uma permutação de $\mathbb{R}$ em $\mathbb{R}$. Para isso, basta mostrarmos que f é uma bijeção. Note que, dados $x_1 \neq x_2$ em $\mathbb{R}$ implica que $f(x_1) = x_1 \neq x_2 = f(x_2)$, logo, f é injetora. Além disso, dado $y \in \mathbb{R}$, existe $x = y$ em $\mathbb{R}$ tal que $f(x) = f(y) = y$, ou seja, f é sobrejetora. Potanto, f é bijetora e, consequentemente, uma permutação.

Observação 2. Note que S(X) munido da operação de composição de funções é um grupo, chamado de Grupo das Permutações de X. De fato, a composição de funções é associativa; além disso, como todo elemento de S(X) é uma bijeção, existe o elemento inverso e, por fim, o elemento neutro é dado pela função $I : \mathbb{X} \to \mathbb{X}$ dada por $I(x) = x$, para todo $x \in X$. Quando $X = \{1, 2, \dots, n\}$ denotamos S(X) por S_n e o chamamos de Grupo Simétrico de Grau n. Observe que a ordem (quantidade de elementos do conjunto) de S_n é n!. De fato, segue da análise combinatória que o número de permutações possíveis para um conjunto com n elementos é $P_n = n!$.

Exemplo 4. Seja $X = \{1, 2, 3\}$. Temos que a ordem de S_3 é $3! = 6$. De fato, podemos montar as seguintes sequências com os elementos de X: $(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)$.

Observação 3. Seja $X = \{1, 2, \dots, n\}$ e f uma permutação de X. Podemos denotar f de S_n na forma de diagrama, $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$, em que a primeira linha representa os elementos do conjunto X e a segunda linha representa a permutação feita com tais componentes. A partir disso, vamos elencar todos os elementos de S_4 na forma de diagrama:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Apresentaremos a seguir uma forma de simplificar a notação de uma permutação, e a denotamos por notação cíclica.

Definição 3. Sejam $a_1, a_2, \dots, a_r$ elementos de $X = \{1, 2, \dots, n\}, n > 1$, e $\sigma \in S_n$ uma permutação tal que

$$\begin{cases} \sigma(a_1) = a_2 \\ \sigma^j(a_1) = a_{j+1} \\ \sigma^r(a_1) = a_1 \\ \sigma(x) = x \qquad \forall x \neq a_i, i = 1, \dots, r. \end{cases}$$

A permutação σ é chamada ciclo de comprimento r ou um r-ciclo. O conjunto $\{a_1, \dots, a_r\}$ é chamado suporte do r–ciclo.

Exemplo 5. Considere a permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$ de S_5. Vamos representá-la em forma de ciclos. Usando a **Definição 3** temos que: $\sigma(1) = 3, \sigma^2(1) = \sigma(\sigma(1)) = \sigma(3) = 4, \sigma^3(1) = \sigma(\sigma^2(1)) = \sigma(4) = 1$, como começamos no 1 e fechamos no 1, podemos montar o 3–ciclo (134), o próximo passo é verificar para os demais elementos, logo, $\sigma(2) = 5, \sigma^2(2) = \sigma(\sigma(2)) = \sigma(5) = 2$; dessa maneira, formamos mais um ciclo, o 2– ciclo (25). Segue assim que nossa permutação pode ser representada pelo produto dos ciclos (134)(25).

Exemplo 6. Agora, vamos representar uma permutação na forma de ciclos usando a noção geométrica. Para isso, considere a permutação $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 6 & 7 & 5 & 2 & 8 & 4 \end{pmatrix}$ de S_8. A figura abaixo mostra o comportamente dessa permutação:

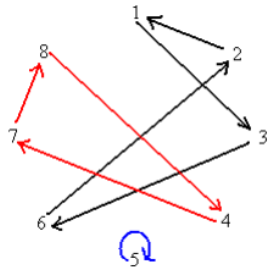


Figura 2: Representação geométrica da permutação

Começando pelo 1 e seguindo a orientação das flechas, formamos o ciclo (1362); dando início pelo 4 forma-se o ciclo (478); e, por fim, compõe-se o ciclo unitário (5). Assim, podemos representar nossa permutação ciclicamente por (1362)(478)(5).

Definição 4. Sejam α um r–ciclo e β um s-ciclo de S_n. Os ciclos α e β são disjuntos se nenhum elemento de ambos é movido ao mesmo tempo, ou seja, para todo $x \in \{1, 2, \ldots, n\}$ $\alpha(x) = x$ ou $\beta(x) = x$.

Observação 4. Sejam α um r–ciclo e β um s–ciclo de S_n. Pensando nos ciclos como conjuntos, dizemos que eles são disjuntos se não têm elementos em comum.

Teorema 1. *Dois ciclos disjuntos de uma permutação $\sigma \in S_n$ comutam entre si.*

Demonstração. Considerando α e β ciclos disjuntos de S_n, cujos conjuntos suportes são respectivamente A e B. Se $x \in I_n$, temos três casos a analisar:

1 . $x \in A$ e $x \notin B$. Então, $(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x)$, bem como $(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \alpha(x)$. Logo, $\alpha\beta$ e $\beta\alpha$ coincidem em A.

2 . $x \notin A$ e $x \in B$ (Análogo ao 1)

3 . $x \notin A$ e $x \notin B$. Neste caso, $(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$, assim como, $(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \beta(x) = x$. Dessa forma, $\alpha\beta$ e $\beta\alpha$ coincidem fora de A e B.

□

Exemplo 7. Considere a notação cíclica do **Exemplo 6**; podemos representá-la por (1362)(478)(5), (5)(478)(1362) ou por (478)(1362)(5); o teorema acima nos diz que é possível comutar os ciclos sem alterar a permutação correspondente.

Teorema 2. *Toda permutação de* $\sigma \in S_n$ *decompõe-se de forma única, a menos da ordem, em produto ciclos disjuntos.*

Exemplo 8. Vamos denotar por $A_{4,k}$ o conjunto das permutações de S_4 que se decompõem em k ciclos disjuntos. Representaremos todas as permutações de S_4 em produto de ciclos disjuntos, como mostra a tabela abaixo.

k	$A_{4,k}$
1	(1234), (1324), (1342), (1432), (1243), (1423)
2	(1)(234), (1)(243), (2)(134), (2)(143), (3)(124), (3)(142), (4)(123), (4)(132), (12)(34), (13)(24), (14)(23)
3	(1)(2)(34), (1)(3)(24), (1)(4)(23), (2)(3)(14), (2)(4)(13), (3)(4)(12)
4	(1)(2)(3)(4)

Tabela 1: Decomposição dos elementos de S_4 em produtos de ciclos disjuntos

3. Os Números de Stirling do Primeiro Tipo

Os números de Stirling são classificados em dois tipos – números de Stirling do primeiro tipo e segundo tipo – ambos fornecem resultados utilizados para resolver problemas de natureza combinatória. Os números de Stirling do 1º tipo representam o total das permutações que podem ser decompostos um conjunto com n elementos em k ciclos disjuntos. Já os do 2º tipo estão relacionados com partições de um conjunto com n elementos.

Os números de Stirling do primeiro tipo podem ser interpretados como o número de maneiras que n pessoas podem sentar-se em torno de mesas circulares sem que nenhuma dessas mesas fique vazia. Entretanto, exploraremos a natureza combinatória que estabelece uma conexão entre os números de Stirling do primeiro tipo e os grupos de permutação de n elementos. A nomenclatura dada a essa sequência deve-se a uma homenagem imposta pelo matemático dinamarquês Neils Nielsen(1865-1931) ao matemático escocês James Stirling (1692-1770). Essa homenagem refere-se ao fato de que Stirling utilizava esses números em seus trabalhos, dentre eles, estão os publicados em 1718, intitulado *Methodus Differentialis Newtoniana Illustrata* e em seu livro *Methodus Differentiallis.* Nesta seção apresentamos alguns dos resultados sobre os números de Stirling que decorrem de [2], sendo um desses uma fórmula de recorrência que descreve os números de Stirling do primeiro tipo. Além disso, descrevemos algumas propriedades inerentes desse conceito.

Definição 5. Sejam $n, k \in \mathbb{N}$, com $n \geq k \geq 1$, o número de Stirling de primeiro tipo é o total de permutações de n elementos que se decompõem em exatamente k ciclos disjuntos. Denotamos o número de Stirling de primeiro tipo por $\left[\begin{matrix} n \\ k \end{matrix} \right]$. Convencionamos $\left[\begin{matrix} 0 \\ 0 \end{matrix} \right] = 1$.

Segue diretamente da definição 5 que: $\left[\begin{matrix} n \\ 0 \end{matrix} \right] = 0$, para $n > 0$; $\left[\begin{matrix} n \\ n \end{matrix} \right] = 1$; $\left[\begin{matrix} n \\ k \end{matrix} \right] = 0$, para $0 < n < k$.

Exemplo 9. Vamos calcular o número de Stirling $\left[\begin{matrix} 4 \\ 2 \end{matrix} \right]$; para isso, basta olhar quantas permutações de 4 elementos decompõem-se em 2 ciclos disjuntos e, pela tabela do **Exemplo 8**, temos que

a resposta é 11. Ou seja, $\left[\begin{matrix} 4 \\ 2 \end{matrix} \right] = 11$. Vale observar que o método utilizado para calcular os números de Stirling para qualquer $n \in \mathbb{N}$ segue de modo análogo ao que fizemos aqui, mas, quanto maior for n mais difícil fica calcular esses números manualmente; assim, recorrer aos programas computacionais é a melhor escolha. A título de curiosidade, se quiséssemos calcular os números de Stirling para $n = 5$, deveríamos primeiro calcular todas as permutações de S_5 e depois decompô-las em ciclos disjuntos, mas, sabemos que a ordem de S_5 é $5! = 120$, então, para $n \geq 4$ torna-se mais trabalhoso calcular os números de Stirling manualmente. A seguir dispomos uma relação que nos permite facilitar o cálculo desses números.

Teorema 3. *Sejam* n, k *números naturais com* $n \geq k \geq 1$, *temos os seguintes resultados:*

a) $\left[\begin{matrix} n \\ 1 \end{matrix} \right] = (n-1)!$;

b) $\left[\begin{matrix} n \\ n-1 \end{matrix} \right] = \left(\begin{matrix} n \\ 2 \end{matrix} \right)$.

Demonstração. a) Temos que $\left[\begin{matrix} n \\ 1 \end{matrix} \right]$ representa o total de permutações $\sigma \in S_n$ com exatamente 1 ciclo, assim, podemos formar $(n-1)!$ permutações com exatamente 1 ciclo a partir de $1, 2, ..., n$, ou seja,

$$\begin{matrix} (1 & 2 & 3 & \dots & n) \\ (2 & 1 & 3 & \dots & n) \\ (3 & 1 & 4 & \dots & n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n-1 & n-2 & n-3 & \dots & n). \end{matrix}$$

b) Temos que $\left[\begin{matrix} n \\ n-1 \end{matrix} \right]$ é o total de permutações $\sigma \in S_n$ decomposta em um produto de $n-1$ ciclos. Para formar permutações de $n-1$ ciclos, temos que escolher dois elementos de $1, 2, ..., n$ para ser uma transposição e o restante fica pré-fixado para ser o ciclo de comprimento 1. Dessa forma, $\left[\begin{matrix} n \\ n-1 \end{matrix} \right] = \left(\begin{matrix} n \\ 2 \end{matrix} \right)$.

□

Definição 6. Os coeficientes binomiais são números inteiros positivos definidos por:

$$\left(\begin{matrix} n \\ k \end{matrix} \right) = \frac{n!}{k!(n-k)!},$$

com $n, k \in \mathbb{N}, n \geq k$.

Esses coeficientes podem ser interpretados como o número de maneiras de combinar n elementos tomados k a k. Além disso, os números binomiais satisfazem uma relação de recorrência na qual o nome foi dado em homenagem ao célebre matemático Michael Stifel (1487-1567), a relação de Stifel ou também conhecida como regra de Pascal, cuja identidade envolve os coeficientes binomiais. Essa relação é dada por:

$$\left(\begin{matrix} n \\ k \end{matrix} \right) = \left(\begin{matrix} n-1 \\ k-1 \end{matrix} \right) + \left(\begin{matrix} n-1 \\ k \end{matrix} \right),$$

com $n \geq k$ naturais.

Por exemplo, seja $A = \{1, 2, 3, 4\}$, em quantas maneiras podemos organizar esses números tomados 2 a 2? Como temos uma quantidade finita e pequena de elementos, o trabalho manual é bem simples, mas, recorrendo à definição dada acima, temos que o número de possibilidades é dado por

$$\left(\begin{array}{c} 4 \\ 2 \end{array} \right) = \frac{4!}{2!(4-2)!} = \frac{4!}{\bullet 2!(2!)} = \frac{4.3.2!}{2!2!} = \frac{4.3}{2} = 6$$

ou seja, temos 6 maneiras de agrupar esses 4 elementos tomados de 2 em 2.

Exemplo 10. Considere o grupo simétrico S_4, vamos calcular $\left[\begin{array}{c} 4 \\ 1 \end{array} \right]$ e $\left[\begin{array}{c} 4 \\ 3 \end{array} \right]$. Pelo teorema 3 é fácil calcular esses números. Sendo assim: $\left[\begin{array}{c} 4 \\ 1 \end{array} \right] = (4-1)! = 3! = 6$ e $\left[\begin{array}{c} 4 \\ 3 \end{array} \right] = \left(\begin{array}{c} 4 \\ 2 \end{array} \right) = \frac{4!}{2!(4-2)!\bullet} = 6$.

O teorema a seguir fornece-nos uma recorrência para os números de Stirling do primeiro tipo que se assemelha à relação de Stifel.

Teorema 4. *Sejam* $n, k \in \mathbb{N}$ *com* $n \geq k \geq 1$. *então:*

$$\left[\begin{array}{c} n \\ k \end{array} \right] = \left[\begin{array}{c} n-1 \\ k-1 \end{array} \right] + (n-1) \left[\begin{array}{c} n-1 \\ k \end{array} \right].$$

Demonstração. Inicialmente vamos indicar por A o conjunto de permutações de S_n que se decompõem em exatamente k ciclos. Segue da definição que $|A| = \left[\begin{array}{c} n \\ k \end{array} \right]$. Particionamos A em dois subconjuntos:

1 . Subconjunto de A, A_1, formado por permutações que contém o 1-ciclo (n);

2 . Subconjunto de A, A_2, formado por permutações cujo elemento n está em um ciclo com mais de um elemento.

Temos que: $A_1 \cap A_2 = \emptyset$. e $A_1 \cup A_2 = A$. Em 1, o total de permutações é $\left[\begin{array}{c} n-1 \\ k-1 \end{array} \right] = |A_1|$, em 2 o total de permutações é $(n-1) \left[\begin{array}{c} n-1 \\ k \end{array} \right] = |A_2|$, pois podemos agora distribuir todos os $n-1$ elementos em k ciclos – afinal, cada ciclo pode ter mais de um elemento – e assim, obtemos $\left[\begin{array}{c} n-1 \\ k \end{array} \right]$ modos. Como temos $n-1$ modos de colocar o elemento n, sem contar sua própria posição, alcançamos pelo princípio multiplicativo $(n-1) \left[\begin{array}{c} n-1 \\ k \end{array} \right]$ permutações de S_n em A_2. Logo,

$$\left[\begin{array}{c} n-1 \\ k-1 \end{array} \right] + (n-1) \left[\begin{array}{c} n-1 \\ k \end{array} \right] = |A| = \left[\begin{array}{c} n \\ k \end{array} \right].$$

□

Exemplo 11. Seja S_4 o grupo simétrico de grau 4. Calculamos $\begin{bmatrix} 5 \\ 2 \end{bmatrix}$ por meio do teorema anterior. Sendo assim:

$$\begin{bmatrix} 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 5-1 \\ 3-1 \end{bmatrix} + (5-1)\begin{bmatrix} 5-1 \\ 3 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix} + (4)\begin{bmatrix} 4 \\ 3 \end{bmatrix} = 11 + 4.6 = 35,$$

o resultado da terceira igualdade foi obtido por meio da Tabela 8.

Exemplo 12. Pelo teorema anterior vimos que a recorrência para os números de Stirling assemelha-se à relação de Stifel, que nos fornece o triângulo de Pascal. Para os números de Stirling do primeiro tipo temos um triângulo análogo, como mostra a figura abaixo:

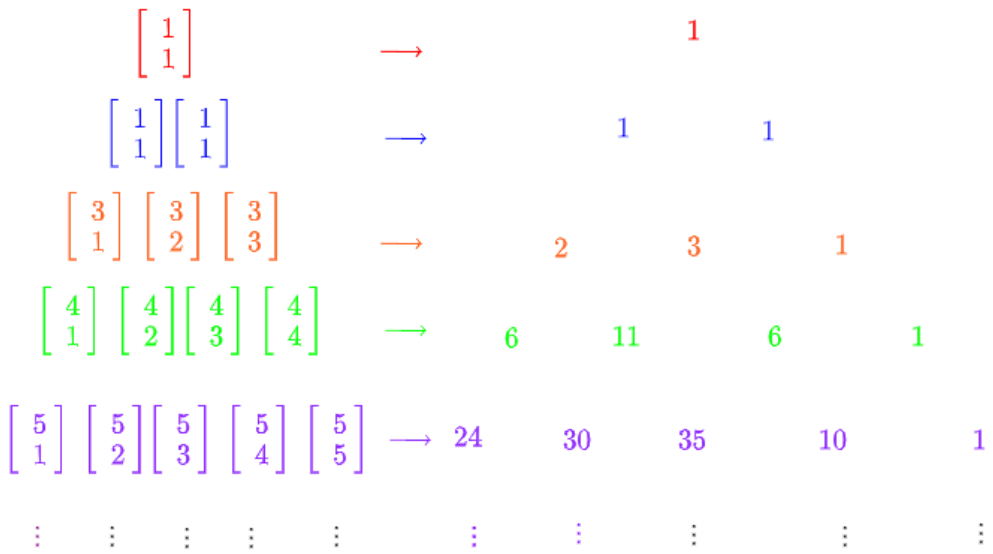


Figura 3: Triângulo similar ao de Pascal para os números de Stirling do primeiro tipo

Teorema 5. *Sejam* $n, k \in \mathbb{N}$ *com* $n \geq k \geq 1$. *então:*

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!.$$

Demonstração. Faremos a prova por indução sobre n. Para $n = 0$, temos que:

$$\sum_{k=0}^{n} \begin{bmatrix} 0 \\ k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1 = 0!$$

Suponha que o resultado seja válido para $n = t > 0$, ou seja, $\sum_{k=0}^{t} \left[\begin{matrix} t \\ k \end{matrix} \right] = t!$. Assim, temos que:

$$\begin{aligned}\sum_{k=0}^{t+1} \left[\begin{matrix} t+1 \\ k \end{matrix} \right] &= \sum_{k=0}^{t+1} \left(\left[\begin{matrix} t \\ k-1 \end{matrix} \right] + t \left[\begin{matrix} t \\ k \end{matrix} \right] \right) = \sum_{k=0}^{t+1} \left[\begin{matrix} t \\ k-1 \end{matrix} \right] + t \sum_{k=0}^{t+1} \left[\begin{matrix} t \\ k \end{matrix} \right] \\ &= \sum_{k=0}^{t+1} \left[\begin{matrix} t \\ k-1 \end{matrix} \right] + t \sum_{k=0}^{t} \left[\begin{matrix} t \\ k \end{matrix} \right] + t \left[\begin{matrix} t \\ t+1 \end{matrix} \right] \\ &= \sum_{k=0}^{t+1} \left[\begin{matrix} t \\ k-1 \end{matrix} \right] + tt! = \sum_{p=o}^{t} \left[\begin{matrix} t \\ p \end{matrix} \right] + tt! = t! + tt! = (t+1)!.\end{aligned}$$

Portanto, $\sum_{k=0}^{n} \left[\begin{matrix} n \\ k \end{matrix} \right] = n!$. □

Exemplo 13. Perceba pela Figura 3 que a soma de cada linha do triângulo corresponde a n!, por exemplo, a soma dos elementos da quarta linha é

$$\sum_{k=1}^{4} \left[\begin{matrix} 4 \\ k \end{matrix} \right] = 6 + 11 + 6 + 1 = 24 = 4!,$$

note que o resultado segue diretamente do Teorema 5.

A relação de recorrência estabelecida no Teorema 4 permite determinar a função geradora ordinária para essa sequência de números, ou seja, podemos obter um polinômio de grau n, cujo coeficiente de x^k é o número de Striling do primeiro tipo. De fato, considere

$$F_n(x) = \sum_{k=1}^{\infty} \left[\begin{matrix} n \\ k \end{matrix} \right] x^k,$$

com $n \geq k \geq 1$, em que n é um inteiro fixado, convencionamos $F_0(x) = 1$. Assim temos que

$$\left[\begin{matrix} n \\ k \end{matrix} \right] x^n = \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right] x^n + (n-1) \left[\begin{matrix} n-1 \\ k \end{matrix} \right] x^n$$

Dessa forma,

$$\sum_{k=1}^{\infty} \left[\begin{matrix} n \\ k \end{matrix} \right] x^k = \sum_{k=1}^{\infty} \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right] x^k + \sum_{k-1}^{\infty} (n-1) \left[\begin{matrix} n-1 \\ k \end{matrix} \right] x^k, k \geq 1$$

Portanto:

$$F_n(x) = x \sum_{k=1}^{\infty} \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right] x^{k-1} + (n-1) \sum_{k=1}^{\infty} \left[\begin{matrix} n-1 \\ k \end{matrix} \right] x^k$$

ou seja, $F_n(x) = xF_{n-1}(x) + (n-1)F_{n-1}(x)$, ou ainda, $F_n(x) = (x+n-1)F_{n-1}(x)$, $8n \geq 1$. Avaliamos a função $F_n(x)$ para $n = 1, 2, 3, \ldots$

$$\begin{aligned} F_1(x) &= (x+1-1).F_{1-1}(x) = x.F_0(x) = x \\ F_2(x) &= (x+2-1).F_{2-1}(x) = (x+1).x \\ &\vdots \\ F_n(x) &= (x+n-1)\ldots(x+4)(x+3)(x+2)(x+1)x. \end{aligned}$$

Dessa forma, ao expandirmos o polinômio $F_n(x)$, o coeficiente de x^k é o número de Stirling do primeiro tipo.

Teorema 6. *Seja o inteiro* n *tal que* $n > 0$, *então a função geradora ordinária para os números de Stirling do primeiro tipo é o polinômio na indeterminada* x

$$F_n(x) = (x + n - 1) \dots (x + 4)(x + 3)(x + 1)x.$$

Exemplo 14. Considere a seguinte identidade em particular:

$$\sum_{k=1}^{4} k \begin{bmatrix} 4 \\ k \end{bmatrix} = \begin{bmatrix} 4+1 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \end{bmatrix} \tag{1}$$

Temos que $\begin{bmatrix} 5 \\ 2 \end{bmatrix} = 50$.

No caso $k = 1$, lado esquerdo da identidade (1), considerando as permutações de $\{1, 2, 3, 4\}$ que se decompõem em um ciclo, e transformando-as em permutações de $\{1, 2, 3, 4, 5\}$ que se decompõem em produtos de dois ciclos, temos que:

$$\begin{aligned}
(2341) &\rightarrow (2341)(5) \\
(2413) &\rightarrow (2413)(5) \\
(3421) &\rightarrow (3421)(5) \\
(1342) &\rightarrow (1342)(5) \\
(4312) &\rightarrow (4312)(5) \\
(4123) &\rightarrow (4123)(5)
\end{aligned}$$

Temos um total de 6 permutações de $\{1, 2, 3, 4, 5\}$, que se decompõem em produto de dois ciclos. No caso $k = 2$, para cada permutação de $\{1, 2, 3, 4\}$ que se separam em dois ciclos, vamos repeti-las duas vezes, sublinhando um dos ciclos para diferenciá-las, como segue:

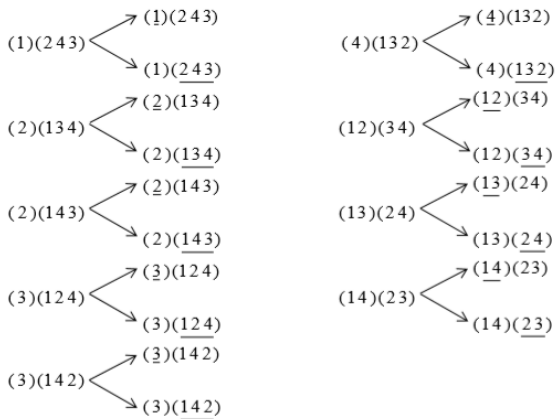


Figura 4: Caso k=2

Para cada uma das permutações duplicadas, vamos associá-la às seguintes permutações de $\{1, 2, 3, 4, 5\}$ que se decompõem em produto de dois ciclos.

$(\underline{1})(234) \to (1)(2345);$
$(1)(\underline{234}) \to (15)(234);$
$(\underline{1})(243) \to (1)(2435);$
$(1)(\underline{243}) \to (15)(243);$
$(\underline{2})(134) \to (2)(1345);$
$(2)(\underline{134}) \to (25)(134);$
$(\underline{2})(143) \to (2)(1435);$
$(2)(\underline{143}) \to (25)(143);$
$(\underline{3})(124) \to (3)(1245);$
$(3)(\underline{124}) \to (35)(124);$
$(\underline{3})(142) \to (3)(1425);$
$(3)(\underline{142}) \to (35)(142);$

$(\underline{4})(123) \to (4)(1235);$
$(4)(\underline{123}) \to (45)(123);$
$(\underline{4})(132) \to (4)(1325);$
$(4)(\underline{132}) \to (45)(132);$
$(\underline{12})(34) \to (12)(345);$
$(12)(\underline{34}) \to (125)(34);$
$(\underline{13})(24) \to (13)(245);$
$(13)(\underline{24}) \to (135)(24);$
$(\underline{14})(23) \to (14)(235);$
$(14)(\underline{23}) \to (145)(23).$

Figura 5: Permutações de 4 associadas a permutações de 5.

Temos um total de 22 permutações de $\{1, 2, 3, 4, 5\}$, que se decompõem em produto de dois ciclos. No caso k = 3, para cada permutação de $\{1, 2, 3, 4\}$ que se decompõe em três ciclos, a repetimos três vezes, sublinhando um dos ciclos para diferenciá-los, como segue:

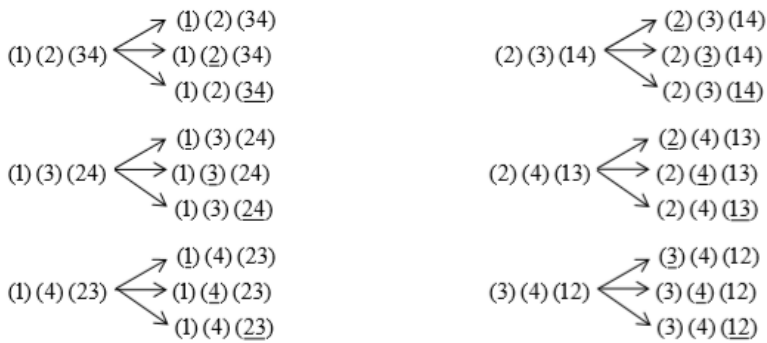


Figura 6: Caso k = 3.

Para cada uma das permutações triplicadas, associamos a seguinte permutação de $\{1, 2, 3, 4, 5\}$ que se decompõem em produto de dois ciclos.

Temos um total de 18 permutações de $\{1, 2, 3, 4, 5\}$, que se decompõem em produto de dois ciclos. No caso k = 4, para cada permutação de $\{1, 2, 3, 4\}$ que se decompõem em quatro ciclos, a saber, $(1)(2)(3)(4)$, as repetimos quatro vezes, sublinhando um dos ciclos para diferenciá-los.

Para cada uma das permutações quadruplicadas, que diferenciamos sublinhando um dos ciclos, associamos uma permutação de $\{1, 2, 3, 4, 5\}$ que se decompõem em produto de dois ciclos.

$$(\underline{1})(2)(3)(4) \to (5432)(1)$$
$$(1)(\underline{2})(3)(4) \to (5431)(2)$$
$$(1)(2)(\underline{3})(4) \to (5241)(3)$$
$$(1)(2)(3)(\underline{4}) \to (5321)(4)$$

$$
\begin{array}{lll}
(\underline{1})(2)(34) \to (1)(5342) & (\underline{1})(4)(23) \to (1)(5234) & (\underline{2})(4)(13) \to (2)(5134) \\
(1)(\underline{2})(34) \to (2)(5134) & (1)(\underline{4})(23) \to (4)(5231) & (2)(\underline{4})(13) \to (4)(5132) \\
(1)(2)(\underline{34}) \to (34)(521) & (1)(4)(\underline{23}) \to (23)(541) & (2)(4)(\underline{13}) \to (13)(542) \\
(\underline{1})(3)(24) \to (1)(5243) & (\underline{2})(3)(14) \to (2)(5143) & (\underline{3})(4)(12) \to (3)(5124) \\
(1)(\underline{3})(24) \to (3)(5241) & (2)(\underline{3})(14) \to (3)(5142) & (3)(\underline{4})(12) \to (4)(5123) \\
(1)(3)(\underline{24}) \to (24)(531) & (2)(3)(\underline{14}) \to (14)(532) & (3)(4)(\underline{12}) \to (12)(543)
\end{array}
$$

Figura 7: Permutações de 4 que se decompõem em 3 ciclos associadas a permutações de 5.

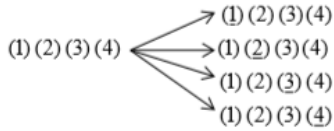


Figura 8: Caso k = 4.

Observe que obtemos um total de 50 permutações de $\{1,2,3,4,5\}$ que se decompõem em produto de dois ciclos.

Proposição 1. *Sejam* n *e* k *números naturais, com* $n, k \geq 0$, *temos que*

$$\sum_{k=1}^{n} k \left[\begin{array}{c} n \\ k \end{array} \right] = \left[\begin{array}{c} n+1 \\ 2 \end{array} \right].$$

A demonstração dessa proposição segue de modo análogo ao desenvolvimento do exemplo 2.

4. Números Harmônicos que são racionais

Esta seção foi fundamentada por meio do artigo [4] em que diversas propriedades envolvem números harmônicos e números de Stirling. Os números harmônicos são somas parciais da série harmônica. O estudo e entendimento da série harmônica [1] teve origem no século VI antes de Cristo com as experiências feitas pelo filósofo e matemático grego Pitágoras. Pelas suas descobertas é possível estabelecer uma relação direta entre melodia e harmonia, sendo que seus conceitos e definições são utilizados até os dias atuais (oitavas, ciclo de quintas etc).

Pitágoras (séc. VI, a.C.), afirmou que qualquer som para ser musical teria que ter altura definida e ser emitido por um instrumento ou por fonte natural, resultando em uma vibração ondulatória regular. Essa vibração é composta pelo som gerador (1^a nota) e outros sons definidos de intensidade menor e frequência mais aguda, chamados de sons harmônicos ou série harmônica.

A série harmônica (som gerador + notas agudas subsequentes) apresenta uma relação intervalar característica e imutável de origem natural ou física. Se tomarmos como exemplo uma corda

de um violão (6ª Corda – Nota Mi Grave) pode-se observar que além de vibrar em toda a sua extensão, também vibra em sua metade, em sua terça parte, em sua quarta parte e quinta parte etc., produzindo sons cada vez mais agudos.

Inicialmente definimos e exemplificamos os números harmônicos e apresentamos algumas propriedades. Por fim, estabelecemos sua relação com os Números de Stirling do primeiro tipo.

Os números Harmônicos são definidos como sendo a soma dos inversos naturais, ou seja,

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}$$

com $n \geq 1$. Vamos convencionar $H_0 = 0$.

As séries harmônicas (ou também conhecidas como séries–p) são da forma $\sum_{k=1}^{n} \frac{1}{k^p}$. Em termos de convergência dizemos que essas séries convergem-se $p < 1$ e divergem se $p \geq 1$. No nosso caso, $p = 1$, logo, nossa série é divergente, ou seja, a somatória não nos dá um número finito. Mais informações sobre convergência de séries podem ser vistas em [9].

Os números harmônicos aparecem como aplicações em outras ciências; um exemplo é na música, para isso veja [7]. A seguir enunciamos e provamos uma propriedade para os números harmônicos.

Proposição 2. *Seja* n *um número natural tal que* $n \geq 1$*, temos que:*

$$\sum_{k=1}^{n-1} H_k = nH_n - n.$$

Demonstração. Temos que

$$\sum_{k=1}^{n-1} H_k = H_1 + H_2 + H_3 + \cdots + H_{n-1}.$$

ou seja,

$$\begin{aligned}\sum_{k=1}^{n-1} H_k &= 1 + 1 + \frac{1}{2} + 1 + \frac{1}{2} + \frac{1}{3} + \cdots + 1 + \frac{1}{2} + \cdots + \frac{1}{n-1} \\ &= (n-1).1 + (n-2).\frac{1}{2} + \cdots + (n-3).\frac{1}{3} + \cdots + [(n-(n-1))].\frac{1}{n-1}.\end{aligned}$$

Assim temos:

$$\begin{aligned}\sum_{k=1}^{n-1} H_k &= n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n-1} \underbrace{-1-1-1-\cdots-1}_{n-1} \\ &= n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n-1} - n + 1 \\ &= n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n-1} - n + \frac{n}{n} \\ &= n\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}\right) - n = nH_n - n.\end{aligned}$$

□

Teorema 7. *Seja* n *natural,* $n \geq 1$*, temos que:*

$$H_n = \frac{1}{n!}\left[\begin{array}{c} n+1 \\ 2 \end{array}\right]$$

Demonstração.

$$\frac{1}{n!}\left[\begin{array}{c} n+1 \\ 2 \end{array}\right] = \frac{\left[\begin{array}{c} n+1 \\ 2 \end{array}\right]}{n!} = \frac{\left[\begin{array}{c} n \\ 1 \end{array}\right] + n\left[\begin{array}{c} n \\ 2 \end{array}\right]}{n!} = \frac{\left[\begin{array}{c} n \\ 1 \end{array}\right]}{n!} + \frac{n\left[\begin{array}{c} n \\ 2 \end{array}\right]}{n!}$$
$$= \frac{(n-1)!}{n!} + \frac{\left[\begin{array}{c} n \\ 2 \end{array}\right]}{(n-1)!} = \frac{1}{n} + \frac{\left[\begin{array}{c} n \\ 2 \end{array}\right]}{(n-1)!} \tag{2}$$

Segue da equação (2) que

$$\frac{\left[\begin{array}{c} n \\ 2 \end{array}\right]}{(n-1)!} = \frac{1}{(n-1)!} + \frac{\left[\begin{array}{c} n-1 \\ 2 \end{array}\right]}{(n-2)!} \tag{3}$$

Substituindo (3) em (2) temos:

$$\frac{1}{n!}\left[\begin{array}{c} n+1 \\ 2 \end{array}\right] = \frac{1}{n} + \frac{1}{n-1} + \frac{\left[\begin{array}{c} n \\ 2 \end{array}\right]}{(n-2)!}.$$

De forma análoga

$$\frac{\left[\begin{array}{c} n-1 \\ 2 \end{array}\right]}{(n-2)!} = \frac{1}{n-2} + \frac{\left[\begin{array}{c} n-2 \\ 2 \end{array}\right]}{(n-3)!}.$$

Repetindo esse processo temos que:

$$\frac{1}{n!}\left[\begin{array}{c} n+1 \\ 2 \end{array}\right] = \frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{2} + 1 = H_n.$$

Portanto,

$$H_n = \frac{1}{n!}\left[\begin{array}{c} n+1 \\ 2 \end{array}\right]$$

□

5. Uma possível abordagem dos Números de Stirling no ensino médio

Segundo a Base Nacional Comum Curricular (BNCC) os estudantes do ensino médio devem ter a habilidade de "Resolver e elaborar problemas de contagem envolvendo diferentes tipos de agrupamento de elementos [...]"; nesse viés, vimos anteriormente que os números de Stirling servem como ferramenta para contar em quantos ciclos disjuntos uma permutação decompõe-se, mas, além de seu caráter combinatório, os números de Stirling do primeiro tipo podem ser desenvolvidos por meio de seu caráter algébrico, para isso, consideremos o polinômio definido por

$$F_n(x) = (x+n)(x+(n-1))\dots(x+1)x$$

para $n > 0$ *e por convenção* $F_0(x) = 1$. *O coeficiente de* x^k *na expansão de* $F_n(x)$ *é* $\left[\begin{matrix} n \\ k \end{matrix} \right]$.

No ensino médio, os números de Stirling podem ser abordados dessa maneira. Além disso, também é possível explorar a natureza combinatória desses números por meio do seguinte problema: qual é o número de maneiras de n *pessoas sentarem-se em* k *mesas circulares idênticas sem que nenhuma delas fique vazia? A resposta para o problema é:* $\left[\begin{matrix} n \\ k \end{matrix} \right]$, *com* $n \geq k > 0$.

O exemplo a seguir dá-nos ideia da natureza combinatória dos números de Stirling do primeiro tipo.

Exemplo 15. De quantas maneiras quatro pessoas podem sentar-se em volta de três mesas circulares idênticas, sem que nenhuma mesa fique vazia?

Esse problema representa uma contagem, em que o número de mesas representa os ciclos, e o número de pessoas os elementos do conjunto A, ou seja, como temos quatro pessoas, o conjunto A poderá ser definido por $A = \{a, b, c, d\}$.

Do enunciado do exemplo sabemos que temos três mesas. Abaixo estão representadas geometricamente as maneiras de organizarmos essa distribuição – vale observar que as letras representam as pessoas e os cículos representam as mesas:

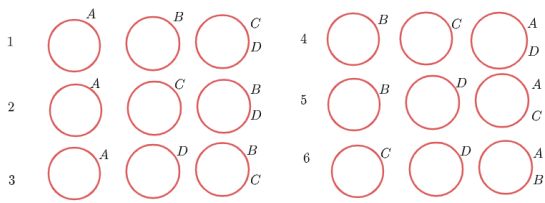


Figura 9: Distribuição de 4 pessoas em torno de 3 mesas circulares idênticas

Neste caso, temos 6 maneiras de realizar a distribuição, ou seja, $\left[\begin{matrix} 4 \\ 3 \end{matrix} \right]$.

Além disso, o item a) do Teorema 3 é um caso particular de permutação circular, pois o número de Stirling do primeiro tipo $\left[\begin{matrix} n \\ 1 \end{matrix} \right]$ *pode ser interpretado como a distribuição de* n *pessoas em torno de 1 mesa circular, e essa é a definição de permutação circular. Dessa forma, podemos interpretar*

a permutação circular como um caso particular dos números de Stirling do primeiro tipo $\begin{bmatrix} n \\ k \end{bmatrix}$, *quando* $k = 1$ *e* $n > 0$. *Vemos assim que os números de Stirling do primeiro tipo podem ser explorados no ensino médio de forma combinatória por meio das permutações circulares. Em [10] é explorada a relação entre as permutações circulares e os números de Stirling do primeiro tipo.*

Referências

[1] Anderle, D; Série Harmônica. Disponível em: <http://www.dirsom.com.br/index_htm_files/Serie>. Acesso em: 13 de outubro de 2019.

[2] Benjamin, A. T; Proofs that Really Count: The Art of Combinatorial Proof. MAA, Washington, 2002.

[3] Brasil. Ministério da Educação; Base Nacional Comum Curricular. Brasília, 2018.

[4] Benjamin, A. T; A Stirling Encounter with Harmonic Numbers. Mathematics Magazine, 2002. Disponível em: <https://www.math.hmc.edu/~benjamin/papers/harmonic.pdf>. Acesso em: 13 de outubro de 2019.

[5] Garcia, A; Lequain, Y.; Elementos de Álgebra. Impa, Rio de Janeiro, 2008.

[6] Silva, N. A; Os números de Stilring. UFGD, Dourados, 2018.

[7] Pereira, M. C; Matemática e Música: De Pitágoras aos dias de hoje. UniRio, Rio de Janeiro, 2013. Disponível em: <http://www2.unirio.br/unirio/ccet/profmat/tcc/2011/tcc-marcos>. Acesso em: 13 de outubro de 2019.

[8] Santos, J. P. O; Mello, M. P; Murari, I. T. C; Introdução à Análise Combinatória. Ciência Moderna, Rio de Janeiro, 2007.

[9] Stewart, J.; Cálculo. Volume 2. Cengarge Learning, São Paulo, 2013.

[10] Permutações circulares e os números de Stirling do primeiro tipo; Clubes de Matemática da Obmep, 2020. Disponível em: <http://clubes.obmep.org.br/blog/sala-de-estudo-permutacoes-circulares-e-os-numeros-de-stirling-do-primeiro-tipo/>. Acesso em: 19 de novembro de 2020.

Gabriel F. Pinheiro
Universidade Federal da Grande Dourados
<freitasgabriel688@gmail.com>

Irene M. Craveiro
Universidade Federal da Grande Dourados
<irenecraveiro@ufgd.edu.br>

Naiguiel A. da Silva
Escola Estadual
<naiguiel_20@hotmail.com>

Recebido: 23/11/2019
Publicado: 21/12/2020

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.5, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo844

O ensino de Matemática: uma experiência com alunos surdos.[1]

Fábio Costa do Amaral Keidna Cristiane Oliveira Souza Alcione Marques Fernandes

Resumo

Este trabalho apresenta o relato de uma experiência vivenciada com quatro alunos surdos do 6º e 9º ano do Ensino Fundamental. O estudo teve o objetivo de realizar uma abordagem sobre o Máximo Divisor Comum (MDC) por meio do Algoritmo de Euclides com os alunos surdos da Sala de Recursos Multifuncionais (SRM) de uma escola conveniada à rede Estadual de Ensino em Gurupi - TO. Com a utilização de recursos visuais e materiais manipuláveis no ensino de Matemática favorecendo a compreensão dos alunos no processo de aprendizagem, as atividades de ensino buscaram identificar as habilidades e dificuldades daqueles discentes, visando contribuir com possíveis sugestões para melhoria da prática pedagógica, no que diz respeito ao ensino e à aprendizagem de Matemática para surdos. Descrevem-se algumas interações dos alunos com as atividades e com o material. Os resultados apontam a importância da utilização de estratégias visuais, para que estudantes surdos possam construir entendimento sobre o objeto matemático.

Palavras-chave: Surdos; Recursos visuais; Ensino de Matemática; MDC

Abstract

This work presents an account of an experience lived with four deaf students from the 6th and 9th grade of Elementary School. The study aimed to carry out an approach on the Maximum Common Divisor (MDC) through the Euclid's Algorithm with deaf students in the Multifunctional Resource Room (SRM) of a school affiliated to the State Teaching Network in Gurupi - TO, with the use of manipulative visual and material resources in the teaching of Mathematics, favoring the understanding of students in the learning process, as teaching activities sought to identify the difficulties and difficulties of the students, he adds with possible suggestions for improving the pedagogical practice, regarding concerns the teaching and learning of mathematics for the deaf. Describe some student interactions with activities and material. The results point out the importance of using

Keywords: Deaf; Visuals aids; Mathematics teaching; MDC

1. Motivação

[1]Este estudo compreende em um recorte da pesquisa de Mestrado do primeiro autor, desenvolvida no Profmat associado à UFT, defendida em setembro de 2019.

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

Trabalho como professor de Matemática há mais de dois anos em uma escola conveniada à rede Estadual de Ensino localizada na cidade de Gurupi - TO. Não tivera, porém, a oportunidade de ministrar aula para alunos surdos, apesar de a instituição possuir uma Sala de Recursos Multifuncionais (SRM) em que é oferecido o Atendimento Educacional Especializado (AEE) cujo objetivo é atender esses e demais alunos com necessidades educacionais especiais.

Diante disso, mesmo através desse atendimento especializado ofertado pela escola, ainda há desafios encontrados por tais alunos e alunas nesse processo inclusivo, principalmente, no que diz respeito à aprendizagem dos conteúdos. Assim, a motivação de realizar este trabalho foi mostrar algo voltado especificamente ao ensino de Matemática, sobretudo buscando estratégias a fim de contribuir no processo de ensino para os alunos surdos, com o propósito de amenizar as dificuldades encontradas no ensino e na aprendizagem.

Portanto, o objetivo da experiência relatada foi realizar uma abordagem sobre o Máximo Divisor Comum (MDC) por meio do Algoritmo de Euclides com os alunos surdos da SRM, contando com a participação de uma intérprete de Língua Brasileira de Sinais (Libras), bem como, a utilização de recursos visuais e materiais manipuláveis para o ensino dos conceitos iniciais, voltado aos alunos surdos do 6º e 9º ano do Ensino Fundamental da referida escola.

Nesse sentido, a escolha de ensinar o MDC com foco no Algoritmo de Euclides é oportunizar aos alunos surdos conhecer outro método de resolução, tendo em vista que a maioria dos livros didáticos não aborda esse algoritmo no Ensino Fundamental. Além disso, outra observação a ser considerada é que o Algoritmo de Euclides possui diversas aplicações teóricas e práticas nos dias de hoje. "O método, chamado de Algoritmo de Euclides, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios" (HEFEZ, 2016, p.77).

2. Estratégias no ensino de Matemática para alunos surdos

Nesse contexto, apresenta-se a seguinte pergunta de pesquisa: como ensinar Matemática ao aluno surdo? As respostas são variadas, pois diversos autores dispõem de estudos e trazem estratégias aos professores, para aplicá-las com os alunos surdos no processo de ensino e de aprendizagem da Matemática.

Resumidamente podemos considerar,

> *As estratégias a serem aplicadas no desenvolvimento dos conteúdos de Matemática, que sejam úteis ao professor, são diversas: experimentação e estudo do meio, o desenvolvimento de projetos, os jogos, os seminários, os debates, a simulação, as propostas que possibilitem ao professor ser esse mediador, responsável por apresentar problemas ao aluno que o desafiem a buscar a solução (BARRETO; VIANA, 2012, p.3).*

Um fator importante para o ensino de Matemática para alunos surdos é a língua, sendo que a maioria dos professores são ouvintes e não possuem proficiência em Libras. Miranda C. e Miranda T. (2011) ressaltam que é possível comunicarmo-nos com os surdos desde que se tenha um pouco de habilidade gestual, porém, o não conhecimento de Libras torna-se uma barreira para um processo de ensino e de aprendizagem eficaz. E é preciso entender que não se pode tratar o surdo como se fosse um ouvinte – eles, os surdos, são capazes de aprender Matemática, contudo de maneira diferente.

Assim, ter o conhecimento do conteúdo ou mesmo da Libras não é suficiente: o professor precisa saber quais são as peculiaridades e também a melhor maneira de proporcionar aprendizagem ao aluno com essa especificidade.

Ainda de acordo com Miranda C. e Miranda T. (2011), a metodologia de ensino torna-se importante quando se trata de educação de surdos, devendo ser adequada, para facilitar e propiciar aos alunos meios de desenvolverem diversas formas de conhecimentos associados ao seu dia a dia. A busca por diferentes alternativas pedagógicas pode ser de suma importância na construção no processo de ensino e de aprendizagem da Matemática desses alunos.

Moreira (2016) esclarece que:

> *[...] não é necessário ter um material instrucional específico para o aluno com surdez. Os mesmos recursos utilizados para os ouvintes podem ser utilizados para os demais alunos, modificando apenas a abordagem e a metodologia, que devem ser adequadas às especificidades de cada grupo de estudantes [...] (MOREIRA, 2016, p.753).*

Cabe comentar que não é necessário um método "especial" para adequar um material para o ensino de Matemática a esses alunos, mas, sim, a forma de apresentá-lo na abordagem dos conceitos ministrados é que pode fazer diferença na aprendizagem dos conteúdos.

Nesse sentido, encontra-se o seguinte entendimento:

> *O elemento visual configura-se como um dos principais facilitadores do desenvolvimento da aprendizagem da população surda. As estratégias metodológicas utilizadas na educação da criança surda devem necessariamente privilegiar os recursos viso-espaciais como um meio facilitador do pensamento, da criatividade e da linguagem [...] (SALES, 2008, p.21).*

Carneiro (2009) acrescenta que, a estratégia "[...] para ser mais eficaz, deveria ser pautada principalmente na percepção visual e na manipulação de material concreto como elementos facilitadores, onde metodologias diferenciadas seriam importantes para atingir esta clientela" (CARNEIRO, 2009, p.127).

Entende-se, portanto, que a utilização de material concreto é importante, estimulando o aluno na construção e aquisição do conhecimento; é, de fato, fundamental a inserção desse material no ensino de Matemática para esses sujeitos.

Por outro lado, em relação aos enunciados de problemas em questões de Matemática, o embate está na questão de alguns surdos não dominarem o Português na forma escrita. Para facilitar o entendimento desses alunos, Silva (2014, p.108) diz que é necessário deixar "[...] a linguagem escrita a mais clara possível, com frases curtas, e sempre levando em consideração a questão viso-espacial".

Com base nisso, faz-se necessária a utilização da maior variedade possível de recursos e estratégias para representar os conceitos matemáticos, principalmente a utilização de experiência visual, a qual tem papel fundamental ao processo educacional dos surdos.

3. Percurso Metodológico

Mostraremos neste tópico o percurso metodológico da pesquisa, o qual detalha o caminho percorrido de cada fase para sua realização. Assim, adotamos deste modo: Local; Os participantes;

Trabalho na sala de recursos multifuncionais; Aulas ministradas e Atividades desenvolvidas pelos alunos surdos.

Dessa forma, partindo do objetivo deste estudo, optamos por uma pesquisa de cunho qualitativo, na qual realizamos análises sobre as aulas e atividades propostas para um grupo de alunos surdos, envolvendo conceitos de conteúdos predeterminados.

No que diz respeito às investigações em sala de aula:

> *[...] o cotidiano da sala de aula [...], por exemplo, são os objetos privilegiados de uma abordagem qualitativa. [...] Graças a seus instrumentos, [...], a pesquisa qualitativa permite mais particularmente estudar esses momentos privilegiados, dos quais emerge o sentido de um fenômeno social (DESLAURIERS E KÉRISIT, 2008, p. 131 apud FERRARI, 2014, p.41).*

Sendo assim, foram realizadas pelos alunos 6 (seis) atividades individualmente, sob a observação e intervenção do professor/pesquisador e da intérprete, buscando auxiliar e compreender as estratégias adotadas por esses participantes na sua resolução, cujos dados foram recolhidos por meio das atividades e das imagens gravadas durante sua realização.

Local

No que se refere ao lugar de realização da pesquisa, destaca-se que foi realizada na Sala de Recursos Multifuncionais (SRM) de uma instituição conveniada com a Rede Estadual de Ensino, em que é oferecido Atendimento Educacional Especializado (AEE), voltado para alunos do Ensino Fundamental I e II. O referido Centro está localizado no município de Gurupi – TO.

Desde 2014, o Centro vem desenvolvendo um trabalho voltado ao educando que possui algum tipo de deficiência ou condutas típicas de algum transtorno na SRM. Dessa forma, o Atendimento Educacional Especializado (AEE) faz parte do currículo dos educandos com necessidades educacionais especiais e organizado para apoiar, complementar e suplementar os serviços educacionais comuns, dentre as atividades curriculares específicas. Logo, dentre as atividades desenvolvidas na SRM, destacam-se: atendimento no contraturno aos educandos, a exemplo, com alguma deficiência, síndromes, Transtorno Espectro do Autismo (TEA) e demais Transtornos; o ensino da Libras, o ensino da Língua Portuguesa Escrita para Surdos, uma vez que esses trabalhos constituem um conjunto de procedimentos específicos mediadores do processo de apropriação e produção de conhecimentos.

É importante mencionar que a instituição, para efetivar esse trabalho na SRM, conta com duas professoras, uma instrutora surda, uma intérprete e uma professora especialista em Libras que atendem 42 alunos matriculados da rede regular de ensino, dentre eles 4 alunos surdos.

Os participantes

Os participantes foram quatro alunos surdos, cursando entre o 6º e o 9º ano do Ensino Fundamental. Portanto, as atividades foram aplicadas no período vespertino, ou seja, no contraturno e, em momentos distintos em que os alunos frequentavam a SRM, no período de janeiro a maio de 2019.

Vale ressaltar que os quatro alunos surdos frequentam a SRM do Centro Educacional, porém estão matriculados em outras escolas regulares comuns da comunidade que não possuem Atendimento Educacional Especializado (AEE).

O desenvolvimento das aulas e atividades com os alunos foi realizado com o auxílio de uma instrutora surda, uma intérprete, uma professora especialista em Libras e o professor/pesquisador. Esses atendimentos ocorreram na maioria das vezes com apenas um aluno, o que, de fato, ajudou

quanto ao desenvolvimento das aulas e em seu entendimento, tendo em vista que a proximidade e a exclusividade do atendimento foram favoráveis para o ensino e para a aprendizagem desses conceitos.

Os quatro alunos surdos são usuários de Libras, um deles é oralizado[2] e frequentam aulas em salas regulares comuns com alunos ouvintes. Para manter o sigilo de suas identidades, os nomes são fictícios e foram dispostos na ordem que eram realizados os encontros semanais, conforme mostra o Quadro 1 abaixo:

Quadro 1= Alunos surdos participantes

Nome	**Sexo**	**Idade**	**Série**	**Idade** (aprendeu libras)	**Grau de surdez**
Joana	Feminino	15 anos	9º Ano	10 Anos	Profunda
Borges	Masculino	15 Anos	9º Ano	6 Anos	Profunda
Sara	Feminino	13 Anos	9º Ano	10 Anos	Profunda
Hélio	Masculino	11 Anos	6º Ano	9 Anos	Profunda

Fonte: Dados da pesquisa

Os alunos participantes nasceram surdos, aprenderam Libras tardiamente e alguns apresentam distorção idade/série, como ilustra o Quadro 1. E são todos filhos de pais ouvintes que não dominam a Libras.

Trabalho na sala de recursos multifuncionais

Inicialmente, uma conversa com a intérprete e a professora especialista em Libras na SRM acerca dos conteúdos necessários como pré-requisito para a realização desta pesquisa. Elas relataram que a maioria dos alunos surdos estava com o desempenho abaixo do nível esperado para o ano cursado. Assim, decidimos realizar no primeiro encontro uma atividade inicial para identificar se os alunos surdos dominavam as quatro operações básicas, com o intuito de começar os estudos iniciais para introdução do Algoritmo de Euclides, proposto na pesquisa.

Desse modo, identificamos pelos resultados da atividade inicial que não seria possível prosseguir na introdução do Algoritmo de Euclides sem que os alunos dominassem as quatro operações básicas. Portanto, decidimos assim ministrar aula por aula juntamente com a aplicação de atividades propostas com os conteúdos de adição, subtração, multiplicação e divisão, com objetivo de tentar minimizar a falta de pré-requisito dos alunos, relacionados a tais conceitos. E, também, rever os

[2]Surdos oralizados são surdos que utilizam sua língua materna para se comunicarem na forma oral ou, leitura labial e/ou leitura e escrita e, fazem ou não uso da Libras.

conteúdos de múltiplos, divisores e máximo divisor comum para efetivar a introdução do Algoritmo de Euclides.

As atividades desenvolvidas foram apresentadas conforme cronograma do Quadro 2 abaixo.

Quadro 2- Atividades desenvolvidas

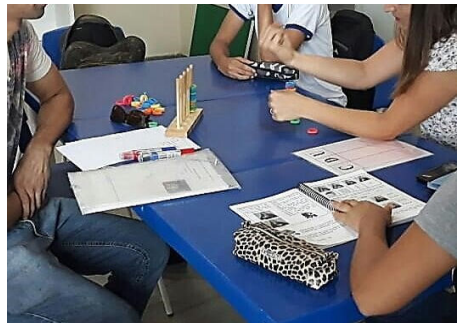
Atividade Inicial	Para verificar o conhecimento prévio dos alunos, com questões abertas envolvendo os seguintes conteúdos: adição, subtração, multiplicação e divisão.
Aula 1	Adição de números naturais; Utilização do material dourado; exemplos e atividades propostas.
Aula 2	Subtração de números naturais; Utilização do ábaco; exemplos e atividades propostas.
Aula 3	Multiplicação de números naturais; Utilização do ábaco, tabuada manipulável e videoaula; exemplos e atividades propostas.
Aula 4	Divisão de números naturais; Utilização do ábaco, tabuada manipulável e videoaula; exemplos e atividades propostas.
Aula 5	Múltiplos e divisores com números naturais; Utilização de tabuada manipulável; exemplos e atividades propostas.
Aula 6	Máximo Divisor Comum (MDC); Utilização de pincel e quadro branco, tabuada manipulável; exemplos e atividades propostas.

Fonte: Dados da pesquisa

Aulas ministradas

As aulas ministradas na SRM aconteceram com o intuito de usar recursos visuais e objetos manipuláveis para melhor assimilação dos conteúdos pelos alunos. Dessa forma, as aulas de Matemática foram todas ministradas em Libras e utilizando-se material manipulável conforme Figura 1.

Figura 1: Aula em Libras



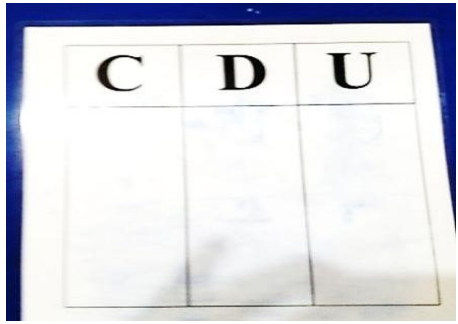
Fonte: Acervo do pesquisador (2019)

Na Aula 1, com adição, por meio do uso do material dourado, buscamos mostrar aos alunos que

nosso sistema de numeração é decimal e posicional, sendo que até então os alunos resolviam as operações sem compreender o processo usado, principalmente quando 10 unidades seriam transformadas em 1 dezena. Eles realizavam as operações automaticamente, e por isso cometiam erros no procedimento do algoritmo da adição realizado.

Na busca em adequar a metodologia de ensino, a intérprete confeccionou um material adaptado representado na figura 2, contendo a classe simples e as ordens da unidade, dezena e centena para desenvolver as operações.

Figura 2: Classe Simples



Fonte: Acervo do pesquisador (2019)

Na Aula 2, com subtração, devido à dificuldade dos alunos em entender o processo do algoritmo e tentar evitar os erros cometidos nas operações, decidimos usar o Ábaco (Figura 3), para que eles fizessem primeiramente a construção dos números e a operação no próprio material. Depois de entendido o procedimento do algoritmo da subtração, os alunos poderiam resolver as atividades propostas para melhor compreensão, tentando assim sanar os erros cometidos anteriormente na atividade inicial.

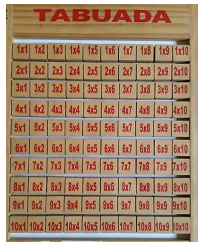
Figura 3: Ábaco Vertical Aberto

Fonte: Acervo do pesquisador (2019)

Na Aula 3, com multiplicação, começamos com o uso da "Tabuada de Pitágoras", material ma-

nipulável (Figura 4), a qual utilizamos posteriormente para introduzir o conceito de múltiplos, através de alguns exemplos. Além disso, contamos com outro recurso denominado "multiplicação pelo método japonês", que foi mostrado aos alunos através de vídeo do *youtube*[3] com o título: "Matemática em Libras (Enem) – Multiplicação método Japonês Fácil", o qual mostrava uma forma diferente de obter os resultados da tabuada, mais "visual", o que contribuiu para facilitar o entendimento dos alunos surdos. Em suma, continuamos com o auxílio do ábaco devido a seu êxito na realização das operações de multiplicação.

Figura 4: "Tabuada de Pitágoras"



Fonte: Acervo do pesquisador (2019)

Sales (2008), também considera importante a utilização de recursos didáticos, como as "mídias tecnológicas" com o uso da Libras – o que promove aos alunos surdos de forma significativa a apropriação dos conceitos matemáticos trabalhados.

Assim, na Aula 4, iniciamos com outro vídeo do *youtube*[4] intitulado "Matemática Básica – Aula 4 – Divisão – Em Libras", com o professor ensinando o processo do algoritmo da divisão, cada aluno assistiu ao vídeo acompanhado pela intérprete e pelo professor/pesquisador. Durante o vídeo houve a interrupção de cada exemplo para verificarmos se ele conseguiu compreender a explicação. Em seguida, cada aluno fez os exemplos e, por fim, as atividades propostas.

Na Aula 5, sobre múltiplos e divisores, foi necessário novamente utilizar a "Tabuada de Pitágoras" como recurso concreto, como mostrado na Figura 5, dessa vez com os resultados das multiplicações para que os alunos tivessem alguns exemplos de múltiplos para então entender o conceito de divisores.

Figura 5: Resultados das multiplicações

Fonte: Acervo do pesquisador (2019)

[3]Disponível em: (https://www.youtube.com/watch?v=FZ7lTUD7sb8). Acesso em: 11-jan.-2019.
[4]4 Disponível em: (https://www.youtube.com/watch?v=rw5y9IDMYKo). Acesso em: 11-jan.-2019.

Na Aula 6, sobre Máximo Divisor Comum (MDC), iniciamos com exemplos listando os divisores de dois números, para depois o aluno encontrar todos os divisores comuns e destacar qual era o maior divisor entre eles; essa forma de calcular o MDC denominamos como o primeiro método. O segundo método foi o Algoritmo de Euclides, no qual foram ensinados os "passos" para sua aplicação e obtenção do MDC.

Para uma melhor compreensão a respeito dos dois métodos utilizados, exemplificaremos como isso pode ser feito.

Utilizando a Listagem de Divisores (primeiro método), para calcular o MDC entre 95 e 30. Pode ser feito da seguinte forma:

- Listar todos os divisores de 30.
  $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$.
- Listar todos os divisores de 95.
  $D(95) = \{1, 5, 19, 95\}$.

Assim, identificamos o maior divisor comum de 30 e 95. Logo, o $MDC(95, 30) = 5$.

Utilizando o Algoritmo de Euclides (segundo método), para calcularmos o MDC entre 95 e 30, Pode ser feito, utilizando-se um diagrama semelhante ao do Quadro 3:

Quadro 3 = Algoritmo de Euclides

Q	3	6	
95	30	5	
R	5	0	

Fonte: Elaborado pelo autor

Observamos que:

- Na primeira linha do diagrama, aparecem os quocientes (Q) das divisões efetuadas;
- Na segunda linha, aparecem os divisores e dividendo das divisões efetuadas;
- Na terceira linha, aparecem os restos (R) das divisões efetuadas.

É possível perceber pelo diagrama que o MDC dos dois números em questão é o último resto não nulo do processo das divisões sucessivas. Logo, o $MDC(95, 30) = 5$.

Em Matemática, o Algoritmo de Euclides é um método eficiente de encontrarmos o Máximo Divisor Comum entre dois números inteiros. O primeiro método em que se listam os divisores para encontrarmos o MDC é "mais fácil" para a compreensão, na opinião dos alunos, porém, dependendo dos números ele não é muito prático, em função da quantidade de divisores que se deve listar.

Outro método que podemos aplicar tanto com os alunos ouvintes, quanto também com os alunos surdos, para enriquecer o estudo do MDC, pode ser tomado pela abordagem sugerida em dois artigos interessantes na *Revista do Professor de Matemática* (RPM), o caderno 29, de 1995, e o caderno 51, de 2003, os quais tratam de um método geométrico para calcular o MDC entre dois

números, favorecendo, assim, um melhor entendimento do conteúdo para os alunos surdos, pois o método contribui na percepção visual para a obtenção do MDC.

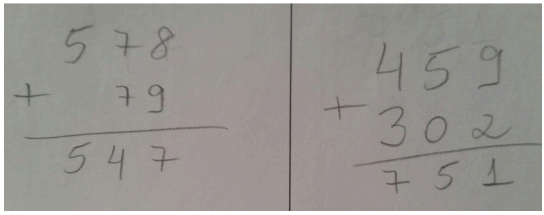
Atividades desenvolvidas pelos alunos surdos

Como bem acentua Sales (2008, p.55) "[...] a criança surda, [...] apesar de ter dificuldades de percepção e apreensão por meio do estímulo sonoro, não apresenta, necessariamente, comprometimento no seu desenvolvimento intelectual". O aluno surdo consegue aprender Matemática, assim como o aluno ouvinte; no entanto, com um "olhar" diferente.

Aluna Joana

A aluna começou a Atividade 1 com adição e na questão 1, em algumas "contas", não fazia a conversão de unidades para dezena e nem de dezena para centena, cometendo assim equívocos na conclusão das operações, como mostrado na Figura 6:

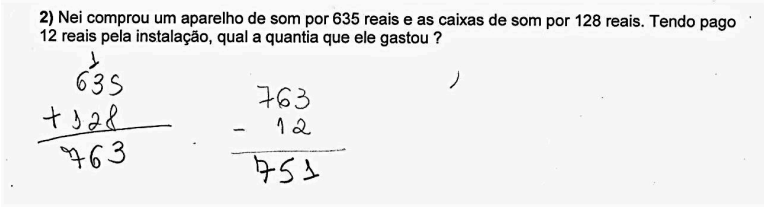
Figura 6: Atividade desenvolvida por Joana



Fonte: Acervo do pesquisador (2019)

Com o apoio do material dourado e o auxílio do professor/pesquisador e da intérprete, a aluna conseguiu finalizar as operações com menos dificuldade. Já na questão 2, que envolvia um problema, a aluna não conseguiu interpretá-lo corretamente. Em vez de adicionar três parcelas, ela adicionou os dois primeiros números e subtraiu o resultado encontrado com o terceiro, conforme Figura 7:

Figura 7: Atividade desenvolvida por Joana



Fonte: Acervo do pesquisador (2019)

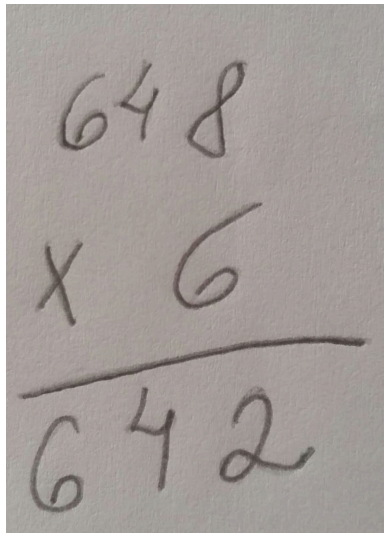
Em relação aos enunciados de questões em situações-problema na Matemática, para facilitar o entendimento desses alunos, Silva (2014, p.108) diz que é necessário deixar "a linguagem escrita a

mais clara possível, com frases curtas, e sempre levando em consideração a questão viso-espacial". Mesmo sendo feita novamente a tradução da atividade pela intérprete, Joana demonstrou dificuldade na interpretação do problema da questão 2, mas verificamos que houve uma evolução quando adicionou as duas primeiras parcelas, pois o fez corretamente.

Na Atividade 2, com subtração, tanto essa aluna quanto os demais alunos surdos tiveram facilidade para subtrair "contas" mais simples, em que o minuendo era maior que o subtraendo, mas quando era o contrário, surgiram mais dificuldades para "pedir emprestado", visto que, para ser possível encontrar a diferença teriam que recorrer à ordem superior mais próxima, causando confusão aos alunos. Além disso, a aluna teve necessidade de usar algum tipo de material concreto para fazer as contagens, recorrendo ao uso das peças do ábaco.

Na Atividade 3 que envolvia multiplicação, a aluna não fez, apenas assistiu à aula. Fez alguns exemplos, demonstrando que não dominava a tabuada e não conseguiu fazer as multiplicações confundindo com subtração, conforme Figura 8.

Figura 8: Exemplo desenvolvido por Joana



Fonte: Acervo do pesquisador (2019)

Observamos que a aluna já faltara aos encontros por várias vezes antes da Aula 3, porém, após assisti-la, por motivos pessoais, Joana não participou de mais nenhum encontro, sendo essa a última atividade desenvolvida pela discente, infelizmente.

Aluno Borges

O aluno Borges, desde as primeiras atividades com adição, demonstrou certa facilidade em fazer cálculo mental. Apenas se confundia quando necessitava fazer as conversões das classes simples, mas na Atividade 1 conseguiu resolver todas as adições da primeira questão corretamente. Na segunda questão, Figura 7, que envolvia um problema, o aluno interpretou sem dificuldade e apenas questionou sobre adicionar três parcelas de uma só vez. Ele foi orientado pela intérprete, que poderiam ser feitas de duas a duas, e assim resolveu corretamente sem nenhuma intervenção.

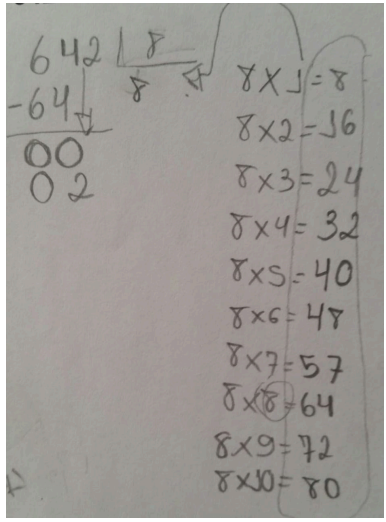
Na Atividade 2, Borges buscou diversas vezes o auxílio do ábaco para facilitar a compreensão e calcular as operações, principalmente na subtração, conseguindo concluí-la com sucesso.

Na situação-problema apresentada na segunda questão, o aluno não entendeu o que pedia o problema e se confundiu ao tentar fazer a subtração do número menor pelo maior, mas com a intervenção e a orientação da intérprete, Borges "armou" a conta de forma correta, mas com o apoio do ábaco a finalizou corretamente.

Na Atividade 3, com multiplicação, o aluno memorizou a tabuada de alguns números fazendo as multiplicações de maneira rápida, às vezes por descuido confundia-se quando a operação tinha o multiplicando e o multiplicador com dois algarismos ou mais, mas com intervenção conseguiu resolver.

Na Atividade 4, com divisão, o aluno demonstrou necessidade de construir a tabuada em todas as questões (Figura 9). Mas demonstrou ter ideia de que os resultados da tabuada podem ser encontrados com a soma do multiplicando com o resultado do anterior, ou seja, somou de dois em dois, de três em três e assim por diante, e com isso facilitou nas construções.

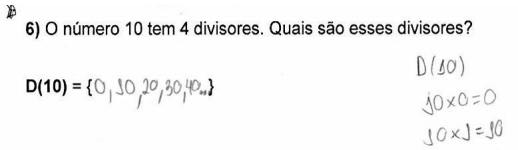
Figura 9: Atividade desenvolvida por Borges



Fonte: Acervo do pesquisador (2019)

Na Atividade 5, Borges entendeu o conceito de múltiplo, mas teve dificuldades para encontrar os divisores, confundindo com o procedimento a ser executado, conforme Figura 10, encontrando os múltiplos de 10 e não os divisores de 10.

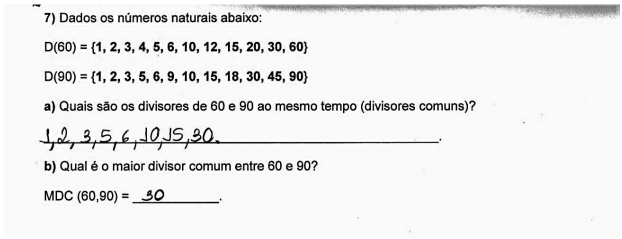
Figura 10: Atividade desenvolvida por Borges



Fonte: Acervo do pesquisador (2019)

Na questão 7, com o intuito de introduzir na aula posterior o MDC, pedimos aos alunos para identificar os divisores comuns e o maior divisor entre eles, conforme Figura 11, em que eles tiveram aproveitamento de cem por cento. Logo, podemos concluir que quando os divisores estavam listados de forma "visual", os alunos não tiveram dificuldades de identificar os divisores comuns e o maior divisor entre eles, diferentemente da questão anterior, em que deveriam listá-los.

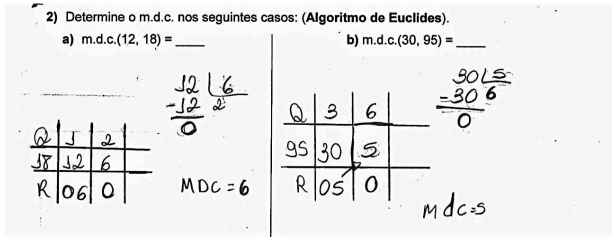
Figura 11: Atividade desenvolvida por Borges



Fonte: Acervo do pesquisador (2019)

Na Atividade 6, com o MDC, iniciamos com exemplos para listar todos os divisores de dois números, caracterizado como o primeiro método. Como segundo método, utilizamos o Algoritmo de Euclides. A partir daí, os alunos utilizaram somente o Algoritmo de Euclides como método principal para determinar o MDC. Nesse caso, não apenas Borges, mas todos os demais alunos conseguiram assimilar a sequência de "passos" que constitui esse algoritmo, conforme Figura 12.

Figura 12: Atividade desenvolvida por Borges



Fonte: Acervo do pesquisador (2019)

Aluna Sara

Na Atividade 1, a aluna desenvolveu os algoritmos com certa facilidade, no entanto, confundia-se nas contagens dos números, nas ordens da classe simples, tendo que refazer algumas vezes, pois ora aumentava uma unidade, ora diminuía uma unidade.

Portanto, Sara desenvolveu a primeira questão da Atividade 2 sem a ajuda do ábaco e notamos que a aluna efetuava as subtrações com a ideia da operação inversa, buscando saber o que faltava para chegar ao valor pretendido e não subtraindo diretamente. Sara preferia fazer as adições das operações inversas a fazer uso das subtrações em cada ordem da classe simples. Foi possível observar também que ela confundiu-se nas adições, fazendo cálculos mentais, necessitando assim de material concreto, recorrendo aos palitos de picolé para fazer as contagens, para efetuar as adições sem cometer erros.

Na questão 2, embora a aluna tivesse entendido o que o problema demandava, cometeu inicialmente o mesmo equívoco do aluno Borges, tentando subtrair o número menor pelo maior. No entanto, mesmo encontrando algumas dificuldades, a aluna conseguiu desenvolver as atividades propostas da Atividade 2.

Na Atividade 3, Sara encontrou muita dificuldade com multiplicação em função da tabuada, sendo assim, em todas as contas recorreu ao apoio de um objeto visual e palpável, fazendo uso do ábaco e até mesmo das próprias peças do material para fazer as contagens. Ela montou conta por conta no ábaco, como lhe foi ensinado. A Figura 13 mostra que ela entendeu o processo do algoritmo da multiplicação, mas sem dominar a tabuada.

Figura 13: Atividade desenvolvida por Sara

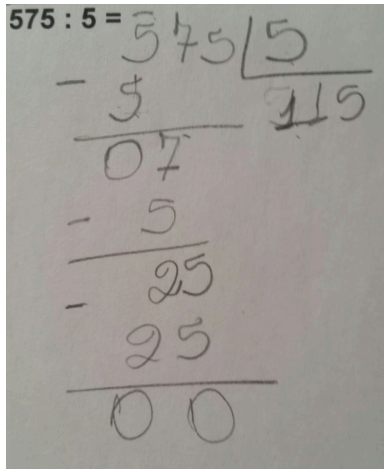
Fonte: Acervo do pesquisador (2019)

Na Atividade 4, depois de assistir ao vídeo e com os exemplos usados na aula com o conceito de divisão, Sara conseguiu entender a sequência de passos que constitui o algoritmo, e melhor do que o aluno Borges. Como observamos na aula anterior, a aluna apresentou dificuldade ao processo de contagem, conta de "um em um" (unidade por unidade) e se perde na contagem por várias vezes, tendo que recomeçar o processo. Na divisão, a aluna consulta a tabuada e "pega" o valor que precisa, mas sem a ideia da operação inversa. Apesar de entender os "passos" do algoritmo da divisão, ela apresenta ainda dificuldades.

Enfim, todos os alunos sentiram dificuldades em dar sequência ao algoritmo quando o número do dividendo não tinha resultado na tabuada, tendo que encontrar o valor mais próximo, nesse caso,

7/5 na divisão, conforme a Figura 14. Não tendo ideia de fazer estimativas ou valor aproximado, porém, com mediações do professor/pesquisador, concluiu corretamente a atividade.

Figura 14: Atividade desenvolvida por Sara

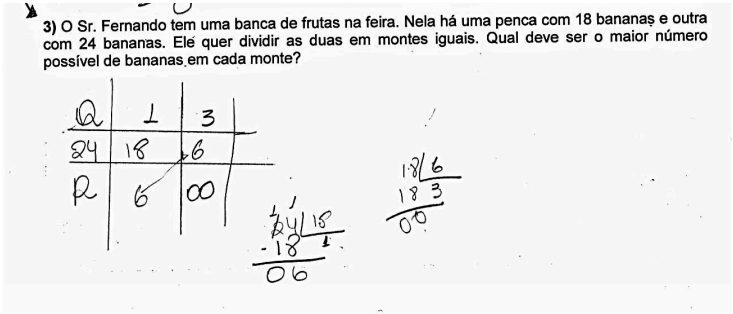


Fonte: Acervo do pesquisador (2019)

Na Atividade 5, a aluna compreendeu o conceito de múltiplo por meio da consulta à "Tabuada de Pitágoras" e também na contagem de palitos, a fim de perceber como a sequência de múltiplos prosseguia. Com os divisores, ela teve dificuldades, assim como Borges, no desenvolvimento das divisões e também por não ter ainda a habilidade de fazer cálculos mentais, visto que procedia a divisão por todos os números naturais menores ou iguais ao número procurado, constatando, assim, quais teriam restos iguais a zero na divisão pelos números naturais.

Na Atividade 6, com MDC, ela compreendeu o Algoritmo de Euclides, mas com dificuldades quando envolvia situações-problema para interpretá-lo. No entanto, a partir do procedimento construído, ela conseguiu executá-los sem dificuldades, de acordo com a Figura 15, pois tanto Sara quanto Borges mostraram evolução com o algoritmo da divisão.

Figura 15: Atividade desenvolvida por Sara



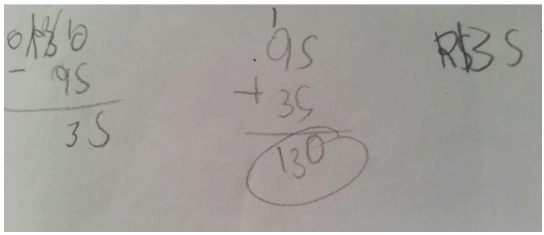
Fonte: Acervo do pesquisador (2019)

Aluno Hélio

O aluno Hélio demonstrou mais facilidade e domínio das quatro operações básicas em relação aos outros alunos surdos. Fizemos todas as atividades sem o auxílio de intérprete, acompanhados somente pela instrutora surda da SRM. O aluno teve facilidade em resolver as adições da Atividade 1, fazendo cálculos mentais rápidos e não tendo dificuldade em ler e interpretar os problemas propostos. O aluno comentou ser "*muito fácil as operações de adição*".

Na Atividade 2, com subtrações, mostrou domínio e agilidade para resolver as questões sem fazer uso de qualquer material concreto de apoio. Na Questão 2, Figura 16, não satisfeito com o resultado, ele ainda o validou, demonstrando domínio também da operação inversa.

Figura 16: Atividade desenvolvida por Hélio



Fonte: Acervo do pesquisador (2019)

Na Atividade 3, com multiplicação, o aluno mostrou também domínio com a tabuada, resolvendo a primeira questão com segurança, sem ter nenhum problema em desenvolver as operações com dois ou três algarismos em cada fator. Além de preencher corretamente a tabuada proposta na atividade "extra", conforme Figura 17, fez observações interessantes a respeito da sequência de números que se repetiam nas linhas e nas colunas, como a exemplo da linha 1 em que a sequência de números é $1, 2, 3, ..., 10$. O mesmo acontece na coluna 1, na linha 2 e coluna 2, e assim por diante. Logo, finalizou preenchendo atividade "extra" sem fazer as multiplicações e sim observando a sequência que se formava.

(x)	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

Fonte: Acervo do pesquisador (2019)

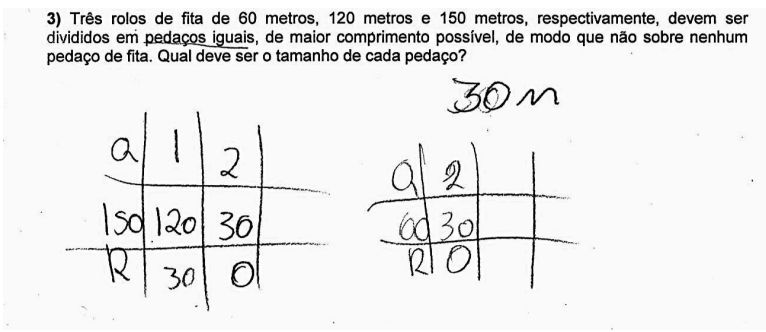
Na Atividade 4, que envolvia divisões exatas e não exatas, Hélio, mais uma vez, demonstrou

tranquilidade em resolvê-las. Nas divisões não exatas, demonstrou ter condições de continuar a divisão, mas com mediação do professor/pesquisador explicando que era necessário considerar o resto da divisão (diferente de zero), pois seria importante para os conceitos futuros para a introdução e desenvolvimento do Algoritmo de Euclides. Nas questões que envolviam problemas, ele também não encontrou dificuldades em interpretá-los, tampouco em resolvê-los.

Na Atividade 5, o aluno Hélio teve inicialmente dificuldades para entender a definição sobre divisores. Foi importante nesse momento o uso do material visual, destacando os resultados das multiplicações da "Tabuada de Pitágoras", o que se tornou um facilitador para a compreensão dos conceitos, para identificar os múltiplos e divisores. Assim, o aluno entendeu as definições e passou a resolver as atividades propostas com facilidade.

Na Atividade 6, o aluno conseguiu entender a sequência de "passos" que constitui o Algoritmo de Euclides e, para encontrar os quocientes e restos nas divisões sucessivas, fez com facilidade, por dominar o algoritmo da divisão de números naturais. Na terceira questão que continha um problema, Hélio não conseguiu interpretá-lo sem a mediação do professor/pesquisador, mas após uma nova leitura, seguida da explicação, compreendeu a situação pedida, porém, ficou confuso sobre como calcular o MDC com três números. Foi-lhe, então, novamente, que o algoritmo em questão é usado para calcular o MDC de dois números diferentes de zero, o qual procedendo-se ao cálculo do MDC com dois quaisquer dos três números que aparece no problema, para, em seguida, finalizar fazendo o MDC entre resultado dos dois primeiros números com o terceiro número que também aparece no problema. Ele compreendeu, mas cometeu um equívoco no cálculo da divisão de 120 por 30, conforme Figura 18, colocou o quociente igual a 2, quando o certo seria 4.

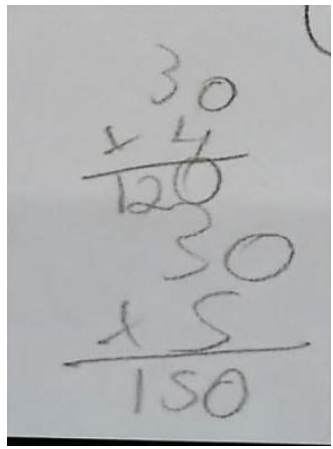
Figura 18: Atividade desenvolvida por Hélio



Fonte: Acervo do pesquisador (2019)

Mesmo com o pequeno erro observado na questão 3, isso não foi suficiente para alterar o resultado final, considerado apenas erro de escrita. E para compreender melhor o que o problema pedia, Hélio fez no rascunho as operações inversas para encontrar 120 e 150 conforme Figura 19, demonstrando ter entendido o problema. O aluno ainda fez uma observação dizendo que "*listar todos os divisores de 150 seria muito cansativo*", mostrando a preferência pelo Algoritmo de Euclides (2º método) em vez da listagem de divisores (1º método).

Figura 19: Atividade desenvolvida por Hélio



Fonte: Acervo do pesquisador (2019)

4. Considerações finais

Neste trabalho, identificamos que apesar de se encontrarem no último ano do Ensino Fundamental, os alunos surdos não possuem os pré-requisitos básicos das operações matemáticas. Assim, as aulas e atividades buscaram desenvolver os conhecimentos não adquiridos pelos alunos em sua trajetória escolar. "A não preocupação com o conteúdo de noções básicas por parte do professor pode causar prejuízo quanto às aquisições realizadas por parte do aluno surdo" (MIRANDA, C.; MIRANDA, T., 2011, p.38).

Dessa forma, nas aulas ministradas, revelou-se a possibilidade de os alunos e o professor/pesquisador superarem suas limitações com os conceitos aplicados. Para isso, foram utilizadas estratégias visuais evidenciando materiais como vídeos, objetos manipuláveis, dentre outros, que são importantes para a construção dos conceitos matemáticos.

Identificamos também que a utilização desses materiais como recursos didáticos contribuíram na percepção visual agindo como meio facilitador, tornando-se assim um elemento quase indispensável ao processo de ensino e de aprendizagem significativo para esses participantes. "O fato de o surdo encontrar dificuldades em adquirir língua oral faz com que ele apreenda o mundo pela visão e pela via tátil" (SALES, 2008, p.21).

Constatamos que os alunos conseguiram entender a sequência de "passos" que constitui o Algoritmo de Euclides. Apesar disso, tropeçaram nos conceitos básicos que ainda não dominam com propriedade como, compreensão do sistema de numeração decimal e posicional, processo de contagem, valor aproximado, cálculo mental, subtração e divisão. Enfim, conceitos esses que requerem tempo e prática para que se tenha domínio adequado, desde que façam uso da Libras e, sobretudo, que os professores utilizem estratégias adequadas para abordar tais conteúdos.

Assim, tendo o privilégio de investigar um pouco mais sobre os sujeitos surdos, fica evidente a necessidade de rever as práticas pedagógicas em sala de aula em relação ao ensino de Matemática com esses alunos, principalmente quanto à imprescindível utilização da Libras como principal meio de comunicação entre professor e aluno. "Quando não se aceita a língua identitária dos surdos,

segregando-o de todas as formas, pretende-se mantê-lo no anonimato e na exclusão. No entanto, não saber LIBRAS, não é impedimento para deixar o aluno de lado [...]" (MOREIRA, 2016, p. 753).

É importante que os professores façam uso de metodologias e estratégias que possibilitem o processo de ensino e de aprendizagem dos alunos surdos, mesmo não dominando a Libras.

Ensinar Matemática para alunos surdos (assim como para os ouvintes) é um desafio, e o processo educacional ao qual os surdos foram submetidos tem sido sentido durante anos na sua educação, por falha no processo de inclusão desses alunos nas escolas regulares comuns de ensino.

Nesse sentido, em relação aos objetivos almejados com a realização deste trabalho, consideramos que os resultados observados foram positivos, principalmente, pela maneira como foram adotadas as estratégias no ensino dos conceitos da disciplina. Portanto, a forma conduzida no ensino surtiu efeito pelo avanço que esses alunos demonstraram no trajeto final das atividades desenvolvidas, em especial nos conteúdos básicos em que alunos surdos não possuíam inicialmente.

Referências

[1] BARRETO, M. C.; VIANA, F. R. *O ensino de matemática para alunos com surdez.* In:Simpósio Internacional de Pesquisa em Educação Matemática, 3, 2012, Fortaleza. Anais do 3º Sipemat , Fortaleza: UFC. p. 1-6.

[2] CARNEIRO, K. T. A. *Cultura surda na aprendizagem matemática: o som do silêncio em uma sala de recurso multifuncional.* 2009. Dissertação (Dissertação do Programa de Pós-Graduação em Educação em Ciências e Matemática) - Universidade Federal do Pará, Belém 2009.

[3] FERRARI, A. C. M. *Atuação do Tradutor-Intérprete de Libras na Aprendizagem Matemática de Surdos no Ensino Fundamental.* 2014. 125 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação em Educação: Conhecimento e Inclusão Social, Universidade Federal de Minas Gerais, Belo Horizonte, 2014. Disponível em: < www.bibliotecadigital.ufmg.br/dspace/handle/1843/BUOS-9JGFY7 >. Acesso em: 16 maio de 2019.

[4] HEFEZ, A. *Aritmética.* 2 ed. Rio de Janeiro: SBM, 2016. 298 p. (Coleção Profmat).

[5] MIRANDA, C. J. de A.; MIRANDA, T. L. de. "O Ensino de Matemática para Alunos Surdos: Quais os Desafios que o Professor Enfrenta?"*Revemat: Revista Eletrônica de Educação Matemática* Florianópolis, v. 06, n°1, pp.31- 46, 2011.

[6] MOREIRA, G. E. *O ensino de matemática para alunos surdos : dentro e fora do texto em contexto.* EMP: Educação Matemática Pesquisa, São Paulo, v. 18, n°2, 2016. Disponível em: < https://revistas.pucsp.br/emp/article/download/23486/pdf>. Acesso em: 01 abril 2019.

[7] OLIVEIRA, Z. C. de. *Uma interpretação Geométrica do mdc.* RPM 29, 1995. Disponível em <http://rpm.org.br/cdrpm/29/5.htm>. Acesso em: 05 de novembro de 2020.

[8] POLEZZI, M. "Como Obter o MDC e o MMC sem Fazer Contas?". RPM 51, 2003. Disponível em: <http://rpm.org.br/cdrpm/51/6.htm>. Acesso em: 05 de novembro de 2020.

[9] SALES, E. R. *Refletir no silêncio: Um estudo das aprendizagens na resolução de problema aditivos com alunos surdos e pesquisadores ouvintes.* 2008. 162 f. Dissertação (Mestrado em Educação em Ciências e Matemáticas) – Programa de Pós-Graduação em Educação em Ciências e Matemáticas, Núcleo Pedagógico de Apoio ao Desenvolvimento Científico, Universidade Federal do Pará, Belém, 2008.

[10] SILVA, E. L. da. *Luz, câmera, ação: adaptando uma teleaula de frações para o público surdo.* 2014. Dissertação (Programa de Pós-Graduação em Educação Matemática) – Universidade Bandeirante, São Paulo, 2014.

Fábio Costa do Amaral
Secretaria Estadual da Educação, Juventude e Esporte do Tocantins-Seduc
<fabiocosta_amaral@hotmail.com>

Keidna Cristiane Oliveira Souza
Universidade Federal do Tocantins-UFT
<keidna@mail.uft.edu.br>

Alcione Marques Fernandes
Universidade Federal do Tocantins-UFT
<alcione@uft.edu.br.>

Recebido: 31/08/2020
Publicado: 22/12/2020

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.5, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo845

Criptografia RSA na Educação Básica: uma necessidade no mundo atual

Danilo de Araújo Moura

Resumo

Este artigo abordará a história da Criptografia e uma aplicação da Criptografia RSA, sigla correspondente às iniciais de seus autores, utilizando congruência, na educação básica, corroborando para difusão de conteúdos aplicados de tecnologia através de conceitos matemáticos, bem como favorecendo o debate sobre a segurança da informação, temáticas fundamentais no mundo atual.

Palavras-chave: Segurança da Informação, Contexto e Problemas da Educação Brasileira; Surgimento da Criptografia; Implantação dos Computadores; O sistema RSA; Metodologia para Desenvolvimento em Sala do Sistema RSA; Aplicação do Sistema RSA.

Abstract

Information Security, Context and Problems of Brazilian Education; Emergence of Cryptography; Computer Deployment; The RSA Method; RSA System Development Methodology; Application of the RSA System.

Keywords: Information Security, Context and Problems of Brazilian Education; Emergence of Cryptography; Computer Deployment; The RSA Method; RSA System Development Methodology; Application of the RSA System.

1. Introdução

Como forma de contextualizar os conceitos de criptografia e segurança da informação, irei, primeiramente, abordar o estado da arte, juntamente com os problemas enfrentados pela educação brasileira.

Atualmente, na era digital, há uma grande preocupação com a garantia da segurança das informações. No Brasil, por exemplo, a certificação digital iniciou-se com o surgimento da infraestrutura de Chaves Públicas, segundo a medida provisória 2.200-2/2001. O certificado digital é um arquivo em meio eletrônico, em que são encontradas informações do usuário (pessoa física ou jurídica) de um estipulado local, garantindo a respectiva identidade e assegurando, por conseguinte, os princípios de segurança da informação (confidencialidade, autenticidade, autoria e não repúdio), tendo como pressuposto as transações eletrônicas assinadas, bem como o intercâmbio de informações, preservando, assim, a integridade, o sigilo e a segurança. Logo, o arcabouço, para esse processo, deve-se ao usufruto da criptografia e padrões específicos.

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

No entanto, as medidas para salvaguardar os verdadeiros destinatários da informação não se restringem ao ambiente nacional. A comunidade internacional vive, constantemente, preocupada com a segurança de seus dados, e aqui podemos citar o episódio envolvendo o ex-administrador da CIA (Central Intelligence Agency) e ex-contratado da NSA (National Security Agency), Edward Joseph Snowden, que abalou o mundo, colocando em xeque os meios de segurança das diversas nações. Além disso, existiram escândalos sobre divulgações de informações particulares dos usuários da maior rede social do mundo, o Facebook, gerenciada por Mark Elliot Zuckerberg, deixando-nos os seguintes questionamentos: Até que ponto nossas informações estão protegidas? Podemos confiar nos meios cibernéticos? Será que devemos abandoná-los em definitivo? Existe um meio de melhorar a segurança cibernética?

Por outro lado, o acesso à internet banda larga de qualidade e irrestrito é uma oportunidade valiosa para uma nação, pois favorecerá o desenvolvimento tecnológico, o crescimento econômico, a diminuição das fronteiras, o ensino inovador e a escalada da produção, a título de exemplo. Além disso, a revista *Exame* de 4 de março de 2020, cuja capa é DEVS (Desenvolvedores de *software*) ratifica a importância do aprimoramento da tecnologia da informação, ressaltando o crescimento exponencial das Startups nas potências mundiais e no Brasil, além das projeções futuras, deixando evidente a importância da ciência de dados para o progresso das nações. O lado indigesto, essencialmente para o nosso país, deve-se à falta de profissionais qualificados nas áreas de tecnologia, ciência, engenharia e matemática. Brasileiros preparados nessas áreas, que desenvolvem *softwares*, são assediados por várias multinacionais e escolhem onde querem exercer suas atribuições bem como a remuneração que acham justas receber, conforme a reportagem. Tudo isso diante de um cenário de crescimento econômico pífio e, ainda, elevados índices de desempregos na República, ou seja, panorama oposto às estatísticas tristes vivenciadas pelo povo brasileiro.

Na perspectiva da singularidade – expressão utilizada no campo da Física para representar eventos extremos desprovidos de equações associadas, ou seja, trata-se de um campo além do previsível – trago a visão do engenheiro e futurista Ray Kwrzweil que considera que a singularidade ocorrerá nos próximos 30 anos. Na matéria publicada no *site* da UOL vestibulares, na parte de atualidade, intitulado: *Você sabe o que é Inteligência Artificial e Singularidade?*, Carolina Cunha retrata muito bem as projeções de Ray, sendo uma delas representada no seguinte trecho:

,

> *"... se imaginarmos o crescimento exponencial no século 21 como uma curva exponencial, ele será equivalente a 20 anos de progresso na velocidade atual"* (Ray Kwrzweil).

Em outro fragmento do artigo, é enaltecido o desenvolvimento tecnológico, como segue:

,

> *"...um computador de mil dólares tem hoje a mesma inteligência de um inseto. No futuro, ele se igualará à capacidade de um rato, de um homem e, finalmente, de toda a humanidade"* (Ray Kwrzweil).

Logo, certos autores, como Ray, vislumbram, em um futuro próximo, a inteligência artificial, em que as próprias máquinas desenvolverão outras mais funcionais sem influência humana.

Diante do retrato mundial, atual e futuro, assim como o exposto anteriormente, percebe-se a necessidade de um aprimoramento constante dos meios de segurança da informação, pois a tecnologia das coisas, da ciência de dados e a transparência digital são fundamentais no mundo competitivo e avançado, e negligenciá-los é naufragar no retrocesso, na desigualdade e no descaso com o futuro de toda uma sociedade. O Brasil, observando o cenário internacional e os relatos acadêmicos, implementou, como objetivo estratégico, o E-Digital – estratégia brasileira para a transformação digital, tendo como um dos temas a confiança no ambiente digital, consoante a imagem abaixo.

Figura 1: *Temas para Transformação Digital Brasileira* (E-Digital, 2018, p.9)

É relevante considerar, também, que um dos grandes problemas enfrentados pela educação nacional é a má formação e a baixa qualidade no ensino de disciplinas atreladas à tecnologia, tais quais ciência, engenharia e matemática, conforme p.19 e p.26 da revista *Exame*, edição 1204, de 4 de Março de 2020. O fato contribui para enormes dificuldades econômicas enfrentadas pelo Brasil ao longo dos anos, gerando grandes *deficits* de profissionais no crescente setor de tecnologia da informação. Ademais, a mesma reportagem da revista *Exame*, edição 1204, de 4 de Março de 2020, página 26, traz o resultado do Pisa e do Enade de 2019, como segue:

,

> *Em 2019, os resultados do Programa Internacional de Avaliação de Estudante (Pisa, na sigla em inglês) mostraram que dois terços dos alunos brasileiros de 15 anos sabiam menos do que o essencial em Matemática. Considerando também as áreas de*

> *leitura e ciência, apenas 2,5% dos estudantes atingiram notas de "alto desempenho" na prova. A média da Organização para Cooperação e Desenvolvimento Econômico (OCDE) é de 15,7%. Essa defasagem continua no ensino superior. Em 2018, apenas 1,7% dos cursos universitários conseguiu nota máxima no Exame Nacional dos Estudantes* (Revista *Exame*, 2020, p.26).

Portanto, observa-se a falta de políticas públicas de incentivo à educação básica, e os reflexos estão nos dados apresentados acima.

Em mais algumas investigações, podemos verificar que há uma lacuna de profissionais trabalhando nas áreas tecnológicas, segundo destaca a mesma reportagem, agora na página 19, no relato abaixo.

,

> *No país há, atualmente, apenas 2 milhões de trabalhadores graduados nas áreas de ciência, tecnologia, engenharia e matemática, o correspondente a 1,9% da força de trabalho, segundo dados da Organização para Cooperação e Desenvolvimento Econômico. De 2019 a 2024, de acordo com Cálculo do Brasscom, a demanda média deve ser de 70.000 profissionais por ano. No entanto, em 2017, de 46.000 profissionais formados, apenas 26.000 entraram no mercado de trabalho, evidenciando uma defasagem no currículo das instituições. Nesse ritmo, ao final do período de seis anos, o* deficit *chegaria a 264.000* (Revista *Exame*, 2020, p.19).

Figura 2: *Gráficos* (*Exame*, 2020, p.19)

Agora, após essa explanação do cenário vigente, temos, iniciando, de fato, o conteúdo, que a criptografia moderna edificou-se em torno dos anos 70 do século XX. Até aquele momento, a Teoria dos Números, da qual a Aritmética é o componente mais primário, era apontada como um dos ramos mais genuínos e abstratos da Matemática, desconectada de qualquer tipo de aplicação concreta. Essa visão modificou-se com o desenvolvimento da Teoria da Informação, que inclui a criptografia, dentre outros tópicos, entusiasmada pelo progresso e disseminação dos computadores e a capacidade de conexão com as grandes redes mundiais. Rotineiramente, a criptografia estava vinculada ao sigilo militar, no entanto foi o manuseio exorbitante dos computadores, pelo público, para assuntos variados, que mais atraiu a expansão da criptografia moderna.

A proposta de resguardar os meios de comunicação gerados por certa população advém do início da civilização, e o pensamento de tutelar os instrumentos de comunicação, bem como o conteúdo da mensagem, pelo método da cifração é, também, rudimentar.

,

> *A criptografia é o estudo de métodos para enviar e receber mensagens secretas. Em geral, há um emissor que tenta enviar uma mensagem para um receptor. Existe também um adversário que deseja interceptar a mensagem. O método utilizado será considerado bem-sucedido se o remetente for capaz de transmitir uma mensagem para o receptor sem que o adversário descubra em que ela consiste* (Stein, 2013, p. 49).

Em Roma, Júlio César utilizou uma criptografia singela para realizar a interlocução com o seu exército. Em sua cifra, na transmissão do conteúdo original, cada letra era lançada três posições à direita e o alfabeto restringia-se a ele mesmo. Ao longo dos tempos, a codificação das frases tornou-se uma atividade cada vez mais elaborada, e o surgimento dos computadores potencializou a comunicação entre as pessoas, bem como diminuiu as distâncias, porém, o meio cibernético não é tão seguro e, nesse contexto, a criptografia expande em importância para assegurar a cifração das informações.

,

> *Não ser decifrado por um adversário é um objetivo difícil. Nenhum código é completamente indecifrável. Se houver um livro de códigos impresso, o adversário poderá roubá-lo. Nem toda a sofisticação matemática pode impedir essa possibilidade já que um adversário pode ter grande poder de computação e recursos humanos dedicados a tentar decifrar um código* (Stein, 2013, p.49).

Um método criptográfico relevante chamado RSA, sigla correspondente às iniciais de seus autores, e bastante difundido no cenário atual, usufrui de conteúdos da Teoria dos Números, em especial congruência e números primos, para desenvolver todo um encadeamento lógico, com auxílio de chaves assimétricas, para proceder a uma significativa segurança na atividade de decifração.

Em razão do exposto, o artigo científico mostrará um pouco da história da criptografia e a utilização da congruência para o desenvolvimento da criptografia RSA, tendo em vista a aplicação de conceitos de Teoria dos Números na educação básica, estimulando, assim, os discentes na inserção do debate da segurança da informação. Ressalto, também, que os conceitos elementares de congruência são pré-requisitos para o bom entendimento do artigo, pois eles devem estar inseridos no currículo dos discentes da educação básica;e enalteço, por fim, a importância da matemática nessa perspectiva toda, sem deixar de influenciar a formação de novos profissionais de outras áreas atreladas às Ciências Exatas e à Tecnologia.

2. Surgimento da Criptografia

A origem da palavra criptografia vem do grego, em que *kriptos* significa oculto, e, assim, criptografia representa "escrita oculta". Há relato de que persas, gregos e chineses desfrutavam de inúmeras práticas para ocultar mensagens. O desenvolvimento criptográfico foi no intuito de não mais esconder fisicamente as mensagens, entretanto desfrutar de artimanhas para encobrir sua interpretação ao público que não correspondessem aos verdadeiros destinatários delas, de maneira que pudessem ser disponibilizadas por meio de um instrumento público de comunicação. É interessante observar que um método utilizado com frequência em Roma, por Júlio César, conhecido como cifra de César, foi fundamentado em ideias criptográficas.

,

> *A criptografia tradicional é conhecida como criptografia de chaves secretas. O remetente e o destinatário concordam com antecedência sobre um código secreto e, em seguida, enviam mensagens usando-o. Por exemplo, um dos mais antigos códigos é uma cifra de César* (Stein, 2013, p.50).

Tal sistema traduz-se em substituir cada letra do alfabeto, na mensagem primária, por outra letra do alfabeto, conforme uma regra bem estipulada. Esse dispositivo criptográfico é nomeado de cifra de substituição simples, no qual as letras de um alfabeto são trocadas por outras. A cifra de César detém ao menos 25 variantes. Um dos pontos vulneráveis nos sistemas criptográficos por substituição simples é o fato de, em um conteúdo (em relação a determinada língua), as letras do alfabeto aparecerem em períodos diversos, além de haver certas disposições rígidas de contato entre elas – conforme o idioma português, que apresenta, com muita intensidade, letras que se seguem após a utilização de outras, como a letra q seguida de u, fornecendo rastros úteis aos que se dedicam ao exercício da quebra dos códigos de outrem: os criptoanalistas. Um método para alterar a análise de frequência é relacionar a cada letra, com periodicidade alta, diversos símbolos diferentes, que estão associados só a essa letra. Ainda assim, o diagnóstico do contato entre letras e a estrutura linguística dá indícios sobre como desvendar um desses códigos. Por outro lado, existe outra linha de sistema criptográfico consubstanciada na transposição, isto é, na geração de anagramas da mensagem original. Por exemplo, um conteúdo com 15 letras origina 15! permutações dissemelhantes das letras, e para mensagem com um número elevado delas, a alta quantidade de permutações torna bastante complicada a tarefa de decifrar, na hipótese de não deter a chave para tal. A grande problemática do molde citado é que a mudança de chaves, entre os clientes do sistema, fica árdua na conjuntura de existirem muitos deles longe uns dos outros, pois demanda uma chave diferente para cada par de usuários. Percebeu-se, então, que a junção dos métodos de substituição de letras e transposição dava origem a sistemas criptográficos mais satisfatórios. O arquiteto italiano Leone Battista Alberti, considerado o pai da criptografia ocidental, sugeriu uma nuance bem mais elaborada da cifra de César, com a utilização da relação de substituição polialfabética. Referia-se ao usufruto de uma aparelhagem designada disco de Alberti, composta de dois discos de mesmo centro com diâmetros distintos, presos por um pino central, o menor sobre o maior, podendo o disco menor girar. Os discos eram fragmentados em 24 grupos similares em que, na borda do disco maior, estavam inscritos, no sentido horário, as seguintes 20 letras: A, B , C, D, E, F, G, I, L, M, N, O, P, Q, R, S, T, V, X, e Z. Além dos números 1, 2, 3 e 4, um em cada setor. Já na extremidade do disco menor, estavam inscritos, em ordem arbitrária, as letras minúsculas do alfabeto, à exceção das letras j ,u e w, além da palavra do latim *et.*

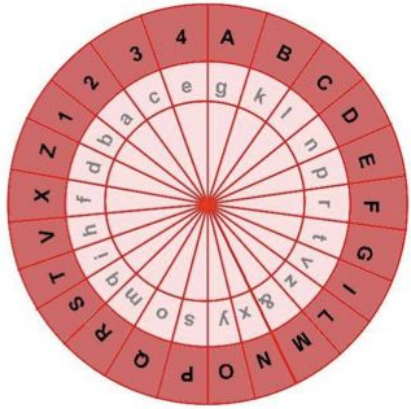


Figura 3: *Disco de Alberti*

,

> *A grande inovação de Alberti foi o uso de cifras polialfabeticas, como segue: a cada grupo de algumas palavras (quatro ou cinco), o pequeno disco é girado aleatoriamente e a nova letra do disco menor correspondente à letra A no disco maior é inserida na mensagem original, indicando que a partir daquele momento é essa a nova posição do disco rotativo (o menor), com relação ao disco fixo (o maior)* (Hefez, 2016, p. 268).

Johannes Trithemius contribuiu significativamente para o avanço da criptografia com a obra nomeada *Poligrafia*, publicado em 1518. No livro, ele descreve um novo método utilizando a *tabula recta*, dispondo de uma tabela, nomeada de *tabula recta*, com a igualdade de linha e colunas, observando que na primeira linha ficará o alfabeto em ordem convencional e, a partir das demais linhas, haverá uma permutação circular da linha anterior. Ele descreve o passa a passo no seguinte trecho:

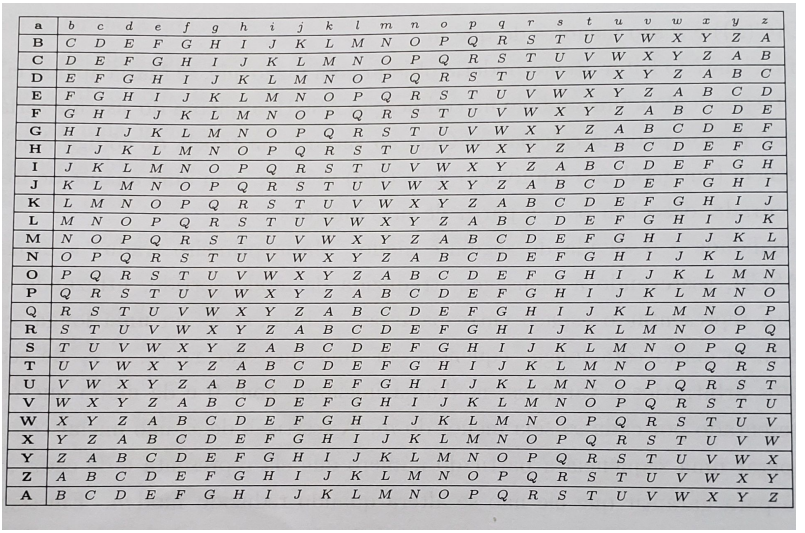
,

> *A cifragem procederia da seguinte forma: a primeira letra da mensagem a ser cifrada é transformada na letra correspondente da segunda linha, a segunda letra é transformada na letra correspondente da terceira linha e assim sucessivamente até esgotar todas as linhas quando se volta para a segunda linha novamente.* (Hefez, 2016, p.268 e p.269)

A tabela posterior, foi retirada do livro *Aritmética- Coleção Profmat- p.276* e retrata a *Tabula recta.*

Analisando a figura acima e seguindo os passos sugeridos na última citação temos, por exemplo, para a palavra:

CRIPTOGRAFIA,



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura 4: *Tabula recta*

a seguinte cifra:

DTLTYUNZJPTM.

Em 1553, com o trabalho do italiano Giovanni Battista Bellaso, divulgado no curto livro *La cifra del seig Giovan Batista Belaso*, foi adotado o pensamento de chave para cifrar e decifrar uma mensagem. O dispositivo faz uso da *tabula recta*, além de compartilhar uma chave, que pode ser uma palavra, um conjunto de letras ou uma frase. Tendo a chave, registra-se em uma linha o conteúdo a ser cifrado e, na linha acima, as letras da chave sobre as letras do texto, repetidas o quanto for necessário.

,

> *A cifragem de Giovanni Battista Belloso ocorre da seguinte forma: caso sobre uma dada letra do texto encontra uma determinada letra da palavra-chave, então substitui essa por aquela que lhe corresponde na sua coluna e na linha que começa com a letra da palavra-chave.* (Hefez, 2016, p.269)

Imagine, a título de exemplo, que a chave seja "Aritmética" e a mensagem enviada, através desse sistema, seja Teoria dos Números. Desta maneira, a cifragem aconteceria do seguinte modo:

aritme tic aaritme

teoria dos numeros

TVWKUE WWU NUDMKAW

Observe que, para cifrar e decifrar, de acordo com o método, recorre-se à mesma chave. O dispositivo foi considerado penoso de ser quebrado, porque era resistente à análise de frequência, visto que uma mesma letra pode ser exibida por diversas outras e existe um número enorme de chaves possíveis. Com a publicação do livro *Traicté des Chiffres*, em 1586, Blaise de Vigenère implementa um sistema baseado em Bellaso, que propõe o conceito de autochave, isto é, a utilização do texto em si como chave. A proposta institui-se de forma que os correspondentes compartilhavam uma chave comum, que era uma letra, e a utilizavam como chave no método de Bellaso para codificar a primeira letra do conteúdo. Posteriormente, essa letra inicial era constituída como chave para cifrar a segunda letra do conteúdo e assim sucessivamente.

Os métodos de cifragem não foram bastante praticados por serem muito desgastantes em suas construções e pelo fato de, observado um erro no processo, gerar uma mensagem praticamente perdida. Por isso, foram empregados, em seus lugares, os livros de códigos intitulados *nomenclators*, em que palavras eram cifradas em espécies de dicionários produzidos com esse efeito. A cifra de Bellaso foi quebrada por volta do século XIX, depois de um longo tempo dada como infalível.

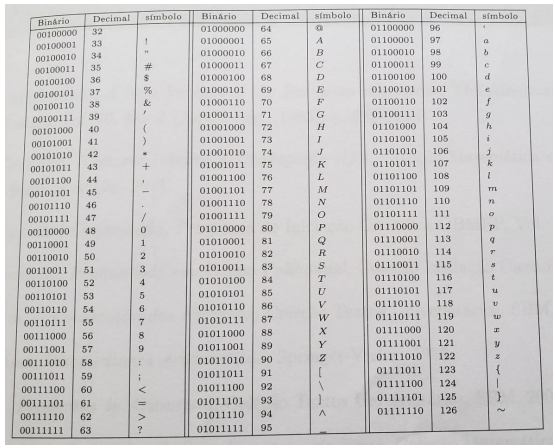
Uma característica relevante é que qualquer dispositivo criptográfico precisa de uma troca de chaves para que as partes possam decifrar as frases que lhes são enviadas e, além disso, deve fazer chegar ao destinatário, de forma segura, a chave da cifra.

Portanto, os métodos criptográficos comentados até aqui fazem uso da mesma chave para cifrar e decifrar um dado conteúdo, ou seja, operam-se com fundamentos nas chaves simétricas.

3. Implementação dos Computadores

Com a chegada dos computadores (PCs), ocorreria uma reviravolta na Teoria da Informação. A popularização dos PCs obrigou uma procura por padronização nos processos. Pelo fato de eles fazerem uso de códigos binários, toda estrutura deveria ser moldada nesse formato. Daí, surgiu o *American Standard Code for Information Inter Change* (ASCII) que significa código padrão americano para o intercâmbio de informação. Tal codificação, construída desde 1960, não representa um sistema de cifragem e sim a tradução para a linguagem binária dos símbolos mais representados. Assim, incorporou-se o código ASCII. Com isso, necessitava-se, agora, uniformizá-lo para o uso de sistemas criptográficos. Foi então que, em 1973, o National Bureau of Standards escolheu o sistema criptográfico Data Encryption Standard (DES), construído pela IBM, com o intuito de ser o sistema oficial americano. O DES era muito complexo e utilizava chaves simétricas, o que ensejava uma grande problemática logística de distribuição de chaves, levando ao surgimento de outros métodos.

A figura abaixo, anexa do livro de *Aritmética-Coleção Profmat-p.277*, mostra a Tabela de código ASCII.



Binário	Decimal	símbolo	Binário	Decimal	símbolo	Binário	Decimal	símbolo
00100000	32		01000000	64	@	01100000	96	`
00100001	33	!	01000001	65	A	01100001	97	a
00100010	34	"	01000010	66	B	01100010	98	b
00100011	35	#	01000011	67	C	01100011	99	c
00100100	36	$	01000100	68	D	01100100	100	d
00100101	37	%	01000101	69	E	01100101	101	e
00100110	38	&	01000110	70	F	01100110	102	f
00100111	39	'	01000111	71	G	01100111	103	g
00101000	40	(	01001000	72	H	01101000	104	h
00101001	41	)	01001001	73	I	01101001	105	i
00101010	42	*	01001010	74	J	01101010	106	j
00101011	43	+	01001011	75	K	01101011	107	k
00101100	44	,	01001100	76	L	01101100	108	l
00101101	45	−	01001101	77	M	01101101	109	m
00101110	46	.	01001110	78	N	01101110	110	n
00101111	47	/	01001111	79	O	01101111	111	o
00110000	48	0	01010000	80	P	01110000	112	p
00110001	49	1	01010001	81	Q	01110001	113	q
00110010	50	2	01010010	82	R	01110010	114	r
00110011	51	3	01010011	83	S	01110011	115	s
00110100	52	4	01010100	84	T	01110100	116	t
00110101	53	5	01010101	85	U	01110101	117	u
00110110	54	6	01010110	86	V	01110110	118	v
00110111	55	7	01010111	87	W	01110111	119	w
00111000	56	8	01011000	88	X	01111000	120	x
00111001	57	9	01011001	89	Y	01111001	121	y
00111010	58	:	01011010	90	Z	01111010	122	z
00111011	59	;	01011011	91	[	01111011	123	{
00111100	60	<	01011100	92	\	01111100	124	|
00111101	61	=	01011101	93	]	01111101	125	}
00111110	62	>	01011110	94	^	01111110	126	~
00111111	63	?	01011111	95	_			

Figura 5: *Tabela de Código ASCII*

Observação: A tabela de código ASCII é apenas uma exemplificação, usada somente para ilustrar. Ela não foi utilizada ao longo do artigo para fazer codificações, portanto, os símbolos e números constantes no artigo não estão associados a ela.

Retomando, temos que o desafio, portanto, voltava-se a desvendar um modo lógico de troca de chaves entre correspondentes e combater o paradigma da impossibilidade da troca de senhas sem a intermediação de um portador. Whitfield Driffie, Martin Hellman e Ralph Merkle utilizaram uma ideia brilhante, baseada na Teoria dos Números, para desmistificar o paradigma. Eles fizeram uso de conceitos de congruência para tentar solucionar o imbróglio da distribuição de chaves. O pensamento dos americanos dá-se da seguinte forma: Pedro e Camila querem trocar entre si uma chave secreta através de uma comunicação não segura. Eles chegam ao consenso sobre um par de números s e t e os tornam públicos. Pedro escolhe um novo número natural c e o mantém em segredo. Com ele, calcula o único número $z < t$ tal que $s^c \equiv z \bmod t$, e o envia para Camila. Por sua vez, Camila indica um número natural h, mantendo-o secreto, e, com ele, calcula o único número $f < t$ tal que $s^h \equiv f \bmod t$; e posteriormente o envia para Pedro.

Daí, Pedro calcula f^c, obtendo:

$$f^c \equiv (s^h)^c \equiv s^{hc} \equiv k \bmod t \text{ , com } k < t.$$

Depois, Maria calcula z^h, extraindo:

$$z^h \equiv (s^c)^h \equiv s^{ch} \equiv k \bmod t \text{ , com } k < t.$$

Concluído! Está trocada a chave secreta k entre Pedro e Camila. Então, são públicas as informações s, t, z, f e são secretas as informações c, que só Pedro conhece, h, que somente Camila sabe, e k, que apenas Pedro e Camila têm.

Vamos mostrar uma aplicação, ou seja, um exemplo para tornar mais didática a ideia em sala de aula. Suponha que Pedro e Camila tenham escolhido de comum acordo $s = 14$ e $t = 151$. Por sua vez, Pedro elege $c = 3$ como sua chave secreta, enquanto Camila escolhe $h = 5$. Fazendo a análise para saber qual a chave k que eles compartilham, obtêm-se:

1. 1 - Pedro elabora a seguinte conta para determinar z e enviá-lo à Camila:

$$s^c \equiv z \bmod t \Rightarrow 14^3 = 14^2 \cdot 14 = 196 \cdot 14 \equiv 45 \cdot 14 = 630 \equiv 26 \bmod 151.$$

Então, z = 26.

Agora, Camila faz o seguinte cálculo para encontrar f e encaminhá-lo a Pedro:

$s^h \equiv f \bmod t \Rightarrow 14^5 = 14^2 \cdot 14^2 \cdot 14 = 196 \cdot 196 \cdot 14 \equiv 45 \cdot 45 \cdot 14 = 630 \cdot 45 \equiv 26 \cdot 45 = 1170 \equiv 113 \bmod 151$.

Para determinar a chave k, Pedro tem que reduzir $f^c = 113^3$ módulo 151.

Daí, $113^2 \cdot 113 = 12769 \cdot 113 \equiv 85 \cdot 113 = 9605 \equiv 92 \bmod 151$. Pedro encontra, por conseguinte, k = 92.

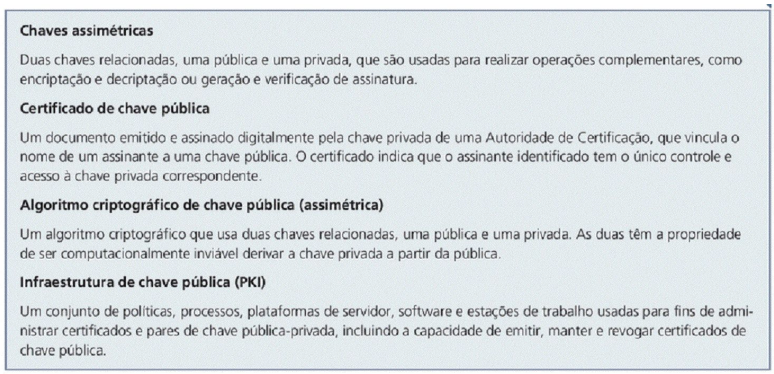
2. 2- Para Maria, tem-se:

$z^h = 26^5$ módulo 151. Porém, $26^5 = 26^2 \cdot 26^2 \cdot 26 = 676 \cdot 676 \cdot 26 \equiv 72 \cdot 72 \cdot 26 = 5184 \cdot 26 \equiv 50 \cdot 26 = 1300 \equiv 92 \bmod 151$. Logo, k = 92, como queríamos mostrar.

O êxito desse método consiste na dificuldade de desvendar qualquer dos três números c, h e k, sabendo somente os dados públicos s, t, z e f. Naturalmente, dado $x \in N$, é de certa forma trivial calcular o resto da divisão de s^x por t, no entanto não é fácil o caminho oposto, ou seja, dado $y \in N$, é trabalhoso achar $x \in N$ de tal forma que y é o resto da divisão de s^x por t. Os restos da divisão de s^x por t, ao variar x, estabelecem-se de maneira caótica. Essa ferramenta tem o defeito de trocar chaves entre dois indivíduos por vez, e, portanto, não é satisfatória no mundo global.

Driffie teve o pensamento de utilizar chaves assimétricas, isto é, cada pessoa teria duas chaves: uma pública, para codificar a mensagem e, outra privada, para decodificá-la. O sistema deveria ser fácil para cifrar e praticamente impossível, sem o uso da chave secreta, para decodificar. Ele somente publicou a teoria e não fez nada na prática.

O quadro abaixo foi extraído do livro *Criptografia e Segurança de Redes: Princípios e Práticas, p.200,* e faz alusão aos aspectos da criptografia assimétrica.



Chaves assimétricas

Duas chaves relacionadas, uma pública e uma privada, que são usadas para realizar operações complementares, como encriptação e decriptação ou geração e verificação de assinatura.

Certificado de chave pública

Um documento emitido e assinado digitalmente pela chave privada de uma Autoridade de Certificação, que vincula o nome de um assinante a uma chave pública. O certificado indica que o assinante identificado tem o único controle e acesso à chave privada correspondente.

Algoritmo criptográfico de chave pública (assimétrica)

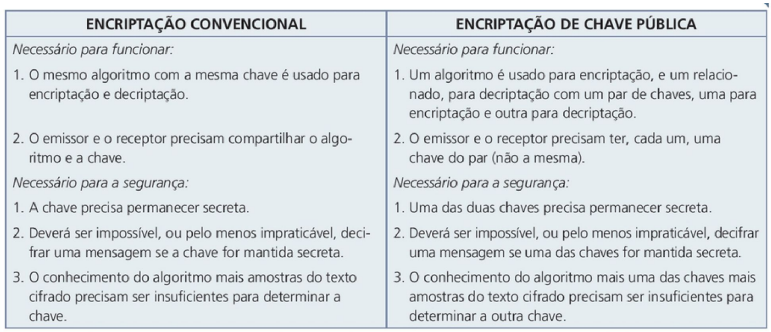
Um algoritmo criptográfico que usa duas chaves relacionadas, uma pública e uma privada. As duas têm a propriedade de ser computacionalmente inviável derivar a chave privada a partir da pública.

Infraestrutura de chave pública (PKI)

Um conjunto de políticas, processos, plataformas de servidor, software e estações de trabalho usadas para fins de administrar certificados e pares de chave pública-privada, incluindo a capacidade de emitir, manter e revogar certificados de chave pública.

Figura 6: *Terminologia relacionada à criptografia assimétrica*

Já o resumo seguinte, por fim, elucida as principais divergências entre a encriptação simétrica (convencional) e a de chaves públicas. A imagem foi tirada, também, do livro *Criptografia e Segurança de Redes: Princípios e Práticas, p.203.*



ENCRIPTAÇÃO CONVENCIONAL	ENCRIPTAÇÃO DE CHAVE PÚBLICA
Necessário para funcionar:	*Necessário para funcionar:*
1. O mesmo algoritmo com a mesma chave é usado para encriptação e decriptação.	1. Um algoritmo é usado para encriptação, e um relacionado, para decriptação com um par de chaves, uma para encriptação e outra para decriptação.
2. O emissor e o receptor precisam compartilhar o algoritmo e a chave.	2. O emissor e o receptor precisam ter, cada um, uma chave do par (não a mesma).
Necessário para a segurança:	*Necessário para a segurança:*
1. A chave precisa permanecer secreta.	1. Uma das duas chaves precisa permanecer secreta.
2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se a chave for mantida secreta.	2. Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem se uma das chaves for mantida secreta.
3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

Figura 7: *Encriptação convencional e de chave pública*

4. O Sistema RSA

Ronald Rivest, Adi Shamir e Leonard Adlman deram, em 1978, um importante progresso no sistema criptográfico idealizado por Driffie. O propósito foi fundamentado na aparente facilidade de encontrar números primos grandes e, simultaneamente, na extrema dificuldade concreta em fatorar o produto de dois desses números, além do uso de fundamentos elementares da Teoria dos Números, conforme a variante do Teorema de Euler ilustrado no Corolário 1.

,

> *Diffie e Hellman apresentaram publicamente os conceitos da criptografia de chaves públicas em 1976. Hellman dá créditos a Merkle com a descoberta independente e simultânea do conceito, embora Merkle não o tenha publicado antes de 1978 [6]. De fato, o primeiro documento não confidencial descrevendo a distribuição de chaves públicas e a criptografia foi uma proposta de projeto de 1974 por Merkle http://merkle.com/1974. Esse, porém, não foi o verdadeiro início. O almirante Bobby Inman, como diretor da National Security Agency (NSA), reivindicou que a criptografia de chave pública tinha sido descoberta na NSA em meados da década de 1960 [8] . A primeira apresentação documentada desses conceitos veio em 1970, do Communucations-Electrons Security Group, o equivalente britânico da NSA, em um relatório confidencial de James Ellis [3]. Ellis referia-se à técnica como criptografia não secreta, e descreve a descoberta em [2]* (Stalling, 2015, p.201).

,

> *O artigo pioneiro de Diffie e Hellaman [1] introduziu uma nova técnica para criptografia e, com efeito, desafiou os criptologistas a encontrarem um algoritmo criptográfico que atendesse os requisitos para os sistemas de chave pública. Diversos algoritmos foram propostos. Alguns deles, embora inicialmente promissores, provaram ser falhos* (Stalling, 2015, p.207).

,

> *Uma das primeiras respostas ao desafio foi desenvolvido em 1977 por Ron Rivest, Adi Shamir e Len Adleman, no MIT, e publicado em 1978 [7]. O esquema Rivest-Shamir-Adleman (RSA), desde essa época, tem reinado soberano como a técnica de uso geral mais aceita e implementada para a encriptação de chaves públicas* (Stalling, 2015, p.207).

Com isso, procurava-se um sistema criptográfico com duas chaves, uma pública e uma privada, para que qualquer pessoa pudesse codificar um conteúdo previamente cifrado em ASCII e somente o seu autêntico destinatário pudesse decifrá-lo.

A proposta, nesse caso, foi construída assumindo, por exemplo, que Pedro quer criar um sistema criptográfico em que uma pessoa encaminhe para ele uma frase cifrada, com uma chave pública, e que ele, e só ele, possa decodificá-la com sua chave secreta.

Então, Pedro escolhe dois números primos p e q muito grandes e, posteriormente, efetua o seu produto, ou seja, $n = p \cdot q$.

Observação: Perceba que é tranquilo encontrar o algarismo n, mas é muito difícil, e computacionalmente duradouro fatorá-lo. Essa é a razão positiva da técnica, ou seja, um processo fácil de realizar, todavia árduo de desfazer.

Continuando o processo, Pedro escolhe uma dupla de números λ e d de modo que:

$$\lambda \cdot d \equiv 1 \bmod \phi(n),$$

onde $\phi(n) = p^{\alpha_1 - 1} \cdot q^{\alpha_2 - 1} \cdot (p-1) \cdot (q-1)$ é um caso particular da função ϕ de Euler. Além disso, como α_1 e α_2 são iguais a 1, pois $n = p \cdot q$, temos que $\phi(n) = (p-1) \cdot (q-1)$.

Observação: É fundamental que λ e $\phi(n)$ e d e $\phi(n)$ sejam coprimos. Para isso, podemos tomar λ tal que $(\lambda, \phi(n)) = 1$ e em seguida determinar a congruência $\lambda \cdot X \equiv 1 \bmod \phi(n)$.

Com isso, Pedro, enfim, disponibiliza os números n e d, ou seja, as chaves públicas, e guarda, consigo, as chaves secretas que são os primos p, q e os números $\phi(n) = (p-1) \cdot (q-1)$ e λ.

Assim, fornecendo-se um valor $b < n$, tal que ele possa ser a representação decimal[1] de um símbolo ASCII, visto conforme um número na base 2, a codificação feita por uma pessoa qualquer, que tenha a chave pública de Pedro (n, d), pode cifrar b, como segue, por exemplo, segundo os passos realizados por Camila.

Ela acha o único $A(b) < n$ tal que:

$$b^d \equiv A(b) \bmod n.$$

Com isso, ela manda A(b) para Pedro.

Pedro, ao receber A(b), utiliza sua chave privada λ para achar $E(A(b)) < n$ de tal forma que:

$$A(b)^\lambda \equiv E(A(b)) \bmod n.$$

Observe que só Pedro pode achar E(A(b)), porque ele é o único que tem a chave λ. No entanto, $E(A(b)) = b$, devido à existência de $r \in N$ tal que $\lambda.d = 1 + r.\phi(n)$. Agora analisando o corolário 1 abaixo, temos:

Corolário 1. *Seja* n *um número inteiro livre de quadrados, então para todo* $b \in Z$ *e todo* $r \in N$, *tem-se que:*

$$b^{r\phi(n)+1} \equiv b \ mod \ n$$

Demonstração. Tomando $n = p_1 \cdot p_2 \cdots p_k$, em que $p_1, p_2, \cdots, p_k$ são números primos diferentes, segue que a função ϕ de Euler, será da forma:

$$\phi(n) = \phi(p_1) \cdots \phi(p_k).$$

Com isso, fazendo $r_i = r \cdot (p_1 - 1) \cdots (p_{i-1} - 1) \cdot (p_{i+1} - 1) \cdots (p_k - 1)$ e sabendo que $8b \in Z$, $8r \in N$ e $8i = 1, \cdots, k$, segue que:

[1] Na realidade, para construção dos cálculos computacionais, não é preciso desfrutar da base 10, tudo pode ser realizado no sistema de numeração convencional da máquina

$$b^{r\cdot\phi(n)+1} = b^{r_i\cdot(p_i-1)+1} \equiv b \bmod p_i.$$

Daí, como $a \equiv b \bmod n_i, \forall i = 1, \cdots, k \Leftrightarrow a \equiv b \bmod [n_1, \cdots, n_k]$, com $a, b \in Z$ e $n, n_1, \cdots, n_k$ inteiros maiores do que 1, além de $[p_1 \cdots p_k] = p_1 \cdots p_k = n$, então obtemos o que queríamos mostrar.

□

Assim, pelo corolário anterior, segue que:

$$E(A(b)) \equiv A(b)^{\lambda} \equiv (b^{d})^{\lambda} = b^{d\lambda} = b^{r\phi(n)+1} \equiv b \bmod n,$$

onde $E(A(b))$ e b são menores do que n.

Podemos questionar que, caso Camila só cifrasse cada algarismo relacionado a um símbolo na codificação ASCII, a quebra do sistema seria rápida, pois qualquer cidadão calcularia os $A(b)$ ao variar b na tabela de códigos ASCII, e com a correlação (nem sempre biunívoca) $b \longrightarrow A(b)$ poderia, com um estudo de frequência na frase cifrada, desvendar os b através de suas imagens $A(b)$. Essa fraqueza, entretanto, é solucionada como segue:

De início, Camila traduz o conteúdo para o código ASCII, relatando a mensagem traduzida de maneira corrida, associando a sequência 0100000 para esboçar o espaço entre palavras. Logra-se, portanto, uma grande sequência de 0 e 1. Divide-se essa imensa sequência em uma sucessão $b_1, b_2, ..., b_k$ de sequências de comprimento arbitrário e diferentes, sem começar com 0 e de forma que os algarismos na base 2, associados por cada b_i seja menor que n.

,

> *A restrição de* b_i *não iniciar com zero é para poder recuperar uma sequência a partir do número que ela representa; e de cada* b_i *ser menor do que* n *é para garantir que ele não se altere quando reduzido mod* n. (Hefez, 2016, p.275)

No próximo passo, Camila acha os valores de $A(b_1), A(b_2), A(b_3), \cdots, A(b_k)$ e os encaminha para Pedro. Logo, Pedro determina $E(A(b_1)) = b_1, E(A(b_2)) = b_2, \cdots, E(A(b_k)) = b_k$ e os dispõe de modo corrido. Posteriormente, fraciona o texto em conjuntos de sete dígitos e os transmuta de ASCII para siglas comuns, e surgirá o texto que Camila propunha para Pedro.

5. Metodologia para Desenvolvimento em Sala do Sistema RSA

Sabendo da importância do desenvolvimento metodológico no intuito de qualificar o ensino no ambiente escolar, trago, resumidamente, uma estrutura distribuída em 5 etapas, para o desenvolvimento do método RSA. Tal instrumento foi baseado no portal do saber, ou seja, na perspectiva do professor Teixeira de Souza. Portanto, devemos seguir as seguintes etapas:

1. Escolha dois números primos p e q;
2. Ache a chave de codificação $n = p \cdot q$;
3. Utilize para codificar a regra $b^{\lambda} \equiv a \bmod n$, tais que $(b, n) = (a, n) = 1$ e que b e a sejam menores que n;

4. Faça a seguinte operação $\lambda \cdot d \equiv 1 \cdot \mod (p-1)\cdot(q-1)$ para encontrar d;

5. Utilize, por fim, para decodificar a regra $a^d \equiv b \bmod n$.

Observação(*): Nos variados exercícios, podemos desfrutar sempre de $\lambda = 3$, recorrendo aos primos p e q da forma:

$$p \equiv 5 \bmod 6$$

$$q \equiv 5 \bmod 6$$

Demonstração. Escolha p e q de forma que:

$$p \equiv 5 \bmod 6 \text{ e } q \equiv 5 \bmod 6,$$

podemos reescrevê-los de tal modo:

$$p \equiv 5 \bmod 6 \equiv p - 1 \equiv 4 \bmod 6$$

$$q \equiv 5 \bmod 6 \equiv q - 1 \equiv 4 \bmod 6.$$

Agora, fazendo o produto $p \cdot q$, que é o relevante, tem-se:

$(p-1)\cdot(q-1) \equiv 16 \equiv 4 \bmod 6$ e, pela divisão euclidiana, sabemos que existe um $w \in Z$, tal que:

$$(p-1)\cdot(q-1) = 6\cdot w + 4 = 6\cdot w + 3 + 1 = 3\cdot(2\cdot w + 1) + 1.$$

Daí, surge uma nova congruência com o formato:

$$3\cdot(2\cdot w + 1) \equiv -1 \cdot \bmod (p-1)\cdot(q-1) \Leftrightarrow 3\cdot(2\cdot w + 1) \equiv -1 \cdot \bmod (6\cdot w + 4).$$

Em seguida, multiplique ambos os lados da congruência por –1, encontrando:

$$3\cdot(-2w - 1) \equiv 1 \bmod (6\cdot w + 4).$$

Somando $6\cdot w + 4$ a ambos os lados da última equivalência, obtemos:

$$3(4w + 3) \equiv 1 \bmod (6w + 4).$$

Enfim, o resultado assegura que o inverso existe e, além disso, fornece um algoritmo para os cálculos; para tanto, basta tomar $\lambda = 3$, $d = 4w + 3$, $(p-1)\cdot(q-1) = 6w + 4$, $p \equiv 5 \bmod 6$ e $q \equiv 5 \bmod 6$.

□

6. Aplicação do Sistema RSA

Assumindo todo o arcabouço teórico evidenciado na seção anterior, vamos elencar um exemplo da aplicação do sistema RSA com o intuito de motivar a introdução do conteúdo, já na educação básica, contribuindo para o enriquecimento formal do discente bem como a sua inserção nas discussões de temas envolvendo segurança da informação, mostrando que a matemática está presente nessa abordagem que é fundamental para a sociedade moderna. Assim, iremos codificar a sigla **"UFG"**, fazendo uso de números primos pequenos para diminuir as contas, pensando na abordagem apresentada em sala de aula. Com isso, faremos uso dos seguintes números primos: p = 5 e q = 17. Além disso, utilizaremos a tabela de conversão abaixo.

A	B	C	D	E	F	G	H	I	J
11	12	18	19	14	21	23	24	26	27
K	L	M	N	O	P	Q	R	S	T
28	29	16	31	32	47	49	36	37	38
U	V	W	X	Y	Z				
39	51	41	42	43	44				

Tabela 1: Tabela de Conversão

Primeiramente, para solução do exercício, perceba que:

p = 5 deixa resto 5 na divisão por 6 e q = 17, também, deixa resto 5 na divisão por 6. Ou seja, $p \equiv 5 \bmod 6$ e $q \equiv 5 \bmod 6$, conforme a observação (*). Então vamos utilizar $\lambda = 3$.

Com isso, para codificar a mensagem, transforme suas letras em números, de acordo com a tabela de conversão acima. Daí, U = 39, F = 21 e G = 23. Ou seja:

39- 21- 23.

Em seguida, calculando a chave de codificação n, temos:

$$n = p \cdot q = 5 \cdot 17 = 85.$$

Aplique, agora, a relação $b^{\lambda} \equiv a \bmod n$. Assim, obtemos:

Para a 1ª letra, ou seja, $U = b_1 = 39$, $\lambda = 3$ e $n = 85$, segue que:

$39^3 = 39^2 \cdot 39 = 1521 \cdot 39 \equiv 76 \cdot 39 = 2964 \equiv 74 \bmod 85$.

Logo, $a_1 = 74$.

Para a 2ª letra, ou seja, $F = b_2 = 21$, $\lambda = 3$ e $n = 85$, segue que:

$21^3 = 21^2 \cdot 21 = 441 \cdot 21 \equiv 16 \cdot 21 = 336 \equiv 81 \bmod 85$.

Logo, $a_2 = 81$.

E, por fim, para a 3ª letra, isto é, $G = b_3 = 23$, $\lambda = 3$ e $n = 85$, segue que:

$23^3 = 23^2 \cdot 23 = 529 \cdot 23 \equiv 19 \cdot 23 = 437 \equiv 12 \bmod 85$.

Logo, $a_3 = 12$.

Encontramos, por conseguinte, o bloco codificado. Isto é:

74- 81 - 12

Para decodificá-lo, primeiramente, ache o valor de d através da congruência:

$$\lambda \cdot d \equiv 1 \bmod (p-1)\cdot(q-1).$$

Procedendo, temos:

$$3 \cdot d \equiv 1 \bmod (5-1)\cdot(17-1)$$

$$3 \cdot d \equiv 1 \bmod 4 \cdot 16$$

$$3 \cdot d \equiv 1 \bmod 64$$

Logo, d = 43.

Com d em mãos, recorra à relação:

$$a^d \equiv b \bmod n,$$

e substitua em "a" os valores 74, 81 e 12 para encontrar os b respectivos e, com isso, volte na tabela de conversão para verificar a sigla original.

Operando, encontramos:

Para $a_1 = 74$, verifica-se que:

$$\begin{aligned} 74^{43} &\equiv [(-11)^6]^7 \cdot (-11) \equiv [1771561]^7 \cdot (-11) \equiv [76]^7 \cdot (-11) \equiv \\ &\equiv [(-9)^2]^3 \cdot (-11) \cdot (-9) = [81]^3 \cdot (-11) \cdot (-9) \equiv [-4]^3 \cdot (-11) \cdot (-9) \equiv \\ &\equiv (21) \cdot (-11) \cdot (-9) = (-231) \cdot (-9) \equiv 24 \cdot (-9) = -216 \equiv 39 \bmod 85. \end{aligned}$$

Então, $b_1 = 39$, que corresponde à letra U, conforme a tabela de conversão.

Prosseguindo, para $a_2 = 81$, verifica-se que:

$$\begin{aligned} 81^{43} &\equiv [(-4)^6]^7 \cdot (-4) = (4096)^7 \cdot (-4) \equiv (16)^7 \cdot (-4) = \\ &= [(16)^2]^3 \cdot (16) \cdot (-4) = (256)^3 \cdot (16).(-4) \equiv \\ &\equiv (1)^3 \cdot (16) \cdot (-4) = -64 \equiv 21 \bmod 85. \end{aligned}$$

Logo, $b_2 = 21$, que corresponde à letra F na tabela de conversão.

E, por fim, para $a_3 = 12$, temos:

$$\begin{aligned} 12^{43} &= [(12)^6]^7 \cdot (12) = [(12)^4]^7 \cdot [(12)^2]^7 \cdot (12) = \\ &= (20736)^7 \cdot (144)^7 \cdot (12) \equiv (81)^7 \cdot [(59)^2]^3 \cdot (59) \cdot (12) \equiv \\ &\equiv (-4)^7 \cdot (3481)^3 \cdot (59) \cdot (12) \equiv (-16384) \cdot (81)^3 \cdot (708) \equiv \\ &\equiv (-64) \cdot (-4)^3 \cdot (28) = (-64) \cdot (-64) \cdot (28) = (4096) \cdot (28) \equiv \\ &\equiv (16) \cdot (28) = 448 \equiv 23 \bmod 85. \end{aligned}$$

Portanto, $b_3 = 23$, que corresponde à letra G na tabela.

Por essa razão, o bloco decodificado fica com o formato:

39 - 21 - 23,

que se refere à mensagem original:

U F G,

como queríamos encontrar.

7. Resultados Principais

O dispositivo RSA é muito inteligente, contudo há a necessidade do usufruto do computador para realizar as operações mais elaboradas. Precisa, também, de números primos bastante grandes e dispor de uma escolha cuidadosa das chaves do sistema. Por isso, o ensino de conteúdos de Teoria dos Números é fundamental, não só na graduação, mas também na educação básica, pois o ingresso na academia ainda é restrito em nosso país e são poucos os calouros que, de fato, terão acesso a tal conhecimento, visto que grande parte deles não cursarão ciências exatas e suas tecnologias. Além do mais, o estudo de criptografia corroborará a introdução de conceitos de segurança da informação, pois, sem dúvida, eles terão amplo acesso aos diversos meios digitais, tais como: *e-mail*, redes sociais, aplicativos e bancos digitais. Por fim, os resultados enaltecem a relevância da Teoria dos Números e a percepção de quão fundamental é a segurança da informação para a economia em larga escala, para a qualidade de vida e, principalmente, no cenário atual, para a grande demanda de ambientes voltados à realização de *home office* com fidúcia, devido, em especial, à pandemia do Coronavírus (Covid-19) e outras doenças que podem surgir ao longo da história da humanidade, prejudicando os trabalhos ⌈in loco.

8. Conclusão

O que se observa é que a cifragem surgiu da necessidade em fornecer dados apenas para cidadãos específicos. Na guerra, por exemplo, uma mensagem sigilosa resgatada pode gerar consequências terríveis e, portanto, os povos embarcaram no exercício de criar ferramentas para codificar suas comunicações. Uma das primeiras foi a de César, que desfrutou do próprio alfabeto para codificar conteúdos, no entanto o dispositivo não logrou êxito, pois os criptoanalistas identificaram, com certa facilidade, desfrutando da análise de frequências, as propostas encaminhadas. Posteriormente, foram produzidos sistemas baseados na tabela recta, em números e em chaves simétricas, disposta, somente, aos que se entretinham no eixo de comunicação. Esse sistema também não funcionou, porque a quebra continuava acontecendo. A incorporação dos computadores deu origem ao Sistema de Informação e veio com ele a necessidade de gerar métodos mais eficazes para garantir a confidencialidade das informações. Essa necessidade partiu do fato de que se percebeu que a internet não é um meio seguro, e criptografar era essencial no processo de salvaguardar as informações. Através das ideias de Driffie, os estudiosos Rivest, Shamir e Adlman propuseram o sistema criptográfico RSA. Foi, então, que observaram a relevância da Teoria dos Números, algo, até aquele momento, abstrato e desprovido de aplicação concreta. Conceberam, agora, um sistema robusto que faz uso de números primos enormes, chaves assimétricas e congruência. O mais engenhoso é que se trata de uma operação simples de se realizar, todavia quase impossível de desfazer. Assim, o artigo elucida o sistema criptográfico RSA, que se embasa na Aritmética Modular, ramo da Teoria dos Números de relevância ímpar, tendo em vista a difusão de conteúdos aplicados de tecnologia e o debate da segurança da informação no ambiente escolar pelo docente.

Referências

[1] Diffie, W. e Hellman,M. *Multiuser Cryptographic Techniques*, IEEE Transaction on Information Theory, 1976.

[2] Ellis, J. *The History of Non-secret Encryption* , Cryptologia, 1999.

[3] Ellis, J. *The Possibility of Secure Non-Secret Digital Encryption* , CESG Repart, 1970.

[4] Hefez, A. *Aritmética*, Sociedade Brasileira de Matemática, 2016.

[5] Quaresma, P. *Criptografia*, Artigo, Disponível em: <https://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/artigo-gazeta08.pdf>. Acesso em: 17 de março de 2020.

[6] Merkle, R. *Secure Communucation Over an Insecure Channel* , Communications of the ACM, 1978.

[7] Rivest, R.; Shamir,A. e Adleman,L. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM, 1978.

[8] Simmons, G. *Cryptology* , Encyclopaedia Britannica, Fifteenth Edition, 1993.

[9] Sousa, F.H.Teixeira de, *Programa de Iniciação Científica da Obmep*, Aritmética, Aula 68, Observações prática, Disponível em: <https://www.youtube.com/watch?v=v1BTf1UlJHw>, Acesso em: 17 de fevereiro de 2020.

[10] Stalling, William *Criptografia e Segurança de Redes: Princípios e Práticas*, Pearson Education do Brasil, 2015.

[11] Stein,Clifford; L.Drysdale,Robert; Bogart,Kenneth *Matemática Discreta para Ciência da Computação*, Pearson Education, 2013.

Danilo de Araújo Moura
Secretaria de Estado de Justiça e Cidadania
Distrito Federal
<daniloaraujo543@gmail.com>

Recebido: 23/04/2020
Publicado: 23/12/2020

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.8, n.5, 2020
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2020/pmo846

Matemática Financeira: uma proposta de abordagem para o Ensino Médio por meio do tesouro direto

Luiz Eduardo da Silva Gomes

Resumo

Neste artigo propomos uma abordagem de ensino de Matemática Financeira para o Ensino Médio, mediante apresentação de atividades que relacionam problemas envolvendo simulações de investimentos no tesouro direto, ver <https://www.tesourodireto.com.br/simulador/>, e alguns conceitos matemáticos aplicados a esse investimento. Essa abordagem visa aproximar tais conceitos à vida cotidiana dos discentes e, além disso, atende as competências e habilidades da área de Matemática e suas tecnologias que estão inseridas na Base Nacional Comum Curricular, quando estabeleceu que "no Ensino Médio o foco é a construção de uma visão integrada da Matemática, aplicada à realidade, em diferentes contextos", ver [9, p.528]. Concluímos esse artigo apresentando as atividades, e suas respectivas resoluções, usando o tesouro direto.

Palavras-chave: Matemática Financeira; Proposta didática; Tesouro direto; Ensino Médio; BNCC.

Abstract

In this article we propose an approach to teaching Financial Mathematics for High School, by presenting activities that relate problems involving investment simulations in the direct treasury, see <https://www.tesourodireto.com.br/simulador/>, and some mathematical concepts applied to this investment. This approach aims to bring such concepts closer to the students' daily lives and, in addition, meets the competencies and skills of the area of Mathematics and its technologies that are inserted in the Common National Curricular Base, when it established that "in High School the focus is on the construction of an integrated view of Mathematics, applied to reality, in different contexts", see [9, p.528]. We conclude this article by presenting the activities, and their respective resolutions, using the direct treasure.

Keywords: Financial math; Didactic proposal; Direct treasure; High school; BNCC.

1. Introdução

A Matemática, reconhecidamente, possui grande importância e aplicabilidade em diversas áreas do conhecimento. Todavia, essa importância e aplicabilidade precisam ser claras também para os estudantes. Qual professor do ensino básico nunca ouviu perguntas do tipo: "Onde vou utilizar esse assunto em minha vida?" ou "Por que precisamos estudar esse assunto?". De fato, não há sentido nem ânimo em se dedicar horas e horas para aprender conceitos que não parecem ter muita utilidade. Fundamentado em nossa experiência em sala de aula, entendemos que quando tal

SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

conteúdo é apresentado evidenciando sua aplicabilidade no cotidiano dos alunos, mais engajados eles estarão para o aprendizado.

Dessa forma, visando dar aos alunos uma maior relevância à área de Matemática, é necessário debruçarmo-nos sobre como abordar determinados conhecimentos de tal forma que o conteúdo faça sentido para eles, desperte o interesse em aprendê-lo, e provoque o reconhecimento e a importância do tema tratado. Isso, certamente, acarretaria o desenvolvimento das competências e habilidades específicas de Matemática na etapa do Ensino Médio descritas na Base Nacional Comum Curricular (BNCC), ver [9]. É importante destacar que a BNCC é um documento que define as aprendizagens essenciais que deverão ser trabalhadas na Educação Básica pelas escolas brasileiras, sejam elas públicas ou privadas. Ela estabelece conhecimentos, competências e habilidades que se espera que todos os estudantes desenvolvam ao longo da escolaridade básica.

> *Ao longo da Educação Básica, as aprendizagens essenciais definidas na BNCC devem concorrer para assegurar aos estudantes o desenvolvimento de dez competências gerais, que consubstanciam, no âmbito pedagógico, os direitos de aprendizagem e desenvolvimento.* [9, p.8].

A própria BNCC traz a definição de competência e habilidade:

> *Na BNCC, competência é definida como a mobilização de conhecimentos (conceitos e procedimentos), habilidades (práticas, cognitivas e socioemocionais), atitudes e valores para resolver demandas complexas da vida cotidiana, do pleno exercício da cidadania e do mundo do trabalho.* [9, p.8].

Ainda sobre o termo competências e habilidades, a Resolução Nº 4, de 17 de dezembro de 2018, que instituiu a Base Nacional Comum Curricular na etapa do Ensino Médio (BNCC-EM) como etapa final da Educação Básica, define esse termo, em seu parágrafo único do art 3º, da seguinte maneira:

> *Parágrafo único. Para os efeitos desta Resolução, com fundamento no caput do art. 35-A e no § 1º do art. 36 da LDB, a expressão "competências e habilidades" deve ser considerada como equivalente à expressão "direitos e objetivos de aprendizagem" presente na Lei do Plano Nacional de Educação (PNE).* [10].

Além disso, é importante que o professor busque e utilize vários recursos e instrumentos que venham ajudá-lo a fortalecer o ensino e, especialmente, a aprendizagem da Matemática, como por exemplo, os recursos tecnológicos.

Convém ressaltar que o uso de tecnologias nas aulas de Matemática tem se consolidado com o passar dos anos, reflexo das aceleradas mudanças e oportunidades de utilização de recursos bem conhecidos como o GeoGebra, planilhas eletrônicas, aplicativos de *smartphone* e simulações. Essa utilização foi objeto de estudo em publicações recentes, ver por exemplo, [13], [15] e [22], que ressalta, dentre outras conclusões, a eficácia da utilização de tais recursos na melhoria de aprendizagem dos estudantes.

Um tema que tem chamado muito a atenção e tem sido frequentemente apresentado em vídeos veiculados na *internet, sites,* revistas e mídias sociais são os investimentos. O homem, desde cedo,

em sua infância, lida com o dinheiro e deverá ser capaz de administrá-lo em toda sua trajetória de vida. Saber, portanto, como administrar e investir o dinheiro é essencial para uma vida financeira de maior qualidade.

O objetivo desse artigo é propor uma abordagem de ensino de Matemática Financeira para o Ensino Médio, mediante apresentação de atividades, que relacionam problemas envolvendo simulações de investimentos no tesouro direto e alguns conceitos matemáticos aplicados a esse investimento. Nessa abordagem usamos como recurso o *site* do tesouro direto, ver <https://www.tesourodireto.com.br/simulador/>, e uma calculadora científica.

2. Alguns conceitos relacionados à economia

Nesta seção, tendo em vista o potencial do tema e suas relações com as competências e habilidades previstas na BNCC, abordaremos alguns conceitos que permeiam este trabalho com um caráter de revisão.

2.1. Inflação

Um conceito muito importante para a Economia é a inflação. Basicamente, o processo inflacionário de uma economia pode ser entendido pelo aumento generalizado dos preços de vários bens e serviços importantes no dia a dia das pessoas, ver [19, p.61]. Por exemplo, se a inflação em determinado mês for de $0,6\%$, isso significa que o aumento médio dos preços desses bens e serviços no período também foi de $0,6\%$. Dessa forma, a inflação implica a diminuição do poder de compra da moeda, ver [6]. Para saber a respeito do conceito de moeda, ver [16, p.105-118]. Quando ocorre a diminuição dos preços de bens e serviços ocorre o fenômeno chamado de deflação, ver [19, p.61].

No Brasil o indicador oficial de inflação é o Índice de Preços para o Consumidor Amplo (IPCA), ver [8]. Ele é calculado mensalmente pelo Instituto Brasileiro de Geografia e Estatística (IBGE) em algumas regiões metropolitanas do país, ver [8]. E apesar de não ser calculado em todo o país, o IPCA é de abrangência nacional, isto é, ele serve como indicador do aumento médio dos preços de determinados bens e serviços de todos os estados do país. A taxa de inflação é a variação do custo da cesta de produtos e serviços, ou cesta do IPCA, durante determinado período. Essa cesta inclui os itens: transporte, vestuário, alimentação e bebidas, habitação, educação, saúde e cuidados pessoais, comunicação e outras despesas pessoais, ver [6]. O Brasil possui uma meta anual de inflação para dar segurança para a economia, ver [5]. Essa é uma forma de garantir que a economia brasileira continue em crescimento e os preços, controlados. A inflação torna-se prejudicial para a economia de um país quando ela sai do controle e atinge altos níveis, fenômeno chamado de hiperinflação.

2.2. Taxa Selic

A taxa Selic, Sistema Especial de Liquidação e Custódia, é a taxa básica de juros da economia usada pelo Banco Central, dentre outras coisas, para controlar a inflação. Ela também é usada como referência em operações e empréstimos realizados entre os bancos, e também afeta os rendimentos de investimentos de renda fixa, dentre eles os títulos públicos e a caderneta de poupança.

Ela é definida a cada 45 dias pelo Comitê de Política Monetária (Copom), ver [3], ligado ao Banco Central, que se baseia em outros indicadores financeiros do país. Atualmente, desde 06 de agosto

de 2020, a Selic alcançou a marca de 2% a.a., ver [1]. Assim, exibimos na Tabela 1 os valores da taxa Selic durante o período entre setembro de 2017 a outubro de 2020, ver [4].

Tabela 1: Taxa Selic do período 09/2017 a 10/2020

Vigência	Número de reuniões do Copom no período de vigência	Taxa Selic (ao ano)
06/08/2020 - 28/10/2020	2	2%
18/06/2019 - 05/08/2020	1	2,25%
07/05/2020 - 17/06/2020	1	3%
19/03/2029 - 06/05/2020	1	3,75%
06/02/2019 - 18/03/2020	1	4,25%
12/12/2019 - 05/02/2020	1	4,50%
31/10/2019 - 11/12/2019	1	5%
19/09/2019 - 30/10/2019	1	5,50%
01/08/2019 - 18/09/2019	1	6%
22/03/2018 - 31/07/2019	11	6,50%
08/02/2018 - 21/03/2018	1	6,75%
07/12/2017 - 07/02/2018	1	7%
26/10/2017 - 06/12/2017	1	7,50%
07/09/2017 - 25/10/2017	1	8,25%

Fonte: [4]

3. Investimenos financeiros

Um investimento financeiro é, basicamente, uma aplicação de um valor em dinheiro em que há uma expectativa de rendimento futuro. Isso ocorre por conta do efeito dos juros compostos sobre as aplicações financeiras, que faz com que o dinheiro aplicado tenha um crescimento nominal com o tempo.

Não é preciso ser um especialista em finanças para começar a investir. No entanto, para evitar prejuízos e ter bons rendimentos é importante conhecer bem o tipo de investimento desejado. Nesta seção falaremos sobre alguns tipos de investimentos do mercado financeiro, dentre eles, os títulos públicos do tesouro direto.

3.1. Caderneta de poupança

A caderneta de poupança é considerada a modalidade de aplicação financeira mais popular do mercado. Seus principais atrativos encontram-se na liquidez imediata (o aplicador pode sacar seu saldo a qualquer momento), na isenção do Imposto sobre Operações Financeiras (IOF), na isenção do Imposto de Renda (IR) e também na cobertura do Fundo Garantidor de Crédito (FGC), o qual protege o investidor em aplicações de até R$ 250.000,00 por Cadastro de Pessoa Física (CPF), por

instituição, respeitando o limite de quatro instituições. É importante salientar que esses atrativos não são exclusivos da poupança, podendo aparecer em outros investimentos.

Um ponto negativo da poupança é o baixo rendimento, podendo até perder dinheiro (de forma mais técnica, perder o poder de compra), caso em que a inflação é maior do que o rendimento oferecido pela poupança. Outro ponto negativo é que os juros da caderneta de poupança são pagos mensalmente no dia do aniversário, ver [7]. O aniversário da poupança pode ser o dia de abertura da conta ou a data em que foi feito o depósito. Como o rendimento da poupança é mensal, retirando-se o dinheiro da conta antes da data de aniversário, perde-se todo o rendimento do período. Por exemplo, depositando-se R$ 75.000,00 na poupança e resgatando todo esse valor antes de completar os 30 dias, não haverá rendimento nesse período.

Atualmente os juros pagos pela aplicação na caderneta de poupança depende do valor da taxa Selic, com acréscimo da Taxa Referencial (TR), que é uma taxa obtida a partir das médias das taxas de juros utilizadas nos certificados de depósito interbancários ofertados por bancos comerciais, ver [7] e [2].

São dois os cenários possíveis de rentabilidade:

1) Se a taxa Selic for superior a $8,5\%$, então a remuneração da poupança será de $0,5\%$ ao mês mais a TR;

2) Caso a Selic seja igual ou menor do que $8,5\%$ ao ano, o rendimento da poupança será de 70% da Selic mais a TR.

Visto que atualmente a taxa Selic está em 2% a.a., o rendimento da poupança segue a regra do segundo cenário. Portanto, o rendimento atual da poupança é dado por $0,70$ x 2% + TR. Como a taxa referencial está em 0%, o rendimento atual (nov. 2020) da caderneta de poupança é de $1,4\%$ a.a.

3.2. Títulos públicos

Os títulos públicos são ativos emitidos pelo governo federal com objetivo de financiar a dívida pública e as atividades do governo tais como educação, saúde, moradia, transporte, infraestrutura, entre outros, permitindo que investidores emprestem dinheiro para o governo visando uma rentabilidade futura. É considerado o investimento de menor risco de uma economia, pois é garantido pelo Tesouro Nacional, ver [27]. O órgão responsável pela emissão e controle dos títulos, e pela administração da dívida mobiliária federal, é a Secretaria do Tesouro Nacional.

O investidor conta com o serviço tesouro direto por meio do qual é possível comprar diretamente, via *site* na *internet*, títulos públicos federais do Tesouro Nacional, ver [21]. Para isso, basta possuir CPF e estar cadastrado em alguma das instituições financeiras habilitadas a operar no tesouro direto, ver [31]. Iremos abordar mais detalhadamente o tesouro direto na seção a seguir.

3.3. Tesouro direto

O tesouro direto é um programa do Tesouro Nacional desenvolvido em parceria com a Bolsa de Valores do Brasil (B3), para venda de títulos públicos federais para pessoas físicas, de forma 100% *online*, ver [27]. Ele foi lançado no ano 2002 com o objetivo de democratizar o acesso aos títulos

públicos, ver [27]. Com pouco mais de R$ 30,00 é possível investir no tesouro direto, ver [27], e não é necessário ser um especialista em investimentos, o que facilita a acessibilidade aos jovens que estão iniciando sua trajetória profissional.

Os investimentos em títulos públicos, por meio do programa tesouro direto, são 100% garantidos pelo Tesouro Nacional, por isso são considerados os investimentos mais seguros do país, ver [27]. Todas as aplicações, resgates e acompanhamentos podem ser realizados pelo *site* do tesouro direto ou por meio do aplicativo oficial do tesouro direto. Para quem está começando no mundo dos investimentos e tem experiência, o tesouro direto é uma excelente alternativa de investimento, pois oferece títulos com diferentes tipos de rentabilidade (prefixada, ligada à variação da inflação ou à variação da taxa de juros básica da economia - Selic), diferentes prazos de vencimento e também diferentes fluxos de remuneração, ver [27].

Basicamente, temos os seguintes tipos de tesouro:

a) Tesouro prefixado, no qual o investidor sabe exatamente a rentabilidade e quanto vai receber na data de vencimento do título e é mais interessante para quem pode deixar o seu dinheiro render até o vencimento do investimento. Em caso de resgate antecipado, o Tesouro Nacional garante sua recompra pelo seu valor de mercado na data de resgate;

b) Tesouro Selic, no qual a rentabilidade da aplicação é baseada na taxa Selic (a taxa básica de juros da economia), é indicado para aqueles que querem realizar investimentos de curto prazo em título com rentabilidade diária vinculada à taxa de juros da economia (taxa Selic). Isso significa que se a taxa Selic aumentar, a sua rentabilidade aumenta. E se a taxa Selic diminuir, sua rentabilidade diminui;

c) Tesouro IPCA, no qual a rentabilidade da aplicação é baseada em uma parte fixa (prefixada) e uma parte atrelada à variação da inflação, medida pelo Índice de Preços ao Consumidor Amplo (IPCA). O tesouro IPCA é indicado para aqueles que querem realizar investimentos de longo prazo, pois ele garante um rendimento acima da inflação.

É importante saber que em todos os tipos de tesouro há a cobrança de imposto de renda sobre a rentabilidade, conforme abaixo:

- Aplicações até 180 dias: $22,5\%$;
- Aplicações de 181 a 360 dias: 20%;
- Aplicações de 361 a 720 dias: $17,5\%$;
- Aplicações acima de 720 dias: 15%.

Essa cobrança ocorrerá na venda do título, no pagamento de juros semestrais ou em seu vencimento, ver [31]. E caso o investidor faça o resgate em menos de 30 dias de aplicação, haverá também a incidência de IOF sobre os rendimentos. A taxa de cobrança do IOF é regressiva, diminuindo com o tempo que o investimento for mantido e desaparecendo ao completar 30 dias de investimento, ver [25].

Além dos dois impostos citados acima há também a cobrança de uma taxa de custódia, cobrada pela B3, que é o lugar onde são negociados os títulos do tesouro direto. O valor cobrado é utilizado

para guardar os títulos, aprimorar o sistema do tesouro e demais serviços do programa. A taxa de custódia é de $0,25\%$ sobre o valor total investido, ver [25]. Ainda há a taxa de administração da instituição financeira, também conhecida como taxa do agente de custódia. A taxa de administração é um valor cobrado pela corretora ou banco para investir no tesouro direto. O percentual da taxa é determinado por cada instituição, podendo ser taxa zero, ver [25]. Dessa forma, para aumentar a competitividade, muitas instituições isentam seus clientes dessa cobrança.

Mostramos na Figura 1 uma tabela retirada do *site* do tesouro direto, ver [26], com as opções de compra de títulos (referência 09/06/2020):

Figura 1: Tesouro direto: preços e taxas dos títulos

Título	Rentabilidade anual	Investimento mínimo	Preço Unitário	Vencimento
TESOURO PREFIXADO 2023	4,29%	R$ 35,92	R$ 898,21	01/01/2023
TESOURO PREFIXADO 2026	6,35%	R$ 35,51	R$ 710,32	01/01/2026
TESOURO PREFIXADO com juros semestrais 2031	7,01%	R$ 37,72	R$ 1.257,60	01/01/2031
TESOURO SELIC 2025	SELIC + 0,03%	R$ 106,24	R$ 10.624,25	01/03/2025
TESOURO IPCA+ 2026	IPCA + 2,69%	R$ 55,85	R$ 2.792,75	15/08/2026
TESOURO IPCA+ 2035	IPCA + 4,07%	R$ 36,34	R$ 1.817,25	15/05/2035
TESOURO IPCA+ 2045	IPCA + 4,07%	R$ 36,62	R$ 1.220,79	15/05/2045
TESOURO IPCA+ com juros semestrais 2030	IPCA + 3,37%	R$ 40,80	R$ 4.080,03	15/08/2030
TESOURO IPCA+ com juros semestrais 2040	IPCA + 3,99%	R$ 42,49	R$ 4.249,36	15/08/2040
TESOURO IPCA+ com juros semestrais 2055	IPCA + 4,08%	R$ 44,61	R$ 4.461,54	15/05/2055

Fonte: [26]

É importante dizer que a cada dia os dados da tabela mostrada na Figura 1 sofrem alterações. Para acessar a tabela atual, ver <https://www.tesourodireto.com.br/titulos/precos-e-taxas.htm>.

Alguns conceitos importantes no ato de investir no tesouro direto são:

a) Vencimento do título: refere-se à data de resgate automático do título pelo sistema. Nessa data, o título deixa de existir e o Tesouro Nacional repassa o valor de resgate ao agente de custódia do investidor, a qual repassa para o investidor, após as deduções dos impostos e taxas, ver [29];

b) Taxa (a.a): é a rentabilidade bruta ao ano obtida, caso o título permaneça até a data de vencimento. Se o investidor optar pela venda antecipada do título, receberá o valor de mercado do mesmo, ver [29];

c) Preço unitário: refere-se ao preço de uma unidade do título vendido, porém não é necessário comprar o título inteiro, pode-se comprar frações do título. A quantidade mínima de compra é de 1% ou 0,01 do título, ver [29].

A liquidação (conclusão do processo) da compra do título não se dá na data de solicitação da compra, mas sim conforme a regra:

a) Para uma aplicação realizada em dias úteis (de 0h00 às 18h00) a liquidação acontecerá a partir das 18h do 1º dia útil após a solicitação de aplicação;

b) Para uma aplicação realizada em dias úteis (de 18h00 às 0h00), finais de semana ou feriado, a liquidação acontecerá a partir das 18h do 2º dia útil após a solicitação de aplicação.

Para mais informações sobre a liquidação, ver [31].

No cálculo da rentabilidade do título é considerado apenas os dias úteis entre a data de liquidação (inclusive) e a data de vencimento (exclusive). Para mais informações sobre a metodologia de cálculo utilizada nos títulos de tesouro direto, ver [30].

No *site* do tesouro direto, ver [28], também encontramos alguns dos objetivos desse programa do Tesouro Nacional:

a) Garantir o acesso do cidadão ao investimento em títulos da dívida pública federal;

b) Promover a educação financeira dos brasileiros;

c) Ser referência de investimento para o cidadão;

d) Estimular a formação de poupança no país;

e) Incentivar a competitividade no mercado financeiro;

f) Ser uma alternativa de investimento conhecida e acessível.

É importante dizer que as aplicações em títulos do tesouro direto precisam ser intermediadas por uma corretora. Na plataforma do programa é possível consultar saldos e extratos, mas não é permitido aplicar sem que haja um intermediador ligando o investidor ao programa. Para isso, o investidor pode utilizar tanto os bancos múltiplos quanto corretoras que atuam com investimentos, ver [23].

Na plataforma do tesouro direto que pode ser acessado pelo *site* ou aplicativo no *smartphone,* é possível, além de consultar saldos e extratos, acessar o simulador de investimentos (ver Figura 2). É esse simulador que será o instrumento usado na abordagem do ensino de Matemática Financeira que objetivamos fazer.

Figura 2: Simulação de investimento no *site* do tesouro direto

Fonte: [26]

Para acessar o simulador do tesouro direto pelo computador basta acessar o *link*: <https://tesourodireto.com.br/simulador/>. Também o acesso pode ser feito pelo aplicativo do tesouro direto.

3.4. Certificado de Depósito Bancário (CDB)

É um título emitido por bancos, corretoras e distribuidoras de títulos e valores mobiliários para captar dinheiro a fim de financiar suas atividades, tais como empréstimos a clientes, crescimento, projetos e pagamento de dívidas. No CDB o investidor empresta dinheiro para a instituição bancária. Em troca desse empréstimo, ele recebe uma rentabilidade a qual é definida no momento da compra, ver [20]. As categorias de rentabilidade do CDB são:

a) CDB prefixados: a rentabilidade já é conhecida no momento da aplicação. Por exemplo, 8% ao ano;

b) CDB pós-fixados: a rentabilidade é atrelada a um indexador da economia. O emissor paga um percentual do índice de referência utilizado, normalmente o Certificado de Depósito Interbancário (CDI). Por exemplo, 112% do CDI ao ano. Como os indexadores podem variar com o tempo, os rendimentos também sofrerão variações até o vencimento. Dessa forma, o investidor só tem uma previsão de quanto irá receber na data de resgate;

c) CDB híbridos: possui taxa de rentabilidade composta por uma parte fixa e uma parte variável, por exemplo, $2,5\% + \text{IPCA}$.

Além da rentabilidade, a liquidez do título é um ponto importante a se considerar antes de investir em um CDB, pois muitos só permitem resgate na data de vencimento. Quanto à segurança, o CDB conta com a proteção do FGC. Dessa forma, se a instituição que emitiu o CDB decretar falência, o dinheiro do investidor, dentro das condições do fundo, estará assegurado, ver [20].

Assim como nos títulos do tesouro direto, se houver resgate em menos de 30 dias de aplicação, haverá incidência de IOF sobre os rendimentos, ver [20]. E no momento de resgate haverá a incidência de IR sobre os rendimentos, conforme abaixo:

- Aplicações até 6 meses: $22,5\%$;
- Aplicações de 6 meses a 1 ano: 20%;
- Aplicações de 1 ano a 2 anos: $17,5\%$;
- Aplicações a mais de 2 anos: 15%.

3.5. Letra de Crédito do Agronegócio (LCA)

A Letra de Crédito do Agronegócio (LCA) é um título privado emitido por instituições financeiras com prazo e taxa definidos no momento da compra, ver [11]. Os recursos captados pelo emissor são utilizados para o financiamento das atividades do setor agrícola. O que a torna bastante interessante é a isenção de IR e de IOF para pessoas físicas, além de contar com a cobertura do FGC em até R$ 250.000,00 por emissor e por CPF, ver [11].

3.6. Letra de Crédito do Imobiliário (LCI)

A Letra de Crédito Imobiliário (LCI) é um título privado emitido por instituições financeiras com prazo e taxa definidos no momento da compra, ver [12]. Os recursos captados pelo emissor são utilizados para o financiamento das atividades do setor imobiliário. Assim como nas LCAs, as LCIs têm isenção de IR e de IOF além de contar com a cobertura do FGC em até R$ 250.000,00 por emissor e por CPF, ver [12].

Como se pode ver, a LCI e LCA são bem parecidas, dessa forma o investidor costuma decidir entre elas baseado tão somente na taxa de rendimento, no prazo de investimento e no valor mínimo para aplicação inicial.

4. Proposta de atividades via simulador do Tesouro Direto

Nesta seção vamos propor uma abordagem de ensino de Matemática Financeira para o Ensino Médio, mediante apresentação de duas atividades que relacionam problemas envolvendo simulações de investimentos no tesouro direto, ver [32], e alguns conceitos matemáticos. Além disso, revelamos um possível percurso de resolução de cada atividade. Observamos que, ao utilizarmos o *site* do tesouro direto em tempo real, os títulos disponíveis e as taxas mudam a cada dia, bem como o próprio *site* passa por periódicas atualizações, podendo assim alterar algum percurso de alguma ferramenta.

É importante dizer que não é o objetivo dessa proposta abordar todos os aspectos relacionados aos cálculos dos investimentos em títulos públicos, devido ao grau de dificuldade que estaria sendo exposto aos alunos do nível médio. Portanto, os alunos farão simulações pelo *site* do tesouro direto e realizarão cálculos aproximados, desconsiderando-se aspectos como dias úteis de um determinado período e cobranças de taxas. Para uma leitura sobre a metodologia de cálculo da rentabilidade dos investimentos do tesouro direto, recomendamos ver [30].

A seguir, vamos descrever cada atividade e sua respectiva proposta de resolução.

Atividade 1.

(a) Uma pessoa possui R$ 250,00 para investir em um título público. Usando o *site* do tesouro direto <https://www.tesourodireto.com.br/>, faça uma simulação de uma aplicação com essa quantia no tesouro Selic 2025 (trata-se da opção (a) da p.651). Qual o valor em reais que ela receberá ao final do vencimento? Se dobrarmos o valor de aplicação, qual será o valor líquido que ela irá receber? Compare o resultado de cada caso com a rentabilidade na caderneta de poupança.

(b) Atualmente, os juros pagos pela caderneta de poupança dependem do valor da taxa Selic, com o acréscimo da Taxa Referencial (TR), seguindo as seguintes regras:

(i) Se a taxa Selic for superior a $8,5\%$ ao ano, então a remuneração da poupança será de $0,5\%$ ao mês mais a TR;

(ii) Caso a taxa Selic seja igual ou menor do que $8,5\%$ ao ano, o rendimento da poupança será de 70% da taxa Selic mais a TR.

Se a taxa Selic está atualmente a 2% a.a. e a taxa de referencial está em 0% ao ano, então qual é a taxa de juros atual da caderneta de poupança?

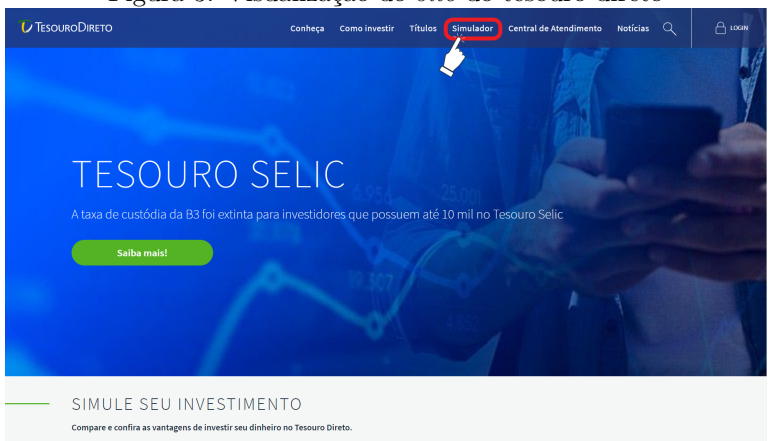
Resolução da Atividade 1.

(a) O aluno irá acessar o *site* do tesouro direto por meio do *link*

<https://www.tesourodireto.com.br/>.

Após o acesso, seu próximo passo será dar início a sua simulação. Para isso, ele deverá clicar na aba "Simulador" (ver Figura 3).

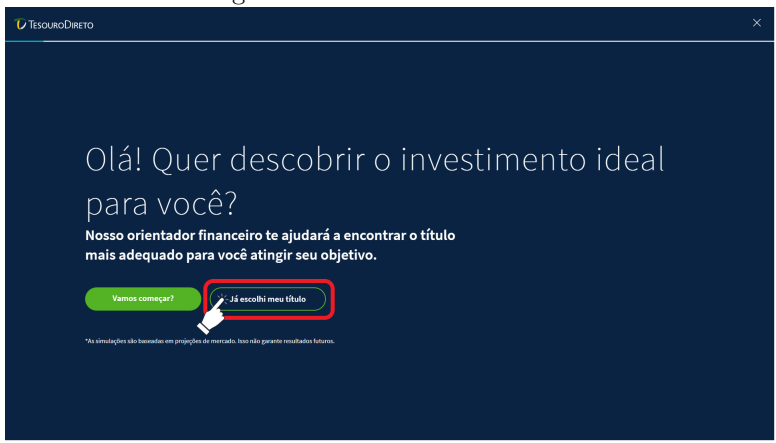
Figura 3: Visualização do *site* do tesouro direto



Fonte: [32]

Posteriormente, o aluno será redirecionado para uma página intitulada como "orientador financeiro" e, consequentemente, deverá escolher entre "Vamos começar?" e "Já escolhi meu título". Como queremos uma aplicação do tesouro Selic 2025, o aluno deverá clicar na opção "Já escolhi meu título" (ver Figura 4).

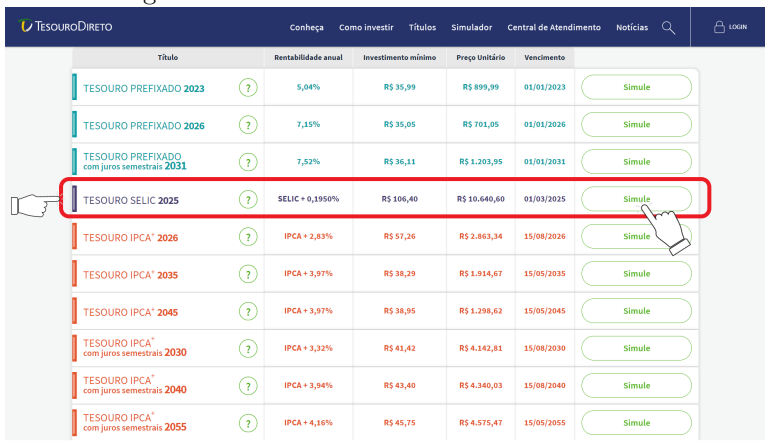
Figura 4: Orientador financeiro



Fonte: [32]

A partir daí, o aluno deverá deslizar a barra rolante da tela para ter acesso a uma tabela, a qual exibe os títulos disponíveis para venda naquele dia. Além disso, ele precisará localizar o termo "TESOURO SELIC 2025" localizado na primeira coluna da tabela e, então, clicar em "Simule", o qual se encontra na mesma linha, em verde (ver Figura 5).

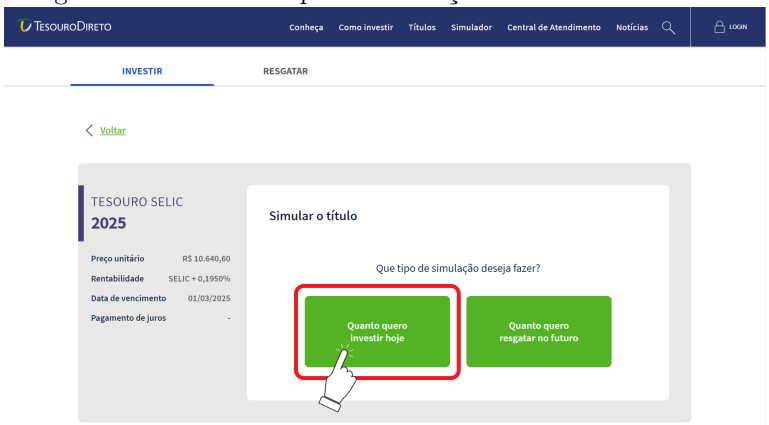
Figura 5: Escolha do título tesouro Selic 2025



Fonte: [26]

O estudante, então, será direcionado à página de simulação, onde receberá algumas informações do título escolhido, alinhadas à esquerda da tela. O *site* exibirá o preço unitário, a rentabilidade e a data de vencimento. Ademais, em destaque, o aluno terá a oportunidade de realizar a simulação desse título. Para isso, o discente deverá escolher entre "Quanto quero investir hoje" e "Quanto quero resgatar no futuro". Para realizar a atividade, o aluno precisa clicar na primeira opção "Quanto quero investir hoje" (ver Figura 6).

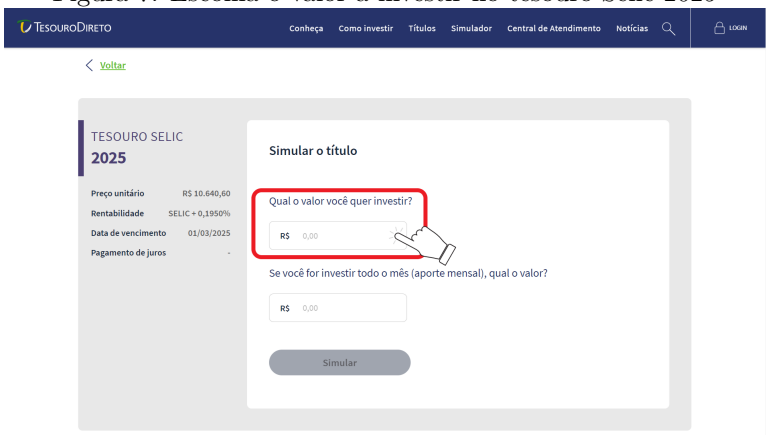
Figura 6: Escolha do tipo de simulação do tesouro Selic 2025



Fonte: [26]

Agora, o aluno poderá digitar o valor que ele pretende investir (ver Figura 7). Observamos que são exibidos dois campos para preenchimento: o campo "Qual o valor que você quer investir", onde ele aplicará um valor específico de uma única vez, e o outro campo que será preenchido caso o aluno queira realizar uma aplicação mensal. No caso em questão, ele fará a simulação de R$ 250,00 no primeiro campo de preenchimento (ver Figura 7).

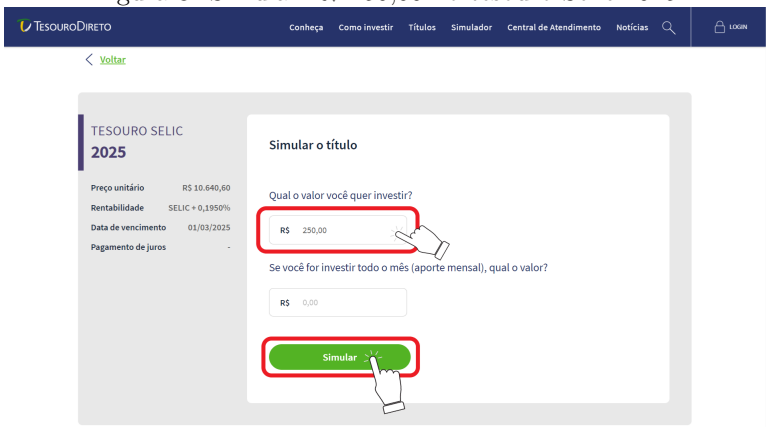
Figura 7: Escolha o valor a investir no tesouro Selic 2025



Fonte: [26]

Neste momento, o aluno poderá digitar no campo exibido o valor de R$ 250,00. Destacamos que assim que ele inserir o valor escolhido, o botão "Simular" ficará verde, sinalizando que ele poderá realizar sua simulação e obter os dados. Para isso, o aluno deverá clicar em "Simular" (ver Figura 8).

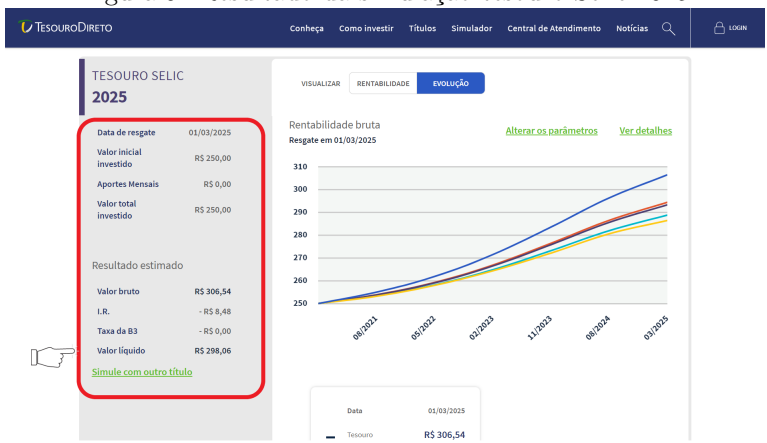
Figura 8: Simular R$ 250,00 no tesouro Selic 2025



Fonte: [26]

Finalmente, o aluno terá acesso à sua simulação. Destacamos que é oferecido um gráfico e outras informações, a saber, data de resgate e valor inicial investido, bem como o resultado estimado (ver Figura 9). Ademais, é feita a comparação com outras modalidades de investimentos do mercado financeiro no mesmo período simulado (ver Figura 9).

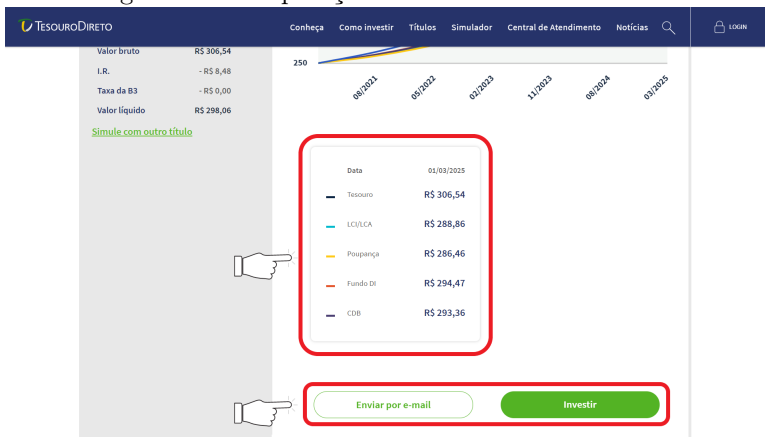
Figura 9: Resultado da simulação tesouro Selic 2025



Fonte: [26]

De acordo com a Figura 9, o valor líquido do tesouro Selic 2025 será de R$ 298,06. Movendo a barra de rolagem da tela para baixo, visualizamos uma tabela de comparação com outros tipos de investimentos, dentre eles podemos ver que o valor obtido na poupança nesse mesmo período será de R$ 286,46 (ver Figura 10). Ademais, aparecerá a opção escolher entre investir ou enviar o resultado por *e-mail*.

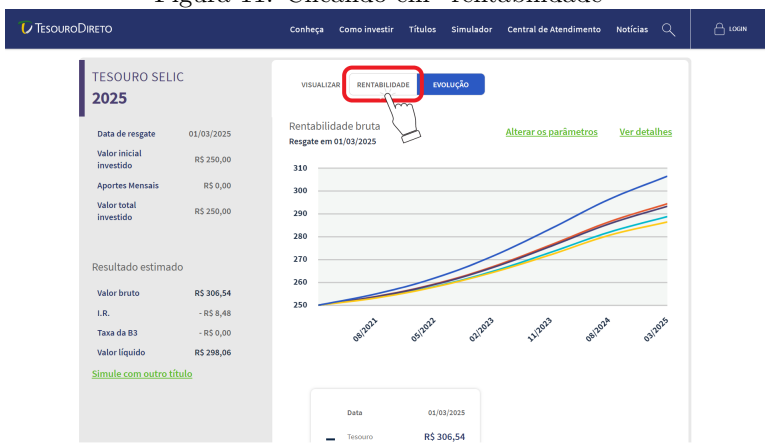
Figura 10: Comparação com outros investimentos



Fonte: [26]

Além disso, clicando em "rentabilidade" (ver Figura 11), será exibido um gráfico de barras comparando o título com outros tipos de investimentos (ver Figura 12).

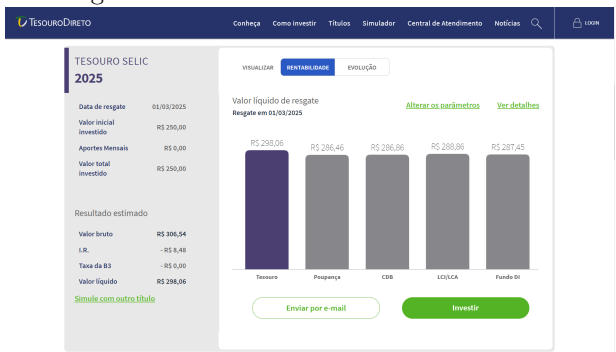
Figura 11: Clicando em "rentabilidade"



Fonte: [26]

Na Figura 11, verificamos também um gráfico de linhas comparando o comportamento do valor bruto de uma aplicação de R$ 250,00 no tesouro Selic 2025 com outros investimentos durante o mesmo período de tempo. Cada cor das linhas está relacionada a um investimento; essa relação pode ser verificada na tabela ilustrada na Figura 10.

Figura 12: Gráfico de barras tesouro Selic

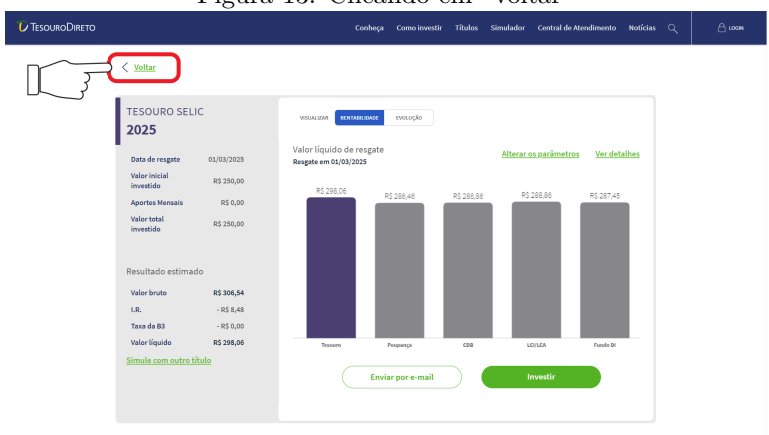


Fonte: [26]

O gráfico de barras, ilustrado na Figura 12, compara o valor líquido de resgate estimado no tesouro Selic 2025 com o valor líquido nos investimentos: poupança, CDB, LCI/LCA e Fundos DI. Note que nessa situação a poupança tem valor líquido menor do que todos os investimentos indicados no gráfico. Importante dizer que no mercado financeiro é possível encontrar CDBs, LCIs/LCAs e Fundos DI com rentabilidade maior do que a do tesouro Selic. Pelo gráfico de barras também vemos que o valor líquido estimado do investimento do tesouro Selic foi de R$ 298,06. Dessa forma, ao investir R$250,00, nesse contexto, ele receberá R$ 48,06 a mais ao final do período. Esse valor representa o valor nominal recebido, isto é, não é considerado o efeito da inflação no período.

Agora, para fazer a simulação do dobro de R$ 250,00, isto é, R$ 500,00, o aluno poderá clicar em "voltar" (ver Figura 13).

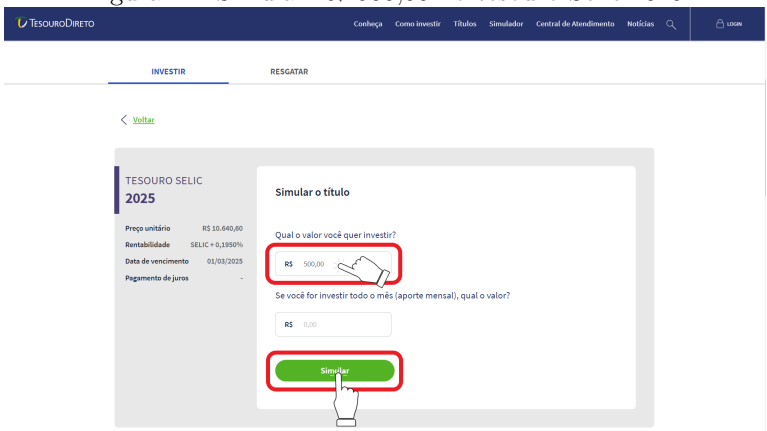
Figura 13: Clicando em "voltar"



Fonte: [26]

Após clicar, ele voltará para a tela de escolha do valor a investir (ver Figura 7). Então, ele digitará 500,00 no primeiro campo e clicará em "Simular" (ver Figura 14).

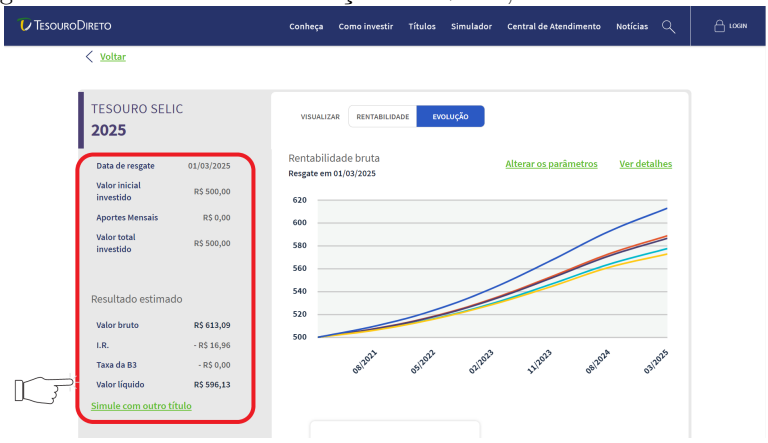
Figura 14: Simular R$ 500,00 no tesouro Selic 2025



Fonte: [26]

Após clicar em ”Simular”ele será direcionado para página com o resultado da simulação (ver Figura 15).

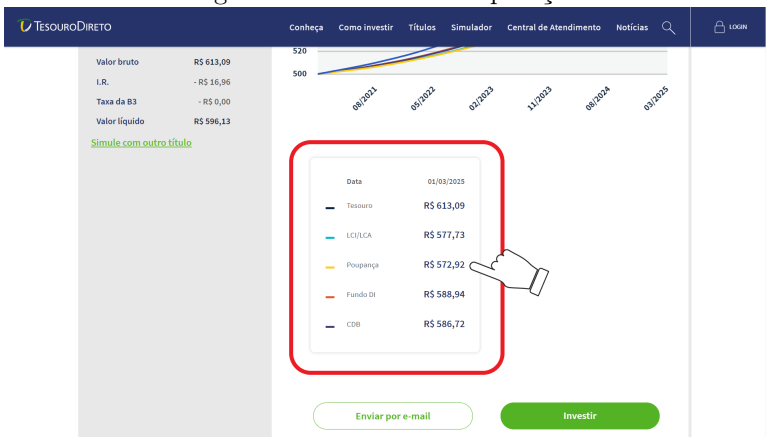
Figura 15: Resultado da simulação de R$ 500,00 no tesouro Selic 2025



Fonte: [26]

De acordo com a Figura 15, o valor líquido será de R$ 596,13. Nessa figura, também podemos visualizar outras informações, como a data de resgate, valor inicial investido, aportes mensais, imposto de renda e taxa B3. Ao centro da figura, há um gráfico de linhas comparando o comportamento do valor bruto de uma aplicação de R$ 500,00 no tesouro Selic 2025 com outros investimentos (poupança, CDB, LCI/LCA, e Fundos DI) durante o mesmo período de tempo. Cada cor das linhas está relacionada a um investimento; essa relação pode ser verificada na tabela ilustrada na Figura 16. Movendo a barra de rolagem da tela para baixo, visualizamos a tabela de comparação, na qual podemos ver que o valor obtido na poupança nesse mesmo período será de R$ 572,92 (ver Figura 16).

Figura 16: Tabela de comparação



Fonte: [26]

A tabela indicada na Figura 16 compara o valor bruto obtido no tesouro Selic 2025 com o valor bruto de outros investimentos: poupança, CDB, LCI/LCA e Fundos DI. Note que, nessa situação, novamente a poupança tem valor menor do que todos os investimentos indicados na tabela.

(b) Como a taxa Selic está a 2%a.a., a rentabilidade da caderneta de poupança está sendo baseada na segunda regra: caso a taxa Selic seja igual ou menor do que $8,5\%$ ao ano, o rendimento da poupança será de 70% da taxa Selic mais a TR. Dessa forma o rendimento será

$$0,7\text{x}2 + \text{TR} = 1,4 + 0 = 1,4.$$

Portanto, o rendimento está em $1,4\%$a.a.

Atividade 2.

(a) Identifique a taxa de rentabilidade anual e o vencimento do tesouro prefixado 2023. Em seguida, expresse, em anos, meses e dias, o período em que o dinheiro permanecerá aplicado até a data de vencimento (X anos, Y meses e Z dias).

(b) Utilizando o período de aplicação encontrado no item (a) e a taxa de rentabilidade anual do tesouro prefixado 2023, calcule uma aproximação do montante, no regime de juros compostos, de uma aplicação de R$ 52,00 no tesouro prefixado 2023 (para isso desconsidere a cobrança de taxas). Após os cálculos, faça uma simulação de R$ 52,00 no tesouro prefixado 2023 e compare os resultados.

(c) Calcule o montante de uma aplicação de R$ 52,00, no regime de juros simples, obtido no mesmo período e com a mesma taxa de rentabilidade do item (a). Qual a diferença dos montantes encontrados no regime de juros simples e compostos?

Resolução da Atividade 2.

(a) O aluno irá acessar o *site* do tesouro direto por meio do *link*

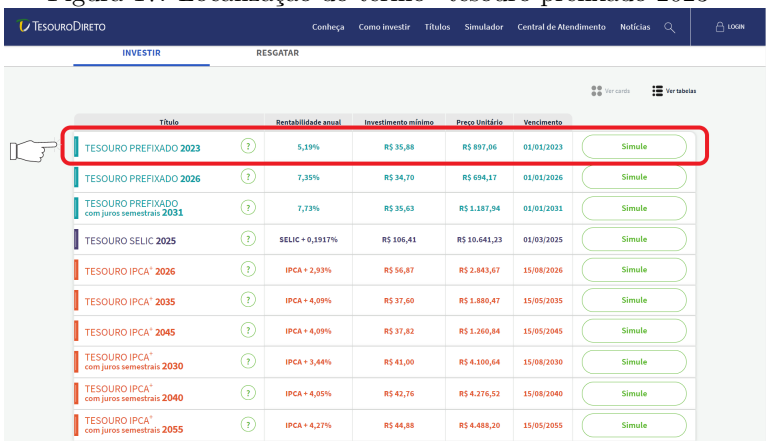
<https://www.tesourodireto.com.br/>.

Após o acesso, seu próximo passo será dar início a sua simulação. Para isso, ele deverá clicar na aba "Simulador" (ver Figura 3).

Posteriormente, o aluno será redirecionado para uma página intitulada como "orientador financeiro" e, consequentemente, deverá escolher entre "Vamos começar?" e "Já escolhi meu título". Como queremos uma aplicação do tesouro prefixado 2023, o aluno deverá clicar na opção "Já escolhi meu título" (ver Figura 4).

A partir daí, o aluno deverá deslizar a barra rolante da tela para ter acesso a uma tabela, a qual exibe os títulos disponíveis para venda naquele dia. Além disso, ele precisará localizar o termo "Tesouro Prefixado 2023" localizado na primeira coluna da tabela (ver Figura 17).

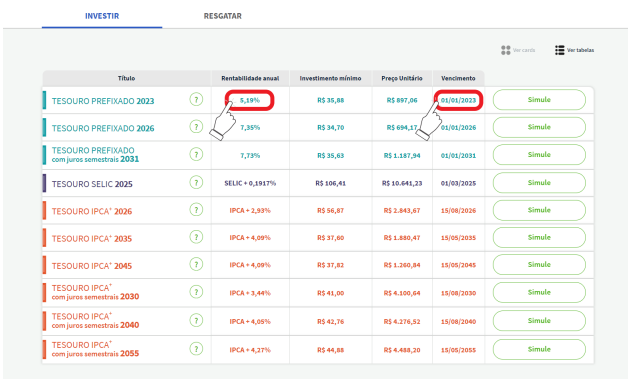
Figura 17: Localização do termo "tesouro prefixado 2023"



Fonte: [26]

Na linha do tesouro prefixado 2023, ele identifica a taxa rentabilidade anual e o vencimento desse título, os quais se encontram na segunda e quarta coluna, respectivamente (ver Figura 18).

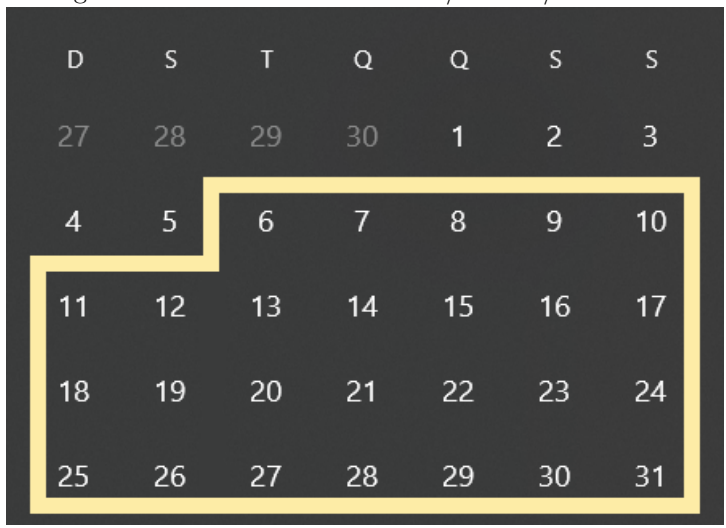
Figura 18: Rentabilidade anual e Vencimento do tesouro prefixado 2023



Fonte: [26]

De acordo com a Figura 18, a taxa de rentabilidade anual é de $5,19\%$a.a. e o vencimento do título será no dia 01/01/2023. Como a aplicação está sendo simulada no dia 05/11/2020, o período de investimento será contado a partir do dia 06/11/2020. Para expressar o período de aplicação em anos, meses e dias, uma possibilidade é o aluno perceber que do dia 06/11/2020 (inclusive) ao dia 05/11/2022 (inclusive) há 2 anos. E do dia 06/11/2022 (inclusive) ao dia 05/12/2022 (inclusive) há 1 mês. Assim, contando a partir do dia 06/12/2022, faltam apenas 26 dias para o vencimento, pois o dinheiro não recebe incidência de juros no dia do vencimento (01/01/2023). Podemos visualizar a quantidade de dias restantes na Figura 19.

Figura 19: Dias restantes entre 06/11 a 31/12 de 2022



Fonte: Autoria própria

Portanto, o período de investimento será de 2 anos, 1 mês e 26 dias. Com isso, concluímos o item (a).

(b) Vamos calcular o montante em três etapas. Inicialmente, devemos encontrar o montante referente aos 2 primeiros anos de investimento, o qual chamaremos M_1, para em seguida calcular a rentabilidade em um mês (06/11/2022 a 05/12/2022) e, finalmente, nos últimos 26 dias, que denominaremos M_2 e M_c, respectivamente. Para maior clareza dos cálculos utilizados aqui, sugerimos a leitura do apêndice ao final do artigo.

Como a taxa de rentabilidade anual (i_a) é de $5,19\%$ e o capital inicial investido (c_1) é de R$ 52,00, substituindo $i_a = 0,0519$ e $c_1 = 52$ em $M_1 = c_1(1 + i_a)^2$, obtemos

$$M_1 = 52(1 + 0,0519)^2 = 57,53766772,$$

isto é, $M_1 \approx$ R$ 57,54.

Agora, a partir do capital $c_2 = M_1$, calcularemos o montante acumulado M_2 referente a um mês de aplicação. Para isso, devemos encontrar uma taxa mensal i_m equivalente à taxa anual i_a. Portanto, utilizamos a equação $1 + i_a = (1 + i_m)^{12}$, ou seja,

$$i_m = (1 + i_a)^{\frac{1}{12}} - 1.$$

Logo, substituindo $i_a = 0,0519$, obtemos

$$i_m = (1 + 0,0519)^{\frac{1}{12}} - 1.$$

Lançando mão de uma calculadora científica, encontramos $i_m = 0,004225406$.
Agora, substituindo $c_2 = 57,54$ e $i_m = 0,004225406$ em $M_2 = c_2(1 + i_m)$, temos

$$M_2 = 57,54(1 + 0,0042225406) = 57,783129861.$$

Daí, $M_2 \approx$ R$ 57,78.
Finalmente, a partir do capital $c_3 = M_2$, calculemos o montante acumulado referente aos 26 dias restantes de investimento, o qual denominamos de M_c. Para isso, calculamos a taxa diária, i_d, equivalente à taxa mensal i_m.
Fazendo $i_m = 0,004225406$, encontramos

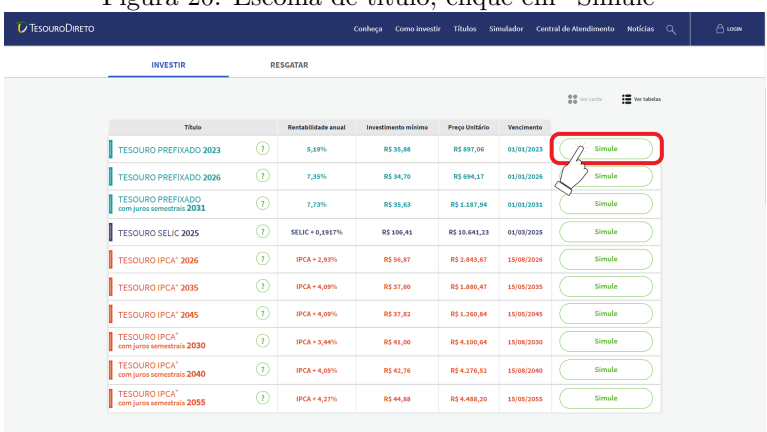
$$i_d = (1 + 0,004225406)^{\frac{1}{30}} - 1 = 0,00014056.$$

Substituindo $c_3 = 57,78$ e $i_d = 0,00014056$ em $M_c = c_3(1 + i_d)^{26}$, obtemos

$$M_c = 57,78(1 + 0,00014056)^{26} = 57,991531903.$$

Logo, $M_c \approx$ R$ 58,00.
Na segunda etapa, após realizar os passos exibidos nas figuras 3, 4 e 17, o aluno clicará em "Simule" (ver Figura 20).

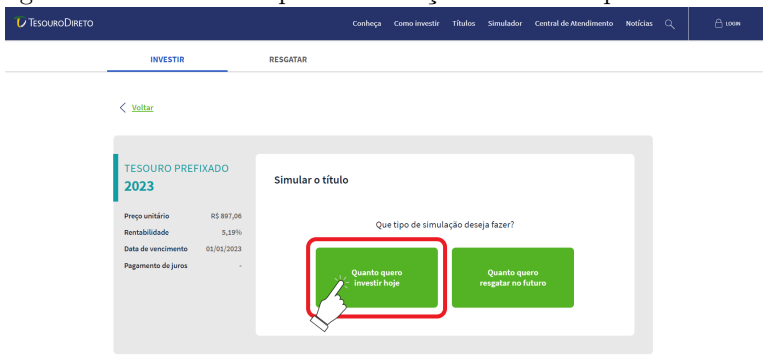
Figura 20: Escolha de título, clique em "Simule"



Fonte: [26]

O estudante será direcionado à página de simulação, onde receberá algumas informações do título escolhido, alinhadas à esquerda da tela. O *site* exibirá o preço unitário, a rentabilidade e a data de vencimento. Ademais, em destaque, o aluno terá a oportunidade de realizar a simulação desse título. Para isso, o discente deverá escolher entre "Quanto quero investir hoje" e "Quanto quero resgatar no futuro". Para realizar a atividade, o aluno precisa clicar na primeira opção "Quanto quero investir hoje" (ver Figura 21).

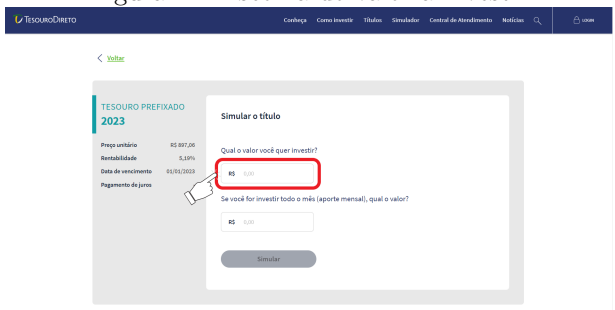
Figura 21: Escolha do tipo de simulação do tesouro prefixado 2023



Fonte: [26]

Agora, o aluno poderá digitar o valor que ele pretende investir (ver Figura 22). Observamos que são exibidos dois campos para preenchimento: o campo "Qual o valor que você quer investir", onde ele aplicará um valor específico de uma única vez, e o outro campo que será preenchido caso o aluno queira realizar uma aplicação mensal. No caso em questão, ele fará a simulação de R$ 52,00 no primeiro campo de preenchimento (ver Figura 22).

Figura 22: Escolha do valor a investir



Fonte: [26]

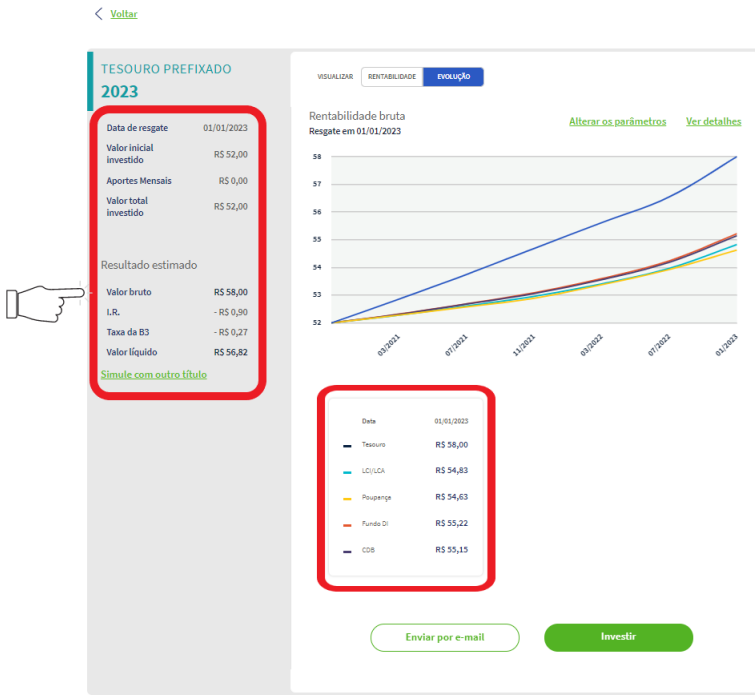
Neste momento, o aluno poderá digitar no campo (ver Figura 23) o valor de R$ 52,00. Destacamos que assim que ele inserir o valor escolhido, o botão "Simular"ficará verde, sinalizando que ele poderá finalizar sua simulação e obter o resultado. Para isso, o aluno deverá clicar em "Simular" (ver Figura 23).

Figura 23: Finalizar a simulação tesouro prefixado 2023

Fonte: [26]

Após clicar em "Simular", ele será redirecionado para o resultado de sua simulação (ver Figura 24).

Figura 24: Resultado da simulação tesouro prefixado 2023



Fonte: [26]

De acordo com a Figura 24, o valor bruto obtido foi de R$ 58,00, ratificando, assim, o cálculo realizado inicialmente com as conversões da rentabilidade e a atualização do montante.

(c) Procederemos por um percurso diferente do item (b). Novamente, para um maior entendi-

mento dos conceitos utilizados nesse item, sugerimos a leitura do apêndice ao final do artigo. Inicialmente, observe que o período total de investimento é 25 meses e 26 dias.

Logo, substituindo $c_1 = 52$ e, $i_m = \frac{i_a}{12} = \frac{0{,}0519}{12} = 0{,}004325$ em $M_1 = c_1(1 + i_m \times 25)$, obtemos

$$M_1 = 52(1 + 0{,}004325 \times 25) = 57{,}6225,$$

ou seja, $M_1 \approx$ R$ 57,62.

A partir de M_1, calculemos o montante acumulado após 26 dias, o qual chamaremos de M_s. Para isso, substituímos $i_d = \frac{i_m}{30} = \frac{0{,}004325}{30} = 0{,}000144167$ e $c_2 = M_1 = 57{,}62$ em $M_s = c_2(1 + i_d \times 26)$.

Portanto,

$$M_s = 57{,}62(1 + 0{,}000144167 \times 26) = 57{,}835979466.$$

Assim, $M_s \approx$ R$ 57,84.

Portanto, a diferença entre os montantes encontrados no regime de juros simples e compostos é de

$$58 - 57{,}84 = 0{,}16.$$

5. Apêndice

5.1. Juro

O juro (j) é a remuneração recebida por quem dispõe de um capital c e o empresta durante certo período a alguém. A soma c + j é chamada de montante e é representada por M. A razão $i = \frac{j}{c}$ é chamada de taxa de juros e ela será sempre referida ao período da operação, ver [18]. O juro pode ser calculado de duas formas:

a) **Juros simples**

No regime de juros simples, a taxa de juros incide somente sobre o capital inicial durante o período de tempo determinado. Pode-se calcular os juros simples utilizando a fórmula

$$j = c \times i \times t,$$

onde j é o juro; i é a taxa; c é o capital e t é o tempo.

Substituindo j na fórmula do montante, obtemos a fórmula:

$$M = c + j = c + (cit) = c(1 + it).$$

O montante no regime de juros simples possui um crescimento linear em relação a variável t.

b) **Juros compostos**

No regime de juros compostos, a taxa de juros sempre incide sobre o montante obtido no período anterior. No regime de juros compostos de taxa i, um principal c transforma-se, em t períodos de tempo, em um montante igual a

$$M = c \times (1 + i)^t.$$

O montante no regime de juros compostos, possui um crescimento exponencial. Como a função exponencial é a inversa da função logarítmica, ressaltamos a importância do uso de logaritmos para resolução de problemas de Matemática Financeira em que a incógnita é o período de investimento. A respeito do uso de logaritmos em problemas de Matemática Financeira indicamos a leitura do capítulo "Aplicações" de [14].

5.2. Taxas proporcionais e equivalentes

Taxas proporcionais. Duas taxas são chamadas de taxas proporcionais se a razão entre elas é igual à razão dos períodos aos quais se referem quando expressos na mesma unidade de tempo, ver [18, p.59]. Ao falarmos em taxas proporcionais estaremos nos referindo ao regime de juros simples.

Exemplo 1. A taxa de 15% ao mês é proporcional à taxa de 0,5% ao dia.

De fato, expressando o período de tempo ao mês para a unidade de tempo ao dia, ou seja, 1 mês = 30 dias, temos a proporção:

$$\frac{15\%}{0,5\%} = \frac{30 \quad \text{dias}}{1 \text{ dia}}.$$

Taxas equivalentes. Duas taxas são chamadas de taxas equivalentes se, quando aplicadas ao mesmo capital inicial, por um mesmo período de tempo, produzem um mesmo montante.

Exemplo 2. A taxa de 0,5% ao dia é equivalente a taxa de 16,14% ao mês.

Detalharemos esse exemplo em breve. Por ora, observe que taxas proporcionais não são taxas equivalentes. Dessa forma, para fazer a conversão, por exemplo, de uma taxa mensal para uma taxa anual, ou vice-versa, no regime de juros compostos, não basta simplesmente multiplicar ou dividir a taxa por uma constante, como se faz nos juros simples. Por exemplo, é um erro achar que juros de 0,5% ao dia, no regime de juros compostos, equivalem a juros mensais de 30 x 0,5% = 15% ao mês, ver [17, p.92]. Na verdade, como citamos no exemplo 2.2, 0,5% ao dia equivale a juros mensais de 16,14%.

Para realizar essa conversão, inicialmente, definiremos i_m como sendo a taxa mensal e i_d como sendo a taxa diária. Da fórmula $M = c \text{ x } (1 + i)^t$, obtemos:

$$c \text{ x } (1 + i_m)^1 = c \text{ x } (1 + i_d)^{30}.$$

Daí, $i_m = (1 + i_d)^{30} - 1$.

Assim, podemos usar a equação $i_m = (1 + i_d)^{30} - 1$ para a conversão de uma taxa diária para a taxa mensal equivalente, ou vice-versa. No exemplo 2.2 temos $i_d = 0,5\%$. Logo, substituindo $i_d = 0,5\% = 0,005$ em $i_m = (1 + i_d)^{30} - 1$, obtemos

$$i_m = (1 + 0,005)^{30} - 1 = (1,005)^{30} - 1.$$

Lançando mão de uma calculadora científica calculamos i_m :

$$i_m \approx 1,1614 - 1,$$

isto é,

$$i_m \approx 0,1614.$$

Ou seja, $i_m \approx 16,14\%$.

Temos, para facilitar a conversão de vários períodos, a seguinte relação:

$$(1+i_d)^{360} = (1+i_m)^{12} = (1+i_b)^6 = (1+i_s)^2 = (1+i_a),$$

onde i_d, i_m, i_b, i_s, i_a são, respectivamente, taxas diária, mensal, bimestral, semestral e anual.

Daí, por exemplo, obtemos:

$$\text{a) } i_d = (1+i_a)^{\frac{1}{360}} - 1 \qquad \text{b) } i_m = (1+i_a)^{\frac{1}{12}} - 1$$

$$\text{c) } i_b = (1+i_a)^{\frac{1}{6}} - 1 \qquad \text{d) } i_s = (1+i_a)^{\frac{1}{2}} - 1$$

$$\text{e) } i_d = (1+i_m)^{\frac{1}{30}} - 1 \qquad \text{f) } i_m = (1+i_d)^{30} - 1.$$

Podemos dizer que no regime de juros simples, a classificação de duas taxas de juros como proporcionais ou equivalentes não fará diferença no resultado final. Isso, porém, não ocorre no regime de juros compostos, como vimos no exemplo anterior.

Agradecimentos

Este artigo é parte do meu Trabalho de Conclusão de Curso (TCC) do Profmat-Ufal. Agradeço ao Prof. Hilário Alencar pela sua orientação. Também sou grato à Larissa Cândido e à Milena Farias pelos comentários e sugestões.

Referências

[1] BANCO CENTRAL DO BRASIL. *Atas do Comitê de Política Monetária (Copom):* 232ª Reunião. Disponível em: <https://www.bcb.gov.br/publicacoes/atascopom/05082020>. Acesso em: 26 out. 2020.

[2] BANCO CENTRAL DO BRASIL. *Calculadora do cidadão*. Disponível em: <https://www3.bcb.gov.br/CALCIDADAO/jsp/index.jsp>. Acesso em: 01 out. 2020.

[3] BANCO CENTRAL DO BRASIL. *Comitê de Política Monetária (Copom)*. Disponível em: <https://www.bcb.gov.br/controleinflacao/copom>. Acesso em: 26 out. 2020.

[4] BANCO CENTRAL DO BRASIL. *Histórico das taxas de juros*. Disponível em: <https://www.bcb.gov.br/controleinflacao/historicotaxasjuros>. Acesso em: 03 nov. 2020.

[5] BANCO CENTRAL DO BRASIL. *Metas para a inflação*. Disponível em: <https://www.bcb.gov.br/controleinflacao/metainflacao>. Acesso em: 27 out. 2020.

[6] BANCO CENTRAL DO BRASIL. *O que é inflação*. Disponível em: <https://www.bcb.gov.br/controleinflacao/oqueinflacao>. Acesso em: 26 out. 2020.

[7] BANCO CENTRAL DO BRASIL. *Remuneração dos Depósitos de Poupança*. Disponível em: <https://www4.bcb.gov.br/pec/poupanca/poupanca.asp?frame=1>. Acesso em: 26 out. 2020.

[8] BRASIL. Instituto Brasileiro de Geografia e Estatística (IBGE). *Inflação*. Disponível em: <https://www.ibge.gov.br/explica/inflacao.php#:~:text=O%20governo%20federal%20usa%20,altera%C3%B5es%20na%20taxa%20de%20juros.>. Acesso em: 27 out. 2020.

[9] BRASIL. Ministério da Educação. *Base Nacional Comum Curricular (BNCC)*. 2018, 600p. Disponível em: <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>. Acesso em: 20 out. 2020.

[10] BRASIL. Ministério da Educação. Conselho Nacional de Educação. *Resolução nº 4, de 17 de dezembro de 2018*. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-n-4-de-17-de-dezembro-de-2018-55640090>. Acesso em: 25 out. 2020.

[11] BTG PACTUAL. *Letra de Crédito de Agronegócio*. Disponível em: <https://www.btgpactualdigital.com/renda-fixa/lca>. Acesso em: 29 out. 2020.

[12] BTG PACTUAL. *Letra de Crédito Imobiliário*. Disponível em: <https://www.btgpactualdigital.com/renda-fixa/lci>. Acesso em: 29 out. 2020.

[13] FARIAS, M.; CÂNDIDO, L. Uso de materiais didático-pedagógicos lúdicos por egressos do Profmat e sua influência no aprendizado em Matemática em Alagoas. *Revista de Ensino de Ciências e Matemática,* v. 10, n°6, pp.340-359, 2019.

[14] LIMA, E. L. *Logaritmos*. 2ª ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 1996.

[15] MATHIAS, C. V.; ALENCAR, H.; LEIVAS, J. C. P. Provas sem palavras, visualização, animação e GeoGebra. *Revista do Instituto Geogebra Internacional de São Paulo,* v. 8, n°2, pp.62-77, 2019.

[16] MENDES, C. M.; TREDEZINI, C. A. de O.; BORGES, F. T. de M.; FAGUNDES, M. B. B. *Introdução à Economia*. 3ª ed. Florianópolis: Departamento de Ciências da Administração/UFSC, 2015.

[17] MORGADO, A. C.; CARVALHO, P. C. P. *Matemática Discreta*. 2ª ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2015.

[18] MORGADO, A. C.; WAGNER, E.; ZANI, S.C. *Progressões e Matemática Financeira*. 6ª ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2015.

[19] NETO, A. *Matemática Financeira e suas Aplicações*. 12.ª ed. São Paulo: Atlas, 2012.

[20] PORTAL DO INVESTIDOR. *CDB (Certificado de Depósito Bancário) e RDB (Recibo de Depósito Bancário)*. Disponível em: <https://www.investidor.gov.br/menu/Menu_Investidor/Old/Valores_Mobiliarios/CDB_RDB.html>. Acesso em: 29 out. 2020.

[21] PORTAL DO INVESTIDOR. *Títulos Públicos*. Disponível em: <https://www.investidor.gov.br/menu/primeiros_passos/Investindo/Tipos_Investimento/Titulos_publicos.html>. Acesso em: 20 out. 2020.

[22] RODRIGUES, G. F.; OLIVEIRA, E. D. de. O uso do GeoGebra no ensino de elipse nas aulas de matemática da Educação Básica. *Revista Professor de Matemática Online,* v. 5, n°1, pp.11-30, 2017.

[23] TESOURO DIRETO. *Bancos e corretoras habilitados*. Disponível em: <https://www.tesourodireto.com.br/conheca/bancos-e-corretoras.htm>. Acesso em: 28 out. 2020.

[24] TESOURO DIRETO. *Calculadora*. Disponível em: <https://www.tesourodireto.com.br/titulos/calculadora.htm>. Acesso em: 28 set. 2020.

[25] TESOURO DIRETO. *Conceitos básicos sobre impostos e taxas*. Disponível em: <https://www.tesourodireto.com.br/videos/impostos-e-taxas-tesouro-direto.htm>. Acesso em: 28 out. 2020.

[26] TESOURO DIRETO. *Confira a rentabilidade de cada título*. Disponível em: <https://www.tesourodireto.com.br/titulos/precos-e-taxas.htm>. Acesso em: 28 set. 2020.

[27] TESOURO DIRETO. *Conheça o tesouro direto:* tudo o que você precisa saber sobre o tesouro. Disponível em: <https://www.tesourodireto.com.br/conheca/conheca-o-tesouro-direto.htm>. Acesso em: 20 out. 2020.

[28] TESOURO DIRETO. *Conheça o Tesouro Nacional e os seus objetivos*. Disponível em: <https://www.tesourodireto.com.br/conheca/institucional.htm>. Acesso em: 31 out. 2020.

[29] TESOURO DIRETO. *Entenda a tabela de preços e taxas*. Disponível em: <https://www.tesourodireto.com.br/data/files/D4/02/8D/39/875FB610FAC28EB6018E28A8/Entenda_tabela.pdf>. Acesso em: 09 nov. 2020.

[30] TESOURO DIRETO. *Módulo 3:* Curso avançado do Tesouro Direto. Disponível em: <https://www.tesourodireto.com.br/data/files/18/A1/2B/35/855FB610FAC28EB6018E28A8/Modulo%203_TesouroDireto%20_2017_.pdf>. Acesso em: 10 nov. 2020.

[31] TESOURO DIRETO. *Saiba as regras do investimento*. Disponível em: <https://www.tesourodireto.com.br/conheca/>. Acesso em: 20 out. 2020.

[32] TESOURO DIRETO. *Site oficial do tesouro direto*. Disponível em: <https://www.tesourodireto.com.br>. Acesso em: 28 set. 2020.

Luiz Eduardo da Silva Gomes
Escola Estadual Onélia Campelo
57075-655, Maceió, Alagoas, Brasil
<luiz.edu.work@gmail.com>

Recebido: 03/11/2020
Publicado: 23/12/2020