CLESSIUS SILVA
MARCELO PEDRO DOS SANTOS
TARCIANA MARIA SANTOS DA SILVA
Organizadores

COLETÂNEA DE ESTUDOS DE EGRESSOS

PROFMAT- UFRPE

VOL 3

Organizadores:
Clessius Silva
Marcelo Pedro dos Santos
Tarciana Maria Santos da Silva

Coletânea de Estudos de Egressos do PROFMAT-UFRPE

Volume III

1ª Edição

Recife
UFRPE
2026

UNIVERSIDADE FEDERAL RURAL
DE PERNAMBUCO - UFRPE

EDITORA UNIVERSITÁRIA DA UFRPE

Organizadores:
Clessius Silva
Marcelo Pedro dos Santos
Tarciana Maria Santos da Silva

Capa
Istockphoto stock images

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Bibliotecária Suely Manzi – CRB/4 - 809

C694 Coletânea de estudos de egressos do PROFMAT-UFRPE / Clessius Silva, Marcelo Pedro dos Santos, Tarciana Maria Santos da Silva, organizadores. – 1. ed. - Recife: EDUFRPE, 2026.
v. 3, 136 p. : il.

Obra publicada em ebook.
Inclui referências.

.1. Educação básica 2. Recursos eletrônicos de informação 3. Matemática – Estudo e ensino 4. Professores de matemática 5. Matemática – Metodologia I. Silva, Clessius, org. II. Santos, Marcelo Pedro dos, org. III. Silva, Tarciana Maria Santos da, org.

CDD 510.7

ISBN FÍSICO nº 978-65-86466-97-3
ISBN DIGITAL nº 978-65-86466-01-0

Sumário

Prefácio

Clessius Silva
Marcelo Pedro dos Santos
Tarciana Maria Santos da Silva

Apresentamos o Volume III da Coletânea de Estudos de Egressos do PROFMAT-UFRPE. Ao longo de seus 113 anos, a Universidade Federal Rural de Pernambuco (UFRPE) consolidou-se como uma instituição de excelência, dedicada ao ensino, à pesquisa e à extensão. Nesse cenário, o Departamento de Matemática destaca-se por suas múltiplas ações e pela oferta do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), coordenado pela Sociedade Brasileira de Matemática (SBM). Lançado em 2011 com o objetivo de transformar o ensino da Matemática no Brasil, o programa abrange hoje quase 80 polos e é reconhecido por sua excelência, mantendo o conceito 5 em avaliações consecutivas da CAPES.

Esta coletânea abarca perspectivas e temas extraídos de algumas das mais de 140 dissertações defendidas no PROFMAT-UFRPE. O resultado é um mosaico de experiências, reflexões e descobertas que evidenciam a riqueza do ensino matemático. Distribuído em cinco capítulos, este terceiro volume constitui um relevante registro histórico e uma expressiva contribuição científica para a formação continuada e a prática docente, conforme detalhado nas seções a seguir.

Estrutura do livro

Capítulo 1: "O Teorema de Chebyshev e o Fascinante Mundo dos Números Primos"- Este trabalho estuda a distribuição dos números primos com base no Teorema de Chebyshev, utilizando exclusivamente resultados matemáticos elementares. Adicionalmente, o texto explora as propriedades, características e os principais resultados referentes aos primos de Fermat, de Mersenne e de Sophie Germain.

Capítulo 2: "Um Estudo Sobre Questões de Geometria do Saepe do 3º Ano do Ensino Médio"-Este trabalho tem o objetivo de investigar as questões de Geometria do Sistema de Avaliação da Educação Básica de Pernambuco (SAEPE) referentes aos anos de 2019, 2021 e 2022, buscando identificar as principais dificuldades enfrentadas pelos estudantes nesse eixo temático. A partir da análise dos itens, o estudo caracteriza os descritores abordados em cada avaliação, apresenta as soluções para as questões de Geometria e propõe sequências didáticas focadas nos temas mais recorrentes. O intuito é subsidiar a prática docente e contribuir para o desenvolvimento da aprendizagem geométrica em sala de aula.

Capítulo 3: "Criptografia Rsa para o Ensino Médio" Este trabalho traz ao conhecimento dos estudantes do Ensino Médio, a importância da criptografia RSA. Além de levar o conhecimento dessa ferramenta de uso no mundo, o trabalho propõe atividades aplicadas em sala de aula simulando a codificação e decodificação de mensagens e chaves públicas geradas na própria sala de aula.

Capítulo 4: "A Teoria de Resposta ao Item como Instrumento de elaboração de Testes para Professores de Matemática"- Neste estudo, examina-se detalhadamente a Teoria da Resposta ao Item (TRI), abordando desde o seu histórico e conceitos básicos até os modelos logísticos e a curva de probabilidade de acerto. Analisam-se, também, a estimação das habilidades e dos parâmetros dos itens, além da estruturação e interpretação das escalas de medida. Destaca-se a aplicação do software EIRT para a geração e análise estatística de dados via TRI. Espera-se que a articulação entre esses elementos teóricos e práticos forneça subsídios para que os professores avaliem suas metodologias e proponham ações de melhoria educacional.

Capítulo 5: "O Uso de Recursos Digitais por Alunos do Ensino Médio no Estudo de Operações Com Frações"-O impacto dos recursos digitais na aprendizagem de operações com frações no Ensino Médio é investigado neste estudo, amparado pelas orientações curriculares sobre tecnologias educacionais. Foram propostas cinco atividades nas plataformas PhET e GeoGebra em duas escolas, avaliadas posteriormente via questionário. Verificou-se uma defasagem na compreensão da multiplicação e divisão de frações sem o uso de regras padronizadas. Em contrapartida, notou-se que as ferramentas interativas contribuíram para o aprimoramento da aprendizagem sobre o conceito geral de frações, números mistos e operações básicas com denominadores distintos.

Ao longo desta coletânea, convidamos o leitor a explorar uma diversidade de aplicações, inspirações e descobertas voltadas ao Ensino de Matemática, fruto das pesquisas de docentes que agora integram o quadro de egressos do PROFMAT-UFRPE. Cada capítulo compõe uma parte fundamental do complexo cenário que é a docência na Educação Básica. Esperamos que esta leitura enriqueça sua compreensão e estimule novas reflexões sobre o nosso papel na educação, em especial no ensino da Matemática.

1 O Teorema de Chebyshev e o Fascinante Mundo dos Números Primos

Ma. Janaína Mirele de Lima Silva[1]
Rodrigo Genuino Clemente[2]

Resumo: Objeto de fascínio para matemáticos em todo o mundo, os números primos e suas propriedades são utilizados em diversos conteúdos da matemática. Como os primos não possuem um padrão que permita identificar o próximo número da sequência, a distribuição dos primos em relação aos números naturais é um campo da teoria que continua a ser aprimorado. Tendo em vista seu papel fundamental na criptografia, que utiliza o produto de primos de ordem maior ou igual a 10^{100} para proteção dos dados, e a certeza da infinitude desses números, estudamos a distribuição dos primos a partir do Teorema de Chebyshev, que utiliza apenas resultados elementares da matemática. Continuamos nossa exploração pelo mundo dos primos, apresentando características, curiosidades e resultados sobre os primos de Fermat, Mersenne e Sophie Germain.

Palavras-chave: Números Primos. Teorema de Chebyshev. Teorema do Número Primo.

1.1 Introdução

Os Números Primos, isto é, aqueles maiores que 1 que são divisíveis apenas por 1 e por ele mesmo, têm sido objeto de curiosidade e fascínio pelos matemáticos há muitos anos. Desde a Grécia Antiga, as propriedades místicas e numerológicas dos primos levaram os matemáticos da época a desenvolverem diversos resultados importantes, que utilizamos até os dias atuais.

Os primos e suas propriedades são utilizados em diversos resultados da matemática. Apresentados desde a educação básica, aparecem na Base Nacional Comum Curricular (BNCC) (BRASIL, 2018) entre as habilidades a serem desenvolvidas com os estudantes do sexto ano do Ensino Fundamental e, apesar de não ser citada diretamente na BNCC do Ensino Médio, a decomposição em fatores primos é utilizada nos cálculos de mínimo múltiplo comum (MMC), máximo divisor comum (MDC), para encontrar raízes n-ésimas, entre outros.

Além de sua importância para a matemática, os números primos desempenham papel fundamental na criptografia. Como a finalidade da criptografia é impedir que senhas e mensagens sejam invadidas por pessoas não autorizadas e mal-intencionadas, a dificuldade em fatorar o produto de primos grandes torna seu uso pertinente.

[1] Secretaria de Educação e Esportes de Pernambuco, jmirele12@gmail.com
[2] Universidade Federal Rural de Pernambuco, rodrigo.clemente@ufrpe.br

A possibilidade de enviar informações secretas é um problema antigo da nossa sociedade e que foi sendo aperfeiçoado com o passar dos anos. Em 1976, surgiu a ideia de criptografia com chave pública, na qual o usuário define as chaves para encifrar as mensagens que irá receber e conhece o algoritmo necessário para decifrá-las, de modo que o acesso às chaves não permite a descoberta do algoritmo para decodificar as informações (LEMOS, 2010).

O primeiro sistema empregando o conceito de chave pública surgiu apenas dois anos depois, utilizando o produto de números primos grandes, e foi denominado RSA em virtude dos sobrenomes de seus criadores: Rivest, Shamir e Adleman. Por exemplo, é fácil encontrar a fatoração do número 10.961 e descobrir que ele é decorrência do produto de 97 e 113. Porém, encontrar os primos que geram o número 2.266.784.329 se torna uma tarefa bem mais complicada.

Como a descoberta dos fatores primos multiplicados é necessária para decifrar a mensagem, a criptografia utiliza números primos da ordem maior ou igual a 10^{100}, o que torna essa tarefa humanamente impossível de ser realizada. Os valores são tão grandes que levaria anos para um computador de alto desempenho encontrar os fatores e, até lá, a informação decifrada já teria se tornado inútil, daí a busca por primos cada vez maiores.

Euclides provou que existem infinitos números primos em 300 a. C. e a demonstração de que todo número natural é primo ou produto de primos é tão importante que conhecemos como o Teorema Fundamental da Aritmética. Entretanto, a distribuição dos primos em relação à infinitude de naturais ainda é um campo da teoria que tem sido aperfeiçoado.

Uma dificuldade no estudo da distribuição dos primos é que eles não possuem um padrão que permite identificar qual será o próximo. Observe a sequência dos primos menores que 100:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Nesse pequeno intervalo analisado, note que a diferença de um primo para o próximo variou entre 1, 2, 4, 6 e 8, e não seguiu uma ordem, o que dificulta a descoberta dos próximos primos da sequência. À medida em que analisamos números muito grandes, fica ainda mais difícil identificar se é um número composto ou não, sendo necessário o uso de tecnologias digitais.

Descoberto em 2018, o maior primo conhecido atualmente é o $2^{82.589.933} - 1$, que possui mais de 24 milhões de dígitos. O número foi encontrado por um norte-americano utilizando o aplicativo gratuito Great Internet Mersenne Prime Search (GIMPS), software que realiza a busca por Primos de Mersenne, sendo uma recompensa em dinheiro oferecida a quem for bem sucedido em sua procura (WOLTMAN, 1996).

Desde sua criação em 1996, o GIMPS contribuiu para a descoberta de 17 primos de Mersenne, porém, mesmo com o uso de tecnologia, tais descobertas são raras e exigem muito tempo. Para provar que $2^{82.589.933} - 1$ é um primo, por exemplo, foram necessários

12 dias ininterruptos de teste por um computador para ter certeza que ele não é divisível por nenhum número menor que ele.

Assim, este trabalho tem como objetivo geral estudar a distribuição dos números primos a partir do Teorema de Chebyshev, utilizando resultados elementares e conhecidos na matemática, em especial o estudo da função $\pi(x)$, que determina a quantidade de primos menores ou igual a x. Como objetivos específicos temos: compreender as propriedades elementares da função $\pi(x)$; demonstrar o Teorema de Chebyshev; explorar resultados acerca dos primos de Fermat, Mersenne e Sophie Germain; além de resolver problemas de competições matemáticas envolvendo números primos.

Vale ressaltar que o estudo dos números primos é um campo de estudo bastante amplo e, por isso, é praticamente impossível reuní-lo em um único documento. Dessa forma, esperamos que esse trabalho sirva de suporte para professores e estudantes que desejam expandir seus conhecimentos, bem como auxilie na elaboração de material para preparação de olimpíadas e no desenvolvimento de projetos acerca do tema.

1.2 Distribuição dos Números Primos

Nesta sessão, apresentaremos resultados elementares da matemática e a prova do Teorema de Chebyshev, utilizando o trabalho de (ANDREWS, 1971) como referência.

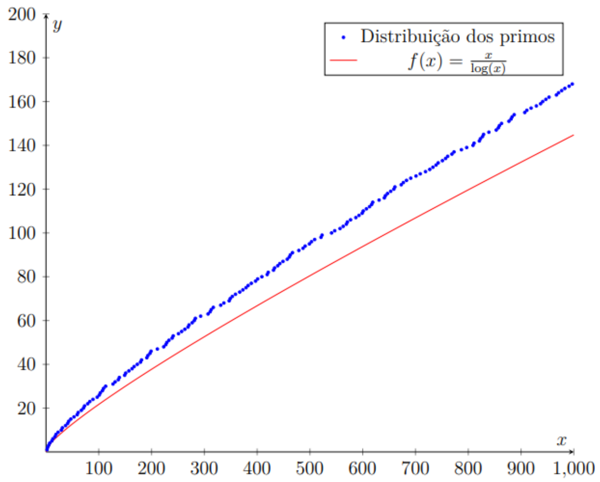
A sequência dos números primos sempre foi um tema fascinante para os matemáticos, sejam eles profissionais ou amadores. Compreender como os primos estão distribuídos entre os naturais é uma discussão que surgiu há muitos anos e ainda continua sendo objeto de interesse dos pesquisadores nos dias atuais.

Gauss foi o primeiro a dar atenção à função $\pi(x)$, o número de primos que não excede x. Ao observar que os valores de $\pi(x)$ eram dados aproximadamente por $x/\log x$, ele conjecturou que

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Tal afirmação ficou conhecida como o Teorema do Número Primo e prevê como se comporta a distribuição dos primos. A Figura 1 exibe o gráfico da função $f(x) = x/\log x$, frequentemente utilizada como estimativa para a quantidade de números primos menores ou iguais a x, evidenciando sua semelhança com a distribuição dos primos até mil.

Figura 1 – Comparação gráfica entre $f(x) = \dfrac{x}{\log x}$ e a distribuição dos primos até mil



Fonte: Produzido pelos autores

A prova dessa conjectura se mostrou extremamente difícil e, apesar de muitos matemáticos tentarem, quase cem anos se passaram até conhecermos sua demonstração. A prova foi publicada em 1896, quando Hadamard e de la Vallée Poussin conseguiram demonstrar o resultado utilizando a função zeta de Riemann e outras técnicas sofisticadas da análise complexa (ANDREWS, 1971).

Outras demonstrações desse teorema foram desenvolvidas ao longo dos anos, contudo ainda fazendo uso de técnicas complexas. Somente em 1949, Selberg e Erdös conseguiram demonstrar o teorema sem o uso das variáveis complexas, entretanto, essa prova é longa e de difícil compreensão, assim como todas as outras conhecidas até o momento.

Como tais demonstrações estão distantes do interesse deste trabalho, optamos por estudar a organização dos números primos por meio de um resultado semelhante, mas que pode ser provado utilizando apenas propriedades elementares da matemática: o Teorema de Chebyshev.

Chebyshev utilizou os coeficientes binomiais centrais para deduzir resultados acerca dos números primos e provou que existem constantes positivas c_1 e c_2 tais que

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x},$$

para todo $x \geq 2$.

Contudo, antes de demonstrar o Teorema de Chebyshev, precisamos analisar e compreender alguns resultados simples acerca de $\pi(x)$.

1.2.1 Propriedades elementares

A seguir apresentaremos algumas propriedades elementares da matemática necessárias para a demonstração do Teorema de Chebyshev.

Definição 1.1 *Dado $x \in \mathbb{R}$, definimos o piso ou parte inteira de x pelo número inteiro que satisfaz a desigualdade $x - 1 < \lfloor x \rfloor \leq x$ ou pela equivalente $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.*

Teorema 1 *Sejam n um inteiro positivo e p um primo, então $\displaystyle\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$ é o exponente de p que aparece na decomposição em fatores primos de $n!$.*

Demonstração 1.1 *Note que se $p > n$, então p não aparece na decomposição em fatores primos de $n!$ e cada termo em $\displaystyle\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$ é zero, como desejamos. Se $p \leq n$, então $\left\lfloor \frac{n}{p} \right\rfloor$ inteiros em $\{1, 2, ..., n\}$ são divisíveis por p, isto é,*

$$p, 2p, 3p, ..., \left\lfloor \frac{n}{p} \right\rfloor p.$$

Desses inteiros, $\left\lfloor \frac{n}{p^2} \right\rfloor$ também são divisíveis por p:

$$p^2, 2p^2, ..., \left\lfloor \frac{n}{p^2} \right\rfloor p^2.$$

Analogamente, $\left\lfloor \frac{n}{p^3} \right\rfloor$ desses inteiros são divisíveis por p uma terceira vez:

$$p^3, 2p^3, ..., \left\lfloor \frac{n}{p^3} \right\rfloor p^3.$$

Após finitas repetições desse argumento, podemos concluir que p divide números em $\{1, 2, ..., n\}$ exatamente $\displaystyle\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$ vezes. Assim, essa soma é o expoente de p que aparece na decomposição em fatores primos de $n!$.

Teorema 2 *Dado $\lfloor x \rfloor$, temos $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$.*

Demonstração 1.2 *Pela definição de $\lfloor x \rfloor$ temos $x - 1 < \lfloor x \rfloor \leq x$. Consequentemente,*

$$2x - 1 < \lfloor 2x \rfloor \leq 2x,$$

e

$$2x - 2 < 2\lfloor x \rfloor \leq 2x.$$

Multiplicando a segunda desigualdade por (-1) e somando à primeira, segue que

$$-1 < \lfloor 2x \rfloor - 2\lfloor x \rfloor < 2.$$

Entretanto, $\lfloor 2x \rfloor - 2\lfloor x \rfloor$ é um inteiro e os únicos inteiros no intervalo $(-1, 2)$ são 0 e 1. Logo, $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$.

Definição 1.2 *O coeficiente binomial* $\binom{n}{k}$ *é o número de formas possíveis de escolher* k *elementos entre as* n *possibilidades. Por se tratar de uma combinação em que não importa a ordem dos fatores, pode ser calculado pela expressão*

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}.$$

Teorema 3 (Relação de Stifel) *Dados* n *e* i *inteiros, com* $0 \leq i \leq n$*, temos*

$$\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}.$$

Demonstração 1.3 *Podemos demonstrar a Relação de Stifel utilizando a definição de coeficiente binomial apresentada anteriormente.*

$$\begin{aligned}
\binom{n}{i} + \binom{n}{i+1} &= \frac{n!}{(n-i)!\ i!} + \frac{n!}{(n-i-1)!(i+1)!} \\
&= \frac{n!}{(n-i)(n-i-1)!\ i!} + \frac{n!}{(n-i-1)!(i+1)\ i!} \\
&= \frac{(i+1)\ n! + (n-i)\ n!}{(n-i)(n-i-1)!(i+1)\ i!} \\
&= \frac{(i+1+n-i)\ n!}{(n-i)!\ (i+1)!} \\
&= \frac{(n+1)\ n!}{(n-i)!(i+1)!} \\
&= \frac{(n+1)!}{(n-i)!(i+1)!} \\
&= \binom{n+1}{i+1}.
\end{aligned}$$

Teorema 4 (Teorema Binomial) *Sejam* x *e* y *números reais e* $n \in \mathbb{N}$*, temos que*

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \ldots + \binom{n}{n-1} x y^{n-1} + y^n.$$

Demonstração 1.4 *Vamos demonstrar a relação utilizando indução matemática em* n*. Para* $n = 0$*, temos* $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0$*. Logo, a relação é válida para* $n = 0$*. Para* $n = 1$ *a igualdade também é válida, pois* $(x+y)^1 = \binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1 = x + y$*. Agora suponha que a relação é válida para algum* $n \geq 1$*. Vamos mostrar que também vale para* $n+1$*. Note que*

$$(x+y)^{n+1} = (x+y) \cdot (x+y)^n.$$

Por hipótese de indução, segue que

$$(x+y)^{n+1} = (x+y) \cdot \left[\binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \ldots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n \right].$$

Aplicando a propriedade distributiva da adição, temos

$$(x+y)^{n+1} = x \cdot \left[\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + ... + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\right]$$
$$+ y \cdot \left[\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + ... + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\right].$$

Daí,

$$(x+y)^{n+1} = \binom{n}{0}x^{n+1} + \binom{n}{1}x^n y^1 + ... + \binom{n}{n-1}x^2y^{n-1} + \binom{n}{n}x^1y^n$$
$$+ \binom{n}{0}x^n y^1 + \binom{n}{1}x^{n-1}y^2 + ... + \binom{n}{n-1}x^1y^n + \binom{n}{n}y^{n+1}.$$

Organizando os termos com o mesmo fator temos

$$(x+y)^{n+1} = \binom{n}{0}x^{n+1} + \left[\binom{n}{0} + \binom{n}{1}\right]x^n y^1 + \cdots + \left[\binom{n}{n-1} + \binom{n}{n}\right]x^1y^n + \binom{n}{n}y^{n+1}.$$

Pela Relação de Stifel (3), segue que

$$(x+y)^{n+1} = \binom{n}{0}x^{n+1} + \binom{n+1}{1}x^n y^1 + ... + \binom{n+1}{n}x^1y^n + \binom{n}{n}y^{n+1}.$$

Por conveniência, podemos escrever $\binom{n}{0} = \binom{n+1}{0}$ *e* $\binom{n}{n} = \binom{n+1}{n+1}$. *Logo,*

$$(x+y)^{n+1} = \binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n y^1 + ... + \binom{n+1}{n}x^1y^n + \binom{n+1}{n+1}y^{n+1}.$$

Assim, a relação é válida para $n+1$ e, consequentemente, para todo n natural.

Teorema 5 *Se* $f(x) = \dfrac{x}{\log x}$, *então:*

1. $f(x)$ *é crescente para* $x > e$;
2. $f(x-2) > \frac{f(x)}{2}$ *para* $x \geq 4$;
3. $f\left(\frac{x+2}{2}\right) < \frac{15f(x)}{16}$ *para todo* $x \geq 8$.

Demonstração 1.5 *Como*

$$f'(x) = \frac{\log x - 1}{(\log x)^2},$$

podemos ver que $f'(x) > 0$ para $x > e$, o que prova (1). Para provar (2), note que se $x \geq 4$, então $x - 4 \geq 0$. Daí, $2x - 4 \geq x$, isto é, $x - 2 \geq x/2$. Assim,

$$f(x-2) = \frac{x-2}{\log(x-2)} \geq \frac{x}{2\log(x-2)} > \frac{x}{2\log x} = \frac{1}{2}f(x).$$

Para provar (3), observe que se $x \geq 8$, $x^3 \geq 8x^2$. Daí $(x/2)^3 \geq x^2$, isto é, $x/2 \geq x^{2/3}$. Além disso, $5x \geq 4x + 8$, logo $x + 2 \leq 5x/4$. Portanto,

$$f\left(\frac{x+2}{2}\right) = \frac{x+2}{2\log((x+2)/2)} < \frac{x+2}{2\log(x/2)} \leq \frac{x+2}{2\log x^{2/3}} \leq \frac{5x/4}{\frac{4\log x}{3}} = \frac{15}{16}f(x).$$

As propriedades demonstradas a seguir estão diretamente relacionadas à função $\pi(x)$. A primeira trata da infinitude dos números primos, provada pelo famoso matemático grego Euclides utilizando a ideia de contradição.

Teorema 6 $\lim_{x \to \infty} \pi(x) = +\infty$, *isto é, existem infinitos números primos.*

Demonstração 1.6 *Suponha que existe um número finito de primos,* p_1, p_2, p_3, ..., p_n. *Considere* $M = p_1 p_2 ... p_n + 1$. *É fácil ver que se dividirmos* M *por qualquer um dos primos* p_1, p_2, ..., p_n, *o resto é 1. Assim, pela nossa hipótese de que há finitos números primos, deduzimos que* M *não possui decomposição em fatores primos. Como isso contradiz o Teorema Fundamental da Aritmética, a única conclusão possível é que há infinitos números primos. Logo,* $\lim_{x \to \infty} \pi(x) = +\infty$.

Por outro lado, é fácil ver que $\pi(x) \leq x$. Os três teoremas a seguir mostram que $\pi(x)$ é, na verdade, muito menor que x e, para demonstrá-los, precisamos conhecer a função ϕ de Euler.

Definição 1.3 *A Função Totiente ou Função* ϕ *de Euler associa a um número inteiro positivo* n *a quantidade de inteiros positivos menores que* n *que são relativamente primos com* n. *Denotaremos por* $\phi(n)$.

Exemplo 1 *Temos* $\phi(10) = 4$, *pois os números 1, 3, 7 e 9 são menores que 10 e relativamente primos com 10.*

Teorema 7 *Se* k *é um inteiro positivo qualquer,*

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}.$$

Demonstração 1.7 *Seja* $\lfloor x \rfloor = kl + r$, *com* $0 \leq r < k$ *e* $\lfloor x \rfloor$ *indicando o maior inteiro que não excede* x. *Podemos dividir os inteiros do intervalo* $[1, x]$ *em* l *conjuntos de* k *inteiros consecutivos mais um conjunto com os* r *inteiros restantes* $kl+1, kl+2, ..., kl+r$. *Entre os inteiros* $1, 2, ..., k$ *há, no máximo,* k *primos. Entre os inteiros* $k+1, k+2, ..., 2k$, *há no máximo* $\phi(k)$ *primos, visto que qualquer inteiro não relativamente primo com* k *tem um fator primo de* k *que é menor ou igual a* k. *Analogamente, em cada conjunto de* k *inteiros consecutivos restante há no máximo* $\phi(k)$ *primos. Por fim, no conjunto de* r *inteiros restante, há no máximo* r *primos. Consequentemente,*

$$\pi(x) \leq k + (l-1)\phi(k) + r \leq 2k + \frac{x}{k}\phi(k).$$

Daí,

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}.$$

O próximo resultado permite estimar o tamanho de $\dfrac{\phi(x)}{k}$.

Teorema 8 *Se $M > 1$ e $p_1, p_2, ..., p_s$ são todos os primos em $\{1, 2, ..., M\}$, então*

$$\sum_{n=1}^{M} \frac{1}{n} < \frac{1}{\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_s}\right)}.$$

Demonstração 1.8 *Da fórmula para a soma de uma série geométrica temos, para cada primo p,*

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ...$$

Consequentemente,

$$\frac{1}{\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_s}\right)} =$$
$$\left(1 + \frac{1}{p_1} + \frac{1}{{p_1}^2} + \frac{1}{{p_1}^3} + ...\right) \cdot \left(1 + \frac{1}{p_2} + \frac{1}{{p_2}^2} + \frac{1}{{p_2}^3} + ...\right) ... \left(1 + \frac{1}{p_s} + \frac{1}{{p_s}^2} + \frac{1}{{p_s}^3} + ...\right)$$
$$= \sum_{n \in \Lambda} \frac{1}{n} > \sum_{n \leq M} \frac{1}{n}$$

em que Λ é o conjunto de todos os inteiros nos quais o maior fator primo é M. É fácil ver que a última igualdade é verdadeira, visto que multiplicando essas séries temos todos os possíveis termos da forma $\frac{1}{{p_1}^{\alpha_1}{p_2}^{\alpha_2}...{p_s}^{\alpha_s}}$, com $p_i \leq M$.

O próximo teorema mostra que $\pi(x)$ é muito menor que x, mas ainda precisamos de mais ferramentas antes de provar o resultado de Chebyshev, que explicitamente descreve o quão pequena é $\pi(x)$.

Teorema 9 $\lim_{x \to \infty} \frac{\pi(x)}{x} = 0.$

Demonstração 1.9 *Como $\frac{\pi(x)}{x} \geq 0$ para todo $x > 0$, precisamos mostrar que podemos fazer $\frac{\pi(x)}{x}$ arbitrariamente pequeno escolhendo x suficientemente grande. O Teorema 7 estabeleceu que*

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}$$

para cada inteiro positivo k. Seja M um inteiro grande e $k = p_1 p_2 ... p_s$, em que $\{p_1, p_2, ..., p_s\}$ é o conjunto de todos os primos que não excedem M. Daí

$$\frac{\phi(k)}{k} = \frac{k\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_s}\right)}{k}$$
$$= \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_s}\right) < \left(\sum_{n=1}^{M} \frac{1}{n}\right)^{-1}.$$

Assim,

$$\frac{\pi(x)}{x} \leq \left(\sum_{n=1}^{M} \frac{1}{n}\right)^{-1} + \frac{2p_1p_2...p_s}{x}. \tag{1.1}$$

Agora basta fazer $\dfrac{\pi(x)}{x}$ *tão pequeno quanto desejarmos. Como* $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n}$ *é uma série divergente (ANDREWS, 1971), podemos escolher* M *grande de modo que* $\displaystyle\sum_{n=1}^{M}\frac{1}{n} > \frac{2}{\epsilon}$*, em que* $\epsilon > 0$ *é um número positivo arbitrário. Daí, para* $x > \dfrac{4p_1p_2...p_s}{\epsilon}$*, temos*

$$\frac{2k}{x} < \frac{2p_1p_2...p_s}{\frac{4p_1p_2...p_s}{\epsilon}} = \frac{2p_1p_2...p_s\epsilon}{4p_1p_2...p_s} = \frac{\epsilon}{2}.$$

Logo,

$$\frac{\pi(x)}{x} < \frac{\epsilon}{2} + \frac{2p_1p_2...p_s\epsilon}{4p_1p_2...p_s} = \epsilon.$$

Para concluir nossa seção de propriedades elementares, vamos apresentar dois resultados complementares para provar o Teorema de Chebyshev.

Lema 1.1 *Dado* $x \geq 5$*, temos* $\pi(x) \geq \pi\left(2\left\lfloor\frac{x}{2}\right\rfloor\right)$.

Demonstração 1.10 *Pela definição de* $\lfloor x \rfloor$*, temos*

$$\frac{x}{2} - 1 < \left\lfloor\frac{x}{2}\right\rfloor \leq \frac{x}{2},$$

isto é,

$$x - 2 < 2\left\lfloor\frac{x}{2}\right\rfloor \leq x.$$

Como $x \geq 2\left\lfloor\frac{x}{2}\right\rfloor$ *e* $\pi(x)$ *é monótona, segue o resultado.*

Lema 1.2 *Para* $x \geq 8$*, temos*

$$\pi(x+1) \leq \pi\left(2\left\lfloor\frac{x+2}{2}\right\rfloor\right).$$

Demonstração 1.11 *Pela definição de* $\lfloor x \rfloor$*, para* x *par, temos* $2\left\lfloor\frac{x+2}{2}\right\rfloor = 2\left(\frac{x+2}{2}\right) = x+2$*. Quando* x *é ímpar, temos* $2\left\lfloor\frac{x+2}{2}\right\rfloor = 2\left(\frac{x+1}{2}\right) = x+1$*. Daí, segue que* $x+1 \leq 2\left\lfloor\frac{x+2}{2}\right\rfloor$ *e, como* $\pi(x)$ *é monótona, segue o resultado.*

1.2.2 Teorema de Chebyshev

Após o estudo das propriedades da função $\pi(x)$, estamos prontos para provar o Teorema de Chebyshev. Vale ressaltar que a demonstração apresentada a seguir é realizada utilizando apenas as propriedades matemáticas elementares. Além disso, quanto mais próximas de 1 forem as constantes c_1 e c_2, mais técnica fica a demonstração. Assim, iremos mostrar que $c_1 = \dfrac{\log 2}{4}$ e $c_2 = 30(\log 2)$ funcionam.

Teorema 10 (Chebyshev) *Para $x \geq 8$,*

$$\frac{\log 2}{4} \cdot \frac{x}{\log x} < \pi(x) < 30(\log 2)\frac{x}{\log x}.$$

Demonstração 1.12 *Vamos começar provando a desigualdade do lado esquerdo. Observe o coeficiente binomial $\binom{2n}{n}$, isto é, o número de combinações de $2n$ objetos distintos tomados n a n. Por definição, temos*

$$\binom{2n}{n} = \frac{(2n!)}{(n!)(n!)} = \frac{2n(2n-1)...(n+1)}{n(n-1)...1}.$$

Agora, cada primo p no intervalo $(n, 2n]$ deve aparecer como fator do numerador de $\binom{2n}{n}$. Uma vez que não pode aparecer no denominador (porque é maior que n), podemos ver que $p \Bigm| \binom{2n}{n}$. Daí, multiplicando todos esses primos temos

$$P_n \Bigm| \binom{2n}{n},$$

em que P_n denota o produto de todos os primos maiores que n que não excedem $2n$. Assim, como cada primo que aparece como fator de P_n é maior que n e como existem $\pi(2n) - \pi(n)$ fatores primos de P_n, podemos ver que

$$n^{\pi(2n)-\pi(n)} < P_n < \binom{2n}{n}. \tag{1.2}$$

Por outro lado, suponha que correspondente a cada primo p definimos r_p pelas desigualdades $p^{r_p} \leq 2n < p^{r_p+1}$. Usando o Toerema 1 para determinar a potência de p que aparece na decomposição em fatores primos de $\binom{2n}{n}$, vemos que o expoente correto é a potência de p que aparece em $(2n)!$ menos a potência de p que aparece em $(n!)(n!)$; em outras palavras, o expoente é $\sum_{j=1}^{r_p}\left(\left\lfloor\frac{2n}{p^j}\right\rfloor - 2\left\lfloor\frac{n}{p^j}\right\rfloor\right)$. Pelo Teorema 2,

$$0 \leq \sum_{j=1}^{r_p}\left(\left\lfloor\frac{2n}{p^j}\right\rfloor - 2\left\lfloor\frac{n}{p^j}\right\rfloor\right) \leq \sum_{j=1}^{r_p} 1 = r_p.$$

Daí, vemos que

$$\binom{2n}{n} \Bigm| Q_n,$$

em que Q_n denota o produto de todos os p^{r_p}. Como cada p^{r_p} não excede $2n$ e Q_n tem $\pi(2n)$ fatores da forma p^{r_p},

$$\binom{2n}{n} \leq Q_n \leq (2n)^{\pi(2n)}. \tag{1.3}$$

Assim que determinarmos o tamanho de $\binom{2n}{n}$, *nós podemos ver que o Teorema de Chebyshev pode ser deduzido de (1.2) e (1.3). Por outro lado, pela definição de coeficiente binomial,*

$$\begin{aligned}\binom{2n}{n} &= \frac{2n}{n}\frac{(2n-1)(2n-2)}{(n-1)(n-2)}\dots\frac{(n+1)}{1}\\ &= 2\cdot\frac{2(2n-1)(n-1)}{(n-1)}\cdot\frac{2(2n-3)(n-2)}{(n-2)}\cdot\dots\cdot\frac{(n+1)}{1}\\ &\geq 2\cdot 2\cdot 2\cdot\dots\cdot 2 = 2^n. \end{aligned}\tag{1.4}$$

Combinando (1.3) e (1.4) temos

$$2^n \leq \binom{2n}{n} \leq (2n)^{\pi(2n)},$$

isto é,

$$2^n \leq (2n)^{\pi(2n)}. \tag{1.5}$$

Aplicando logaritmo de ambos os lados de (1.5), obtemos a desigualdade

$$\log 2^n \leq \log(2n)^{\pi(2n)},$$

logo,

$$n\log 2 \leq \pi(2n)\log 2n,$$

ou ainda,

$$\pi(2n) \geq \frac{n\cdot\log 2}{\log 2n}. \tag{1.6}$$

Daí, se $x \geq 5$ *e* $f(x) = x/\log x$, *por (1), (2) e (1.6), segue que*

$$\begin{aligned}\pi(x) &\geq \pi\left(2\left\lfloor\frac{x}{2}\right\rfloor\right) \geq \frac{\left\lfloor\frac{x}{2}\right\rfloor\log 2}{\log 2\left\lfloor\frac{x}{2}\right\rfloor} = \frac{\log 2}{2}\cdot\frac{2\left\lfloor\frac{x}{2}\right\rfloor}{\log 2\left\lfloor\frac{x}{2}\right\rfloor}\\ &= \frac{\log 2}{2}f\left(2\left\lfloor\frac{x}{2}\right\rfloor\right) > \frac{\log 2}{2}f(x-2) > \frac{\log 2}{2}\cdot\frac{1}{2}f(x)\\ &= \frac{\log 2}{4}\cdot\frac{x}{\log x},\end{aligned}$$

o que conclui a desigualdade do lado esquerdo do teorema 10. Pelo Teorema Binomial (4),

$$(1+x)^{2n} = 1 + \binom{2n}{1}x + \binom{2n}{2}x^2 + \dots + \binom{2n}{n}x^n + \dots + x^{2n}.$$

Por isso, com $x = 1$, *encontramos*

$$2^{2n} = 1 + \binom{2n}{1} + \binom{2n}{2} + \dots + \binom{2n}{n} + \dots + 1 > \binom{2n}{n}. \tag{1.7}$$

Para mostrar que $\pi(x) < 30 \cdot \log 2 \cdot \dfrac{x}{\log x}$, *combinamos (1.2) e (1.7). Assim,*

$$n^{\pi(2n)-\pi(n)} < \binom{2n}{n} < 2^{2n},$$

ou seja,

$$n^{\pi(2n)-\pi(n)} < 2^{2n}. \tag{1.8}$$

Aplicando logaritmo de ambos os lados de (1.8), encontramos que

$$\begin{aligned}[\pi(2n) - \pi(n)] \log n &< 2n \cdot \log 2 \\ \pi(2n) - \pi(n) &< \frac{n}{\log n} \cdot 2 \log 2.\end{aligned}$$

Portanto,

$$\pi(2n) < (2 \log 2) \frac{n}{\log n} + \pi(n). \tag{1.9}$$

Agora, por indução matemática, vamos mostrar que

$$\pi(2n) < 32(\log 2) \frac{n}{\log n}, \textit{ para } n > 1. \tag{1.10}$$

Inicialmente, note que (1.10) é verdade para $2 \leq n \leq 8$*:*

$$\begin{aligned}\pi(4) = 2 < \pi(6) = 3 < \pi(8) &= \pi(10) = 4 \\ &< \pi(12) = 5 < \pi(14) = \pi(16) = 6 < 64 \\ &= 32 \cdot 2 = 32(\log 2) \frac{2}{\log 2}.\end{aligned}$$

Agora suponha (1.10) verdade para todos os inteiros $n \leq k$, *com* $k \geq 8$. *Daí, para* $k+1$, *segue por (1.9) com* $f(x) = x/\log x$ *que*

$$\begin{aligned}\pi(2k+2) &< 2(\log 2) f(k+1) + \pi(k+1) \\ &\leq 2(\log 2) f(k+1) + \pi\left(2\left\lfloor \frac{k+2}{2} \right\rfloor\right) \\ &< 2(\log 2) f(k+1) + 32(\log 2) f\left(\left\lfloor \frac{k+2}{2} \right\rfloor\right) \\ &\leq 2(\log 2) f(k+1) + 32(\log 2) f\left(\frac{k+2}{2}\right) \\ &< 2(\log 2) f(k+1) + 32(\log 2) \frac{15}{16} f(k+1) \ \textit{(por 3)} \\ &= 32(\log 2) f(k+1) \\ &= 32(\log 2) \frac{k+1}{\log(k+1)}.\end{aligned}$$

Assim, por indução matemática, temos

$$\pi(2n) < 32(\log 2) \frac{n}{\log n} \textit{ para todo } n > 1.$$

Daí, para todo número real $x \geq 8$,

$$\begin{aligned}\pi(x) < \pi\left(2\left\lfloor\frac{x}{2}\right\rfloor+2\right) &< 32(\log 2)f\left(\left\lfloor\frac{x}{2}\right\rfloor+1\right)\\ &\leq 32(\log 2)f\left(\frac{x+2}{2}\right)\\ &< 32(\log 2)\frac{15}{16}f(x)\ \textit{(por 3)}\\ &= 30(\log 2)f(x)\\ &= 30(\log 2)\frac{x}{\log x},\end{aligned}$$

o que conclui a prova do Teorema de Chebyshev.

Exemplo 2 *Sabemos que* $\pi(10) = 4$*, pois apenas* $2,\ 3,\ 5$ *e* 7 *são primos e menores que 10. Pelo Teorema de Chebyshev, quando* $x = 10$ *temos*

$$\frac{\log 2}{4}\cdot\frac{10}{\log 10}\approx 0,75.$$

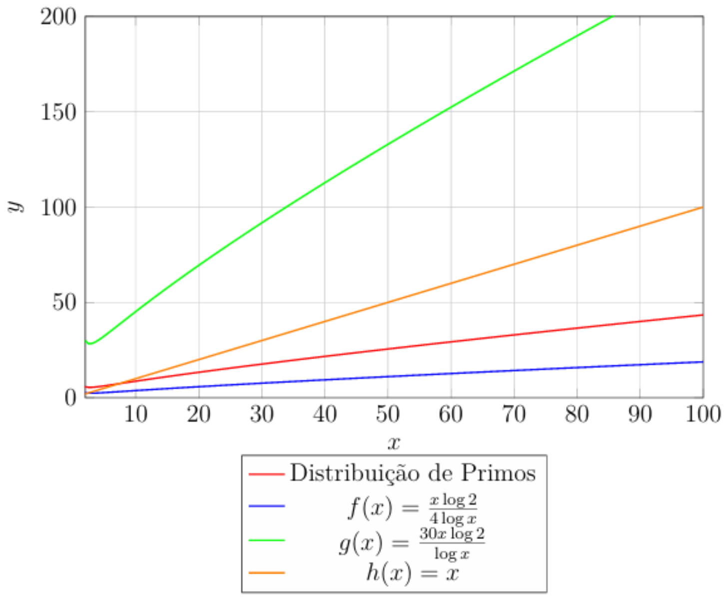
O que nos diz que há pelo menos 1 primo que não excede o valor de 10. Já pela estimativa do lado direito, há no máximo 90 primos, pois

$$30(\log 2)\frac{10}{\log 10}\approx 90,31.$$

Logo, $\pi(10) \in [1, 90]$.

É claro que o valor de $\pi(x)$ deve ser menor (ou igual) que x e por isso a estimativa inferior é o resultado mais interessante deste teorema, pois nos permite estipular o número mínimo de primos que não excedem determinado x, como podemos ver no gráfico a seguir.

Figura 2 – Representação gráfica do Teorema de Chebyshev



Fonte: Produzido pelos autores

Podemos observar, por meio da representação gráfica do Teorema de Chebychev, que, de fato, a função $\pi(x)$ está situada entre as funções $f(x) = \frac{\log 2}{4} \cdot \frac{x}{\log x}$ e $g(x) = 30 \log 2 \cdot \frac{x}{\log x}$ e que se aproxima mais da estimativa inferior. Isso acontece pois $\frac{\log 2}{4} \approx 0,075$ está mais próximo de 1 que $30(\log 2) \approx 9,031$ e quanto mais próximo de 1 forem as constantes c_1 e c_2, mais próximas do valor de $\pi(x)$ serão as estimativas do teorema.

Além disso, notamos que a estimativa superior excede o valor de x no domínio apresentado. Entretanto, em determinado ponto, elas se cruzam e o valor de x passa a ser maior que $g(x)$. De fato, observe que, para encontrar o valor de x onde as funções $g(x)$ e $h(x)$ se encontram, basta igualar as duas funções. Assim,

$$x = \frac{30x \log 2}{\log x}.$$

Como estamos analisando as funções para $x > 0$, podemos simplificar ambos os lados da equação por x. Daí,

$$1 = \frac{30 \log 2}{\log x}.$$

Logo,

$$\log x = 30 \log 2.$$

Resolvendo o logaritmo, temos que as funções se cruzam em $x = 2^{30} = 1.073.741.824$. A partir desse ponto, a função $g(x)$ passa a ser menor que x, tornando a estimativa de Chebyshev interessante para números primos maiores que 2^{30}.

1.3 Primos Especiais e Curiosidades

Nesta sessão, vamos apresentar e explorar alguns resultados relacionados aos chamados primos especiais por suas características únicas, incluindo os primos de Mersenne, Sophie Germain e Fermat. Além disso, discutiremos alguns problemas não resolvidos envolvendo números primos, como a conjectura de Goldbach.

1.3.1 Os primos de Mersenne

Marin Mersenne (1588 - 1648) foi um monge e matemático francês que contribuiu para o desenvolvimento de importantes resultados da teoria dos números, ficou conhecido por sua conjectura acerca dos números primos que seriam batizados em seu nome.

Definição 1.4 *É considerado um número de Mersenne, e indicado por M_n, todo número da forma $2^n - 1$ com $n \in \mathbb{N}$. Se $2^n - 1$ é primo, então M_n é um Primo de Mersenne.*

Em 1644, Mersenne publicou em seu livro *Cogita physico mathematics* (DEZA, 2022) a seguinte conjectura: os números da forma $2^n - 1$ são primos para $n = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 e composto para os demais inteiros do intervalo $2 \leq n \leq 257$.

Teorema 11 *Seja $n \in \mathbb{N}$. Se $2^n - 1$ é um primo de Mersenne, então n é primo.*

Demonstração 1.13 *Suponha que n não é primo. Logo, n é composto e pode ser escrito como o produto de dois inteiros a e b maiores que 1. Desse modo, temos*

$$\begin{aligned} 2^n - 1 &= 2^{a \cdot b} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1) \cdot [(2^a)^{b-1} + (2^a)^{b-2} + ... + (2^a)^1 + (2^a)^0] \\ &= (2^a - 1) \cdot [(2^a)^{b-1} + (2^a)^{b-2} + ... + (2^a)^1 + 1]. \end{aligned}$$

Analogamente,

$$\begin{aligned} 2^n - 1 &= 2^{a \cdot b} - 1 \\ &= (2^b)^a - 1 \\ &= (2^b - 1) \cdot [(2^b)^{a-1} + (2^b)^{a-2} + ... + (2^b)^1 + (2^b)^0] \\ &= (2^b - 1) \cdot [(2^b)^{a-1} + (2^b)^{a-2} + ... + (2^b)^1 + 1]. \end{aligned}$$

Assim, para n composto, temos que $2^n - 1$ também é composto.

Inicialmente, acreditava-se que $2^p - 1$ era primo se, e somente, p era primo. Entretanto, em 1563, o matemático Hudalricus Regius mostrou que, para $n = 11$, temos

$$2^{11} - 1 = 2047 = 23 \cdot 89,$$

ou seja, não é primo.

Temos que se $2^n - 1$ é primo, então n é primo, mas n ser primo não é condição suficiente para que $2^n - 1$ também o seja, conforme o contraexemplo visto acima.

Mersenne não conseguiu provar sua teoria e, durante séculos, muitos matemáticos se dedicaram a estudar os números $2^n - 1$ e descobrir se eram primos ou compostos. Por quase dois séculos, o maior número primo de Mersenne conhecido era o $M_{19} = 2^{19} - 1 = 524.287$, encontrado pelo italiano Pietro Cataldi em 1603.

Quase três séculos se passaram até que os matemáticos conseguissem testar todos os números da conjectura de Mersenne. O mais impressionante é que ele tenha cometido apenas cinco erros em sua lista: a inclusão dos primos $n = 67, 257$, que geram números compostos; e a ausência de $n = 61, 89, 107$.

Para Tanner É. Lucas, Mersenne criou sua lista considerando como condição suficiente os primos até 257 que podiam ser escritos como $2^{2n} + 1$, $2^{2n} \pm 3$ ou $2^{2n+1} - 1$, com $n \in \mathbb{N}$ (DEZA, 2022). De fato, ao calcular os primos $2 < p < 258$ que podem ser escritos por uma das fórmulas acima, podemos observar que

- Para $p = 2^{2n} + 1$, temos $5, 17, 257$;
- Para $p = 2^{2n} - 3$, temos $13, 61$;

- Para $p = 2^{2n} + 3$, temos $7, 19, 67$;
- Para $p = 2^{2n+1} - 1$, temos $7, 31, 127$.

Colocando em ordem crescente, encontramos uma lista de primos quase idêntica à da conjectura,

$$5, 7, 13, 17, 19, 31, 61, 67, 127, 257.$$

Sendo a diferença o número 61, que não estava incluso na lista de Mersenne. Além disso, há um erro na limitação dos valores, visto que para $p = 3$ temos $2^3 - 1 = 7$ primo, porém 3 não pode ser escrito em nenhuma das formas acima.

Tanner provou que apesar de $p = 67$ ser primo, o número $2^{67} - 1$ é composto. Logo, p ser escrito em uma dessas formas não é condição suficiente para que $2^p - 1$ seja primo. Os números $257, 1021$ e 8191 são outros exemplos de que essa condição não é suficiente. Além disso, o número $2^{89} - 1$ é primo, mas $p = 89$ não pode ser escrito em nenhuma das formas apresentadas.

Os primos de Mersenne são raros e ainda não se sabe se há infinitos ou não. Atualmente conhecemos apenas 51 deles e, desde 1997, todos os M_p encontrados foram por meio do GIMPS, que une esforços de amadores e profissionais.

1.3.2 Os primos de Sophie Germain

Sophie Germain (1776 - 1831) foi uma matemática autoditada francesa, que ficou conhecida por suas contribuições para a demonstração do Último Teorema de Fermat.

Definição 1.5 *Dizemos que p é um primo de Sophie Germain se $2p+1$ também é primo, sendo este chamado de Primo Seguro.*

Exemplo 3 *O menor primo de Sophie Germain é o 2, pois $2 \cdot 2 + 1 = 5$ é primo.*

A sequência dos primos de Sophie Germain é

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, ...$$

E, assim como os primos de Mersenne, ainda não foi provado se há infinitos primos de Sophie Germain.

Definição 1.6 *Uma Cadeia de Cunningham de primos de Sophie Germain é definida pela sequência $\{p,\ 2p + 1,\ 2(2p + 1) + 1, ...\}$.*

Exemplo 4 *A sequência $\{2, 5, 11, 23\}$ é uma Cadeia de Cunningham de primos de Sophie Germain. Note que esta cadeia termina em 23, pois o próximo número seria $23 \cdot 2 + 1 = 47$, que não é um primo de Sophie Germain.*

Em 1750, Euler anunciou um teorema relacionando os primos de Sophie Germain com os números compostos de Mersenne, que só foi provado 25 anos depois por Lagrange.

Teorema 12 *Se p é primo diferente de 3 e da forma $4k+3$ com $k \in \mathbb{Z}$, então $2p+1$ é primo se, e somente se, $2p+1$ divide $M_p = 2^p - 1$. Nesse caso, p é um primo de Sophie Germain.*

Exemplo 5 *Observe que $p = 11 = 4 \cdot 2 + 3$. Além disso, temos $2p+1 = 23$ e*

$$M_{11} = 2048 - 1 = 2047 = 23 \cdot 89.$$

Logo, $2p+1 \mid M_p$. Portanto, 23 é primo e 11 é um primo de Sophie Germain.

A demonstração deste teorema não será apresentada neste trabalho, pois requer uma compreensão sobre resíduos quadráticos e outros resultados da aritmética modular que ultrapassam o âmbito de nossa pesquisa. O leitor pode encontrar a demonstração em (CALDWELL, s.d.).

A relevância dos primos de Sophie Germain para a matemática está relacionada com o Último Teorema de Fermat, no qual o matemático afirma que $x^n + y^n = z^n$ não possui solução inteira para $n > 2$. Enquanto Fermat provou para $n = 4$ e Euler fez uma prova não muito rigorosa para $n = 3$, Germain foi uma das primeiras pessoas a tentar provar o teorema de forma geral e não apenas para valores pequenos. Para isso, ela dividiu o problema em dois casos:

- Caso 1: Dados x, y, z primos entre si e $p \nmid xyz$;
- Caso 2: Dados x, y, z primos entre si e $p \mid xyz$;

E então provou o primeiro caso para todos os primos $p \leq 197$.

1.3.3 Os primos de Fermat

Pierre de Fermat (1601 - 1665) foi um advogado e matemático francês que ficou conhecido por seus trabalhos na Teoria dos Números, em especial, pelo Pequeno Teorema de Fermat.

Definição 1.7 *Um número da forma $F_n = 2^{2^n} + 1$ com $n \geq 0$ é chamado de número de Fermat. Se F_n é primo, dizemos que se trata de um Primo de Fermat.*

Os cinco primeiros números de Fermat são primos:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257 \text{ e } F_4 = 65537.$$

Fermat conjecturou que todos os números da forma $2^{2^n} + 1$ são primos para $n \geq 0$. Entretanto, em 1732, Euler provou que a conjectura de Fermat é falsa mostrando que F_5 é um número composto divisível por 641, pois

$$F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6.700.417.$$

Até maio de 2024, o maior primo de Fermat conhecido é o $F_4 = 65537$ e ainda não sabemos se há infinitos primos de Fermat. Enquanto o maior número composto de Fermat conhecido é o $F_{18.233.954}$, cujo fator primo $7 \cdot 2^{18.233.956} + 1$ só foi encontrado em outubro de 2020.

Já foi provado que F_n é composto para todo $5 \leq n \leq 32$, porém, a fatoração completa dos números de Fermat só foi encontrada para $n \leq 11$.

1.3.4 Problemas não resolvidos sobre primos

Apesar de ser um tema abordado desde a educação básica, ainda existem problemas elementares sobre os números primos que até hoje não foram provados. Apresentaremos a seguir dois desses problemas que, apesar da dificuldade em prová-los, podem ser facilmente compreendidos por estudantes do ensino médio e abordados nas salas de aula.

Um dos problemas mais antigos e sem solução da teoria dos números é a conjectura de Goldbach: *todo número par maior que dois é a soma de 2 primos.* Apesar de ser facilmente compreendida e verificada para números pequenos, como

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 3 + 7 = 5 + 5,\ ...,$$

não é uma combinação trivial de ser encontrada quando observamos números muito grandes. Na verdade, para números maiores é possível fazer mais de uma combinação de primos; por exemplo,

$$118 = 5 + 113 = 11 + 107 = 17 + 101 = 29 + 89 = 47 + 71 = 59 + 59.$$

Goldbach não conseguiu provar sua afirmação para todos os números pares. Por meio de uma carta em 1742, pediu ajuda de Euler para demonstrar o resultado, mas este também não obteve sucesso (ANDREWS, 1971). Quase 300 anos depois de ser proposto, esse problema continua sem solução, mas já houve avanços que podem contribuir para a demonstração do resultado. O matemático russo I. M. Vinogradov provou que todos os grandes inteiros ímpares são a soma de três primos utilizando a teoria das variáveis complexas; já Nils Pipping provou que a afirmação de Goldbach é verdadeira para todos os pares até 100.000; mas se é verdade para *todo* par maior que 2 ainda não sabemos.

Outro problema não resolvido é o famoso Problema dos Primos Gêmeos. No século XIX, o matemático alemão Paul Stäckel chamou de primos gêmeos um par de primos p tal que $p + 2$ também é primo. Mais uma vez, é fácil ver que existem vários pares quando analisamos números pequenos; por exemplo, 3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31 e assim por diante.

Mas será que existem *infinitos* primos gêmeos? Para Euclides, a resposta é *sim*! Responsável pela elegante prova de que há infinitos números primos apresentada no início do capítulo, a Euclides também é atribuída a infinitude dos primos gêmeos. Porém, até os dias atuais, nenhum matemático conseguiu provar essa afirmação.

Alguns outros problemas sobre primos, como a hipótese de Riemann, requer uma base de conhecimentos matemáticos considerável até mesmo para a compreensão das afirmações, o que está além do objetitvo deste trabalho e por isso não serão abordados.

1.4 Considerações Finais

O objetivo deste trabalho é explorar o universo dos números primos, analisando sua distribuição entre os números naturais através do teorema de Chebyshev. Para tanto, realizamos um estudo aprofundado de resultados elementares da matemática, apresentando e demonstrando propriedades fundamentais da teoria dos números, como o teorema fundamental da aritmética e o teorema binomial.

Apresentamos o teorema de Chebyshev, que permite estimar o valor da função $\pi(x)$, a qual retorna a quantidade de números primos menores ou iguais a x. Este enfoque permite uma compreensão mais ampla e acessível dos conceitos envolvidos, visto que utiliza resultados básicos em sua demonstração.

Devido à amplitude do tema, acreditamos que este trabalho possa inspirar professores a explorar o fascinante mundo dos números primos com seus alunos, especialmente no ensino médio. Primos especiais como os de Mersenne, Sophie Germain e Fermat, bem como os problemas não resolvidos apresentados, trazem resultados intrigantes que podem despertar o interesse dos estudantes.

Desejamos que este trabalho desperte o interesse pela participação em competições matemáticas, estimulando o raciocínio lógico dos alunos e seu engajamento em atividades desafiadoras, sendo este material útil para a preparação de professores e estudantes interessados.

Por fim, considerando as mudanças trazidas pelo Novo Ensino Médio e a inclusão de itinerários formativos pela BNCC (BRASIL, 2018), sugerimos a criação de uma disciplina eletiva dedicada à apresentação e exploração de curiosidades sobre os números primos. Essa abordagem pode estimular a curiosidade e o interesse dos estudantes pela matemática, tornando o aprendizado mais envolvente e motivador.

Referências

ANDREWS, George E. **Number Theory**. Philadelphia: W. B. Saunders Company, 1971.

BRASIL. **Base Nacional Comum Curricular**. Brasília: Ministério da Educação, 2018.

CALDWELL, Chris. **Euler and Lagrange on Mersenne Divisors**. [S.l.: s.n.], s.d. Disponível em: `https://t5k.org/notes/proofs/MerDiv2.html`. Acesso em: 6 ago. 2024.

DEZA, Elena. **Mersenne numbers and Fermat numbers**. NJ: World Scientific Publishing Co. Pte. Ltd., 2022.

LEMOS, Manoel. **Criptografia, Números Primos e Algoritmos**. Rio de Janeiro: IMPA, 2010.

WOLTMAN, George. **GIMPS: Great Internet Mersenne Primes Search**. [S.l.: s.n.], 1996. Disponível em: https://www.mersenne.org. Acesso em: 10 ago. 2024.

2 UM ESTUDO SOBRE QUESTÕES DE GEOMETRIA DO SAEPE DO 3º ANO DO ENSINO MÉDIO

Me. Mayco Douglas Lima de Sales[1]
Dr. Eudes Mendes Barboza[2]
Dr. Thiago Yukio Tanaka[3]

Resumo: O Sistema de Avaliação da Educação Básica de Pernambuco (SAEPE) é composto pelas áreas do conhecimento de Língua Portuguesa e Matemática, que englobam diversos temas, incluindo Geometria. Seu objetivo é monitorar o desempenho dos estudantes da Educação Básica no estado de Pernambuco. Essa avaliação é realizada anualmente com estudantes do 2º, 5º e 9º ano do Ensino Fundamental, bem como do 3º ano do Ensino Médio. Observa-se que estes últimos têm enfrentado dificuldades no eixo de Geometria, o que se reflete em seu desempenho nessa avaliação. Neste trabalho, com o objetivo de investigar as questões de Geometria do SAEPE nos anos de 2019, 2021 e 2022, identificamos algumas das dificuldades enfrentadas pelos estudantes em relação a esse eixo. Ao analisar as questões, caracterizamos os Descritores do SAEPE abordados em cada uma das avaliações consideradas, apresentamos soluções para cada questão do eixo em foco e propomos sequências didáticas sobre os temas de Geometria mais recorrentes nas provas dos anos analisados, a fim de contribuir com os professores para o desenvolvimento da aprendizagem desse eixo em sala de aula.
Palavras-chave: Avaliação Externa; Geometria; SAEPE; Proficiência em Matemática; Descritores.

2.1 Introdução

As Avaliações Externas são instrumentos que, no âmbito escolar, servem para verificar o andamento da aprendizagem. Com o intuito de orientar políticas públicas, elas podem garantir maior eficácia na tomada de decisões por parte dos dirigentes, tanto nas escolas quanto nos órgãos governamentais, como as secretarias ou o Ministério da Educação.

Dentre as avaliações externas existentes, podemos citar, em escala mundial, o Programa Internacional de Avaliação de Estudantes (PISA), que contempla as disciplinas de Matemática e Ciências e é desenvolvido pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

[1] UFRPE, mayco.sales@ufrpe.br
[2] UFRPE, eudes.barboza@ufrpe.br
[3] UFRPE, thiago.tanaka@ufrpe.br

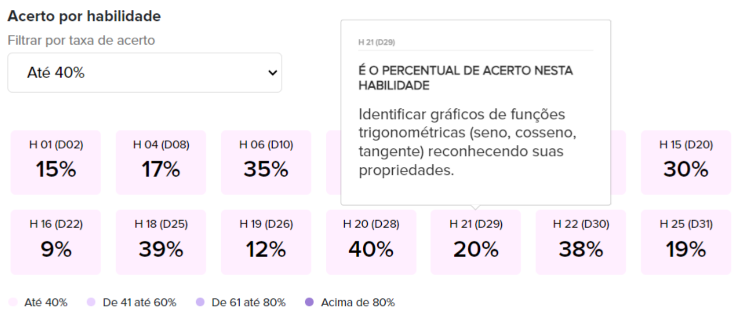
No âmbito nacional, o Sistema Nacional de Avaliação da Educação Básica (SAEB) avalia estudantes em Língua Portuguesa e Matemática em todo o território brasileiro, com o objetivo de fornecer informações sobre a qualidade da educação básica no país. Os resultados são utilizados na composição do Índice de Desenvolvimento da Educação Básica (IDEB), desenvolvido e aplicado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP).

No estado de Pernambuco, destaca-se o Sistema de Avaliação da Educação Básica de Pernambuco (SAEPE), que avalia estudantes do Ensino Fundamental e Médio nas disciplinas de Língua Portuguesa e Matemática. O sistema coleta informações sobre a qualidade da educação básica no território estadual, contribuindo para o cálculo do Índice de Desenvolvimento da Educação de Pernambuco (IDEPE). De modo mais específico, a prova do SAEPE é uma avaliação externa anual composta por 52 questões, sendo 26 de Língua Portuguesa e 26 de Matemática, focadas em verificar o desenvolvimento de habilidades previstas nos descritores da sua Matriz de Referência, elaborada de acordo com o Currículo de Pernambuco. O resultado dessa avaliação é denominado proficiência e, juntamente com outros parâmetros, como a taxa de aprovação e o fluxo escolar, compõe o IDEPE, servindo como base para subsidiar tomadas de decisão em políticas públicas voltadas ao efetivo desenvolvimento da Educação Básica em Pernambuco.

A Matriz de Referência do SAEPE é dividida em eixos estruturantes: Geometria, Grandezas e Medidas, Números e Operações/Álgebra e Funções, além de Estatística, Probabilidade e Combinatória. Cada eixo contempla descritores que indicam as habilidades a serem desenvolvidas pelos estudantes.

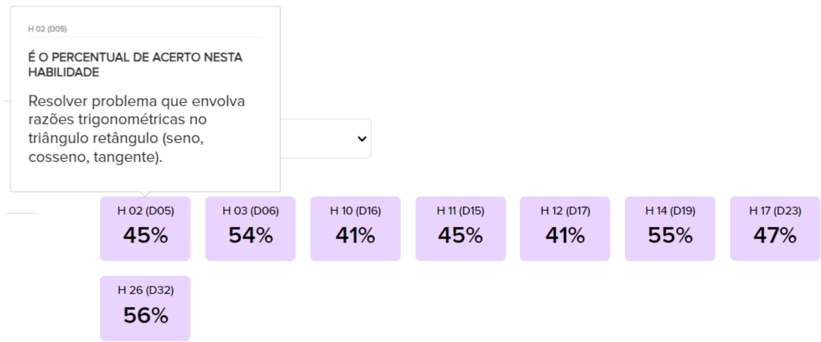
Ao observar os resultados do Eixo de Geometria no SAEPE aplicado ao 3º ano do Ensino Médio, identificamos um baixo desempenho. Tomando como base os dados disponibilizados no site do Centro de Políticas Públicas e Avaliação da Educação (CAED) relativos à prova aplicada em 2022, por exemplo, as duas questões relativas a esse eixo apresentaram menos de 50% de acertos. Como pode ser visto nas Figuras 3 e 4.

Figura 3 – Índice de acertos da questão sobre relações métricas - SAEPE 2022



Fonte: (CAED, 2023)

Figura 4 – Índice de acertos da questão sobre Razões Trigonométricas - SAEPE 2022



Fonte: (CAED, 2023)

Diante disso, buscamos analisar as questões de Geometria do SAEPE dos anos de 2019, 2021 e 2022, propondo resoluções para cada uma delas. A partir dessa análise, sugerimos estratégias de ensino com o objetivo de auxiliar os professores de Matemática das escolas públicas de Pernambuco a promover um ensino mais efetivo relativo a esse eixo e, consequentemente, melhorar o desempenho dos estudantes nessa avaliação. Além disso, identificamos as principais dificuldades enfrentadas pelos alunos, bem como estratégias para superá-las.

Dessa forma, neste trabalho, abordamos inicialmente as avaliações e seus respectivos tipos, com ênfase nas avaliações externas, especialmente o SAEPE. Apresentamos brevemente o contexto histórico dessa avaliação, sua estrutura e os documentos oficiais que a fundamentam, como o Currículo de Pernambuco — que serve de base para a avaliação das habilidades —, bem como sua Matriz de Referência. Em seguida, são apresentadas as questões do SAEPE relacionadas ao eixo de Geometria, organizadas por ano de aplicação. Cada questão analisada é acompanhada do gabarito oficial, seguida de uma proposta de resolução, um comentário explicativo sobre o raciocínio utilizado para resolvê-la, os conceitos envolvidos nela e a indicação da habilidade do Currículo de Pernambuco abordada. Por fim, é apresentada uma sugestão de como a questão pode ser explorada em sala de aula.

2.2 Avaliações

Avaliação, de acordo com Fernandes (2009) (FERNANDES, 2009), pode ser entendida como todo e qualquer processo deliberado e sistemático de coleta de informações, mais ou menos participativo e interativo, mais ou menos negociado, mais ou menos contextualizado, acerca do que os estudantes sabem e são capazes de fazer em uma diversidade de situações. Quando conduzida pelos próprios funcionários ou membros de uma instituição, a avaliação é dita Avaliação Interna. Quando é realizada por pessoas ou organizações que não fazem parte da instituição ou organização avaliada, é denominada Avaliação Externa. Segundo Arretche (2012) (ARRETCHE, 2012), a Avaliação Externa é um processo relevante para a efetividade de políticas públicas. Dessa forma, contribui para garantir sua eficácia, além de fornecer informações importantes para a tomada de decisões. Ainda de acordo com a autora, a avaliação externa pode ser utilizada para analisar a relevância, o impacto e a sustentabilidade dessas políticas.

A título de exemplo, o SAEB é uma avaliação externa aplicada pelo INEP desde 1990. Seu objetivo é avaliar a qualidade da Educação Básica em todo o território brasileiro, por meio da aplicação de testes em larga escala a estudantes do 5º e 9º anos do Ensino Fundamental e do 3º ano do Ensino Médio. Os resultados obtidos são utilizados como um dos indicadores para subsidiar políticas públicas, bem como para o planejamento e a gestão das redes de ensino em todo o país.

2.2.1 SAEPE

O Sistema de Avaliação da Educação Básica de Pernambuco (SAEPE) é uma Avaliação Externa aplicada anualmente a estudantes da rede pública estadual de ensino, com o objetivo de qualificar o desempenho em leitura, escrita e matemática. Foi criado em 2000 como uma versão estadual do SAEB, adaptado às especificidades do contexto pernambucano, e com o intuito de oferecer um instrumento de avaliação que permitisse à Secretaria de Educação do Estado de Pernambuco (SEE-PE) identificar as principais dificuldades e potencialidades da educação no estado.

Em seu primeiro ano, foram aplicados testes de desempenho em Língua Portuguesa (leitura e escrita) e Matemática para estudantes da 2ª série/3º ano, 4ª série/5º ano e 8ª série/9º ano do Ensino Fundamental, além do 3º ano do Ensino Médio/Normal Médio, das redes estadual e municipal. Desde então, o exame vem sendo aplicado de forma sistemática, com o intuito de avaliar e monitorar a qualidade da educação oferecida pelas escolas públicas do estado.

Nos anos de 2002 e 2005, o formato da avaliação permaneceu o mesmo adotado em 2000, com a avaliação das mesmas disciplinas. Em 2008, houve uma modificação na sua estrutura, a qual permanece vigente até hoje, exceto no ano de 2020, quando não houve aplicação devido à pandemia de *Covid*-19.

O SAEPE é um dos indicadores que servem para obter o Índice de Desenvolvimento da Educação de Pernambuco (IDEPE), que é um indicador criado pelo Governo do Estado de Pernambuco em 2008. Para seu cálculo, além dos resultados de proficiência do SAEPE, inclui-se também dados sobre a frequência escolar dos estudantes e informações sobre o perfil socioeconômico das escolas e dos estudantes.

A estrutura do SAEPE está baseada em sua matriz de referência. A Matriz de Referência de Matemática do 3º ano do Ensino Médio do SAEPE apresenta quatro eixos estruturantes, que são:

- Geometria: envolve conceitos como formas geométricas, relações métricas, entre outros;
- Grandezas e medidas: envolve medidas de comprimento, área, volume, entre outros;
- Números e operações/Álgebra e funções: envolve conceitos como números reais, operações básicas, frações, proporções, porcentagens além de conceitos como equações, inequações, sistemas de equações, funções, gráficos, entre outros;
- Estatística, Probabilidade e Combinatória: envolve conceitos como estatística, análise de gráficos, cálculo de probabilidade, entre outros.

Esses eixos estruturantes são utilizados para orientar a elaboração das questões da prova de Matemática do SAEPE para o 3º ano do Ensino Médio, avaliando a capacidade dos estudantes em resolver problemas e aplicar conceitos matemáticos relacionados a cada um deles. Os eixos são subdivididos em 35 (trinta e cinco) descritores. Segundo o (CAED, 2023):

> Para uma escola ser considerada eficaz, ela deve proporcionar padrões de aprendizagem adequados a todos os estudantes, independentemente de suas características individuais, familiares e sociais. Se apenas um grupo de estudantes consegue aprender com suficiente qualidade o que é ensinado, aumentam as desigualdades educacionais e, como consequência, elevam-se os indicadores de repetência, evasão e abandono escolar.

Esses "Padrões" estão associados aos conhecimentos e habilidades esperados dos estudantes em cada série avaliada. Por exemplo, no 3º ano do Ensino Médio, o nível de desempenho adequado é esperado para estudantes que tenham competência para aplicar os conceitos matemáticos dos quatro eixos da matriz de referência, resolver problemas contextualizados e interpretar informações matemáticas apresentadas em diferentes formatos. Esses conhecimentos e habilidades são divididos em 9 níveis obtidos pela proficiência alcançada por cada estudante. A Tabela 1 mostra os níveis de proficiência do 3º ano:

Tabela 1 – NÍVEIS DE PROFICIÊNCIA

PADRÃO DE DESEMPENHO	PROFICIÊNCIA	NÍVEL
ELEMENTAR I	0-249	NÍVEL 1
ELEMENTAR II	250-274	NÍVEL 2
	275-299	NÍVEL 3
BÁSICO	300-324	NÍVEL 4
DESEJÁVEL	325-349	NÍVEL 5
	350-374	NÍVEL 6
	375-399	NÍVEL 7
	400-424	NÍVEL 8
	Acima de 425	NÍVEL 9

Fonte: Produzido pelo Autor

Em que

- ELEMENTAR I - Este padrão reúne estudantes com carência de aprendizagem para o desenvolvimento das habilidades e competências mínimas requeridas para a conclusão da etapa de escolaridade em que se encontram. São estudantes que necessitam de ações pedagógicas de recuperação.
- ELEMENTAR II - Este padrão agrupa estudantes que ainda não demonstram ter desenvolvido adequadamente as habilidades e competências essenciais para a sua etapa de escolaridade. Demandam atividades de reforço na aprendizagem.
- BÁSICO - Este padrão reúne estudantes que consolidaram o desenvolvimento das habilidades e competências previstas para a etapa de escolaridade. Entretanto, ainda requerem ações para aprofundar a aprendizagem.
- DESEJÁVEL - Este padrão agrupa estudantes com desenvolvimento além do esperado para a sua etapa de escolaridade, os quais precisam de estímulos para continuar avançando no processo de aprendizagem.

2.2.2 Documentos oficiais para diretrizes da Educação Básica

A Base Nacional Comum Curricular (BNCC) é um documento normativo que estabelece os conhecimentos, competências e habilidades essenciais que todos os estudantes brasileiros devem desenvolver ao longo de sua trajetória escolar. Este documento não apenas estabelece diretrizes para o currículo nacional, mas também serve como um guia orientador para o desenvolvimento de documentos curriculares em níveis regionais, como é o caso do Currículo de Pernambuco. Ao se alinhar com os princípios e objetivos da BNCC, o Currículo pernambucano busca garantir que os estudantes do estado desenvolvam as competências e habilidades essenciais definidas nacionalmente, ao mesmo tempo em que integram aspectos regionais e locais relevantes para a formação desses estudantes.

O alinhamento entre o Currículo de Pernambuco e a BNCC se reflete também nas avaliações educacionais como o SAEPE. Através desse alinhamento, avaliações como esta podem medir adequadamente o progresso dos estudantes em relação aos padrões estabelecidos pela BNCC, fornecendo informações valiosas para aprimorar continuamente o ensino e a aprendizagem no estado.

Dessa forma, a BNCC tem implicações diretas nas Avaliações Externas, uma vez que os conteúdos e as competências nela definidos servem como referência para a elaboração dessas avaliações, conforme indicado em (BRASIL, 2018),

> desde as décadas finais do século XX e ao longo deste início do século XXI, o foco no desenvolvimento de competências tem orientado a maioria dos Estados e Municípios brasileiros e diferentes países na construção de seus currículos. Esse enfoque nas competências também é refletido em avaliações internacionais importantes, como o Programa Internacional de Avaliação de estudantes (PISA) coordenado pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e o Laboratório Latino-americano de Avaliação da Qualidade da Educação para a América Latina (LLECE) instituído pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO).

Essas referências internacionais demonstram a relevância da BNCC não apenas no contexto nacional, mas também em uma perspectiva global de avaliação e aprimoramento da educação.

2.2.2.1 Currículo de Pernambuco

O Currículo de Pernambuco é um documento crítico que estabelece e norteia a educação no estado. Em 2020, em função das mudanças determinadas pela Lei 13.415/2017, que promoveu a Reforma do Ensino Médio no Brasil, o Currículo do Ensino Médio de Pernambuco foi atualizado e passou a ser concebido em duas partes interligadas: a Formação Geral Básica (FGB), organizada por áreas de conhecimento, e os Itinerários Formativos (IF), que se conectam às expectativas e interesses individuais dos estudantes, fomentando seus projetos de vida.

É possível encontrar nesse documento informações sobre Princípios Norteadores, Educação Especial na Perspectiva da Inclusão, Competências e Habilidades, Concepções Sobre o Processo de Ensino e Aprendizagem, Formação de Professores, Avaliação da, para e como Aprendizagem, além de Temas Transversais e Integradores do Currículo.

Trazendo um olhar para o Ensino Médio, a FGB é composta de 04 (quatro) áreas de conhecimentos:

- Linguagens e suas Tecnologias (Artes, Educação Física, Língua Inglesa e Língua Portuguesa);
- Matemática e suas Tecnologias;
- Ciências da Natureza e suas Tecnologias (Biologia, Física e Química);
- Ciências Humanas e Sociais Aplicadas (Filosofia, História, Geografia e Sociologia).

Quando adentramos à área de conhecimento de Matemática e suas tecnologias, o Currículo trás que a BNCC (BRASIL, 2018) está organizada em Unidades Temáticas agrupadas em Números e Álgebra, Geometria e Medidas e Probabilidade e Estatística, às quais expressam um conjunto de habilidades a serem desenvolvidas, tais como:

1. Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, das questões socioeconômicas ou tecnológicas, divulgados por diferentes meios, de modo a contribuir para uma formação geral.
2. Propor ou participar de ações para investigar desafios do mundo contemporâneo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas sociais, como os voltados a situações de saúde, sustentabilidade, das implicações da tecnologia no mundo do trabalho, entre outros, mobilizando e articulando conceitos, procedimentos e linguagens próprios da Matemática.
3. Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.
4. Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.
5. Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando estratégias e recursos, como observação de padrões, experimentações e diferentes tecnologias, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas.

2.3 Análise das Questões de Geometria no SAEPE

A análise das questões de Geometria no Sistema de Avaliação da Educação Básica de Pernambuco (SAEPE) ao longo dos anos é uma etapa essencial para compreender como os conteúdos e habilidades dessa disciplina têm sido abordados e avaliados. Neste trabalho, será realizado um levantamento minucioso das questões de Geometria nas edições de 2022, 2021 e 2019 do SAEPE. O objetivo é identificar os problemas mais recorrentes e as habilidades que foram destacadas nas avaliações. Esse processo fornecerá informações úteis, contribuindo para o ensino de Geometria no 3º ano do Ensino Médio em Pernambuco. Serão apresentados os resultados do levantamento, destacando as tendências observadas nas questões de Geometria do SAEPE ao longo dos anos.

É importante ressaltar que o site oficial do SAEPE não disponibiliza sugestões de resolução ou referências detalhadas para as questões das avaliações. Portanto, nossa análise baseia-se exclusivamente nos gabaritos fornecidos pela instituição responsável pela aplicação do exame.

A análise detalhada de cada questão inicia-se com a apresentação do enunciado e de suas respectivas alternativas. Em seguida, é indicado o **Gabarito Oficial**, conforme disponibilizado pelo CAED. Também é apontada a habilidade do Currículo de Pernambuco ou o descritor do SAEPE que orienta a elaboração da questão.

Posteriormente, é apresentada uma **Solução da questão**, acompanhada de um **Comentário** explicativo que tem como objetivo esclarecer o raciocínio utilizado na resolução, destacar os conceitos envolvidos nela e indicar a Habilidade do Currículo de Pernambuco associada à questão. Essa análise detalhada contribui para uma compreensão mais aprofundada da estrutura da questão e das estratégias necessárias para sua resolução.

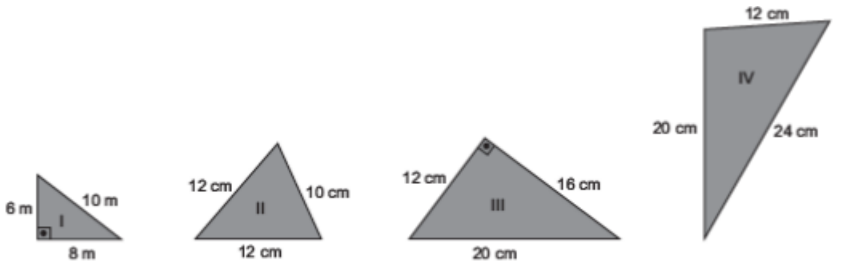
Além disso, discutimos a **Aplicação em sala** da questão analisada ou de uma questão semelhante, explorando possíveis abordagens pedagógicas para sua introdução, bem como estratégias de ensino que favoreçam uma compreensão mais efetiva por parte dos estudantes. São considerados aspectos como a adequação ao currículo, o nível de dificuldade e as possibilidades de adaptação para diferentes contextos educacionais.

Por meio dessa análise detalhada, busca-se não apenas compreender a questão em si, mas também explorar suas implicações no processo de ensino e aprendizagem da Matemática, contribuindo para o desenvolvimento de práticas pedagógicas mais eficazes e significativas.

2.3.1 Análise das questões de 2019

Em 2019, foram identificadas 04 (quatro) questões que versam sobre Semelhança de Triângulos, Teorema de Pitágoras, Planificação de Sólidos e Relação de Euler, que serão detalhadas a seguir.

Questão 2.1.1 (Currículo de Pernambuco - EM13MAT308PE24) No desenho abaixo estão representados os triângulos I, II, III e IV e suas medidas em centímetros.



O par de triângulos semelhantes nesse desenho é:

(A) I e II. **(B)** I e III. **(C)** I e IV. **(D)** II e IV. **(E)** III e IV.

Gabarito oficial: Letra B.

Solução: Para determinar se dois triângulos são semelhantes, é necessário verificar se eles possuem ângulos congruentes ou lados proporcionais.

No diagrama fornecido, os triângulos I, II, III e IV estão representados com as suas medidas de seu lados em centímetros. Precisamente temos:

- O triângulo I tem lados com medidas de 6 cm, 8 cm e 10 cm.
- O triângulo II tem lados com medidas de 10 cm, 12 cm e 12 cm.
- O triângulo III tem lados com medidas de 12 cm, 16 cm e 20 cm.
- O triângulo IV tem lados com medidas de 12 cm, 20 cm e 24 cm.

Ao analisar essas medidas, observamos que os triângulos I e III possuem lados proporcionais, pois as medidas dos lados do triângulo III são o dobro das medidas dos lados do triângulo I. Os outros triângulos não possuem dois ângulos correspondentes com medidas iguais e não têm os três lados correspondentes com medidas proporcionais. Portanto, a dupla de triângulos semelhantes neste diagrama é **(B)**, I e III.

Comentário: Nesta questão, estamos lidando com o conceito de semelhança de triângulos e proporção de medidas de seus lados. A semelhança de triângulos é uma propriedade fundamental na Geometria que nos permite estabelecer relações entre diferentes formas geométricas. Ao comparar as medidas dos lados dos triângulos e identificar padrões de proporção, podemos determinar quais pares são semelhantes. Essa habilidade é essencial para resolver uma variedade de problemas geométricos e é amplamente aplicada em áreas como arquitetura, engenharia e *design*. A capacidade de reconhecer padrões de proporção entre os elementos geométricos é uma competência valiosa que promove o raciocínio crítico e a habilidade de resolver problemas de forma eficaz. Embora a questão não mencione especificamente o currículo escolar, o domínio desse conceito pode enriquecer o aprendizado dos estudantes, fornecendo-lhes uma base sólida para explorar e compreender conceitos mais avançados em Geometria.

Essa competência é abordada na habilidade EM13MAT308PE24 do Currículo de Pernambuco que destaca a importância de aplicar as relações métricas e as leis de seno e cosseno, ou as noções de congruência e semelhança, para resolver e elaborar situações-problema que envolvam triângulos. Isso mostra como o domínio do conceito de semelhança de triângulos é fundamental para o desenvolvimento do pensamento matemático e para a resolução de problemas práticos em diversas áreas do conhecimento.

Aplicação em sala: Para abordar o conceito de semelhança de triângulos e proporção de medidas de seus lados em sala de aula, o professor pode seguir as seguintes etapas:

1. Introdução ao Conceito de Semelhança de Triângulos:

- Iniciar a aula revisando os conceitos básicos de triângulos e suas propriedades.
- Destacar o que significa dois triângulos serem semelhantes e quais condições devem ser satisfeitas para que isso ocorra.

2. Identificação de Triângulos Semelhantes:

- Apresentar exemplos de pares de triângulos e guiar os estudantes na identificação de pares que são semelhantes.
- Demonstrar como comparar as medidas dos lados dos triângulos para verificar a semelhança.

3. Discussão sobre Proporção de Lados:

- Incentivar os estudantes a discutir a importância da proporção de medidas dos lados na determinação da semelhança entre triângulos.
- Explorar situações do mundo real na qual a semelhança de triângulos e a proporção de medidas podem ser aplicadas, como na construção civil ou na arte.

4. Atividades Práticas e Exercícios:

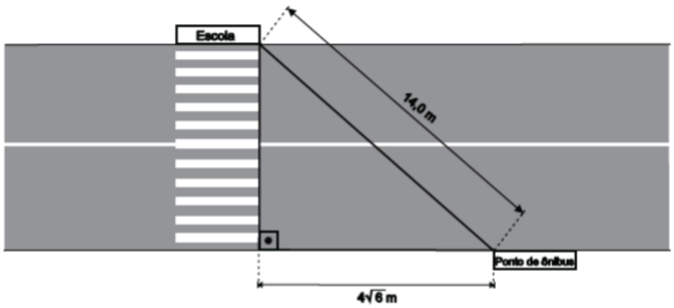
- Propor exercícios que envolvam a comparação de medidas de lados de triângulos e a determinação de semelhança.
- Realizar atividades práticas, como desenhos ou construções geométricas, para reforçar o conceito de semelhança de triângulos na prática.

5. Revisão e Reforço:

- Fazer uma revisão dos conceitos abordados, fornecendo exemplos adicionais e esclarecendo dúvidas.
- Destacar a importância da compreensão da semelhança de triângulos como uma ferramenta útil na resolução de problemas geométricos.

Ao seguir essas etapas, os estudantes poderão ser capazes de compreender e aplicar o conceito de semelhança de triângulos de forma significativa, desenvolvendo habilidades de raciocínio crítico e resolução de problemas na Geometria.

Questão 2.1.2 (Currículo de Pernambuco - EM13MAT308PE24) Para evitar que os estudantes de uma escola atravessassem a rua de forma desordenada até o ponto de ônibus ou vice-versa, foi solicitada a demarcação de uma faixa de pedestre em frente a essa escola. A figura abaixo apresenta as localizações da escola e do ponto de ônibus, a faixa de pedestre que foi demarcada e algumas distâncias.



Quantos metros, no mínimo, um estudante percorre ao atravessar essa faixa de pedestre para ir da escola até o ponto de ônibus?

(A) 10,0. **(B)** 13,1. **(C)** 14,0. **(D)** 17,1. **(E)** 23,6.

Gabarito Oficial: Letra A.

Solução da Questão: Na imagem, o segmento que une a escola ao ponto de ônibus representa a hipotenusa a do triângulo retângulo formado. O segmento que liga o ponto de ônibus ao fim da faixa corresponde a um dos catetos, que chamaremos de cateto b, enquanto o outro cateto, c, representa o comprimento da faixa.

Se utilizarmos o Teorema de Pitágoras para calcular o valor c obtemos:

$$14^2 = (4\sqrt{6})^2 + c^2.$$

Daí,

$$c = 10.$$

Portanto, o comprimento da faixa de pedestres a ser construída é de 10 metros, conforme indicado no item A.

Comentário: Nesta questão, é apresentado um problema que envolve a aplicação do Teorema de Pitágoras para calcular o comprimento de uma faixa de pedestres. O Teorema de Pitágoras é uma ferramenta fundamental na Geometria, que relaciona os comprimentos dos lados de um triângulo retângulo. Ao aplicar esse teorema, podemos encontrar medidas desconhecidas de um triângulo retângulo, o que é útil em muitas situações práticas, como no caso da demarcação de faixas de pedestres.

É importante destacar que, embora a BNCC do Ensino Médio não informe diretamente a habilidade ligada ao tema, a habilidade é encontrada na BNCC do Ensino Fundamental anos finais (EF09MA14) além do próprio Currículo de Pernambuco (EM13MAT308PE24), que aborda a resolução e elaboração de problemas de aplicação do Teorema de Pitágoras ou das relações de proporcionalidade envolvendo retas paralelas cortadas por secantes. Isso mostra como o uso do Teorema de Pitágoras é uma competência importante que é desenvolvida ao longo do Ensino Fundamental e continua sendo aplicada em contextos práticos no Ensino Médio.

Aplicação em sala: Para abordar essa questão em sala de aula e explorar o Teorema de Pitágoras, o professor pode seguir as seguintes etapas:

1. Introdução ao Teorema de Pitágoras:

- Revisar o Teorema de Pitágoras e sua aplicação em triângulos retângulos.
- Discutir exemplos simples de como o Teorema de Pitágoras pode ser usado para calcular medidas desconhecidas em triângulos.

2. Apresentação do Problema:

- Apresentar o problema da demarcação da faixa de pedestres e destacar as informações fornecidas na figura.
- Enfatizar que uma das possibilidades de solução do problema é a aplicação do Teorema de Pitágoras.

3. Resolução do Problema:

- Demonstrar passo a passo como aplicar o Teorema de Pitágoras para calcular o comprimento da faixa de pedestres, utilizando as medidas fornecidas na questão.
- Incentivar os estudantes a trabalharem juntos para resolver o problema, discutindo estratégias e ideias.

4. Prática Adicional:

- Propor problemas adicionais envolvendo o Teorema de Pitágoras, para que os estudantes pratiquem a aplicação desse conceito em diferentes contextos.

- Incluir exercícios que exijam a resolução de problemas do mundo real, como o cálculo de distâncias, alturas ou comprimentos de objetos.

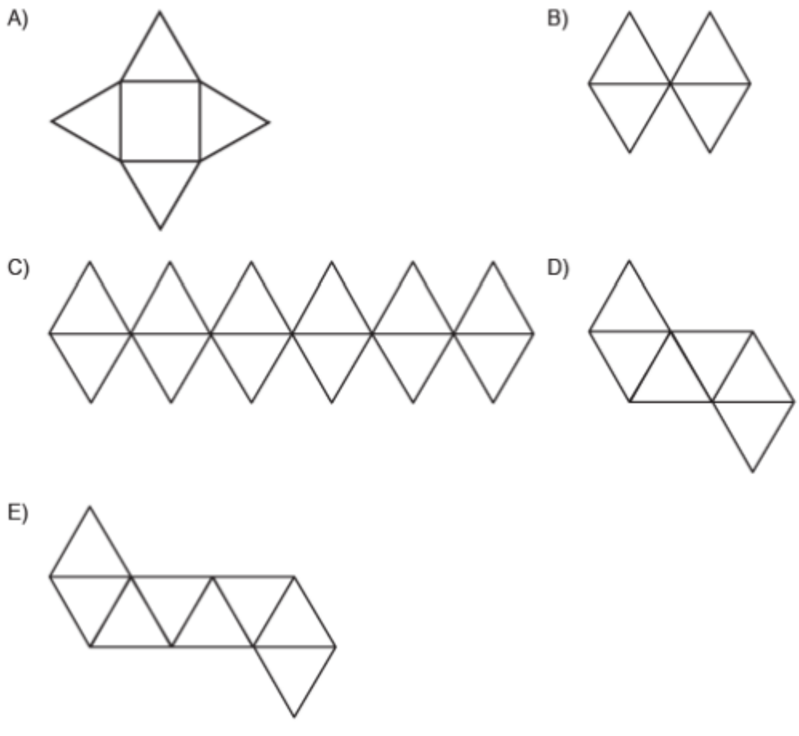
5. Discussão e Reflexão:

- Conduzir uma discussão em sala de aula sobre a importância do Teorema de Pitágoras na resolução de problemas práticos.
- Estimular os estudantes a refletirem sobre como podem aplicar o Teorema de Pitágoras em suas vidas cotidianas e em outras disciplinas além da matemática.

Ao seguir essas etapas, os estudantes poderão compreender melhor o Teorema de Pitágoras e desenvolver habilidades para aplicá-lo em diversos problemas do mundo real, promovendo uma compreensão mais profunda da Geometria e sua relevância na resolução de problemas.

Questão 2.1.3 (Descritor do SAEPE - D03) Observe o sólido geométrico desenhado abaixo.

Uma planificação desse sólido está representada em



Gabarito Oficial: Letra E.

Solução da Questão: Observa-se na imagem que o sólido apresentado trata-se de um octaedro que possui 8 faces, 6 vértices e 12 arestas. portanto, a planificação da superfície está corretamente representada na figura E.

Comentário: Nesta questão, é apresentado o sólido geométrico conhecido como octaedro, juntamente com sua representação planificada correta. O octaedro é um dos sólidos platônicos, caracterizado por possuir 8 faces, 6 vértices e 12 arestas. A planificação correta do octaedro é essencial para entender sua estrutura tridimensional e suas propriedades geométricas. Além disso, a explicação sobre a semelhança do octaedro com duas pirâmides quadrangulares unidas destaca sua forma peculiar e sua relação com outros sólidos geométricos.

É relevante observar que a planificação é mencionada na BNCC dos Anos Finais, mais especificamente na habilidade (EF05MA16), bem como no Descritor D03 da Matriz do SAEPE, que consiste em associar figuras espaciais às suas planificações (prismas, pirâmides, cilindros e cones), além de analisar, nomear e comparar seus atributos. Isso evidencia como a compreensão das planificações das figuras geométricas é uma etapa importante no desenvolvimento matemático dos estudantes, fornecendo-lhes uma base sólida para a exploração de conceitos mais avançados no Ensino Médio e além.

Aplicação em sala: Para abordar essa questão em sala de aula e explorar o conceito de octaedro e sua planificação, o professor pode seguir as seguintes etapas:

1. Introdução ao Octaedro:

- Apresentar o conceito de sólidos geométricos e destacar a definição do octaedro como um dos sólidos platônicos.
- Exibir imagens ou modelos tridimensionais de um octaedro para os estudantes visualizarem sua forma.

2. Características do Octaedro:

- Explicar as características do octaedro, incluindo o número de faces, vértices e arestas.
- Comparar o octaedro com outros sólidos geométricos, como o cubo, para destacar suas diferenças e semelhanças.

3. Planificação do Octaedro:

- Mostrar aos estudantes a representação planificada do octaedro e explicar como ela corresponde à sua forma tridimensional.
- Demonstrar como a planificação pode ser montada para formar o octaedro, permitindo que os estudantes visualizem a relação entre as faces, vértices e arestas.

4. Discussão e Atividades Práticas:

- Promover uma discussão sobre as propriedades e características do octaedro, incentivando os estudantes a fazerem perguntas e compartilharem suas observações.
- Propor atividades práticas, como a construção de modelos de octaedro utilizando papel ou materiais de manipulação tridimensional, para que os estudantes explorem a estrutura do octaedro em mãos.

5. Aplicações Adicionais:

- Discutir aplicações do octaedro na vida cotidiana ou em outras áreas, como na química (por exemplo, em moléculas com estrutura octaédrica) ou na arquitetura (por exemplo, na concepção de telhados ou estruturas ornamentais).
- Estimular os estudantes a explorarem mais sobre os sólidos geométricos e suas propriedades, incentivando a pesquisa independente e o aprendizado autônomo.

Ao seguir essas etapas, os estudantes poderão compreender melhor o conceito de octaedro, sua representação planificada e suas características geométricas, promovendo uma compreensão mais profunda da Geometria tridimensional e dos sólidos geométricos.

Questão 2.1.4 (Descritor do SAEPE - D04) A molécula de metano é composta por um átomo de carbono e átomos de hidrogênio. O número de ligações simples entre o átomo de carbono e os átomos de hidrogênio define uma Geometria molecular na forma de um poliedro convexo formado por 4 faces triangulares e cujos vértices são compostos pelos átomos de hidrogênio. Qual é o número de átomos de hidrogênio existentes na molécula de metano?

(A) 12. **(B)** 10. **(C)** 8. **(D)** 4. **(E)** 2.

Gabarito Oficial: Letra D.

Solução da questão:A molécula de metano possui um átomo de carbono e átomos de hidrogênio dispostos ao redor do carbono. A disposição espacial desses átomos forma um poliedro convexo composto por 4 faces triangulares, ou seja, um tetraedro regular. Para encontrar o número de átomos de hidrogênio na molécula de metano, basta contar o número de vértices do tetraedro, pois cada vértice corresponde a um átomo de hidrogênio. O tetraedro possui 4 vértices, portanto, há 4 átomos de hidrogênio na molécula de metano. Assim, a resposta correta é o item D.

Comentário: Esta questão é um excelente exemplo de como a geometria molecular pode ser compreendida por meio do conceito de poliedro convexo. Ao descrever a estrutura da molécula de metano, que consiste em um átomo de carbono e átomos de hidrogênio dispostos ao seu redor, a questão destaca a formação de um tetraedro regular. Um tetraedro é um poliedro convexo composto por quatro faces triangulares e vértices nos quais os átomos de hidrogênio estão localizados. Ao contar o número de vértices do tetraedro, é possível determinar o número de átomos de hidrogênio presentes na molécula de metano, evidenciando a conexão entre a geometria molecular e os poliedros convexos.

Além disso, a habilidade (EM13MAT505) da Base Nacional Comum Curricular (BNCC) do Ensino Médio complementa essa análise que também está associada ao Descritor D04. Esta habilidade envolve a resolução de problemas sobre ladrilhamento do plano, com ou sem apoio de aplicativos de Geometria dinâmica, para conjecturar a respeito dos tipos ou composição de polígonos que podem ser utilizados em ladrilhamento, generalizando padrões observados. Embora esta habilidade não esteja diretamente relacionada à Geometria molecular, ela destaca a importância de compreender os padrões e relações geométricas em contextos diversos, incluindo o estudo dos poliedros convexos na química orgânica. Isso evidencia a interdisciplinaridade entre Matemática e Ciências, promovendo uma compreensão mais ampla e integrada dos conceitos geométricos.

Entretanto, é importante considerar que, na elaboração da questão, a introdução do termo "Geometria Molecular"pode desviar o foco do estudante da aplicação direta da relação de Euler para a identificação de vértices, faces e arestas. Ao mencionar a Geometria Molecular, a questão pode levar o estudante a concentrar-se mais na disposição espacial dos átomos na molécula, em vez de focar exclusivamente na análise da estrutura topológica. Assim, para garantir que os estudantes mantenham o foco na aplicação da relação de Euler, seria mais eficaz apresentar a questão de forma mais direta, sem mencionar explicitamente a Geometria Molecular.

Aplicação em sala: Para abordar essa questão em sala de aula e explorar o conceito de poliedros convexos e sua relação com a Geometria Molecular, o professor pode seguir as seguintes etapas:

1. Introdução ao Conceito de Poliedros Convexos:

- Iniciar a aula revisando o conceito de poliedros e destacando as características dos poliedros convexos.
- Apresentar exemplos de poliedros convexos e discutir suas propriedades, enfatizando a importância dos vértices e faces na definição desses sólidos.

2. Discussão sobre a Estrutura Molecular do Metano:

- Descrever a estrutura molecular do metano, destacando a disposição dos átomos de hidrogênio ao redor do átomo de carbono.

- Explicar como essa disposição forma um tetraedro regular, um exemplo de poliedro convexo.

3. Identificação do Número de Átomos de Hidrogênio:

- Apresentar a questão sobre o número de átomos de hidrogênio na molécula de metano e discutir a solução utilizando o conceito de vértices de um tetraedro.
- Encorajar os estudantes a visualizarem a relação entre a estrutura molecular e a Geometria do poliedro convexo.

4. Atividades Práticas:

- Propor atividades práticas, como modelagem de moléculas de metano usando modelos tridimensionais ou representações gráficas.
- Realizar exercícios que envolvam a identificação do número de vértices e faces de diferentes poliedros convexos.

5. Revisão e Reforço:

- Fazer uma revisão dos conceitos abordados, destacando a importância da compreensão da Geometria molecular na química e da relação entre poliedros convexos e estruturas moleculares.
- Estimular os estudantes a relacionarem os conceitos aprendidos com aplicações práticas em outras áreas, como na química orgânica e na nanotecnologia.

Ao seguir essas etapas, os estudantes poderão compreender melhor a relação entre a Geometria molecular e os poliedros convexos, além de fortalecerem suas habilidades de visualização espacial e resolução de problemas.

2.3.2 Análise das questões de 2021

Em 2021, foram identificadas 04 (quatro) questões que versam sobre Relação de Euler, Semelhança de Triângulos, Relações Trigonométricas no Triângulo Retângulo e Planificação de Sólidos, que serão apresentadas a seguir.

Questão 2.2.1 (Descritor do SAEPE - D04) Para uma exposição de lançamento de marcas, serão colados 2 adesivos com os nomes das empresas participantes em cada uma das faces de um poliedro convexo de 16 arestas e 10 vértices, feito de papelão. Quantos adesivos ao todo serão colados nesse poliedro de papelão?

(A) 52 m. **(B)** 48 m. **(C)** 44 m. **(D)** 20 m. **(E)** 16 m.

Gabarito Oficial: Letra E.

Solução da questão: Para um poliedro convexo, a Fórmula de Euler estabelece a relação entre o número de vértices V, o número de arestas A e o número de faces F:

$$V - A + F = 2.$$

Neste caso, o poliedro de papelão tem $V = 10$ vértices e $A = 16$ arestas. Queremos encontrar o número de faces F. Considerando que cada empresa tem seu próprio adesivo e que cada adesivo de uma única empresa é colado em cada face, o número total de adesivos dessa empresa é igual ao número de faces. Rearranjando a Fórmula de Euler para resolver para F:

$$F = A - V + 2.$$

Daí,

$$F = 8.$$

Assim, há 8 faces no poliedro de papelão. Como dois adesivos(um de cada empresa) serão colados em cada face, o número total de adesivos será:

$$\text{Número total de adesivos} = 2 \times F = 2 \times 8 = 16.$$

Portanto, ao todo, serão colados 16 adesivos nesse poliedro de papelão.

Comentário: Essa questão envolve a aplicação da Fórmula de Euler em um contexto de Geometria de poliedros. A fórmula é utilizada para relacionar o número de vértices V, arestas A e faces F em um poliedro convexo. A Fórmula de Euler $V - A + F = 2$ é manipulada para encontrar o número de faces F em termos de vértices e arestas. Substituindo os valores conhecidos ($V = 10$ e $A = 16$), determinamos que o poliedro possui $F = 8$ faces.

Assim, o número total de adesivos é calculado multiplicando o número de faces pelo número de adesivos por face ($2 \times F$). Neste caso, 16 adesivos serão colados no poliedro de papelão.

Mesmo que essa questão proporcione uma oportunidade para os estudantes aplicarem conceitos geométricos e a Fórmula de Euler em um contexto prático, no Currículo de Pernambuco, não foi encontrada a previsão dessa habilidade em nenhuma das etapas do Ensino Médio, porém está prevista na Matriz do SAEPE no descritor D04.

Aplicação em sala: Para abordar essa questão em sala de aula e explorar o conceito de poliedros convexos, a Fórmula de Euler e sua aplicação, o professor pode seguir as seguintes etapas:

1. Introdução ao Conceito de Poliedros:

- Iniciando a aula revisando o conceito de poliedros, destacando as características de poliedros convexos.

- Apresentar exemplos de poliedros convexos e não convexos, enfatizando as propriedades que definem essa classe de sólidos.

2. Fórmula de Euler:

- Pergunta-se aos estudantes se conseguem encontrar um padrão e em seguida apresenta-se a Fórmula de Euler $V - E + F = 2$ explicando seu significado.
- Mostre como ela pode ser usada para calcular o número de faces F quando o número de vértices V e arestas A é conhecido.

3. Discussão e Aplicações Práticas:

- É importante incentivar os estudantes a discutir a aplicação prática da Fórmula de Euler e como ela pode ser útil em contextos reais, como no problema apresentado.
- Estimular a reflexão sobre outras situações em que a fórmula pode ser aplicada também é uma forma de ratifica a aprendizagem.

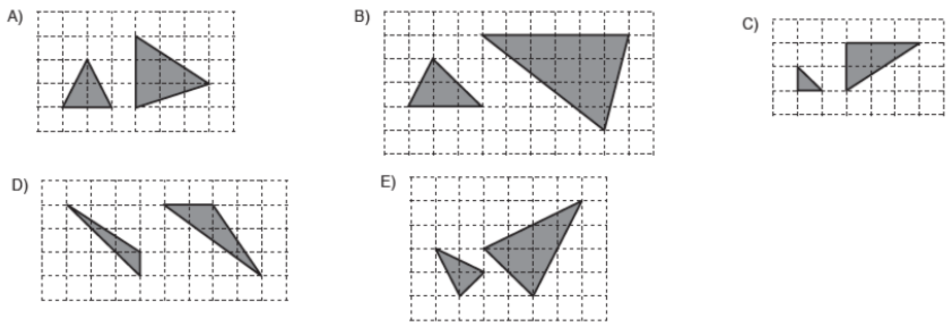
4. Atividades Práticas e Exercícios:

- Fornecer exercícios semelhantes para os praticarem o uso da Fórmula de Euler em diferentes contextos.
- Atividades práticas, como a construção de poliedros convexos e a aplicação da fórmula também contribuem para o fortalecimento da aprendizagem.

5. Revisão e Reforço:

- Fazer uma revisão dos conceitos abordados, esclarecendo dúvidas e destacando a importância da Fórmula de Euler na compreensão das características dos poliedros convexos proporciona uma compreensão mais profunda, promovendo o pensamento crítico, resolução de problemas e aplicação prática de fórmulas matemáticas.

Questão 2.2.2 (Currículo de Pernambuco - EM13MAT308PE24) Um professor de Matemática desenhou vários triângulos em uma malha quadriculada. Qual par de triângulos desenhados pelo professor representa triângulos semelhantes?



Gabarito Oficial: Letra E.

Solução da questão: Ao resolver problemas de semelhança entre triângulos, é importante observar algumas características. A semelhança entre dois triângulos ocorre quando os ângulos correspondentes são congruentes, e as razões entre os comprimentos dos lados correspondentes são proporcionais.

Alguns critérios de semelhança estabelecem condições necessárias para determinar quando dois triângulos são semelhantes:

1. *LLL* (Lados Lados Lados): Dois triângulos são semelhantes se todos os seus lados forem proporcionais.

2. *LAL* (Lado Ângulo Lado): Dois triângulos são semelhantes se tiverem um lado congruente e os ângulos adjacentes a esse lado também forem congruentes.

3. *AAA* (Ângulo Ângulo Ângulo): Dois triângulos são semelhantes se tiverem todos os três pares de ângulos correspondentes congruentes.

Analisando item a item temos que:

A. O triângulo menor é isósceles e o maior não, ou seja, os ângulos correspondentes não são congruentes, logo esse par não é semelhante.

B. As bases e catetos têm razões diferentes entre si, respectivamente.

C. Os dois triângulos são retângulos, porém o menor tem os catetos com tamanhos iguais, diferente do que acontece com o triângulo maior, ou seja, a razão entre os comprimentos dos lados correspondentes não são proporcionais, logo o par não é proporcional.

D. Considerando o lado menor que forma o ângulo obtuso, percebemos que a razão entre essas bases é 1:2, enquanto a altura relativa à base é igual, portanto não são semelhantes.

E. Seja T_1 e T_2 os triângulos menor e maior, respectivamente, desse item. Podemos observar que um dos lados de T_1 compreende na diagonal de um quadrado da malha quadriculada. Podemos ver também que um dos lado de T_2 é a diagonal do quadrado formado por 4 quadrados dessa mesma malha quadriculada e que esse lados se correspondem, ou seja, tem uma razão de 1 para 2. O T_1 está contido em um quadrilátero regular formado por 4 quadrados da malha,e os vértices do lado menor estão exatamente nos pontos médios de dois lados adjacentes desse quadrilátero, como o terceiro vértice de T_1 coincide com vértice do quadrilátero, os lados que contem esses pontos tem o mesmo tamanho, logo T_1 é isósceles. Analogamente, T_2 também é isósceles. Como as áreas dos quadriláteros em que T_1 e T_2 estão contidos, estão numa razão de 1:4, os lados correspondentes de T_1 e T_2 tem razão 1:2 também, concluímos que, pelo critério LLL, os triângulos T_1 e T_2 são semelhantes.

Portanto, a resposta correta é o item E.

Comentário: A questão apresenta a importância de observar ângulos correspondentes congruentes e a proporcionalidade entre os lados.

Os itens devem ser analisados individualmente, e a resposta correta é fundamentada na aplicação do critério de semelhança LLL (Lados Lados Lados), LAL (Lado Ângulo Lado) ou AAA (Ângulo Ângulo Ângulo).

No Currículo de Pernambuco a habilidade EM13MAT308PE24 destaca que:

> Aplicar as relações métricas e as leis de seno e cosseno ou as noções de congruência e semelhança para resolver e elaborar situações-problema que envolvam triângulos em variados contextos, com e/ou sem o uso de tecnologias digitais.

Logo, verificamos que a questão atende às perspectivas do Currículo do Estado.

Em resumo, a questão oferece uma oportunidade para os estudantes aplicarem conceitos de semelhança de triângulos, exercitando o pensamento geométrico e a interpretação de critérios específicos em um contexto prático.

Aplicação em Sala: Abordagem em Sala de Aula:

1. Introdução ao Tema:

- Explique o conceito de semelhança entre triângulos, ressaltando a importância de ângulos correspondentes congruentes e proporcionalidade entre lados.

2. Exemplificação Visual:

- Apresente triângulos desenhados em uma malha quadriculada.
- Destaque visualmente os ângulos correspondentes e a disposição na malha.

3. Critérios de Semelhança:

- Breve revisão dos critérios (LLL, LAL, AAA) de semelhança entre triângulos.

4. Reflexão Conjunta:

- Conduza uma discussão em sala de aula.
- Destaque aspectos importantes da análise e corrija possíveis equívocos.

5. Atividade Prática:

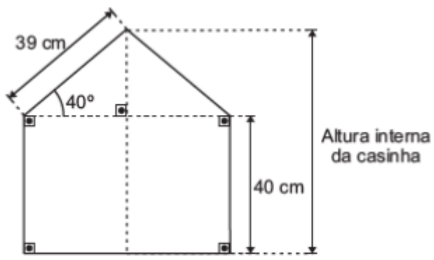
- Proporcione outras figuras ou malhas quadriculadas para que os estudantes pratiquem a identificação de triângulos semelhantes.

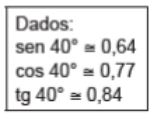
6. Reforço e Exercícios:

- Proporcione exercícios adicionais para casa, reforçando a aplicação dos critérios de semelhança.

Essa abordagem permite uma exploração prática do conceito de semelhança entre triângulos, proporcionando uma compreensão sólida por meio da análise visual e da aplicação dos critérios específicos.

Questão 2.2.3 (Currículo de Pernambuco - EM13MAT308) Juliano fez uma casinha de madeira para o seu cachorro. Algumas medidas internas da parede traseira dessa casinha estão indicadas na figura abaixo.





Qual é a medida da altura interna dessa casinha?

(A) 64,96 *cm*. **(C)** 72,76 *cm*. **(E)** 79,00 *cm*.

(B) 70,03 *cm*. **(D)** D) 78,36 *cm*.

Gabarito Oficial: Letra A

Solução da questão: A altura total da casinha é dada pela soma da altura do triângulo isósceles e a altura do retângulo. Podemos utilizar a relação trigonométrica do seno (sen) para calcular a altura do triângulo isósceles.

O triângulo que forma o telhado da casinha é isósceles. portanto, sua altura $h_{\text{triângulo}}$ pode ser encontrada usando a fórmula:

$$h_{\text{triângulo}} = \text{lado} \times \text{sen}(\alpha),$$

onde α é o ângulo formado pela base e um dos lados adjacentes. Substituindo os valores fornecidos:

$$h_{\text{triângulo}} = 39 \times \text{sen}(40^\circ) = 39 \times 0,64 \approx 24,96\,cm.$$

A altura total da casinha é então a soma da altura do triângulo e a altura do retângulo:

$$\text{Altura total} = h_{\text{triângulo}} + \text{Altura do retângulo} = 24,96 + 40 \ \approx 64,96\,\text{cm}.$$

Portanto, a medida da altura interna da casinha é aproximadamente $64,96\,\text{cm}$.

Comentários: Essa questão envolve a aplicação de conceitos de Geometria e Trigonometria para calcular a altura interna de uma casinha com formato composto por um triângulo isósceles sobre um retângulo, prevista na habilidade EM13MAT308 do Currículo de Pernambuco que versa:

> Aplicar as relações métricas, incluindo as leis do seno e do cosseno ou as noções de congruência e semelhança, para resolver e elaborar problemas que envolvem triângulos, em variados contextos

Ao perceber que a altura total é a soma da altura do triângulo isósceles e a altura do retângulo, utiliza-se a relação trigonométrica do seno (sen) para determinar a altura do triângulo que ao ser somada a altura do retângulo encontra-se o resultado da questão.

Esse tipo de questão proporciona aos estudantes a oportunidade de aplicar conhecimentos adquiridos fortalecendo a compreensão de conceitos pré estabelecidos.

Aplicação em sala: Para trabalhar essa questão em sala de aula, o professor pode seguir uma abordagem mais simplificada e direta, enfocando nos conceitos-chave.

1. Contextualização:

- Apresentar a situação da casinha e destacar que sua forma é composta por um triângulo isósceles sobre um retângulo.

2. Revisão de Trigonometria:

- Relembrar conceitos básicos de trigonometria, especialmente as funções seno, cosseno e tangente.

3. Análise da Estrutura:

- Explorar a estrutura da casinha, identificando as duas figuras geométricas e a necessidade de calcular a altura total.

4. Aplicação da Trigonometria:

- Demonstrar como utilizar a função seno para calcular a altura do triângulo isósceles, considerando a base como um dos lados do retângulo.

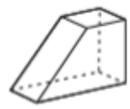
5. Resolução em Etapas:

- Incentivar os estudantes a resolver a questão em etapas, aplicando cada conceito aprendido.

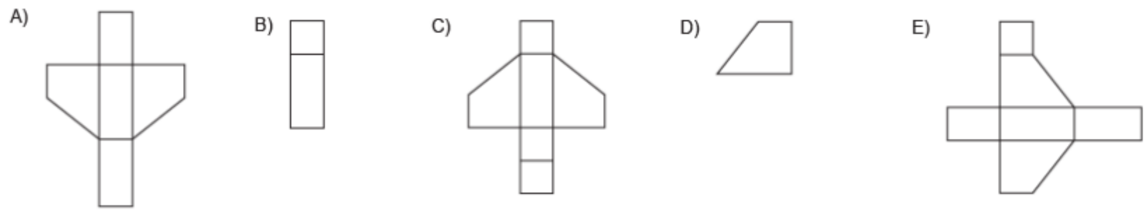
6. Atividades Relacionadas:

- Propor atividades adicionais envolvendo a aplicação de trigonometria em situações do dia a dia.

Questão 2.2.4 (Descritor do SAEPE - D03) Observe o sólido geométrico abaixo.



Uma planificação desse sólido está representada em



Gabarito Oficial: Letra E.

Solução da questão:O objeto possui 6 faces. Portanto, sua planificação deve conter seis figuras planas. Observe que apenas os itens C e E apresentam uma possível planificação com seis figuras planas. Contudo, é importante destacar que apenas no item E as figuras possuem exatamente o formato e o tamanho das faces do objeto. Portanto, a alternativa correta é o item E."

Comentário: A questão aborda o conceito de planificação, que envolve o processo de desdobrar um objeto tridimensional em figuras planas bidimensionais. A habilidade de planificar é essencial para compreender a estrutura e a forma de objetos tridimensionais.

Embora esteja prevista como habilidade necessária para o Ensino Médio no Descritor D03, não encontramos uma habilidade específica no Currículo de Pernambuco.

Ao apresentar diversas alternativas de planificação para um objeto, os estudantes são desafiados a identificar a representação correta. A solução destaca que apenas o item E apresenta seis figuras planas que correspondem exatamente às faces do objeto tridimensional, evidenciando a aplicação prática do conceito.

Essa questão estimula os estudantes a desenvolverem a capacidade de visualização espacial, a análise crítica de configurações planas e a correlação entre figuras bidimensionais e objetos tridimensionais.

Aplicação em sala: Estratégia para Trabalhar em Sala de Aula:

1. Introdução:

- Introduza o conceito de planificação, explicando que é o processo de desenhar as faces de um objeto tridimensional quando desdobrado em duas dimensões.

2. Exemplo Prático:

- Mostre um objeto tridimensional (por exemplo, uma pirâmide) e explique que os estudantes precisarão visualizar como suas faces seriam dispostas em um plano.

3. Análise dos Itens:

Apresente diferentes alternativas de planificação do objeto.

- Destaque que o objeto tem um certo número de faces, portanto, sua planificação deve ter essa mesma quantidade figuras planas.

4. Discussão em Grupo:

- Divida os estudantes em grupos.
- Peça que analisem cada item, considerando a quantidade de figuras planas e sua correspondência com as faces do objeto tridimensional.

5. Justificativas:

- Solicite que cada grupo justifique sua escolha, enfatizando a contagem das figuras planas e a correspondência com as faces do objeto.

6. Análise Conjunta:

- Realize uma análise conjunta das justificativas de cada grupo.
- Destaque as características que tornam uma planificação correta em relação ao objeto tridimensional.

7. Solução da Questão:

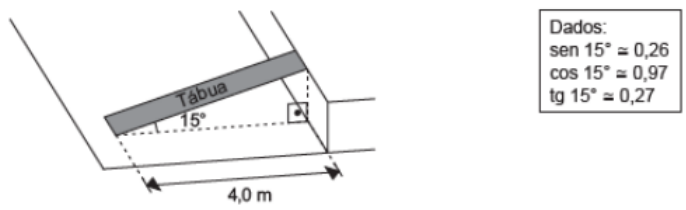
- Introduza a questão específica sobre o objeto com 6 faces.
- Utilize a solução fornecida para reforçar a compreensão da planificação correta.

Essa abordagem pode promover aos estudantes a explorarem ativamente o conceito de planificação e desenvolvam a habilidade de visualizar e representar objetos tridimensionais em duas dimensões.

2.3.3 Análise das questões de 2022

Em 2022, foram identificadas 02 (duas) questões que versam sobre Relações Trigonométricas no Triângulo Retângulo, Relações Métricas no Triângulo Retângulo, que estarão dispostas a seguir.

Questão 2.3.1 (Currículo de Pernambuco - EM13MAT308) Os operários de uma construção irão instalar uma tábua entre dois patamares para utilizarem como rampa de transporte de materiais. No desenho abaixo, está representada a distância entre esses patamares, bem como a disposição e a inclinação com que essa tábua será instalada.



De acordo com essas informações, aproximadamente, qual será a extensão, em metros, dessa tábua?

(A) 3,03 m.

(B) 3,88 m.

(C) 4,12 m.

(D) 14,81 m.

(E) 15,38 m.

Gabarito Oficial: Letra C.

Solução da questão: Para resolver esse problema, podemos usar a Trigonometria, mais especificamente, a definição de cosseno em triângulos retângulos, considerando o ângulo de inclinação da tábua. No caso da tábua inclinada a 15° em relação ao chão, temos que:

$$cos(15°) = \frac{\text{Cateto Adjacente}}{\text{Hipotenusa}} = \frac{4,0}{\text{Hipotenusa}}.$$

Daí

$$\text{Hipotenusa} = \frac{4,0}{0,97} = 4,12.$$

Comentário: Aqui podemos abordar a habilidade EM13MAT308,

> Aplicar as relações métricas, incluindo as leis do seno e do cosseno ou as noções de congruência e semelhança, para resolver e elaborar problemas que envolvem triângulos, em variados contextos.

Esta questão envolve a aplicação de conceitos trigonométricos em um contexto prático, onde os estudantes devem determinar o comprimento de uma tábua inclinada. Ao utilizar o cosseno do ângulo de inclinação e a distância entre o pé da tábua e a parede, os estudantes são incentivados a prestar atenção à precisão nas operações matemáticas, o que resulta em uma resposta mais próxima da realidade. Isso ressalta a importância da atenção aos detalhes e da interpretação correta dos dados fornecidos.

Portanto, essa questão oferece uma excelente oportunidade para integrar a trigonometria à prática, estimulando os estudantes a aplicarem seus conhecimentos matemáticos em situações cotidianas. Dessa forma, contribui para o fortalecimento da compreensão e das habilidades na resolução de problemas.

Aplicação em sala: Esse tipo de questão pode ser trabalhada em sala de aula da seguinte maneira:

1. Contextualização: Apresente uma situação-problema aos estudantes, destacando o contexto em que ela ocorre (exemplo: instalação de uma escada em uma construção).

2. Revisão de Trigonometria: Faça uma revisão rápida dos conceitos básicos de trigonometria, especialmente os relacionados aos triângulos retângulos e às funções trigonométricas.

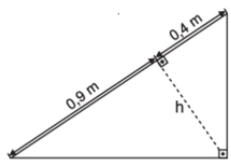
3. Discussão da Estratégia de Resolução: Explique aos estudantes como eles podem utilizar a definição de cosseno em um triângulo retângulo para determinar o comprimento da escada, dado o ângulo de inclinação e a distância até a parede.

4. Apresentação das Soluções: Peça a alguns grupos que compartilhem suas soluções com a turma, explicando o raciocínio utilizado para resolver o problema.

5. Avaliação e Discussão: Forneça *feedback* sobre as respostas dos estudantes e conduza uma discussão em sala de aula para esclarecer dúvidas e destacar os pontos-chave da resolução.

6. Exercícios: Proporcione aos estudantes outras questões semelhantes para que pratiquem a aplicação dos conceitos aprendidos em diferentes situações.

Questão 2.3.2 (Currículo de Pernambuco - EM13MAT308) Uma estrutura metálica em formato de triângulo retângulo será reforçada com a soldagem de uma nova barra de metal. Essa barra será fixada na posição do segmento que representa a altura h relativa à hipotenusa desse triângulo, conforme ilustrado na figura abaixo.



Qual é a medida, em metros, dessa nova barra de metal que será soldada nessa estrutura?

(A) 0,28 m.

(B) 0,36 m.

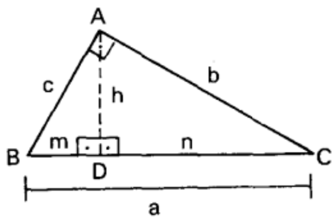
(C) 0,40 m.

(D) 0,50 m.

(E) 0,60 m.

Gabarito Oficial: Letra E.

Solução da questão: Para solucionar essa questão é necessário fazer uso das Relações Métricas no Triângulo Retângulo.



Considerando Triângulo ABC temos os seguintes elementos:

- Lados: Os lados do triângulo são denotados como a, b e c.
- Hipotenusa (a): A hipotenusa é o lado oposto ao ângulo reto e é denotada por a.
- Catetos (c, b): Os catetos c e b são os lados que formam o ângulo reto.
- Altura (h): A altura de um retângulo é a linha perpendicular da hipotenusa ao vértice oposto ao ângulo reto. A altura é frequentemente denotada por h.
- Projeções(m,n): m e n são as projeções dos catetos c e b sobre a hipotenusa a.

As relações métricas no triângulo retângulo conhecidas são:

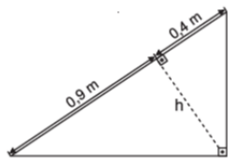
1. $a^2 = b^2 + c^2$ (Teorema de Pitágoras)

2. $h^2 = m \cdot n$

3. $b^2 = a \cdot m$

4. $c^2 = a \cdot n$

5. $a \cdot h = b \cdot c$



Usando $h^2 = m \cdot n$ temos:

$$h^2 = 0,4 \cdot 0,9 = 0,36.$$

Daí,

$$h = \sqrt{0,36} = 0,6m.$$

Comentário: Essa questão oferece uma oportunidade para explorar a habilidade (EM13MAT308) prevista no Currículo de Pernambuco, em sala de aula:

> Aplicar as relações métricas, incluindo as leis do seno e do cosseno ou as noções de congruência e semelhança, para resolver e elaborar problemas que envolvem triângulos, em variados contextos.

Ao apresentar um problema prático envolvendo um triângulo retângulo e a soldagem de uma nova barra de metal, os estudantes podem aplicar o Teorema de Pitágoras para resolver a questão. Durante uma discussão em sala, os estudantes podem ser incentivados a identificar as informações fornecidas, estabelecer relações variadas e desenvolver estratégias para encontrar a medida da nova barra de metal. A abordagem da resolução, destacando a aplicação prática dos conceitos aprendidos, pode contribui para a compreensão mais profunda desses temas.

Aplicação em sala: Um professor pode trabalhar esse tipo de questão em sala de aula da seguinte maneira:

1. Contextualização: Apresente a situação-problema aos estudantes, destacando o contexto em que ela ocorre (reforço de uma estrutura metálica com a soldagem de uma nova barra).

2. Revisão de Geometria: Faça uma revisão rápida dos conceitos básicos de Geometria, especialmente os relacionados a triângulos retângulos e as relações métricas nesses triângulos.

3. Discussão da Estratégia de Resolução: Explique aos estudantes como eles podem utilizar as relações métricas no triângulo retângulo para determinar a medida da nova barra de metal, destacando a importância do Teorema de Pitágoras nesse contexto.

4. Apresentação das Soluções: Peça a alguns estudantes que compartilhem suas soluções com a turma, explicando o raciocínio utilizado para resolver o problema e destacando as relações métricas aplicadas.

5. *Feedback* e Discussão: Forneça *feedback* sobre as respostas dos estudantes e conduza uma discussão em sala de aula para esclarecer dúvidas e destacar os pontos-chave da resolução, incentivando os estudantes a pensar criticamente sobre o problema.

6. Prática Adicional: Proporcione aos estudantes outras questões semelhantes para que pratiquem a aplicação dos conceitos aprendidos em diferentes situações, consolidando assim seu entendimento sobre as relações métricas no triângulo retângulo.

2.4 Considerações Finais

É possível perceber que cada questão analisada foca em uma única habilidade prevista no Currículo de Pernambuco, o que torna a resolução das questões simples e direta. O objetivo é avaliar as habilidades do eixo estruturante de maneira objetiva. No entanto, apesar das questões parecerem simples, a taxa de acerto nesse eixo é bastante baixa, como demonstrado nas Figuras 3 e 4, o que indica uma grande dificuldade dos estudantes em relação a esse eixo.

Ao analisar as avaliações de matemática dos anos de 2019, 2021 e 2022, observa-se que, das 26 questões presentes em cada uma das provas, menos de 25% são dedicadas ao Eixo Estruturante de Geometria, com a distribuição conforme a tabela a seguir.

Tabela 2 – CONTEÚDO/QUANTIDADE DE QUESTÕES

Conteúdo	**Quantidade de Questões**
Semelhança de Triângulos	2
Relação Métrica no triângulo Retângulo	1
Relações Trigonométricas no Triângulo Retângulo	2
Teorema de Pitágoras	1
Relação de Euler	2
Planificação de Sólidos	2

Fonte: Produzido pelo Autor

Este estudo contribui para a criação de materiais de apoio voltados ao desenvolvimento dos conhecimentos necessários para a construção das habilidades previstas na avaliação do SAEPE, especificamente no Eixo Estruturante de Geometria. Apresentamos informações sobre o contexto histórico do SAEPE e sua estrutura, além de seus objetivos. Também evidenciamos as dificuldades enfrentadas pelos estudantes no desenvolvimento dessas habilidades, especialmente no eixo de Geometria, como demonstrado pelos resultados do último ano disponível, corroborados por conversas com outros professores de matemática com experiência em sala de aula.

A análise das questões revelou uma visão geral de como as habilidades relacionadas ao eixo de Geometria têm sido cobradas nas provas do SAEPE, de forma direta, sem uma integração entre elas ou com outras habilidades.

No entanto, acreditamos que pesquisas adicionais podem ser realizadas para aprofundar os conhecimentos nos outros Eixos Estruturantes do mesmo nível ou nos níveis do ensino fundamental em que o SAEPE é aplicado, criando um banco de questões que possa orientar o desenvolvimento de aulas voltadas à melhoria dos resultados na Avaliação Externa Estadual.

Portanto, consideramos que este trabalho contribui para os esforços de outros estudos que buscam analisar e propor ações voltadas para o SAEPE.

Referências

ARRETCHE, Marta. **Avaliação de políticas públicas: uma revisão crítica**. Editora Unesp: Cortez, 2012.

BRASIL, Ministério da Educação. **Base Nacional Comum Curricular**. [S.l.: s.n.], 2018. Disponível em: <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>. Acesso em: 14 jul. 2024.

CAED. **Centro de Políticas Públicas e Avaliação da Educação**. [S.l.: s.n.], 2023. Disponível em: <https://avaliacaoemonitoramentopernambuco.caeddigital.net/#!/resultados>. Acesso em:

FERNANDES, Domingos. **Avaliar para aprender: fundamentos, práticas e políticas.** São Paulo: UNESP, 2009. P. 20.

3 Criptografia Rsa para o Ensino Médio

Simes, Eliton[1]
Gomes, Antônio[2]

Resumo: Este trabalho traz ao conhecimento dos estudantes do Ensino Médio, a importância da criptografia RSA, ferramenta primordial na codificação de mensagens, mantendo sua originalidade e integridade. Utilizando a aritmética dos restos, e sem tratar com a congruência modular, o trabalho mostra como criptografar uma mensagem pré-codificada ao associar cada caractere, da mensagem original, a um número estabelecido em uma tabela sequenciada para posterior codificação e obtendo uma sequência de números a ser transmitida. O trabalho também mostra a decodificação, bem como, estabelece os parâmetros e critérios necessários para que a criptografia seja possível, o porquê de o método funcionar e ter sua segurança garantida. Além de levar o conhecimento dessa ferramenta de uso no mundo, o trabalho propõe atividades aplicadas em sala de aula simulando a codificação e decodificação de mensagens e chaves públicas geradas na própria sala de aula.
Palavras-chave: Criptografia, RSA, Ensino Médio.

3.1 Introdução

A palavra criptografia deriva do grego ***kriptos*** (oculto) e ***graphein*** (escrever) e, o ato de criptografar sempre esteve presente em nossa História. Conforme Simon Singh, em sua obra *O livro dos códigos*, “Durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos(...)” (SINGH, 2001, p. 11). A ideia de propor, em sigilo, mensagens relevantes foi um fator preponderante no avanço da ciência, uma vez que, houve uma busca histórica na melhoria das comunicações sigilosas. Com o desenvolvimento da tecnologia e a implementação de ferramentas tecnológicas no cotidiano das pessoas, principalmente, no decorrer da evolução da internet, o ato de enviar e receber mensagens, dados e informações, com o sigilo na transmissão sempre foi uma busca constante. Advindas das guerras, as mensagens criptografadas eram peças fundamentais nas estratégias e tomadas de decisão. Durante a Segunda Guerra Mundial, vários esforços foram despendidos por ambos os lados para interceptar e desvendar as informações coletadas mobilizando inúmeros profissionais da área como matemáticos e outros cientistas. Não era tarefa fácil, mas grandes cientistas mostraram que, até então, nenhum método de criptografia tinha sido tão eficaz que não pudesse ser quebrado. Com contribuições do matemático Alan Turing na busca por

[1] UFRPE, elitonsimes@me.com
[2] UFRPE, antonio.fgomes@ufrpe.br

decodificar mensagens que levassem os Aliados a vitória, essa busca fez criar métodos, pós-guerra, que não foram tão efetivos e caíram ao longo do tempo, deixando lacunas e, talvez, evitando o avanço da tecnologia de transmissão de dados mesmo que de maneira indireta, deixando espaço para que a ciência buscasse um mecanismo efetivo e definitivo para preencher esses intervalos. A busca por transmitir e receber mensagem com a intenção de manter em segredo as estratégias de uma guerra não foi exclusividade das guerras contemporâneas, mas uma vertente de todo o embate entre oposição de ideias ao longo da história. Dentre os métodos criados, efetivamente, o mais conhecido é o RSA. Como diz Coutinho, até a edição do seu livro: "Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no *Nestscape*, o mais popular dos *softwares* de navegação da *Internet*" (COUTINHO, 2005, p. 3).

Com as iniciais dos seus inventores Ronald Linn Rivest, Adi Shamir e Leonard Max Adleman, o sistema de criptografia RSA tem eficiência garantida pela aritmética dos restos fazendo uso de números primos, mas não quaisquer primos, e sim imensos primos dificultando a fatoração, fortalecendo o método e tornando, praticamente, impossível a quebra do sigilo das mensagens, de modo a garantir a integridade e originalidade dos dados. Em sua obra Números Inteiros e Criptografia RSA, Coutinho fala de números primos de 60 ou mais algarismos. O algoritmo foi descrito em 1978, mas método equivalente foi criado pelo criptólogo britânico, Clifford Christopher Cocks, em 1973, mas ele não foi revelado até 1997. Evidentemente, na atualidade, o método de criptografia utilizando as Curvas Elípticas é uma realidade e, a partir do momento em que os computadores quânticos se popularizarem, com sua velocidade de processamento, o RSA se tornará obsoleto. Contudo, em nosso trabalho, trataremos a Criptografia RSA como, entre os métodos, o mais seguro e também é o primeiro método a possibilitar uma criptografia com chaves públicas com assinatura digital. Um usuário do sistema RSA cria uma chave pública com dois números primos muito grandes e publica juntamente com um valor auxiliar. Com os números primos em segredo, de posse da chave pública qualquer pessoa pode encriptar uma mensagem utilizando o método já publicado e, evidentemente, sendo a chave pública imensamente grande, apenas o alguém de posse dos números primos pode decodificar a mensagem de forma viável.

O sistema de criptografia RSA é de chave assimétrica e pública e o algoritmo utiliza um tema bem comum da Aritmética, a congruência modular. O tema não é abordado comumente na educação básica, especificamente, no Ensino Médio. Podemos dizer que raras as vezes um estudante da educação básica trate esse tema com real valor. Talvez, para um conjunto finito de estudantes, a congruência seja estudada para as provas olímpicas. O não estudo do assunto impossibilita o aprofundamento do algoritmo de criptografia e os estudantes passam por todo o Ensino Médio sem ouvir falar em criptografia, pelo menos, não o RSA. Isso é um fato, pois congruência não é tema do currículo escolar de

Pernambuco.

> "Pensando dessa forma, entende-se que o currículo não é meramente uma prescrição, mas, acima de tudo, um campo de lutas e tensões que traduz a escola e a sociedade que se pretende construir (SILVA, 2002). Compreendido como fruto de uma construção coletiva e democrática, ele não visa aqui apenas definir os conhecimentos a serem aprendidos e ensinados, mas permitir práticas educativas críticas, reflexivas e contextualizadas, que estejam pautadas na dialogicidade como ato primordial na busca do conhecimento daqueles que fazem o processo educativo no seu dia a dia (FREIRE, 1987)."(PERNAMBUCO, 2021, p. 19).

Dessa forma, a dissertação propõe apresentar ao professor o algoritmo de criptografia sem a necessidade de o estudante estudar as congruências modulares. É um desafio proposto e o trabalho tenta dialogar com o Novo Ensino Médio, apresentando práticas educativas que visam estimular e a desafiar o estudante, na busca de uma educação de qualidade e que incremente no seu projeto de vida mais um sentido ao estudo da matemática, em especial a Aritmética.

3.2 Fundamentos Teóricos e Metodológicos

Iniciaremos com a apresentação dos Teoremas Importantes que fundamentaram o nosso trabalho.

Divisibilidade é uma propriedade matemática que indica se um número pode ser dividido completamente por outro, sem deixar resto. Se um número é divisível por outro, dizemos que é um múltiplo do outro. A notação "b|a" indica divisibilidade. Se b|a é verdadeira, então "b" divide "a". Neste caso, "b" é divisor de "a" e, por sua vez, "a" é um múltiplo de "b". Por exemplo, 3|6 é verdadeiro, pois 3 é divisor de 6 e 6 é um múltiplo de 3.

Definição: Sejam a e $b \in \mathbb{N}$, se b divide a $(b|a)$, então existe $q \in \mathbb{N}$ tal que $a = bq$. A exemplo, $3|6$, então $6 = 3 \times 2$. A negativa dessa afirmação é representada por $b \nmid a$, significando que não existe nenhum número natural q tal que $a = bq$. Por exemplo, $3 \nmid 4$. Suponha que $b|a$ e seja $q \in \mathbb{N}$ tal que $a = bq$. O natural q é chamado de quociente da divisão de a por b. Em seguida, estabeleceremos algumas propriedades da divisibilidade.

Propriedade 2.2.1. Sejam a, b e $c \in \mathbb{N}$. Tem-se que

$i)$ $1|c$, $a|a$, $a|0$ e $0|0$.

$ii)$Se $c|b$ e $b|a$, então $c|a$.

Demonstração: Em i) decorre do fato de $c = c \cdot 1$, $a = a \cdot 1$ *e* $0 = a \cdot 0$. *Já em ii), se* $c|b$ *e* $b|a$, *então existem* $m, n \in \mathbb{N}$, *tais quais* $b = c.m$ *e* $a = b.n$. *Agora, substituindo o valor de* *b da primeira equação na segunda, temos $a = c.m.n = c.(m.n)$, o que nos mostra que $c|a$.*

Propriedade 2.2.2. Sejam a, b, c, $d \in \mathbb{N}$, com $a \neq 0$ e $c \neq 0$, então se $a|b$ e $c|d$ implica em dizer que $a.c|b.d$.
Demonstração: Se $a|b$ e $c|d$, então existem m e n naturais, tais quais $b = ma$ e $d = nc$. Portanto, $b \cdot d = (m \cdot a) \cdot (n \cdot c) = (a \cdot c) \cdot (m \cdot n)$, logo $a.c|b.d$.

Propriedade 2.2.3. Sejam a, b, $c \in \mathbb{N}$, com $a \neq 0$ e $b > c$, tais quais $a|(b + c)$ ou $a|(b-c)$. Então $a|b \Leftrightarrow a|c$.
Demonstração: Suponha que $a|(b+c)$, então existe $m \in \mathbb{N}$ tal que $b+c = am$. Se $a|b$, existe $n \in \mathbb{N}$ tal que $b = an$. Substituindo a segunda igualdade na primeira, temos $an + c = am$ e, como $c \in \mathbb{N}$, tem-se $am > an$ e, consequentemente, $m > n$. Portanto, da última igualdade, segue que $c = am$ - $an = a(m$ - $n)$, o que implica em $a|c$. Analogamente, se $a|c \Rightarrow a|b$. Por outro lado, suponha que $a|b$ e $a|c$, existem $m, n \in \mathbb{N}$, tais quais $b = am$ e $c = an$. Somando ambos os lados da igualdade, temos $b + c = am + an = a(m + n)$, o que implica em $a|(b + c)$. Para $a|(b-c)$ a demonstração é análoga.

Propriedade 2.2.4. Se a, b, $c \in \mathbb{N}$, com $a \neq 0$, e x, $y \in \mathbb{N}$ são tais quais $a|b$ e $a|c$, então $a|(xb + yc)$ e, se $xb > yc$, então $a|(xb - yc)$.
Demonstração: Como a/b e a/c, existem m e n naturais tais quais b = ma e c = na. Então, xb + yc = x(ma) + y(na) = a(xm + yn), o que nos mostra que a/(xb + yc). Para a/(xb – yc) a demonstração é análoga.

Propriedade 2.2.5. Dados a, $b \in \mathbb{N}^*$, temos que se $a|b$ então $a \leq b$.
Demonstração: Se $a|b$ então existe $c \in N^*$ tal que $b = ac$. Como c é natural, então $c \geq 1$, que por sua vez, multiplicando ambos os lados por a, temos $ac \geq a$, e como $b = ac$, decorre em $b = ac \geq a$ como queríamos mostrar.

Propriedade 2.2.6. Sejam a, b, $n \in \mathbb{N}$, com $a > b > 0$. Temos que $(a - b)|(a^n - b^n)$.
Demonstração: Usaremos indução sobre n.
Para $n = 0$ a afirmação é verdadeira, pois $a - b$ divide $a^0 - b^0 = 0$. Suponhamos que $(a - b)|(a^n - b^n)$. Vamos provar que a afirmação é válida para $n + 1$. Usaremos a técnica de somar e subtrair o mesmo termo. Escrevamos, $a^{n+1} - b^{n+1} = a.a^n - b.b^n = a.a^n - b.a^n + b.a^n - b.b^n = (a - b).a^n + b.(a^n - b^n)$. Como $(a - b)|(a - b)$ e, pela hipótese $(a - b)|(a^n - b^n)$, então, pela propriedade 2.2.4, decorre que $(a - b)|(a^{n+1} - b^{n+1})$.

Propriedade 2.2.7. Sejam a, b, $n \in \mathbb{N}$, com $a + b \neq 0$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$.

Demonstração: Usaremos indução sobre n e a mesma técnica de somar e subtrair o mesmo termo.
Obviamente, a afirmação é válida para $n = 0$, *pois* $a + b$ *divide* $a^{2.0+1} + b^{2.0+1} = a + b$. *Suponha que* $a + b$ *divida* $a^{2n+1} + b^{2n+1}$ *e vamos provar que a afirmação vale para* $n + 1$. *Temos* $a^{2(n+1)+1} + b^{2(n+1)+1} = a^{2n+1+2} + b^{2n+1+2} = a^2.a^{2n+1} + b^2.b^{2n+1} = a^2.a^{2n+1} - b^2.a^{2n+1} + b^2.a^{2n+1} + b^2.b^{2n+1} = (a^2 - b^2).a^{2n+1} + b^2.(a^{2n+1} + b^{2n+1})$. *Como* $(a + b)|(a^2 - b^2)$, *pois* $a^2 - b^2 = (a + b)(a - b)$ *e, pela hipótese de indução,* $(a + b)|(a^{2n+1} + b^{2n+1})$, *decorre que* $(a + b)|(a^{2(n+1)+1} + b^{2(n+1)+1})$.

Propriedade 2.2.8. Sejam a, b, $n \in \mathbb{N}$, com $a > b > 0$. Temos que $a + b$ divide $a^{2n} - b^{2n}$.
Demonstração: Mais uma vez, usaremos indução em n.
A afirmação é verdadeira para $n = 0$, *pois* $a + b$ *divide* $a^{2.0} - b^{2.0} = 1 - 1 = 0$. *Suponha que* $(a + b)|(a^{2n} - b^{2n})$ *para algum n natural. Queremos provar que é verdade para* $n + 1$. *Escrevamos* $a^{2(n+1)} - b^{2(n+1)} = a^{2n+2} - b^{2n+2} = a^2.a^{2n} - b^2.b^{2n} = a^2.a^{2n} - b^2.a^{2n} + b^2.a^{2n} - b^2.b^{2n} = (a^2 - b^2).a^{2n} + b^2.(a^{2n} - b^{2n})$. *Como* $(a + b)|(a^2 - b^2)$ *e, pela hipótese de indução* $(a + b)|(a^{2n} - b^{2n})$, *decorre que, pela propriedade 2.2.4,* $(a + b)|(a^{2(n+1)} - b^{2(n+1)})$.

O algoritmo da divisão é um método para calcular o quociente e o resto de uma divisão entre dois números. Ele consiste em subtrair sucessivamente o divisor do dividendo, contando quantas vezes o divisor pode ser subtraído até que o dividendo se torne menor que o divisor. O número de vezes que o divisor foi subtraído é o quociente da divisão. Suponha que desejamos dividir o número a por b, $b \neq 0$, e admita que seja possível subtrair b um número q máximo de vezes de tal forma que $0 \leq a - bq < b$. Esta diferença, $a - bq = r$, é chamada de resto e q é o quociente. Dessa última igualdade, concluímos que $a = bq + r$. Por exemplo, queremos dividir 1000 por 12. Podemos subtrair 12 de 1000 um número máximo de 83 vezes, pois $0 \leq 1000 - 12 \times 83 = 4 < 12$. Nesse exemplo, temos quociente igual a 83 e resto igual a 4, sendo possível escrever $1000 = 12.83 + 4$. De acordo com S. C. Coutinho (COUTINHO, 2005, p. 20) e A. Hefez (HEFEZ, 2011, p. 35), podemos escrever o algoritmo de divisão assim:

Algoritmo de divisão
Entrada: inteiros positivos a e b. Saída: inteiros não negativos q e r tais quais $a = bq + r$ e $0 \leq r < b$.
Etapa 1: Comece fazendo $q = 0$ e $r = a$.
Etapa 2: Se $r < b$ escreva o quociente é q e o resto é r e pare; senão vá para a Etapa 3.
Etapa 3: Se $r \geq b$ subtraia b de r, incremente q de 1 unidade e volte à Etapa 2.

Como podemos interpretar essas etapas?

A entrada é fornecida por dois inteiros positivos a e b, enquanto a saída é composta por dois inteiros não negativos q e r, tal que $a = bq + r$ e $0 \leq r < b$. O algoritmo consiste de três etapas:

Etapa 1: Comece fazendo $q = 0$ e $r = a$.

Isso significa que inicialmente o quociente é definido como 0 e o resto é definido como o valor de a.

Etapa 2: Se $r < b$ escreva o quociente é q e o resto é r e pare; senão vá para a Etapa 3.

Se o resto for menor do que b, então a divisão inteira está completa e o quociente e o resto são escritos como q e r, respectivamente. Caso contrário, o algoritmo continua para a próxima etapa.

Etapa 3: Se $r \geq b$ subtraia b de r, incremente q de 1 unidade e volte à Etapa 2.

Se o resto for maior ou igual a b, então b é subtraído do resto, o quociente é incrementado em 1 unidade e o algoritmo volta para a Etapa 2 para continuar a divisão inteira. A cada ciclo de etapas damos o nome de laço. Vejamos um exemplo.

Vamos dividir 19 por 5 seguindo os passos do algoritmo:

Na entrada temos $a = 19$ e $b = 5$ e na saída teremos q e r. Na etapa 1, o quociente começa com $q = 0$ e o resto $r = 19$. Seguindo para a etapa 2, é verificado se $r = 19 < 5 = b$, como não é, segue para a etapa 3. Nesta, é feito o teste se $r = 19 \geq 5 = b$ e, como é, então será subtraído $b = 5$ de $r = 19$, ficando $r = 19 - 5 = 14$ e será incrementado uma unidade em $q = 0 + 1$. Neste momento, foi concluído o primeiro laço e voltaremos para a etapa 2 para que o novo resto $r = 14$ seja testado. Na etapa 2, é verificado se $r = 14 < 5 = b$ e, como não é, segue para a etapa 3. Nesta, verifica-se que $r = 14 \geq 5 = b$, então será subtraído $b = 5$ de $r = 14$, ficando $r = 14 - 5 = 9$ e será incrementado uma unidade em $q = 1 + 1 = 2$. Neste momento, fecha-se o segundo laço e voltaremos para a etapa 2 para que o novo resto $r = 9$ seja testado. Na etapa 2, novamente, é verificado se $r = 9 < 5 = b$ e, como não é, segue para a etapa 3. Nesta, verifica-se que $r = 9 \geq 5 = b$, então será subtraído $b = 5$ de $r = 9$, ficando $r = 9 - 5 = 4$ e será incrementado uma unidade em $q = 2 + 1 = 3$. Neste momento, encerra-se o terceiro laço e voltaremos para a etapa 2 para que o novo resto $r = 4$ seja testado. Na etapa 2, verifica-se que $r = 4 < 5 = b$ e, dessa vez como ele é, o algoritmo escreverá "O quociente é 3 e o resto é 4" e ele para de testar.

O que garante que esse laço terá fim?

Ora, uma sequência de laços nos fornece a seguinte sequência de valores:

Valor inicial	1º laço	2º laço	3º laço	...
a	$a - b$	$a - 2b$	$a - 3b$	...

Estamos diante de uma sequência decrescente de inteiros. Sabemos que, entre a e 0, existe uma quantidade finita de inteiros, então essa sequência é finita e, eventualmente, chegará a um valor menor que b. Logo, o algoritmo sempre para.

Podemos perceber que o resultado fornecido pelo algoritmo está dentro das especificações de saída (é perceptível no exemplo dado). Perceba que q e r são obtidos pelo algoritmo, onde $r = a$ - bq e $r < b$ e, conforme a finalização de cada laço, vamos obtendo restos cada vez menores. Podemos nos perguntar: *Não corre o risco de* $r < 0$*?* A resposta é não! No algoritmo, o processo para no laço de número q. Então, o laço anterior é de número (q - 1) e, nesse caso, o resto é a - $b(q$ - $1)$ que ainda é maior ou igual a b pois haverá mais um laço para chegar no laço de número q. Sendo assim, a - $b(q$ - $1) \geq b$ e, no último laço, subtraindo b de ambos os lados da desigualdade a - $b(q$ - $1)$ - $b \geq b$ - b chegamos a a - $bq \geq 0$, mostrando que o resto $r = a$ - $bq \geq 0$.

Além disso, em $a = bq + r$, os valores de q e r são únicos. Mas o que significa dizer que q e r são únicos?

Suponha que dados os números inteiros positivos a e b a duas pessoas, a intenção seja obter q e r da forma que elas quiserem satisfazendo a relação $a = bq+r$ com $0 \leq r < b$. A unicidade do quociente e do resto significa dizer que estas pessoas encontrarão os mesmos valores.

Digamos que uma delas tenha encontrado q e r, $0 \leq r < b$ e a outra q' e r', $0 \leq r' < b$. Por enquanto, sabemos apenas que $a = bq + r$ e que $a = bq' + r'$ e o objetivo é mostrar que $q = q'$ e $r = r'$. Sem perda de generalidade, seja $r \geq r'$, e das duas equações obtemos $r = a - bq$ e $r' = a - bq'$.

Subtraindo uma da outra, obtemos $r - r' = (a - bq) - (a - bq') = b(q' - q)$. Por outro lado, tanto r como r' são menores do que b e como estamos supondo $r \geq r'$, então $r - r' \geq 0$ e, por sua vez, $0 \leq r - r' < b$. Dessa forma, como $r - r' = b(q' - q)$, concluímos que $0 \leq b(q' - q) < b$. Desta última desigualdade, suponha que q' - $q \geq 1$, e multiplicando ambos os lados da desigualdade por b temos $b(q'$ - $q) \geq b$ e isso é um absurdo pois sabemos que $b(q' - q) < b$. Logo, $0 \leq q'$ - $q < 1$, então q' - $q = 0 \Rightarrow q' = q$. Disto segue, de imediato, que $r - r' = b(q' - q) = b(q' - q') = b \cdot 0 = 0$ e, sendo assim, $r - r' = 0 \Rightarrow r = r'$ e a unicidade fica verificada.

MÁXIMO DIVISOR COMUM (MDC)

Sejam a e b números naturais diferentes de zero. Definimos o máximo divisor comum (mdc) entre a e b o número d, tal que d satisfaz as seguintes condições:

1) d é um divisor comum de a e b;

2) d é divisível por todo divisor comum de a e b, ou seja, se c é um divisor comum de a e b, então $c|d$.

Então, se d é o mdc de a e b, e c é um divisor comum desses números, tem-se $c|d$ pois d é o maior divisor comum de a e b. Logo $d = c \cdot k$, com k natural e $k \geq 1$ e, multiplicando ambos os lados da última desigualdade por c, temos $d = c \cdot k \geq c$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os seus divisores comuns. Além disso, se d e d' são dois mdc's de um mesmo par de números a e b, então $d \leq d'$ e $d' \leq d$ nos levando a concluir que $d = d'$. Dessa forma, o mdc de dois números é único. Denotamos o mdc de a e b como sendo (a, b). Se a e b são números naturais, tem-se que $(1, a) = 1$, $(a, a) = a$ e $(a, a \cdot n) = a$. Ainda mais, se

$$a|b \Leftrightarrow (a, b) = a$$

De fato, se $a|b$, então $b = a \cdot k$ com $k \geq 1$ e o $(a, a \cdot k) = a$. Reciprocamente, se $(a, b) = a$, segue-se que $a|b$. Vejamos como Euclides prova a existência do mdc de dois números.

(Lema de Euclides). Sejam a, b, $n \in \mathbb{N}$ com $a < na < b$. Se existe $(a, b - na)$, então (a, b) existe e $(a, b) = (b, b - na)$.
Demonstração: Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que, pela propriedade 2.2.4, $d|na$ e $d|(b - na + na) = b$. Logo, d é um divisor comum de a e b. Agora, conforme a condição 2), imagine que c seja um divisor comum de a e b. Logo, $c|a \Rightarrow c|na$ e, como $c|b$, pela propriedade 2.2.4, $c|(b - na)$ e, portanto, $c|d$. Tudo isso nos prova que $d = (a, b)$.

(Algoritmo de Euclides). O algoritmo de Euclides é um método iterativo para o cálculo do máximo divisor comum (MDC) de dois números e, também, é conhecido como o método das divisões sucessivas. Nas escolas, entre os alunos, é conhecido como o método do jogo da velha.
Dados dois naturais a e b, tal que $1 < b < a$ e $b \nmid a$, aplicaremos sucessivamente o algoritmo da divisão para obter a sequência de igualdades:

$$\begin{array}{ll}
a = bq_1 + r_1 & \text{onde } 0 \leq r_1 < b \\
b = r_1 q_2 + r_2 & \text{onde } 0 \leq r_2 < r_1 \\
r_1 = r_2 q_3 + r_3 & \text{onde } 0 \leq r_3 < r_2 \\
r_2 = r_3 q_4 + r_4 & \text{onde } 0 \leq r_4 < r_3 \\
\ldots & \ldots \\
r_{n-2} = r_{n-1} q_n + r_n & \text{onde } 0 \leq r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} &
\end{array}$$

Este procedimento não terá iterações indefinidamente, se assim fosse, teríamos uma sequência infinita de números naturais $a > r_1 > r_2 > r_3 > \ldots$ pois, como a e os $r_{i's}$ são elementos de um subconjunto não vazio dos naturais, então ele terá um elemento mínimo. Dessa forma, para algum n, teremos $r_n | r_{n-1}$. Temos, então, o $mdc(a, b) = r_n$, sendo r_n o último resto não nulo no processo de divisão anterior. De fato, pois sejam a e b números naturais e (a, b) o mdc desses números. Então,

$(a,b) = (bq_1 + r_1, b)$ e pelo Lema de Euclides, teremos
$(a,b) = (bq_1 + r_1$ - $bq_1, b)$
$(a,b) = (r_1, b)$ e por sua vez $b = r_1q_2 + r_2$
$(a,b) = (r_1, r_1q_2 + r_2)$
$(a,b) = (r_1, r_1q_2 + r_2$ - $r_1q_2)$
$(a,b) = (r_1, r_2)$
$(a,b) = (r_2q_3 + r_3, r_2)$
$(a,b) = (r_2, r_2q_3 + r_3$ - $r_2q_3)$
$(a,b) = (r_2, r_3)$
...
$(a,b) = (r_{n-2},\, r_{n-1})$ e como $r_{n-2} = r_{n-1}q_n + r_n$
$(a,b) = (r_{n-1}q_n + r_n, r_{n-1})$
$(a,b) = (r_{n-1}, r_{n-1}q_n + r_n - r_{n-1}q_n)$
$(a,b) = (r_{n-1},\, r_n) = r_n$

O algoritmo acima pode ser escrito, na prática, da forma a seguir. Eis o motivo, pelo qual, os alunos conhecerem o método como jogo da velha por fazer uma intertextualidade com o famoso passa-tempo. Para iniciar, façamos a divisão $a = bq_1 + r_1$ escrevendo conforme o esquema:

	q_1	
a	b	
r_1		

Continuaremos fazendo a divisão $b = r_1q_2 + r_2$ ainda no esquema.

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Vamos prosseguindo, enquanto possível, até a obtenção de um r_n divisível por r_{n-1}.

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a,b)$
r_1	r_2	r_3	r_4	...	r_n	0	

Vejamos o exemplo: Calculemos o mdc de 657 e 306.

	2	6	1	4
657	306	45	36	9
45	36	9	0	

Observando, no exemplo acima, o algoritmo de Euclides nos fornece os restos:
$9 = 45 - 1 \cdot 36$
$36 = 306 - 6 \cdot 45$
$45 = 657 - 2 \cdot 306$

Substituindo esses restos, temos:
$9 = 45 - 1 \cdot (306 - 6 \cdot 45) = 7 \cdot 45 - 306 = 7 \cdot (657 - 2 \cdot 306) - 306 = 7 \cdot 657 - 15 \cdot 306$

Temos, então, que
$(657, 306) = 9 = 7 \cdot 657 - 15 \cdot 306$

Perceba que conseguimos, por meio do Algoritmo de Euclides, escrever de trás para frente, o $(657, 306) = 9$ como um múltiplo de 657 menos um múltiplo de 306. O Algoritmo de Euclides nos fornece um meio prático de escrever o mdc de dois números por meio de uma diferença entre dois múltiplos desses números.

O TEOREMA DE BÈZOUT

O Teorema de Bèzout, também conhecido como identidade de Bèzout, afirma que para quaisquer dois números inteiros a e b, existem inteiros x e y tais quais $ax + by = (a, b)$, onde (a, b) é o máximo divisor comum de a e b. Em outras palavras, o teorema de Bèzout garante que é sempre possível expressar o máximo divisor comum de dois números inteiros como uma combinação linear deles, utilizando coeficientes inteiros.

Teorema de Bèzout: Sejam a, $b \in \mathbb{Z}^*$, existem $x, y \in \mathbb{Z}$, tais quais, $ax + by = (a, b)$, onde (a, b) é o mdc de a e b.

Demonstração: Seja o conjunto $X = \{ax+by/x, y \in \mathbb{Z}\}$ e o subconjunto $S = X \cap \mathbb{N}^* \subseteq \mathbb{N}$. S é não vazio, pois, tomando $x = a$ e $y = b$, temos $ax + by = a \cdot a + b \cdot b = a^2 + b^2 \geq 2$. Sendo S um subconjunto dos naturais, sabemos que existe um elemento mínimo e, digamos, que seja $d \geq 1$. Se $d \in S$, então $d = ax_0 + by_0$. Se $d = (a, b)$, então d satisfaz as duas condições abaixo:

1) *$d|a$ e $d|b$;*
2) *Se $c|a$ e $c|d \Rightarrow c|d$.*

Em 1), suponha por absurdo, que $d|a$ e $d|b$ é falso, isto é, $d \nmid a$ ou $d \nmid b$. Sem perda de generalidade, suponha que $d \nmid a$. Então, $a = dq + r$, onde $1 \leq r < d$, e, por conseguinte, $r = a$ - dq. Perceba que $r \in S$, pois r pode ser escrito na forma $r = ax + by$. De fato, substituindo $d = ax_0 + by_0$, temos $r = a$ - $dq = a$ - $q(ax_0 + by_0) = a(1$ - $x_0q) + b(-y_0q)$. Mas $r < d$ é absurdo, uma vez que, d é o menor elemento de S. Logo, $d|a$ e $d|b$.

Em 2), se $c|a$ e $c|b$, então c divide qualquer combinação linear de a e b, ou seja, $c|(ax_0 + by_0) = d$. Dessa forma, $c|d$.

OS NÚMEROS PRIMOS

A seguir, apresentamos a demonstração da infinitude dos números primos conhecida como prova por contradição ou redução ao absurdo. Segundo Singh(SINGH, 2016, p. 20), esta é a forma como Euclides abordou o assunto em uma linguagem atual:

Supondo que o número de primos seja finito e que todos esses primos tenham sido reunidos em uma lista: $p_1, p_2, p_3, \cdots, p_n$, podemos explorar as consequências dessa declaração multiplicando todos os primos dessa lista e incrementando 1, o que cria um novo número: $N = p_1 \times p_2 \times p_3 \times \cdots \times p_n + 1$. Esse novo número N pode ser ou não ser um primo, mas, de qualquer forma, contradiz a afirmação inicial, pois, se N é primo, então não se encontra na lista original. Por consequência, a afirmação de que temos uma lista completa é falsa; se N não é primo, então deve ter divisores primos. Esses divisores devem ser novos primos, pois os primos contidos na lista original produzirão o resto 1 se dividir N. Portanto, mais uma vez, a afirmação de que temos uma lista completa é falsa.

Sendo assim, de fato, a lista de primos é infinita!

Se temos p e q primos e a um número natural, podemos analisar dois fatos:
I) Se $p \mid q$ (p divide q), como q é primo, então decorre que $p = 1$ ou $p = q$. Como p também é primo, então segue que $p = q$.
II) Se $p \nmid a$ (p não divide a), então $(p, a) = 1$. De fato, pois se $(p, a) = d$, então d divide a e divide p. Como p é primo então só resta $d = 1$.

Ainda sobre, considere a, b e p naturais não nulos, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$. Para tal, basta provar que, se $p \mid ab$ e $p \nmid a$, então $p \mid b$. Mas, se $p \mid ab$, então $ab = pc$ e, dessa forma, se $p \nmid a$ então $(a, p) = 1$ e existem m e n, naturais, tais quais $an - pm = 1$. Multiplicando, ambos os lados, por b ficaremos com $abn - bpm = b$. Agora, basta substituir nesta última identidade ab por pc e ficaremos com $pcn - bpm = b$ que, evidenciando p, temos $p(cn - bm) = b$, na qual $p \mid b$.

(Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de forma única, a não ser pela ordem, como um produto de primos.

Demonstração: Usaremos indução. Se $n = 2$, o resultado fica verificado. Suponha que o resultado seja válido para todo natural menor do que n e temos que provar que vale para n. Se n é primo, nada temos a demonstrar. Vamos supor que n é composto, então existem n_1 e n_2 tais quais $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, existem primos $p_1, p_2, \ldots, p_s$ e $q_1, q_2, \ldots, q_r$ tais quais $n_1 = p_1 \cdot p_2 \cdot \cdots \cdot p_s$ e $n_2 = q_1 \cdot q_2 \cdot \cdots \cdot q_r$. Sendo assim, $n = p_1 \cdot p_2 \cdot \cdots \cdot p_s \cdot q_1 \cdot q_2 \cdot \cdots \cdot q_r$. Sabemos que essa forma é única então, para provar sua unicidade, suponha que $n = p_1 \cdot p_2 \cdot \cdots \cdot p_s = q_1 \cdot q_2 \cdot \cdots \cdot q_r$. Podemos imaginar que $p_1 \mid q_1 \cdot q_2 \cdot \cdots \cdot q_r$, mas como os $q_{i's}$ são primos, então, $p_1 = q_i$, para algum i podemos supor que seja $p_1 = q_1$ (propriedade forte dos números primos). Consecutivamente, reorganizando e, portanto, $p_2 \cdot \cdots \cdot p_s = q_2 \cdot \cdots \cdot q_r$. Como $p_2 \cdot \cdots \cdot p_s < n$, a hipótese de indução nos leva a $s = r$ e os p_j e q_i são iguais aos pares.

TEOREMAS PARA O RSA

Teorema 1. Seja a, b e n, números naturais. Se r_a e r_b são os restos das divisões de a por n e de b por n, respectivamente, então o resto da divisão de $a+b$ por n é igual ao resto da divisão de $r_a + r_b$ por n.

Demonstração: Seja $a = n.q_a + r_a$ *e* $b = n.q_b + r_b$*, com* $0 \leq r_a, r_b \leq n$*, logo* $a + b = n.q_a + r_a + n.q_b + r_b = n.(q_a + q_b) + r_a + r_b$ (1)

E seja r *o resto da divisão de* $r_a + r_b$ *por* n*. Então, podemos escrever esta soma como sendo* $r_a + r_b = n.q + r$*,* $0 \leq r \leq n$*, e substituindo esta soma em* (1)*, temos:*

$a + b = n.(q_a + q_b) + r_a + r_b = n.(q_a + q_b) + n.q + r$

$a + b = n(q_a + q_b + q) + r.$ ■

Considere que r_i, com $i \in \mathbb{N}$ e $i \geq 1$ e, ainda $0 \leq r_i \leq n$, sejam os restos das divisões de a_i por n. Seja $a_i = n.q_i + r_i$ e, fazendo a soma de todos esses $a_{i's}$, temos:

$$a_1 + a_2 + a_3 + \cdots + a_k = n.q_1 + r_1 + n.q_2 + r_2 + n.q_3 + r_3 + \cdots + n.q_k + r_k \Leftrightarrow$$
$$a_1 + a_2 + a_3 + \cdots + a_k = n.(q_1 + q_2 + q_3 + \cdots + q_k) + (r_1 + r_2 + r_3 + \cdots + r_k) \ (1).$$

Seja r o resto da divisão de $r_1 + r_2 + r_3 + \cdots + r_k$ por n. Então, podemos escrever esta soma como sendo $r_1 + r_2 + r_3 + \cdots + r_k = n.q + r$, $0 \leq r \leq n$, e substituindo esta soma em (1), temos:

$$a_1 + a_2 + a_3 + \cdots + a_k = n.(q_1 + q_2 + q_3 + \cdots + q_k) + n.q + r \Leftrightarrow$$
$$a_1 + a_2 + a_3 + \cdots + a_k = n.(q_1 + q_2 + q_3 + \cdots + q_k + q) + r.$$

Dessa forma, o Teorema 1 é válido para k parcelas.

Vejamos, agora, um exemplo que será bem frequente no método de criptografia RSA, o resto da divisão de produtos entre números.

Sabendo que o resto da divisão de 1023 por 20 é 3, pois $1023 = 20.q+3$ e o resto da divisão de 247 por 20 é 7, pois $247 = 20.t+7$, qual o resto da divisão $1023 \times 247 = 252681$ por 20?

Fazendo $1023 \times 247 = (20.q + 3).(20.t + 7)$ e desenvolvendo a distributividade, temos:

$1023 \times 247 = 20q.20t + 20q.7 + 3.20t + 3.7$

$1023 \times 247 = 20(20qt + 7q + 3t) + 21$

Perceba que, ao multiplicar 1023 por 247 temos, como resultado, um múltiplo de 20 mais o produto dos restos (21). É possível reescrever essa identidade:

$1023 \times 247 = 20(20qt + 7q + 3t) + 21 = 20(20qt + 7q + 3t) + 20 + 1$ que equivale a $1023 \times 247 = 20(20qt + 7q + 3t + 1) + 1.$

E assim, o resto da divisão do produto $1023 \times 247 = 252681$ por 20 é 1, exatamente o resto da divisão do produto dos restos por 20. Com essa premissa, podemos determinar o resto da divisão de $1027^2 = 1027 \times 1027$ por 20. Como 1027 deixa resto 7 na divisão por 20, então 1027^2 deixará resto igual ao resto da divisão de 7^2 por 20. Logo, $7^2 = 49$, deixa resto 9. O resto da divisão de 1027^2 por 20 é 9.
O teorema abaixo formaliza o nosso exemplo e estende para k fatores.

Teorema 2. Sejam os naturais r_1, r_2, ..., r_k os restos das divisões de a_1, a_2, ..., a_k por n, respectivamente, com $k \in \mathbb{N}$. O resto da divisão de $a_1 \times a_2 \times ... \times a_k$ por n é igual ao resto da divisão de $r_1 \times r_2 \times ... \times r_k$ por n.

Demonstração: Primeiramente, mostremos para dois naturais.
Sejam $a_1 = n.q_1 + r_1$ *e* $a_2 = n.q_2 + r_2$ *e* $0 \leq r_1, r_2 < n$ *naturais. Então,*
$a_1 \times a_2 = (n.q_1 + r_1).(n.q_2 + r_2)$
$a_1 \times a_2 = n^2q_1q_2 + nq_1r_2 + nq_2r_1 + r_1r_2 = n(nq_1q_2 + q_1r_2 + q_2r_1) + r_1r_2$
Considere $r_1r_2 = n.m + r$, *com* $0 \leq r < n$, *que substituindo na igualdade acima temos:*
$a_1 \times a_2 = n(nq_1q_2 + q_1r_2 + q_2r_1) + n.m + r$
$a_1 \times a_2 = n(nq_1q_2 + q_1r_2 + q_2r_1 + m) + \boldsymbol{r}$
Sendo $nq_1q_2 + q_1r_2 + q_2r_1 + m = p$ *um natural. Então,* $a_1 \times a_2 = np + r$ *deixa resto* r *na divisão por* n. *Dessa forma, o resto da divisão do produto de dois naturais por n é igual ao resto da divisão do produto dos restos por n.*

Agora, vamos estender para k fatores:

Considere o produto $a_1 \times a_2 \times \cdots \times a_{k-1} \times a_k$. *Como os* $a_{i's}$ *são números naturais e a multiplicação é uma operação fechada no conjunto dos números naturais, temos que* $a_1 \times a_2 \times ... \times a_{k-1}$ *também é um número natural e pode ser escrito na forma* $a_1 \times a_2 \times ... \times a_{k-1} = nq + r_{k-1}$, *onde* $0 \leq r_{k-1} = a_1 \times a_2 \times ... \times a_{k-1} - nq < n$. *Sendo assim,* $a_1 \times a_2 \times ... \times a_{k-1} \times a_k = (nq + r_{k-1}).a_k$. *Sabendo que* $a_k = nq_k + r_k$, *então* $(nq + r_{k-1}).a_k = (nq + r_{k-1}).(nq_k + r_k) = n(qq_k + qr_k + q_kr_{k-1}) + r_{k-1}.r_k$. *Seja* r *o resto da divisão de* $r_{k-1}.r_k$ *por* n. *Então podemos escrever esse produto como sendo* $r_{k-1}.r_k = np + r$, $p \in \mathbb{N}$, *e substituindo na igualdade anterior temos,* $(nq + r_{k-1}).a_k = n(qq_k + qr_k + q_kr_{k-1} + p) + r$.

Corolário. Em particular, se r_a é o resto da divisão de a por n, então o resto da divisão de a^k por n é igual ao resto da divisão de $(r_a)^k$ por n.

Demonstração: Sejam a, n, q, p *e* r_a, *números naturais, tais quais,* $a = nq + r_a$ *e o natural* $k > 1$. *Fazendo* a^k, *temos* $a^k = a \times a \times a \times \cdots \times a$, *que é equivalente a* $a^k = (nq + r_a) \times (nq + r_a) \times (nq + r_a) \times \cdots \times (nq + r_a)$. *Pelo Teorema 2, pode-se escrever* $a^k = (nq + r_a) \times (nq + r_a) \times (nq + r_a) \times \cdots \times (nq + r_a) = np + (r_a)^k$. *Sendo assim, uma* *vez sabendo r_a, o resto da divisão de a^k por n é igual ao resto da divisão de $(r_a)^k$ por n.*

Vejamos um exemplo:

Obtenha o resto da divisão 13^7 **por** 35.

Fazendo $13^2 = 169$, percebemos que ele deixa resto 29 na divisão por 35 pois $169 = 4 \cdot 35 + 29$. Como $13^7 = (13^2)^3.13$, o resto da divisão 13^7 por 35, fazendo o uso do Corolário, é equivalente ao resto de $(29)^3.13$, e assim, podemos escrever como sendo $29^2.29.13$. Sabendo que $29^2 = 841$ deixa resto 1 na divisão por 35 pois $841 = 35.24 + 1$, então apliquemos mais uma vez o Corolário e o resto de $29^3.13 = 29^2.29.13$ por 35 é equivalente ao resto de $1.29.13 = 377$ que deixa resto 27 na divisão por 35. Então, o número 13^7 deixa resto na divisão por 35 igual a 27.

UTILIZAÇÃO DA CALCULADORA NA OBTENÇÃO DE RESTOS

O uso da calculadora deve ser estimulado pelo professor em sala de aula desde que o estudante já domine os algoritmos das operações. Então, podemos utilizar a calculadora no auxílio da obtenção do resto da divisão de números grandes.

Teorema 3. Sejam n e d números naturais. Para encontrar o resto da divisão de n por d, pela calculadora, basta dividir n por d, depois subtrair a parte inteira e, em seguida, multiplicar por d.

Demonstração: Seja $n = d \cdot q + r$, com $r < d$. Façamos, na calculadora, a divisão de n por d e teremos:

$$\frac{n}{d} = \frac{dq}{d} + \frac{r}{d} = q + \frac{r}{d} \text{ onde } q \text{ é a parte inteira e } \frac{r}{d} \text{ é parte decimal pois } \frac{r}{d} < 1.$$

Logo, subtraindo a parte inteira q de $q + \frac{r}{d}$, teremos $q + \frac{r}{d} - q = \frac{r}{d}$. Agora, multipliquemos esse resultado por d e encontraremos o resto da divisão de n por d. E segue, $\frac{r}{d} \times d = \boldsymbol{r}$.

Vejamos alguns exemplos:

Qual é o resto da divisão 18.435 por 141?

Dividindo, na calculadora, obtemos 130,7446808510638. Subtraiamos a parte inteira 130 e ficamos com 0,7446808510638. Agora, multipliquemos pelo divisor 141 e obteremos o resto: 0,7446808510638 x 141 = 105.

O resto da divisão de 18.435 por 141 é igual a 105.

Obtenha o resto da divisão 13^7 por 35.

Para encontrar a potência de 13^7, na calculadora científica, primeiramente, teclamos o 13, depois a tecla x^y, depois o expoente 7 e a tecla de igualdade (=) encontrando 62.748.517. Divida este resultado por 35 e encontraremos $1.792.814, 7714285714285714285714286$. Subtraindo a parte inteira 1.792.814, encontraremos $0, 7714285714285714285714286$. Agora, basta multiplicar esse decimal por 35 e encontraremos o resto: $0, 7714285714285714285714286 \times 35 = 27$.

O resto da divisão 13^7 por 35 é igual a 27.

CODIFICANDO UMA MENSAGEM PELO MÉTODO RSA

Partiremos da escolha da palavra que queremos codificar. Vamos escolher a palavra **RECIFE**. Antes de iniciar o processo, por razões óbvias, toda mensagem seja ela uma letra, número ou um caractere tem que ser submetido a uma pré-codificação. Utilizaremos a tabela de pré-codificação abaixo:

Tabela 3 – Pré-codificação do alfabeto

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

Fonte: Feita pelo autor

A escolha em começar essa pré-codificação pelo 10 ou 11 é arbitrária, ficando a cargo do leitor, se assim desejar, alterar a tabela e começar por outro número. *Deve-se, apenas, levar em consideração a exigência de todas as letras e caracteres estarem associados a números com a mesma quantidade de dígitos para evitar confusões futuras na decodificação.* Por exemplo, se começássemos a pré-codificação do 1, então, no número 12 não saberíamos dizer se temos AB ou a letra L, letra esta que está na décima segunda posição. Dito isto, a mensagem a ser codificada **(Recife)** será representada pelo número **271412181514**. O próximo passo é a determinação do par de números **(n, e)**, **Chave de Codificação do Sistema RSA**, com n = p·q, sendo p e q números primos e o **mdc** [**e, (p - 1).(q - 1)**] = **1**, sendo **e** qualquer número que satisfaça este mdc. Para efeito de praticidade, utilizaremos os primos **p = 5** e **q = 7**, gerando a Chave de Codificação **n = 35** e **e = 7**. O processo de criptografia requer alguns critérios que devem ser seguidos e um deles é: separar a mensagem a ser criptografada em blocos, não importando se serão blocos de um, dois, três ou mais algarismos ou até mesmo tamanhos variados, exige-se que cada bloco não seja maior do que n. Tratando-se do nosso exemplo, para uma chave pequena, ficamos limitados a blocos de no máximo dois dígitos, mas, quando os primos são muito grandes gerando uma imensa chave, fica evidente a liberdade de tomarmos esses blocos de tamanhos variados. Outro critério é não iniciar os blocos por 0 e, **MUITO IMPORTANTE** é, uma vez os blocos codificados, não poderemos juntá-los e formar um longo número. Se isso for feito, será impossível decodificar a mensagem. Dessa forma, os blocos a serem codificados são **27-14-12-18-15-14**.

Vamos, agora, codificar cada bloco por vez e, para isso, o método impõe uma regra: devemos pegar cada bloco **b** a ser codificado e elevar ao número natural **e**, obtendo o resto **a** da divisão por **n**, onde **a** será a codificação do bloco **b**. Ou seja, em termos matemáticos, nós queremos obter:

$$b^e = n \cdot q + \mathbf{a} \text{ com } 0 \leq a < n$$

Essa é a regra de codificação do método RSA!

Tomaremos o primeiro bloco 27, e assim, vamos obter o resto da divisão de 27^7 por 35.

Então, tome $27^7 = (27^2)^3 \cdot 27$. Como $27^2 = 729$ deixa resto 29 na divisão por 35, nos apoiando no Corolário, podemos procurar o resto $(29)^3 \cdot 27$ que, automaticamente podemos fatorar $29^2 \cdot 29 \cdot 27$. Sabendo que $29^2 = 841$ e este deixa resto igual a 1 na divisão por 35 ($841 = 24 \cdot 35 + 1$), podemos encontrar, nos apoiando no Teorema 2, o resto da divisão por 35 do número $1 \cdot 29 \cdot 27 = 783$ que deixa resto 13 na divisão por 35. Dessa forma, o número 27^7 deixa resto 13 na divisão por 35.
Logo, o primeiro bloco 27, criptografado é igual a 13

Vamos encriptar o segundo bloco 14 e procurar o resto da divisão de 14^7 por 35. Fatorando de maneira análoga, $(14^2)^3 \cdot 14$, como $14^2 = 196$ deixa resto 21 na divisão por 35 ($196 = 5 \cdot 35 + 21$), usando o Corolário, podemos procurar o resto da divisão de $(21)^3 \cdot 14$ por 35 que, por sua vez, podemos escrever $21^2 \cdot 21 \cdot 14 = 441 \cdot 294$. Perceba que 441 e 294 deixam resto 21 e 14, respectivamente, na divisão por 35. Então, usando o Teorema 2, procuremos o resto da divisão de $21 \cdot 14 = 294$ por 35. Este deixa resto 14 na divisão por 35. Dessa forma, o número 14^7, ao ser dividido por 35, deixa resto 14.
Logo, o segundo bloco 14 criptografado é igual a 14.

Tomando o terceiro bloco 12, vamos buscar o resto da divisão de 12^7 por 35. Fatorando para uma potência mais simples, temos $12^7 = (12^2)^3 \cdot 12$. Como $12^2 = 144$ deixa resto 4 na divisão por 35, utilizando o Corolário, vamos buscar o resto da divisão de $(4)^3 \cdot 12 = 768$ por 35 e obtemos 33.
Logo, o terceiro bloco 12 criptografado é igual a 33.

Agora, tome o quarto bloco 18 e vamos procurar o resto da divisão de 18^7 por 35. Fatorando $18^7 = (18^2)^3 \cdot 18$ e sabendo que $18^2 = 324$ deixa resto 9 na divisão por 35, mais uma vez usando o Corolário, vamos buscar o resto da divisão $(9)^3 \cdot 18$ por 35. Nesse caso, de maneira alternativa ao que estamos fazendo, podemos efetuar esse produto sendo igual a 13.122 e obtemos resto 32 na divisão por 35. Dessa forma, o resto da divisão de 18^7 por 35 é igual a 32.
Logo, o quarto bloco 18 criptografado é igual a 32.

Tomando o penúltimo bloco 15, vamos procurar o resto da divisão de 15^7 por 35. Como $15^7 = (15^2)^3 \cdot 15$, e sabendo que $15^2 = 225$ deixa resto 15 na divisão por 35, fazendo uso do Corolário, podemos buscar o resto da divisão de $(15)^3 \cdot 15$ e, por sua vez, $15^2 \cdot 15^2$ e como já sabemos que 225 deixa resto 15 na divisão por 35, então esse produto pode ser trocado por $15 \cdot 15 = 225$, com base no Teorema 2, que deixa resto 15 na divisão por 35. Dessa forma, 15^7 deixa resto 15 na divisão por 35.
Logo, o quinto bloco 15 criptografado é igual 15.

Chegamos ao último bloco 14 que já foi criptografado.

Sendo assim, os blocos **27-14-12-18-15-14** serão transmitidos criptografados sob os blocos **13-14-33-32-15-14.**

DECODIFICANDO UMA MENSAGEM CODIFICADA EM RSA

Mostraremos como fazer o processo inverso, a decodificação de mensagem, utilizando como exemplo a mensagem encriptada anteriormente, no caso, **13-14-33-32-15-14**. Para decodificar precisaremos de uma chave de decodificação e essa chave é o par **(n, d)**, onde **d** é o número que multiplicado por **e** deixará resto 1 na divisão por **[(p - 1)(q - 1)]** sendo **e** expoente e **p, q** primos utilizados no processo de codificação. Ou seja, temos que encontrar o **d** que resolva a identidade $e \cdot d = t \cdot [(p-1)(q-1)] + 1$, onde t é um número natural, o quociente da divisão de $(e \cdot d)$ por $[(p-1)(q-1)]$. Como $(d \cdot e)$ deixa resto 1 na divisão por $(p-1)(q-1)$, então d é chamado de inverso de e com respeito à $(p-1)(q-1)$. Lembrando que, no exemplo que fizemos a codificação da palavra RECIFE, os primos escolhidos foram o p = 5 e q = 7 gerando a chave n = 35 e e = 7. Então, como d é o inverso de e, devemos resolver a seguinte identidade:

$$7 \cdot d = t \cdot [(5-1)(7-1)] + 1$$
$$7 \cdot d = t \cdot (24) + 1$$

Estamos procurando o primeiro número natural que multiplicado por 7 dê resto 1 na divisão por 24. Fazendo uma varredura para alguns naturais, começando de 1, percebemos que essa resposta é o 7 pois $7 \cdot 7 = 49 = 2 \cdot (24) + 1$. Logo, d = 7. Uma vez estabelecido o valor de d, vamos usar uma regra similar a que nós utilizamos na codificação:

$$a^d = k \cdot n + b$$

Onde **n** é a chave de encriptação que utilizamos para codificar, **b (mensagem original)** será o resto da divisão de a^d por **n** e, por conseguinte, a decodificação da mensagem **a (mensagem codificada)**. Precisamos esclarecer um ponto facilitador: quando falamos em "Encontrar a solução da identidade $a^d = k \cdot n + b$", significa nos limitar, apenas, a encontrar o resto b da divisão, não nos importando qual valor assumido por k, uma vez que, o objetivo do nosso trabalho é codificar e decodificar em RSA e o método exige a obtenção de restos.

Sendo assim, para o primeiro bloco 13, vamos encontrar a solução da igualdade $13^7 = k_1 \cdot 35 + b$ que é equivalente a procurar o resto da divisão de 13^7 por 35. Como $13^7 = (13^2)^3.13$, sabemos que $13^2 = 169$ e deixa resto 29 na divisão por 35 pois $169 = 4 \cdot 35 + 29$. Fazendo o uso do Corolário, podemos procurar o resto, na divisão por 35, de $(29)^3 \cdot 13$ que pode ser reescrito, para facilitar, como $(29)^2 \cdot 29 \cdot 13$. A potência $29^2 = 841$ deixa resto 1 na divisão por 35 e o produto $29 \cdot 13 = 377$ deixa resto 27 na divisão por 35. Então, se apoiando no Teorema 2, 1.27 = 27 que deixa resto 27 na divisão por 35. Dessa forma, 13^7 deixa resto 27 na divisão por 35.
Logo, o bloco 13 decodificado é igual a 27.

Uma maneira de estimular o pensamento do estudante a buscar uma forma prática, uma vez que, não estamos usando a calculadora, é pensar que a potência 13^2 *deixa resto* -6 *na divisão por 35* $(13^2 = 5 \cdot 35 - 6)$, *e assim, buscar o resto da divisão de* $(-6)^3 \cdot 13 = -216 \cdot 13$ *por 35 que é mais prático. Perceba que* -216 *deixa resto* -6 *na divisão por 35 pois* $-216 = (-6) \cdot 35 - 6$ *(neste caso, basta assumir os valores em módulo) e assim,* $-6 \cdot 13 = -78$ *e, somando o menor múltiplo de 35* $(-78 + 3 \cdot 35)$, *encontraremos 27. Cabe ao professor estimular seu aluno a novas formas de pensar dando possibilidades de escolhas para seguir o melhor caminho.*

Tomando o segundo bloco, 14, vamos encontrar o resto da divisão de 14^7 por 35, ou seja, queremos a solução da igualdade $14^7 = k_2 \cdot 35 + b$. Sendo assim, queremos o resto da divisão de 14^7 por 35. Podemos fatorar essa potência como sendo $14^7 = (14^2)^3 \cdot 14$ e como $14^2 = 196$ deixa resto 21 na divisão por 35, e pelo Corolário, temos $(21)^3 \cdot 14$ que reescrevemos como sendo $(21)^2 \cdot 21 \cdot 14$. A potência $21^2 = 441$ deixa resto 21 na divisão por 35, e assim, pelo Corolário, podemos procurar o resto de $21 \cdot 21 \cdot 14 = 441 \cdot 14$ e, usando o Corolário novamente, $21 \cdot 14 = 294$ que deixa resto 14 na divisão por 35. Dessa forma, 14^7 deixa resto 14 na divisão por 35.

Logo, o bloco 14 decodificado é igual a 14.

Passemos para o bloco 33. Queremos encontrar o resto da divisão de 33^7 e isso é equivalente a encontrar a solução da identidade $33^7 = k_3 \cdot 35 + b$. Tomando a fatoração de $33^7 = (33^2)^3 \cdot 33$, na qual temos a potência $33^2 = 1089$ e deixa resto igual a 4 na divisão por 35. Então, pelo Corolário, basta procurar o resto de $(4)^3 \cdot 33$ na divisão por 35. Fica fácil perceber que $4^3 = 64$ e deixa resto -6 na divisão por 35 ($64 = 2 \cdot 35 - 6$) e, pelo Teorema 2, $-6 \cdot 33 = -198$ deixa resto -23 e somando 35 a este valor encontramos 12. Dessa forma, 33^7 deixa resto igual a 12 na divisão por 35.
Logo, o bloco 33 decodificado é igual a 12.

Chegamos ao bloco 32 e queremos resolver a igualdade $32^7 = k_4 \cdot 35 + b$. Fazendo uso do Corolário e do método prático mencionado anteriormente, perceba que 32 está a -3 unidade de 35, logo, vamos buscar o resto da divisão de $(-3)^7$ por 35 e, por sua vez, essa potência é fatorável a $(-3)^4 \cdot (-3)^3 = 81 \cdot (-27)$. É fácil ver que 81 deixa resto 11 e adicionando 35 a -27 obtemos 8, o que equivale a procurar o resto da divisão de $11 \cdot 8 = 88$ por 35, conforme o Teorema 2, deixando resto 18. Dessa forma, 32^7 deixa resto igual a 18 na divisão por 35.
Logo, o bloco 32 decodificado é igual a 18.

Resta-nos o último bloco 15 uma vez que já fizemos a decodificação do 14. Tome $15^7 = (15^2)^3 \cdot 15$, como $15^2 = 225$ deixa resto 15 na divisão por 35, conforme o Corolário, podemos procurar o resto da divisão por 35 do número $(15)^3 \cdot 15 = 15^2 \cdot 15^2 = 225 \cdot 225$. Como 225 deixa resto 15 na divisão por 35, pelo Teorema 2, vamos procurar o resto de $15 \cdot 15 = 225$ por 35, e sabemos que deixa resto 15. Dessa forma, 15^7 deixa resto 15 na divisão por 35.
Logo, o bloco 15 decodificado é igual a 15.

Dessa forma, resolvendo as identidades:

$$\begin{aligned}
\mathbf{13}^7 &= k_1 \cdot 35 + \mathbf{27} \\
\mathbf{14}^7 &= k_2 \cdot 35 + \mathbf{14} \\
\mathbf{33}^7 &= k_3 \cdot 35 + \mathbf{12} \\
\mathbf{32}^7 &= k_4 \cdot 35 + \mathbf{18} \\
\mathbf{15}^7 &= k_5 \cdot 35 + \mathbf{15} \\
\mathbf{14}^7 &= k_2 \cdot 35 + \mathbf{14}
\end{aligned}$$

encontramos a mensagem original **27-14-12-18-15-14** que, de acordo com a nossa tabela de pré-codificação, corresponde a palavra **RECIFE**.

É possível escolhermos (p, q) e o número (e) não conflitantes. Mas, como estamos diante de um resumo, essa explicação o leitor terá que consultar a dissertação. Nela, você também encontrará o Pequeno Teorema de Fermat e a justificativa do funcionamento do método de criptografia RSA.

A SEGURANÇA DO MÉTODO RSA

Vimos que o sistema de criptografia é de chave pública e que a dupla (n, e) é a chave de codificação ou chave pública. Sendo assim, todos os usuários têm acesso a chave de codificação e o que torna o método seguro é a dificuldade em fatorar n e, por isso, o método exige números primos p e q grandes para que essa fatoração seja extremamente difícil mesmo com o uso dos atuais computadores.

Para calcular d precisamos de $[(p-1)(q-1)]$ e e, o que nos obriga a saber os valores de p e q, mas para isso precisamos fatorar n, uma vez que, os primos escolhidos ficam em total sigilo. E é por esse fato, a fatoração, que o método se torna altamente seguro. Não temos um algoritmo rápido de fatoração. Contudo, ainda não provaram que exista um algoritmo de fatoração rápido e eficiente a ponto de fatorar n em tempo hábil e, assim, quebrar o código. Encontrar esse algoritmo e fatorar n é considerado, pelos analistas, um problema equivalente a quebra do RSA. Portanto, para números primos suficientemente grandes, o RSA é seguro, dado a esse problema da fatoração de inteiros grandes.

A tabela abaixo, divulgada pelos próprios criadores do RSA, mostra o tempo estimado para um computador atual, levando em consideração o número de dígitos e o número de operações matemáticas necessárias para tal.

Tabela 4 – Tempo estimado da fatoração por um computador

Quantidade de dígitos do número **n**	Número de operações	Tempo estimado
50	$1,4 \times 10^{10}$	3,9 horas
70	$9,0 \times 10^{12}$	104 dias
100	$2,3 \times 10^{15}$	74 anos
200	$1,2 \times 10^{23}$	$3,8 \times 10^{9} anos$
300	$1,5 \times 10^{29}$	$4,9 \times 10^{15}$ anos
500	$1,3 \times 10^{39}$	$4,2 \times 10^{25}$ anos

Fonte: A method for obtaining digital signature

3.3 Considerações Finais

Este trabalho foi idealizado com o objetivo de levar ao conhecimento dos estudantes ferramentas matemáticas significativas, apresentadas em forma de teoremas aplicados à criptografia, tema importante que vivemos, cotidianamente, mostrando sua relevância prática e de como a matemática fornece o devido suporte ao desenvolvimento de diversas áreas do conhecimento.

O método proposto tem, como ferramentas, conteúdos apropriados para a educação básica, envolvendo características e propriedades da teoria dos números, o uso de ferramentas de suporte como a calculadora e o contexto histórico da evolução da criptografia, oportunizando ao estudante manipular uma das mais belas aplicações da aritmética na contemporaneidade.

Os resultados colhidos, em forma de índices de aprendizagem, foram satisfatórios levando em consideração o grau de amadurecimento de cada turma do Ensino Médio e, talvez, com sensíveis adaptações, poderemos aplicar em forma de oficina para as séries finais do Ensino Fundamental.

Decerto, como não obtemos resultados satisfatórios com a turma do primeiro ano, pois percebemos que ela não acompanhou no mesmo nível as séries seguintes, o processo necessita de alguns ajustes. Acreditamos que o resultado esteja ligado ao grau de maturidade da turma e aos anos anteriores vividos em plena pandemia.

Uma forma de melhoria dos processos seria dispor de mais tempo, em cada sequência didática, e inserir mais itens com diversos outros exemplos com a finalidade de desenvolver habilidades sobre a temática.

Referências

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2005. P. 226.

HEFEZ, Abramo. **Elementos de Aritmética**. 2. ed. Rio de Janeiro: SBM, 2011. P. 176.

PERNAMBUCO, Seduc. **Secretaria de Educação e Esportes. Currículo de Pernambuco**. 1. ed. Pernambuco: Ensino Médio, 2021.

SINGH, Simon. **O livro dos códigos**. 15. ed. Rio de Janeiro: Record, 2001. P. 456.

________. **Os Segredos Matemáticos dos Simpsons**. 1. ed. Rio de Janeiro: Record, 2016. P. 360.

4 A Teoria de Resposta ao Item como Instrumento de elaboração de Testes para Professores de Matemática

Bruno Ramos Sales Mendes de Barros[1]
Fabiano Barbosa Mendes da Silva[2]

Resumo: Partindo da realização de uma pesquisa com professores que lecionam matemática no enino básico sobre alguns aspectos da Teoria da Resposta ao Item (TRI), na qual constatou-se que esses professores apresentavam um baixo nível de conhecimento acerca desse tema, esta investigação apresenta em detalhes a TRI abordando os principais aspectos, como definições, conceitos, história, modelos logísticos e construção da curva de probabilidade de acerto em um item. São também abordados alguns pontos importantes, como a estimação das habilidades e dos parâmetros dos itens e a construção e a interpretação das escalas de habilidades. Como destaque, é apresentado o *software* EIRT, que possibilita a geração e a análise dos dados estatísticos de um teste baseado na TRI, e que, juntamente aos elementos teóricos evidenciados, pode servir para que os professores revisitem suas práticas pedagógicas e proponham ações que visem à melhoria do ensino-aprendizagem em suas redes de ensino.
Palavras-chave: Teoria de Resposta ao Item, software EIRT, escalas de habilidade, modelos logísticos unidimensionais, banco de itens.

4.1 Introdução

As avaliações educacionais de larga escala, dentre outros objetivos, utilizam testes como ferramentas para a obtenção de informações que visam subsidiar a construção de diagnósticos e possibilitar a elaboração ou a manutenção de diversas ações na área educacional. Segundo (KLEIN; FONTANIVE, 1995), essas avaliações devem ser realizadas também para fornecer um contínuo monitoramento do sistema educacional com o objetivo de detectar os efeitos positivos ou negativos de políticas adotadas.

(LUCKESI, 2008) afirma que o ato de avaliar

> implica coleta, análise e síntese dos dados que configuram o objeto da avaliação, acrescido de uma atribuição de valor ou qualidade, que se processa a partir da comparação da configuração do objeto avaliado com um determinado padrão de qualidade previamente estabelecido para aquele tipo de objeto. O valor ou qualidade atribuídos ao objeto conduzem a uma tomada de posição a seu favor ou contra o objeto, ato ou curso de

[1] Secretaria de Educação do Estado de Alagoas, prof.brunoramos@hotmail.com
[2] Universidade Federal Rural de Pernambuco, fabiano.msilva@ufrpe.br

> ação, a partir do valor ou qualidade atribuídos, conduz a uma decisão nova: manter o objeto como está ou atuar sobre ele.

Nesse sentido, uma das questões fundamentais no contexto educacional é determinar como realizar essas comparações que, em geral, são alcançadas a partir de testes. Um teste, segundo (**css**), pode ser definido simplesmente como "um dispositivo ou procedimento que visa medir uma variável [latente]". Porém, é mais complexo medir quando essa variável expressa fenômenos que não podem ser observados diretamente, como, por exemplo, autoestima, personalidade e depressão. Assim, como seria possível medir a inteligência ou alguma habilidade de uma pessoa? Questões como essa têm ocupado gerações de pesquisadores no campo da mensuração psicológica, a Psicometria, incluindo a área educacional. A psicometria pode ser definida em termos gerais "como o conjunto de métodos, técnicas e teorias envolvidas na medição das variáveis psicológicas" (MUÑIZ, 2018). Desse modo, pode-se afirmar que é nessa área que se concentram os estudos sobre a construção e a interpretação de testes com qualidade estatisticamente comprovada.

Normalmente quando o instrumento utilizado na avaliação é o teste, tradicionalmente os resultados obtidos levam apenas em conta a soma das pontuações das questões acertadas, cuja análise central está no teste como um todo. Essa abordagem está relacionada com a Teoria Clássica dos Testes (TCT), que ainda é muito utilizada em provas escolares e em alguns vestibulares. No entanto, nessa perspectiva, os resultados dependem tanto do nível das questões quanto da amostra dos respondentes a qual o teste foi aplicado, e isso constitui um problema intrínseco a essa teoria, pois inviabiliza, por exemplo, a comparação entre os sujeitos que realizarem diferentes testes em uma mesma avaliação.

Por outro lado, a Teoria de Resposta ao Item (TRI) surgiu para preencher as lacunas observadas na TCT. Na TRI, a análise central é focada no item (questão) e não no teste como um todo. Nesse sentido, a TRI analisa a probabilidade de um sujeito acertar cada item de um teste em função da sua habilidade e das características desse item; e é a partir dessas análises -realizadas conforme os postulados dessa teoria e apoiada em alguns métodos estatísticos - que se pode encontrar o valor mais verossímil para a habilidade de um sujeito que realizou um teste, bem como pode-se estimar os parâmetros que caracterizam cada item.

No Brasil, desde a década de 1990, as avaliações externas em larga escala têm se mostrado importantes "por proporcionarem um *feedback* necessário para a tomada de decisões educacionais que conduzem ao acerto de ações e direcionamento de políticas públicas"(VIANNA, 2003). Assim, os resultados nessas avaliações podem fornecer indícios importantes para que se reflita sobre o desenvolvimento do trabalho no âmbito escolar, pois "informam sobre os resultados educacionais de escolas e redes de ensino a partir do desempenho dos alunos em testes ou provas padronizadas que verificam se estes aprenderam o que deveriam ter aprendido, permitindo inferências sobre o trabalho educativo" (BLASIS; GUEDES et al., 2013).

Nesse sentido, mesmo que nas últimas décadas os resultados nas avaliações em larga escala tenham se mostrado de grande relevância para a educação, muitos profissionais de escolas e de secretarias de educação desconhecem sua importância ou não compreendem sobre o seu funcionamento e, desse modo, os dados gerados por essas avaliações não são utilizados para propor ações com o intuito de melhorar o ensino-aprendizagem nas escolas e redes de ensino, o que pode configurar um problema no desenvolvimento da educação.

É possível ainda afirmar que a TRI é um tema essencial na educação escolar, posto que algumas avaliações, como Saeb e Enem, utilizam-se dessa teoria para estimar as proficiências dos estudantes e os parâmetros que caracterizam os itens (questões) desses testes. Desse modo, é necessário que os professores que atuam no ensino básico possuam certo conhecimento sobre os conceitos fundamentais, seja para interpretar resultados de uma avaliação ou mesmo para construir testes utilizando essa teoria.

Com o objetivo de apontar o nível de conhecimento dos professores sobre a TRI, foi realizada uma pesquisa com os professores de matemática da educação básica que atuam nas redes de ensino de Alagoas, cujos resultados indicaram a necessidade de aprofundamento sobre o tema. Isso serviu como elemento motivador para a realização deste estudo, cuja centralidade reside na apresentação e discussão dos principais conceitos e elementos da TRI e na utilização do *software* EIRT para determinação dos dados estatísticos relativos a essa teoria de testes. Mais precisamente:

1. Objetivo Geral: Apresentar os conceitos fundamentais sobre a TRI, exemplificando a sua aplicação em algumas avaliações.

2. Objetivos Específicos:

- Investigar o conhecimento que os professores de matemática das redes de ensino de Alagoas têm acerca da Teoria de Resposta ao Item.

- Destacar as principais diferenças entre a Teoria Clássica dos Testes e Teoria de Resposta ao Item.

- Utilizar o *software* EIRT para calcular as estatísticas básicas relativas à TRI.

4.2 Fundamentos Teóricos e Metodológicos

Nesta seção, serão abordados os principais conceitos subjacentes à Teoria da Resposta ao Item, bem como os resultados obtidos de um questionário aplicado a professores que lecionam matemática nas redes de ensino de Alagoas acerca de seu conhecimento sobre a TRI.

4.2.1 A Teoria de Resposta ao Item

Construtos psicológicos e educacionais como inteligência, habilidade, depressão, personalidade, autoestima, capacidade matemática e compreensão da leitura não podem ser observados ou medidos no mesmo sentido físico em que (digamos) se pode medir a altura e o peso de uma pessoa (BAKER, 2001). Como então os construtos psicológicos e educacionais são medidos pelos testes? Em resposta a essa pergunta, diferentes modelos foram propostos pela Psicometria, ramo da Psicologia e se concentra nos problemas de medição, utilizando a Estatística como um dos pilares para a elaboração de teorias e desenvolvimento de métodos específicos.

Nas seções subsequentes serão apresentados os principais aspectos teóricos da TRI, que revela ser uma importante teoria psicométrica quando se trata de avaliações na área educacional.

4.2.1.1 Uma breve visão sobre a psicometria aplicada a avaliações

Os testes psicométricos representam uma importante forma de avaliar os constructos psicológicos relacionados à educação. De acordo com (PASQUALI, Luiz, 2017), a Psicometria procura justificar o sentido das respostas dadas pelos indivíduos aos itens de um teste. O modelo psicométrico mais tradicional para estabelecer esse contexto é a Teoria Clássica dos Testes (TCT), cujo objetivo principal é explicar o resultado obtido através da soma das pontuações de uma série de itens acertados, o que é denominado de escore total. Em geral, quando se trata de processo de seleção utilizando esse modelo, quanto maior a quantidade de itens acertados maior a classificação. Assim, por exemplo, se em um teste X com 10 itens, em que um acerto vale 1 ponto e um erro vale 0, um sujeito A acerta os itens 1, 2, 4, 5 e 7 e o sujeito B acerta os itens 3, 6, 8, 9 e 10, significa que ambos tiraram 5 pontos. Para a TCT, tanto o sujeito A quanto o sujeito B têm a mesma aptidão, pois essa teoria preocupa-se apenas com o escore total. Pode-se então perguntar: será que esses dois sujeitos, que obtiveram a mesma pontuação, mas acertaram itens distintos, têm as mesmas habilidades? Certamente não, mas a TCT não diferencia esses sujeitos em relação às suas habilidades.

Por outro lado, era inevitável que outra teoria surgisse para preencher algumas lacunas deixadas pela TCT. Nesse sentido, a Teoria de Resposta ao Item (TRI) apresentou-se como uma alternativa trazendo “suposições adicionais que permitirão responder problemas que a TCT não conseguiu” (MUÑIZ, 2018). Desse modo, a análise pela TRI no teste X, descrito anteriormente, não se dá pelo o escore total, mas o seu interesse, nesse caso, concentra-se em avaliar as características de cada um dos 10 itens desse teste e também descobrir o traço latente (habilidade/proficiência) do respondente que melhor explica a probabilidade do conjunto de itens desse teste ser acertado ou errado, a partir das suas respostas.

Como explica (URBINA, 2007), a TCT já está bem estabelecida, é relativamente simples e amplamente utilizada. Já a TRI ainda está em evolução, é considerada mais complexa do ponto de vista matemático e ainda desconhecida por muitos profissionais. Além disso, (PASQUALI, Luiz, 2017) afirma que a TCT tem interesse em produzir testes de qualidade; já a TRI preocupa-se em produzir itens de qualidade.

A Figura 5, mais adiante, apresenta um quadro que resume algumas diferenças entre TCT e TRI. Como destaca (RABELO, 2013), as principais diferenças estão no fato que na TCT as interpretações da prova são feitas como um todo, posto que o resultado é calculado simplesmente pelo escore total, não levando em conta as características de cada item do teste, e na TRI essa análise está centrada em cada item, de modo que a habilidade/proficiência do examinando é estimada por modelos estatísticos. O mesmo autor afirma ainda que na TCT a comparação dos escores dos indivíduos se dá, normalmente, na mesma prova; por outro lado, na TRI, os indivíduos podem ser comparados em provas distintas, seja em uma mesma edição de um exame ou ao longo de uma série temporal.

Figura 5 – Quadro comparativo entre TCT e TRI

Teoria Clássica dos Testes (TCT)	Teoria de Resposta ao Item (TRI)
Análise e interpretações estão associadas à prova como um todo.	Elementos centrais são os itens e não a prova como o todo.
Resultado: expresso pelo escore bruto ou padronizado.	Resultado: proficiência estimada pelo modelo estatístico.
Base numérica da comparação: o escore pode ser comparado com o escore de outro indivíduo submetido à mesma prova.	Base numérica da comparação: indivíduos e itens são colocados em uma escala comum, mesmo se submetidos a provas diferentes.

Fonte: (RABELO, 2013)

Portanto, com base nas diferenças apresentadas, as características da TRI revelam-se extremamente importantes, principalmente para as avaliações externas de larga escala por propiciar a comparação dos resultados dos examinandos ao longo do tempo.

4.2.1.2 Características da TRI

Diversos modelos da TRI foram construídos ao longo dos tempos, de modo que, mesmo sendo diferentes em alguns aspectos, todos eles têm em comum algumas características básicas que, segundo (HAMBLETON; SWAMINATHAN; ROGERS, 1991), são:

> a) O desempenho de um examinando em um item de um teste pode ser previsto (ou explicado) por um conjunto de fatores chamados traços, traços latentes ou habilidades.
>
> b) A relação entre o desempenho de um examinando em um item e o conjunto de traços subjacentes ao desempenho no item podem ser descritos por uma função monotonicamente crescente chamada de função característica do item ou curva característica do item (CCI).

Além disso, todos os modelos da TRI especificam que a probabilidade de responder a um item corretamente depende da(s) habilidade(s) dos examinandos e das características dos itens. Como todos os modelos, eles incluem um conjunto de suposições sobre os dados aos quais se aplicam. As principais premissas são unidimensionalidade e independência local, apresentadas a seguir:

- Unidimensionalidade: Quando um modelo da TRI pressupõe que há apenas uma habilidade dominante (representada por θ), que é responsável por responder um conjunto de itens de um teste, diz-se que ele é unidimensional. Modelos desse tipo são os mais comuns que se apresentam nas avaliações educacionais.

- Independência local: O postulado da independência local diz que um determinado desempenho do sujeito em um item de um teste não afeta o desempenho em um outro item desse teste, isto é, as probabilidades de um sujeito acertar ou errar a um conjunto de itens são independentes entre si (PASQUALI, Luiz, 2018). Assim, a probabilidade de acerto da sequência das respostas dadas pelos sujeitos será o produto das probabilidades de acerto (ou erro) em cada item de forma independente, e representa-se matematicamente como:

$$P(U_1, U_2, ..., U_n|\theta) = P(U_1|\theta) \cdot P(U_2|\theta) \cdots P(U_n|\theta) = \prod_{i=1}^{n} P(U_i|\theta) \qquad (4.1)$$

em que θ é a habilidade dominante, U_i (i = 1, 2, 3, ... , n) representa a resposta de um indivíduo ao item i e $P(U_i|\theta)$ é a probabilidade de um sujeito com habilidade θ acertar ou errar o item i. Se o sujeito responder corretamente, $U_i = 1$; caso contrário, $U_i = 0$. Convém observar que $P(U_i = 0|\theta) = Q(U_i|\theta) = 1 - P(U_i = 1|\theta)$.

Quando um examinando responde a um conjunto de itens, o resultado é um um padrão de respostas formado por acertos (valor = 1) e erros (valor =0). A título de ilustração, suponha-se que um sujeito respondeu a um teste formado por 4 itens, de modo que tenha acertado os itens 1, 2, e 4, e errado o item 3. O padrão de suas respostas é $U_1 = 1$, $U_2 = 1$, $U_3 = 0$, $U_4 = 1$, ou seja, 1101. Daí, pela independência local descrita em (4.1), tem-se que:

$$P(U_1, U_2, U_3, U_4|\theta) = P(U_1|\theta) \cdot P(U_2|\theta) \cdot Q(U_3|\theta) \cdot P(U_4|\theta), \qquad (4.2)$$

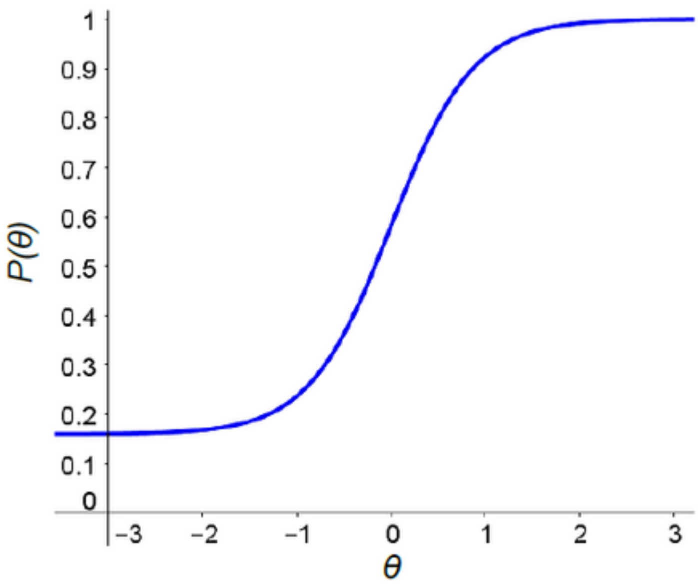
Essa característica é importante, pois é a partir dela que pode ser encontrada a habilidade mais plausível para um sujeito baseada no seu padrão de respostas, bem como para a estimação dos parâmetros dos itens de um teste.

4.2.1.3 Modelos logísticos da TRI

Os modelos logísticos da TRI constituem-se como modelos matemáticos que têm como objetivo representar a probabilidade de um indivíduo dar uma resposta correta a um item em função da sua habilidade e dos parâmetros desse item. Assim, se a habilidade de um sujeito é expressa como θ, pode-se definir que a probabilidade de acerto em um item i é a função probabilidade $P_i(\theta)$, cujos valores funcionais variam em uma escala contínua de 0 a 1 (de 0% a 100%). Desse modo, é natural conjecturar que um sujeito que tem maior habilidade terá uma probabilidade maior de acertar um determinado item do que um sujeito com habilidade inferior. Nesse sentido, à medida que a habilidade cresce, também cresce $P_i(\theta)$, representando graficamente como uma curva em uma forma de S, denominada Curva Característica de um Item (CCI).

A Figura 6, a seguir, apresenta a curva característica de um item na TRI. O eixo horizontal representa a habilidade (θ) e o eixo vertical denota a probabilidade de acerto no item. Desse modo, a probabilidade de acerto é pequena nos níveis mais baixos de habilidade e aproxima-se de 1 nos mais altos.

Figura 6 – Curva Carterística de um Item



Fonte: (BARROS, 2022)

Como cada item em um teste pode ser descrito por sua CCI, essa curva é a unidade conceitual básica dos modelos da TRI.

Embora existam vários modelos logísticos na TRI, os mais utilizados são os modelos logísticos unidimensionais, sobretudo aqueles que consideram 1, 2 ou 3 parâmetros, quais sejam, a discriminação (a), a dificuldade do item (b) e o acerto ao acaso (c).

Os modelos logísticos de 1 ou 2 parâmetros não consideram que sujeitos com baixa habilidade possam acertar itens ao acaso. Com o objetivo de eliminar essa lacuna, (BIRNBAUM, 1968), desenvolveu o modelo logístico de 3 parâmetros (3PL), acrescentando aos casos anteriores o parâmetro c, que representa a probabilidade de acerto ao acaso quando não se conhece a resposta. A função que representa o modelo logístico de três parâmetros (3PL) é dada por (BAKER, 2001):

$$P_i(\theta) = c_i + (1 - c_i)\frac{1}{1 + e^{-Da_i(\theta - b_i)}}. \tag{4.3}$$

Em (4.3), $P_i(\theta)$ é a probabilidade de um sujeito com habilidade θ responder corretamente um item i, a_i é o parâmetro de discriminação do item i, que "mede se o item consegue diferenciar alunos com baixa proficiência de alunos com alta proficiência em relação à dificuldade da questão, definindo assim a sinuosidade da curva [CCI]" (BOR-

TOLUCCI; FINI et al., 2013), b_i é o parâmetro de dificuldade do item i, c representa a probabilidade de acerto das respostas dadas ao acaso, ou seja, é o valor de $P(\theta)$ quando $\theta \to -\infty$, θ é a variável que representa a habilidade, e representa o número de Euler, cujo valor aproximado é 2,718 (com três casas decimais), e D denota uma constante que serve como um fator de escala igual a 1.

Em algumas avaliações de larga escala, como o Exame Nacional do Ensino Médio (Enem) e o Sistema de Avaliação da Educação Básica (Saeb), as estimativas dos parâmetros que caracterizam os itens e das habilidades dos estudantes são realizadas através do modelo 3PL.

4.2.2 Transformações de escalas

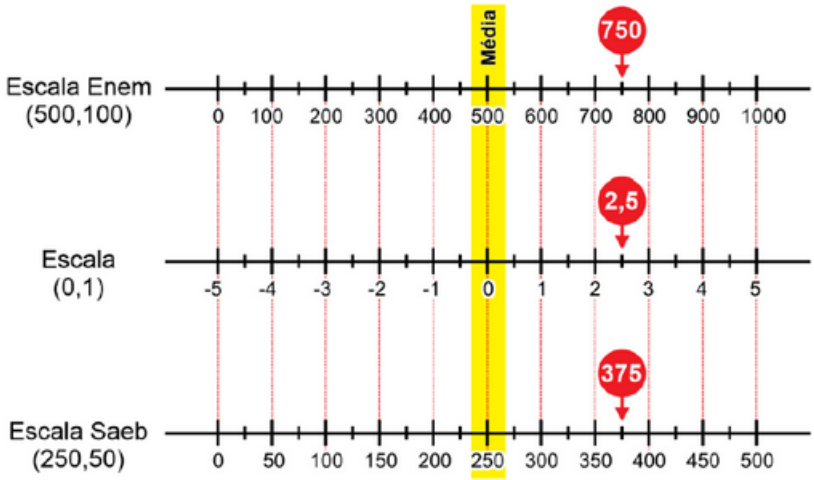
Uma escala de habilidade constitui uma espécie de "régua", graduada para qualquer valor real entre $-\infty$ e $+\infty$, construída com base na TRI. Para tal, são consideradas duas grandezas: o valor médio e o desvio-padrão das habilidades dos indivíduos da população em estudo. Em geral, esses valores são representados através da notação, (m,d) em que m é a média (ou habilidade média) e d refere-se ao desvio-padrão.

Normalmente a escala (0,1) é a mais utilizada, mas não faz diferença usar outros valores para média e desvio-padrão, pois a interpretação feita sobre duas escalas diferentes é a mesma. Segundo (RABELO, 2013), o importante é a relação de ordem entre seus pontos.

Assim, por exemplo, na escala (0,1), um sujeito com habilidade 2,5 está 2,5 desvios-padrão acima da habilidade média. Nesse sentido, na escala do Saeb, que foi arbitrada com média de 250 e desvio-padrão de 50 (250,50), esse mesmo sujeito teria habilidade 375 e consequentemente estaria 125 pontos acima da média, o equivale dizer que ele também estaria a 2,5 desvios-padrão acima da média. Já na escala do Enem (500, 100), o mesmo indivíduo teria uma habilidade de 750 e estaria a 250 pontos acima da média (que da mesma forma equivale a 2,5 desvios-padrão). A figura a seguir ilustra as equivalências acima pontuadas, destacando em amarelo as médias e em vermelho as habilidades.

Da mesma forma que foram analisados os pontos destacados na Figura 7, pode-se realizar essa equivalência para qualquer ponto da escala. Além disso, é comum a utilização de algumas transformações lineares para ajustar os valores da habilidade e dos parâmetros dos itens com o objetivo de facilitar a interpretação na escala, uma vez que a mudança procura transformar valores negativos ou com múltiplas casas decimais em números inteiros e positivos. Detalhes sobre essas transformações, bem como o passo a passo para as mudanças de escalas e ainda alguns exemplos, podem ser encontrados em (BARROS, 2022).

Figura 7 – Equivalências entre as escalas (0,1), Enem (500,100) e Saeb (250,50)



Fonte: Adaptado de (RABELO, 2013)

4.2.3 Recursos computacionais na TRI

Atualmente a TRI é uma teoria bastante difundida e utilizada em diversas avaliações ao redor do mundo, mas o seu crescimento e popularização estiveram atrelados ao desenvolvimento dos computadores e softwares que viabilizassem a sua utilização, pois, na prática, os cálculos estatísticos envolvidos nessa teoria são demasiadamente trabalhosos, não sendo realizáveis manualmente ou por calculadora. Embora alguns pesquisadores prefiram desenvolver os seus próprios softwares computacionais para esse fim, em geral os cálculos são realizados a partir da utilização de softwares já consolidados, sejam eles gratuitos ou não. Os softwares mais utilizados para estatísticas da TRI são o BILOG, o BILOG-MG, o TESTFACT14 e o PASCALE, que são pagos; e outros, como o software R ou o EIRT, são gratuitos. Uma lista ampliada dos softwares aplicados à TRI pode ser observada no quadro a seguir:

No Brasil os *softwares* mais utilizados para análises estatísticas da TRI é o BILOG e o BILOG-MG15. Esses dois programas permitem fazer as estimativas para os modelos com 1, 2 ou 3 parâmetros para itens dicotômicos ou dicotomizados, em métricas logísticas ou normais. Ademais, pode-se obter as curvas características e de informação de cada item e do teste, além de calcular alguns elementos da TCT, como, por exemplo, porcentagem de acerto em cada item, correlação bisserial e ponto-bisserial. Em geral, a diferença básica entre os dois programas é que o BILOG-MG permite a análise de mais de um grupo de respondentes, enquanto o BILOG permite apenas análises de respondentes considerados como proveniente de uma única população (ANDRADE; TAVARES; VALLE, 2000).

Como alternativa aos programas computacionais mencionados, este estudo evidenciará o uso do *software* EIRT, que é um suplemento do Excel para o cálculo das estatísticas relativas a TRI em testes educacionais. Esta escolha se deu por ele ser livre, gratuito e de fácil utilização, não necessitando que o usuário tenha o domínio de linguagem de

Figura 8 – Alguns programas de computador para estimação na TRI

Programa	Modelo	Desenvolvedor(es)/ano
BIGSTEPS	Modelo de Rasch e derivados	Linacre e Wright (1998)
BILOG	1p, 2p, 3p	Mislevy e Bock (1984)
BILOG-MG	1p, 2p, 3p, DIF e equiparação	Zimowski, Muraki, Mislevy e Bock: http://www.ssicentral.com
ConQuest	1p, multi-categoria, multidimensional	Adams, Wu e Wilson (2015)
DIMENSION	Multidimensional	Hattie e Krakowski (1994)
flexMIRT	Multidimensional	Cai (2013)
IRTPRO	1p, 2p, 3p, multi-categoria	Cai, Thissen e Du Toit (2011)
LOGIST	1p, 2p, 3p	Wingersky (1983). Wingersky et al. (1982)
MICROSCALE	Multicategoria (lp)	Mediax Interactive Technologies (1986)

Fonte: Adaptado de (MUÑIZ, 2018)

programação, como no caso do software R.

4.2.3.1 O *software* EIRT

O *software* EIRT (Item Response Theory applications using Excel) é um suplemento (add-in) para o Excel que faz alguns cálculos da TRI e TCT aplicados aos modelos unidimensionais, em que os itens para as análises podem ser do tipo binário, múltipla escolha e graduado. Além disso, pode utilizar os modelos logísticos com até três parâmetros para os dados binários, o modelo de resposta nominal para os dados de múltipla escolha e ainda o modelo de resposta gradual para os dados graduados.

Com o objetivo de apresentar a utilização do EIRT para obter as estatísticas da TRI (e também da TCT) em um teste, tomou-se como base de dados uma situação hipotética composta de uma amostra de 100 respondentes a um teste, submetidos a 20 itens - em que cada item possui uma única alternativa correta dentre quatro possibilidades (A, B, C e D). As questões sem marcação (em branco) foram consideradas como erradas.

Essa situação hipotética será ilustrada a seguir:

Na Figura 9, a primeira coluna apresenta os 100 sujeitos e as demais colunas evidenciam os 20 itens com as respostas atribuídas por cada sujeito e a primeira linha traz o gabarito. Desse modo, é possível enviar um comando ao *software* EIRT para que os dados apresentados sejam utilizados para a construção das estatísticas a serem consideradas para a análise dos sujeitos, levando em conta ainda a matriz de respostas, exemplificada na próxima figura.

A Figura 10, que pode ser vista mais adiante, apresenta a matriz de respostas no formato binário, obtida da matriz da Figura 9 atribuindo-se o valor 1 para o acerto e o valor 0 para o erro no item, após a realização das correções. Desse modo, a partir

Figura 9 – Parte da matriz de respostas de 100 sujeitos submetidos a 20 itens.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1		i1	i2	i3	i4	i5	i6	i7	i8	i9	i10	i11	i12	i13	i14	i15	i16	i17	i18	i19	i20
2	GABARITO	A	B	D	C	A	A	B	C	D	C	A	A	D	B	D	D	A	B	D	D
3	SUJEITO 1	A	D	D	C	A	A	D	B	D	B	A	B	D	D	A	B	A	B	C	B
4	SUJEITO 2	D	B	A	C	A	A	C	D	A	B	A	C	D	B	B	A	A	B	D	D
5	SUJEITO 3	A	B	D	C	A	A	B	C	D	D	A	A	D	B	D	D	A	B	D	A
6	SUJEITO 4	D	C	D	C	A	C	A	B	A	D	C	C	C	C	A	D	C	B	C	A
7	SUJEITO 5	D	B	D	C	A	B	C	D	B	A	A	B	D	B	D	C	C	D	B	D
⋮																					
101	SUJEITO 99	A	B	D	C	A	A	B	C	D	C	A	A	D	B	D	D	A	B	D	D
102	SUJEITO 100	D	C	B	D	B	B	C	D	A	B	C	B	C	A	B	B	C	D	A	A

Fonte: (BARROS, 2022)

das respostas dispostas em uma dessas duas matrizes, o EIRT pode produzir as principais estatísticas relativas à TRI, tais como curvas características e parâmetros dos itens, curvas de informações e habilidade θ dos sujeitos, dentre outros, além de elementos da TCT.

Figura 10 – Parte da matriz de respostas na forma binária após correção.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1		i1	i2	i3	i4	i5	i6	i7	i8	i9	i10	i11	i12	i13	i14	i15	i16	i17	i18	i19	i20
2																					
3	SUJEITO 1	1	0	1	1	1	1	0	0	1	0	1	0	1	0	0	0	1	1	0	0
4	SUJEITO 2	0	1	0	1	1	1	0	0	0	0	1	0	1	1	0	0	1	1	1	1
5	SUJEITO 3	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0
6	SUJEITO 4	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
7	SUJEITO 5	0	1	1	1	1	0	0	0	0	0	1	0	1	1	1	0	0	0	0	1
⋮																					
101	SUJEITO 99	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
102	SUJEITO 100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fonte: (BARROS, 2022)

Com o intuito de fornecer ao professor uma noção de como as estatísticas da TRI (e/ou da TCT) podem ser realizadas através do *software* EIRT, foi elaborada uma sequência de etapas para o uso desse *software*, como um tutorial, que pode ser encontrado em (BARROS, 2022). Os resultados obtidos são apresentados em um relatório contendo as informações selecionadas pelo usuário, como no exemplo ilustrado abaixo:

Analisando o parâmetro **a** da Figura 11, observa-se que o item mais discriminativo é o item 9 e o que menos discrimina os sujeitos do teste é o item 8. Isso significa que o item 9 consegue diferenciar alunos com baixa proficiência de alunos com alta proficiência em relação à dificuldade do item. Já o item 8 não consegue diferenciar significativamente os respondentes desse teste.

Essas conclusões decorrem dos comportamentos das curvas características. Conforme pode ser observado na Figura 12, a seguir, a CCI do item 9 caracteriza-se por ser mais íngreme no ponto de inflexão, enquanto que a CCI do item 8 apresenta um comportamento mais suave.

Figura 11 – Parte do relatório de estimação dos Parâmetros a, b e c.

Item	Parâmetro a	Parâmetro b	Parâmetro c
1	0,697	0,648	0,167
2	1,662	0,194	0,156
3	0,896	1,032	0,159
4	0,956	-0,188	0,161
5	0,986	-2,382	0,165
6	1,454	0,031	0,144
7	0,779	0,726	0,177
8	0,586	1,329	0,156
9	2,522	0,978	0,203
10	0,700	1,124	0,177
11	1,603	0,407	0,190
12	0,761	0,314	0,168
13	2,131	-0,316	0,164
14	1,340	-0,202	0,161
15	1,208	1,346	0,147

Fonte: (BARROS, 2022)

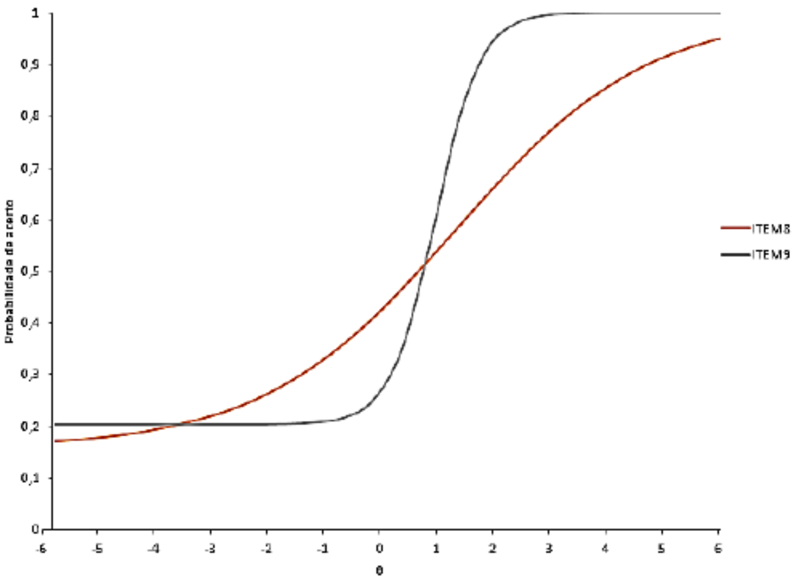
Os resultados apresentados na Figura 11 podem ser classificados utilizando-se o parâmetro **b**, que representa o índice de dificuldade do item.

Observa-se na Figura 13 (utilizando também os resultados da Figura 11) que o item mais fácil é o 5 (b = -2,382) e o item 16 (b = 1,706) é o mais difícil desse teste. Ainda assim, o item 20 foi considerado muito fácil, enquanto que os itens 8 e 15 foram considerados muito difíceis. Isso deve-se ao fato dos resultados estimados serem próximos dos resultados em destaque. Ademais, a classificação apresentada destacou ainda os itens fáceis, medianos e difíceis.

Os gráficos das Curvas Características dos itens 5 e 16 ajudam a ilustrar essa dificuldade, pois neles é possível observar que a CCI do item mais difícil (16) encontra-se do lado direito, indicando que sujeitos com maior habilidade têm maior probabilidade de acerto nesse item.

Em relação ao parâmetro **c**, o *software* EIRT permite tirar algumas conclusões: como cada questão de múltipla escolha desse teste possui quatro alternativas, espera-se que o parâmetro c, para cada item, seja menor ou igual 1/4=0,25, isto é, deve ter probabilidade de ocorrer entre 0 e 25%. Nesse sentido, analisando a coluna "Parâmetro c" na Figura

Figura 12 – Curvas características dos itens 8 e 9.



Fonte: (BARROS, 2022)

Figura 13 – Classificação dos itens conforme o índice de dificuldade (parâmetro b).

Classificação	Itens
Muito fáceis	5, 20
Fáceis	18, 17
Medianos	13, 14, 4, 6, 2, 19, 12, 11
Difíceis	1, 7, 9, 3, 10
Muito difíceis	8, 15, 16

Fonte: (BARROS, 2022)

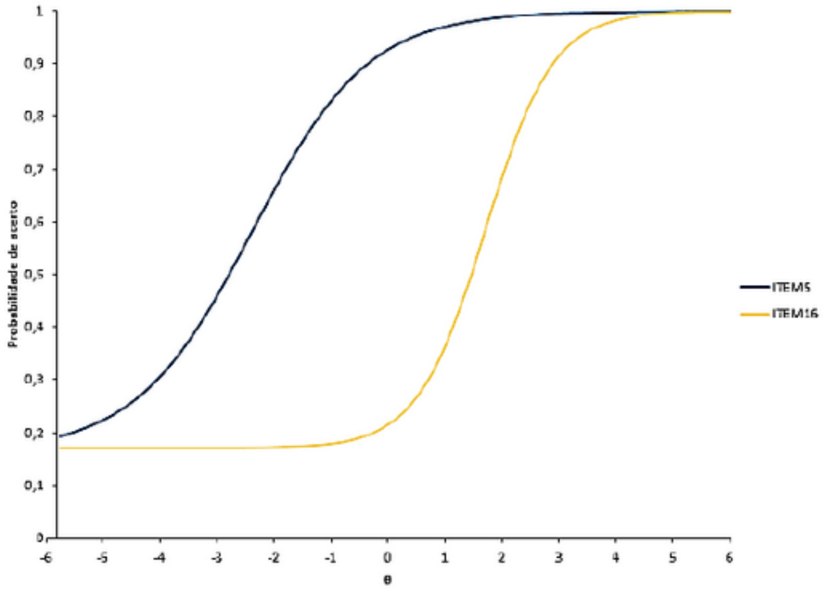
11, conclui-se que todos os valores estão dentro do esperado. Isso indica que no teste realizado os sujeitos com baixa habilidade não tiveram alta probabilidade de acertar os itens ao acaso.

Resultados como esses em relação ao parâmetro **c** são muito relevantes e devem ser buscados quando se elaboram testes através da TRI. Pode-se afirmar que os itens do exemplo, em relação ao parâmetro c, foram bem elaborados, pois indicam que um sujeito com baixa habilidade terá baixa probabilidade de acerto "o chute".

Outra representação destacada e que pode ser observada no relatório do *software* EIRT é a curva característica dos itens do teste, que pode ser construída individualmente (como na Figura 6) ou em conjunto, em plano único.

A partir das curvas características dos itens, o elaborador do teste pode fazer diversas análises, sobretudo em relação à probabilidade de acerto em cada item e estabeler

Figura 14 – Curvas características dos itens 5 e 16.



Fonte: (BARROS, 2022)

comparações entre eles segundo suas características.

Outra ferramenta fundamental que o EIRT pode proporcionar é a construção de gráficos relacionados à Função de Informação, que indica quais os itens que carregam mais informação em relação a uma habilidade. Isso é fundamental para a elaboração de um banco de itens, pois é através dessas informações que cada item é classificado e armazenado em um banco de testes.

Por fim, o EIRT também pode ser utilizado para comparar as pontuações (scores) obtidas pela TCT e as habilidades obtidas pela TRI, além de possibilitar a comparação dos itens em diversas escalas, como (0,1), Enem e Saeb, por exemplo.

4.2.4 O conhecimento do professor de matemática acerca da Teoria da Resposta ao Item

O estudo aqui apresentado relaciona-se a uma pesquisa que tem por objetivo colher as impressões dos professores do ensino básico, que lecionam matemática nas redes de ensino no estado de Alagoas, acerca do seu conhecimento sobre a TRI, que é amplamente utilizada em diversas avaliações de larga escala.

4.2.4.1 Metodologia

A pesquisa foi realizada com uma amostra aleatória de 67 professores que lecionam matemática nas redes de ensino do estado de Alagoas. Ela possui uma abordagem quantitativa e caracteriza-se como sendo exploratória com levantamento de dados sobre o que os professores conhecem acerca da TRI. As informações e dados foram obtidos a partir de um questionário contendo 8 questões de informações gerais e 17 questões específicas sobre a TRI, que foi aplicado de forma on-line por meio de um formulário eletrônico (Google Forms) durante o período de 07 a 12/07/2021. As questões foram objetivas (com a seleção de apenas uma alternativa como resposta) com exceção da questão 4 (Qual a rede de ensino que você leciona?), em que o professor tinha a possibilidade de selecionar mais de uma opção. Em algumas questões havia um campo aberto para que o professor (opcionalmente) justificasse a sua escolha.

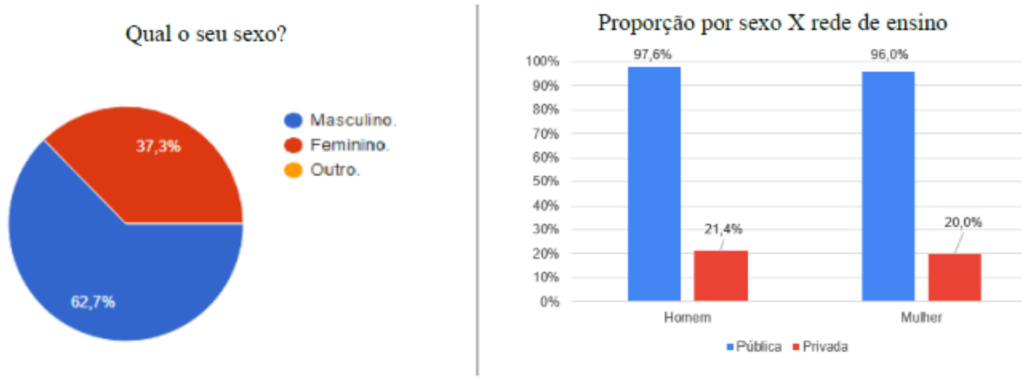
O questionário completo, bem como todas as análises envolvendo o perfil dos professores e as respectivas respostas aos itens relacionados aos conhecimentos específicos sobre a TRI, podem ser consultados em (BARROS, 2022). A seguir, são apresentados alguns destaques:

4.2.4.2 Análise das informações gerais sobre os professores de matemática

As informações aqui contidas versam sobre o perfil do professor de matemática, coletadas a partir de perguntas sobre sua formação e tempo de ensino na educação básica, dentre outras. A figura a seguir evidencia o perfil relativo ao sexo e rede de ensino.

Inicialmente, observa-se na Figura 15, abaixo, que dos 62,7% dos professores do sexo masculino, 97,6% lecionam na rede pública e 21,4% atuam na rede privada. Já dos 37,3% de professores do sexo feminino, tem-se que 96% lecionam na rede pública e 20% na rede privada. Nenhum participante escolheu a opção “outro” em relação ao seu sexo.

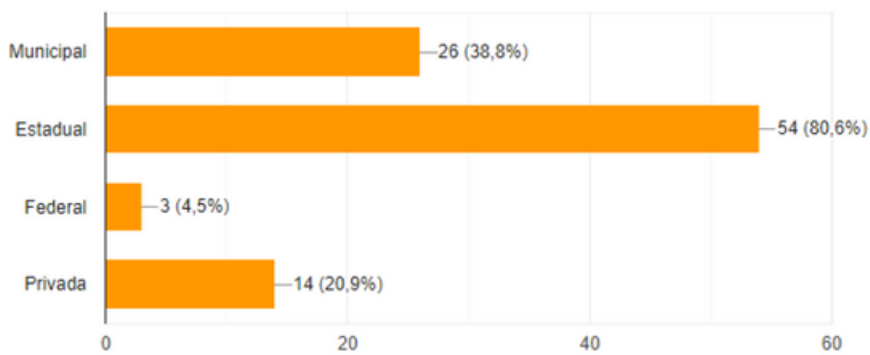
Figura 15 – Professores por sexo (esquerda) e por sexo x rede de Ensino (direita)



Fonte: (BARROS, 2022)

Já na Figura 16 nota-se que a maioria dos professores que responderam ao questionário atuam na rede estadual de ensino (80,6%), e desses, 48,1% atuam concomitantemente em outras redes. Dos professores das redes municipais de ensino (38,8%), tem-se que 80,8% também atuam em outras redes de ensino. Além disso, dos professores que lecionam na rede privada (20,9%) tem-se que 85,7% também atuam em outras redes, e todos os professores que lecionam no ensino federal (4,5%) atuam exclusivamente nessa rede de ensino.

Figura 16 – Quantidade de professores por rede de ensino



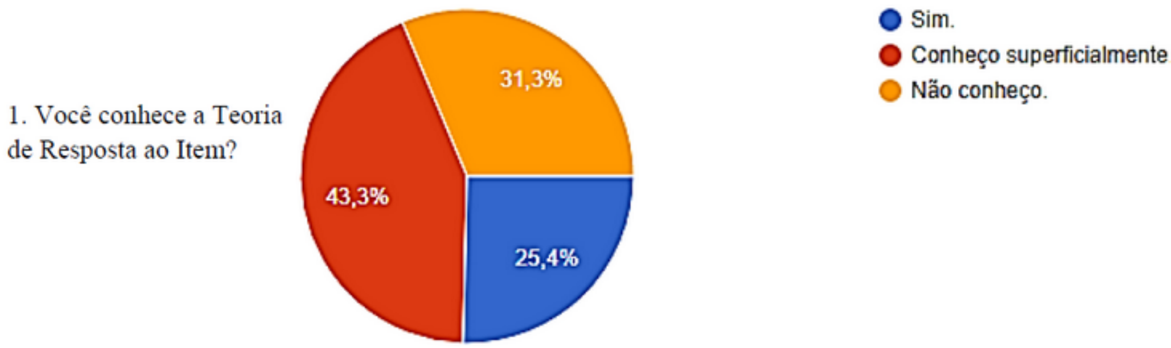
Fonte: (BARROS, 2022)

Complementarmente, como pode ser visto em (BARROS, 2022), 92,5% dos professores que participaram do estudo possuem Licenciatura em Matemática. Dos demais, dois possuem Licenciatura em Química, um professor é formado em Ciências (com habilitação em Matemática) e um é graduando em Matemática. Além disso, desses professores, 89,6% cursaram algum tipo de pós-graduação.

4.2.4.3 Análise das respostas dos professores sobre o seu conhecimento acerca da Teoria de Resposta ao Item

Compreender as principais ideias da TRI deve/deveria ser fundamental para quem leciona no ensino básico, já que diversas avaliações em larga escala utilizam essa teoria para avaliar o conhecimento dos alunos em testes, mas como será pontuado adiante, o questionário indicou que a maioria dos professores pesquisados não conhece a TRI, tampouco os principais conceitos a ela subjacentes. Talvez isso seja uma consequência da precária formação acadêmica inicial e/ou continuada do professor ou ainda pela falta de tempo para estudos complementares devido à excessiva de carga de trabalho.

Figura 17 – Conhecimento dos professores sobre a TRI



Fonte: (BARROS, 2022)

Analisando as informações contidas no gráfico da Figura 17, pode-se constatar que 74,6% dos professores possuem um conhecimento superficial ou não conhecem o tema. É impactante perceber que quase 1/3 deles $(31,3\%)$ sequer conhece sobre a TRI. Além das estatísticas apresentadas acima, 51,7% dos professores, que afirmaram ter um conhecimento superficial, apresentaram as justificativas como as elencadas abaixo:

a) "Tenho a ideia do que seja, mas nunca tive nenhuma formação sobre."

b) "Acho que o ENEM é elaborado assim."

c) "Li sobre o assunto em alguns textos, mas nada profundo."

d) "Esse método estatístico consegue diminuir as chances de que o candidato tenha uma boa nota a partir de chutes, uma vez que identifica incoerências e, assim, atribui notas mais justas."

e) "Apenas sei que se um aluno responde corretamente um item considerado difícil e erra um considerado fácil, a nota gerada será menor do que a esperada."

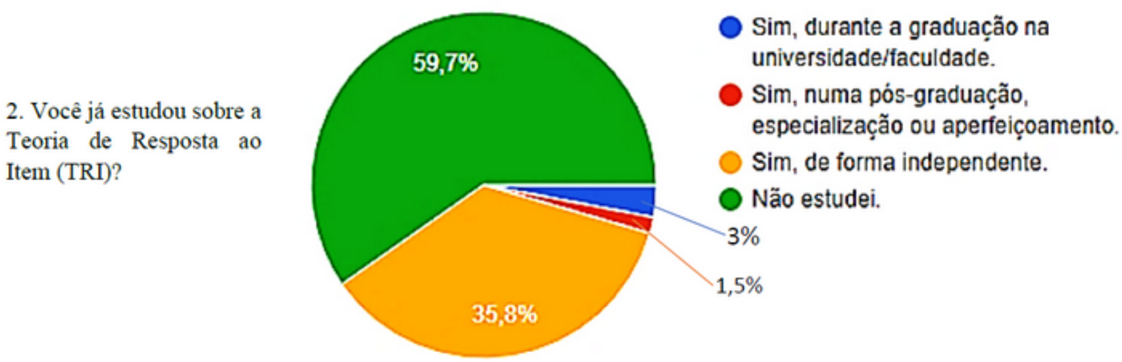
f) "Conheço muito pouco, sei que nas provas do SAEB utilizam-se desse conhecimento para avaliar mais qualitativamente o desempenho do estudante."

Pode-se observar que alguns professores afirmaram já terem lido sobre o tema, mas sem dar explicações, como visto em "a" e "c", e um único professor, o "f", afirmou saber que essa é a teoria adotada pelo SAEB e que ela é utilizada para avaliar os alunos de forma qualitativa. Outros professores, como em "b" e "g", apenas reconhecem a TRI como o método utilizado no Enem. Por fim, os professores das justificativas “d” e “e” explicaram que a coerência no padrão de respostas dos alunos reflete em melhores notas.

Similarmente, alguns professores que afirmaram ter conhecimento sobre a TRI apresentaram algumas justificativas, mas quase todas de modo genérico e superficial, o que indica, para o universo da amostra, que a maior parte dos participantes não conhece ou conhece muito pouco sobre a Teoria de Resposta ao Item. Um fator que pode contribuir para essa lacuna é a ausência de estudos sobre a TRI na formação acadêmica dos professores.

No gráfico apresentado na Figura 18, a seguir, nota-se que aproximadamente 60% nunca estudaram sobre o tema em questão e esse dado é importante, pois a grande maioria desses professores (72,5%) leciona na educação básica há mais de 10 anos. Apenas 4,5% estudaram na graduação ou pós-graduação, indicando uma possível lacuna na construção dos programas dos cursos de graduação ou pós-graduação, relativo a esse tema. Ademais, essa questão pode ser observada no gráfico acima, onde 35,8% dos professores estudaram de forma independente sobre a TRI e essa escolha possivelmente se deu pelo fato desses professores não terem estudado esse tema durante a sua formação acadêmica.

Figura 18 – Professores x Estudo da TRI durante a formação acadêmica

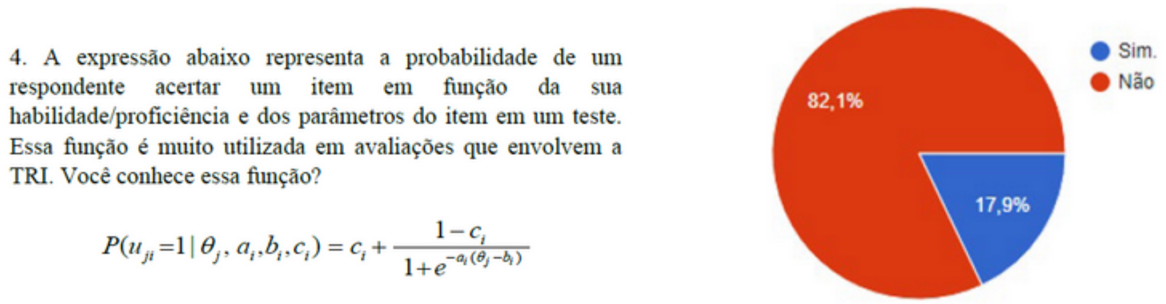


Fonte: (BARROS, 2022)

Conhecer sobre os modelos utilizados na TRI constitui uma importante ferramenta para compreender o funcionamento dessa teoria. Para tanto, quando se quer saber a probabilidade de um sujeito acertar um item, em função da sua habilidade e dos parâmetros (a, b e c), é necessário conhecer os modelos propostos por essa teoria. Na questão a seguir foi apresentado o modelo logístico de três parâmetros (3PL), que é o mais utilizado nas avaliações de larga escala no Brasil.

Esperava-se, desse modo, que os professores conhecessem esse modelo, mas como se pode observar nas respostas evidenciadas através do gráfico da Figura 19, na página seguinte, nota-se que a maioria dos professores (82,1%) não conhece a função apresentada na questão. Esse dado reforça o baixo conhecimento desses professores sobre o tema, já que a função probabilidade de acerto é um dos conceitos básicos apresentados nos estudos introdutórios sobre a TRI.

Figura 19 – Função probabilidade de acerto em um item

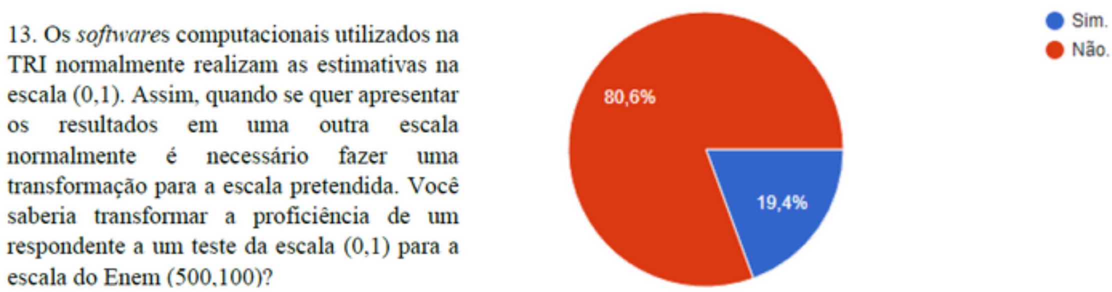


Fonte: (BARROS, 2022)

Por outro lado, outro fator que pode justificar esse resultado reside no fato de que muitos professores estudam a TRI utilizando apenas o manual do Enem "Entenda sua nota no Enem", que contém 33 páginas e traz essa função, sem muitas explicações e detalhamentos, nas suas últimas páginas.

Outro tema abordado no questionário foi o da mudança de escalas de habilidades, pois quando se utilizam alguns softwares computacionais, como o EIRT ou o software R, a escala utilizada é a tradicional, com média 0 e desvio padrão 1, cuja notação é (0,1). Porém, quando se quer apresentar os resultados em uma outra escala - aqui representada genericamente por (m,d), em que m é a média e d o desvio padrão, é importante compreender como são transformadas as proficiências e os parâmetros dos itens de modo a apresentar esses resultados conforme planejado pelo construtor do teste. Sobre esse conhecimento seguem os resultados na Figura 20, a seguir:

Figura 20 – Compreensão dos professores sobre mudanças de escalas na TRI

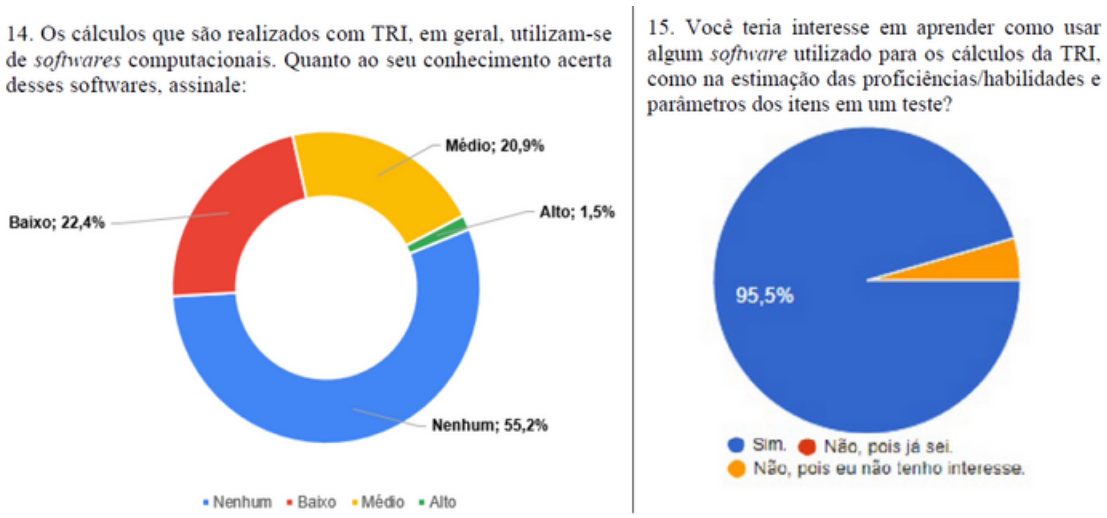


Fonte: (BARROS, 2022)

Observa-se que a maioria dos professores (80,6%) não domina essa questão, o que impossibilitaria a interpretação de alguns textos relacionados à TRI. Ademais, a ausência desse entendimento dificultaria a interpretação – ou a construção- da Curva Característica do Item e também a compreensão do valor numérico da proficiência para os diferentes testes que utilizam a TRI, já que a escolha da escala em cada avaliação é arbitrária e as avaliações normalmente apresentam escalas diferentes.

O questionário apresenta ainda uma questão que versa sobre o conhecimento do professor em relação aos *softwares* computacionais utilizados para dos cálculos da TRI. Os dados obtidos são a seguir apresentados:

Figura 21 – Conhecimento sobre os *softwaress* utilizados na TRI

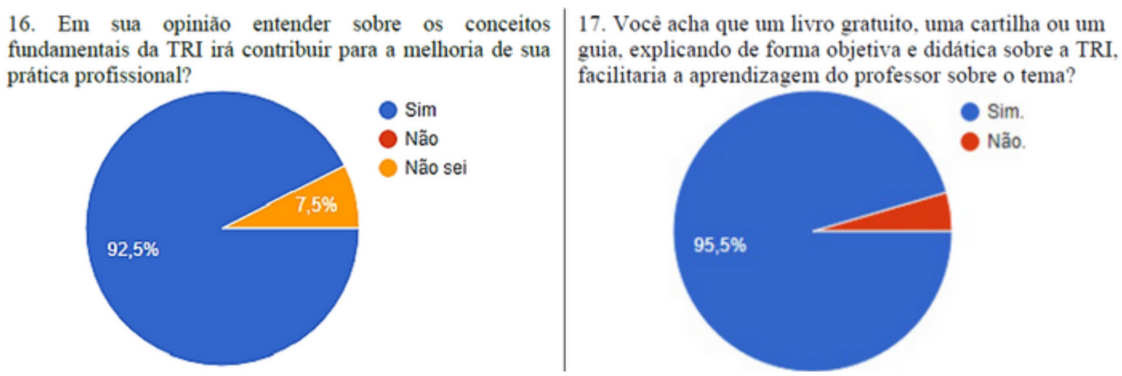


Fonte: (BARROS, 2022)

No gráfico da Figura 21, acima (à esquerda), observa-se que 77,6% dos professores indicaram ter baixo ou nenhum conhecimento sobre esses softwares. Entretanto, o gráfico da direita aponta que 95,5% dos professores afirmaram ter interesse em aprender como utilizá-los para calcular as proficiências e parâmetros dos itens. Essas informações podem indicar que se os professores tiverem acesso a esse conhecimento, poderiam desenvolver habilidades necessárias para produzir os seus próprios testes utilizando a TRI, bem como realizarem com clareza a interpretação dos dados referentes a avaliações como Saeb, Prova Brasil e ENEM, baseadas na TRI.

Por fim, as questões 16 e 17 focaram em dois aspectos: se o entendimento do professor acerca dos conceitos fundamentais da TRI poderia contribuir para a melhoria da sua prática pedagógica e também se um livro, cartilha ou guia gratuito poderia ser útil para sua aprendizagem sobre esse tema. Os resultados estão apresentados a seguir.

Figura 22 – A compreensão sobre a TRI pode contribuir para a melhoria da prática profisssional?



Fonte: (BARROS, 2022)

Nota-se do gráfico da Figura 22 (à esquerda), que 92,5% dos professores acreditam que entender os conceitos fundamentais da TRI contribuirá para a melhoria da sua prática profissional. Em vista disso, 95,5% responderam que um material de apoio pedagógico, como um guia, cartilha ou livro, versando sobre a TRI, facilitaria a aprendizagem dos professores e consequentemente poderia impactar positivamente para uma melhoria da realidade de seu contexto educacional.

Como consequência das respostas dadas pelos professores ao questionário da pesquisa, é possível inferir que mesmo que grande parte tenha afirmado não conhecer ou não compreender os conceitos fundamentais relacionados à Teoria de Resposta ao Item, ficou evidenciado que há um grande interesse em aprender sobre esses temas. Desse modo, o resultado deste estudo pode ser utilizado como um mote para o desenvolvimento de discussões acerca das ideias abordadas, bem como servir de referência para que se possa propor estratégias e ações nas unidades de ensino, ou ainda políticas públicas realizadas pelas secretarias de educação no estado de Alagoas, objetivando a melhoria da educação a partir do uso da TRI como instrumento de elaboração de testes.

4.3 Considerações Finais

A Teoria da Resposta ao Item (TRI) constitui uma nova abordagem para as análises dos testes na área educacional, pois permite resolver certos problemas de medição inatacáveis pela Teoria Clássica de Testes (TCT). Segundo Muñiz (2018) a TRI não contradiz os pressupostos fundamentais da Teoria Clássica dos Testes, mas traz novos elementos e suposições que implicou em uma grande reviravolta para a medição dos construtos em testes psicológicos ou educacionais.

(PASQUALI, L., 1996) diz que essa teoria psicométrica é

> predominante no dito Primeiro Mundo de hoje. Embora ela seja teoricamente complexa e praticamente exigente em seus procedimentos analíticos, parece imprescindível que todos os que trabalham com testes psicológicos [ou educacionais] tenham conhecimento da mesma e dela façam uso na elaboração de seus instrumentos.

Porém, atualmente, com a disponibilidade de softwares computacionais para a TRI, sejam pagos ou gratuitos, os cálculos se tornaram facilitados e com isso poupando tempo para que as pessoas envolvidas nos processos de análise em uma avaliação se concentrem nas interpretações qualitativas dos resultados de um teste. Nesse sentido, foi mostrado que o software EIRT pode ser considerado como uma excelente ferramenta para ajudar os professores na compreensão dos resultados de um teste quando se utiliza a TRI, bem como pode auxiliá-lo na construção de seus próprios testes. Para (COUTO; PRIMI, 2011), a construção de testes com a utilização de teorias psicométricas - como a TRI - constitui uma tarefa necessária para se ter instrumentos de medidas de qualidade, e é desejável que os construtores e usuários tenham algum conhecimento sobre o funcionamento da TRI em testes, seja para utilizar na construção dos seus próprios testes ou pesquisas, ou ao menos compreender os conceitos quando são apresentados em trabalhos alheios.

Contudo, ainda há um grande desconhecimento acerca da TRI no Brasil e isso vem a complicar no que tange a construção e interpretação de instrumentos psicológicos, principalmente na área educacional (PASQUALI, L., 1996). Assim, mesmo que nos últimos anos as revistas especializadas estejam repletas de pesquisas sobre diversos aspectos da TRI muitos professores sequer conhecem os temas afins a essa teoria, o que constitui um problema. Segundo (MARCONI; LAKATOS, 2002) um “problema é uma dificuldade, teórica ou prática, no conhecimento de alguma coisa de real importância, para a qual se deve encontrar a solução”.

Nesse sentido, o estudo apresentado nesse trabalho revelou que os professores participantes, em sua maioria, possuem um baixo (ou nenhum) conhecimento sobre a Teoria de Resposta ao Item (74,6%), evidenciando um problema que precisa ser solucionado – seja de forma autônoma pelo professor ou ainda por meio de formações continuadas promovidas por secretarias de educação, por exemplo, pois a compreensão acerca dessa teoria deveria ser um dos temas centrais em propostas de qualificação docente. Ademais, a compreensão pelos professores em relação as avaliações que utilizam a TRI, como o Exame Nacional do Ensino Médio (Enem) e o Sistema de Avaliação da Educação Básica (Saeb), constitui um tema fundamental na educação básica, pois é a partir das interpretações dos resultados nessas avaliações que se pode propor ações para a melhoria da educação.

Nesse estudo, percebeu-se ainda que a grande maioria dos professores sequer estudaram esse tema na universidade/faculdade (95,5%), o que também constitui um aparente problema, pois essa realidade encontrada poderia ter se apresentado de maneira oposta caso a TRI fosse ofertada durante a graduação (ou pós-graduação) desses professores. Uma possível solução para esse problema seria a realização de formação continuada promovida pelas secretarias de educação como previsto na LDB, Art. 62, § 1º, que diz “A União, o Distrito Federal, os Estados e os Municípios, em regime de colaboração, deverão promover a formação inicial, a continuada e a capacitação dos profissionais de magistério” ou ainda em colaboração com as universidades, como observado no Art. 63 dessa lei, que diz que “os institutos superiores de educação manterão: III - programas de educação continuada para os profissionais de educação dos diversos níveis” (BRASIL, 1996).

De toda sorte, essa investigação pôde trazer à luz a informação de que a maioria dos professores pesquisados afirmou ter interesse em estudar/entender sobre os conceitos fundamentais que permeiam essa teoria e que essa aprendizagem contribuirá na melhoria de sua prática profissional, mostrando-se ser um tema relevante para esses professores. Espera-se que este trabalho contribua para auxiliar o professor da educação básica na compreensão acerca da TRI, seja para a interpretação dos resultados em uma avaliação ou ainda na utilização para construção dos seus próprios testes. Ademais, o resultado da pesquisa também poderá ser utilizado como base de dados para se propor ações relativas às formações continuadas sobre o tema para os professores de matemática das redes de ensino em Alagoas.

Referências

ANDRADE, Dalton Francisco de; TAVARES, Héliton Ribeiro;
VALLE, Raquel da Cunha. Teoria da Resposta ao Item: conceitos e aplicações. **São Paulo: Associação Brasileira de Estatística**, 2000.

BAKER, Frank B. **The basics of item response theory**. 2. ed. Winsconsin: ERIC, 2001.

BARROS, Bruno R. S. M. **A Teoria de Resposta ao Item como instrumento de elaboração de testes para professores de matemática**. 2022. F. 150. Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT – Universidade Federal Rural de Pernambuco, Recife.

BIRNBAUM, Allan. Some latent trait models and their use in inferring an examinee's ability. **Statistical theories of mental test scores**, Addison-Wesley, 1968.

BLASIS, Eloisa; GUEDES, Patricia Mota et al. **Avaliação e aprendizagem: Avaliações externas: perspectivas para a avaliação pedagógica e a gestão do ensino**. [S.l.]: Fundação Itaú Social, 2013.

BORTOLUCCI, R. S.; FINI, M. E. et al. **Relatório Pedagógico SARESP 2012: Matemática. Material de Apoio Pedagógico**. São Paulo: Secretaria de Educação de São Paulo, 2013.

BRASIL. **Lei nº 9.394, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da Educação Nacional**. Brasília: Ministério da Educação. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9394.htm>. Acesso em: 10 set. 2021, 1996.

COUTO, Gleiber; PRIMI, Ricardo. Teoria de resposta ao item (TRI): conceitos elementares dos modelos para itens dicotômicos. **Boletim de Psicologia**, Associação de Psicologia de São Paulo, v. 61, n. 134, p. 1–15, 2011.

HAMBLETON, Ronald K; SWAMINATHAN, Hariharan; ROGERS, H Jane. **Fundamentals of item response theory**. Newbury Park, CA: Sage, 1991. v. 2.

KLEIN, Ruben; FONTANIVE, Nilma. **Avaliação em larga escala: uma proposta inovadora**. v. 15. Brasília: [s.n.], 1995. P. 29–34.

LUCKESI, Cipriano. **Avaliação da aprendizagem escola: estudos e proposições**. 19. ed. São Paulo: Cortez, 2008. P. 272.

MARCONI, M. A. M; LAKATOS, E. M. **Técnicas de pesquisa: planejamento e execução de pesquisas, elaboração, análises e interpretação de dados**. 5. ed. São Paulo: Atlas, 2002.

MUÑIZ, José. **Introducción a la Psicometría: Teoría clásica y TRI**. La Paz: Pirámide, 2018.

PASQUALI, L. A teoria de resposta ao item - TRI: Uma introdução. In: TEORIA e métodos de medida em ciências do comportamento. 1. ed. Brasília: MEC/SEDIAE-INEP, 1996. P. 173–195.

PASQUALI, Luiz. **Psicometria: teoria dos testes na psicologia e na educação**. Petrópolis: Editora Vozes Limitada, 2017.

________. **TRI–Teoria de resposta ao item: Teoria, procedimentos e aplicações**. Curitiba: Editora Appris, 2018.

RABELO, Mauro. Avaliação educacional: fundamentos, metodologia e aplicações no contexto brasileiro. **Rio de janeiro: SBM**, v. 29, p. 30–31, 2013.

URBINA, Susana. **Fundamentos da testagem psicológica**. Porto Alegre: Artmed Editora, 2007.

VIANNA, Heraldo Marelim. Avaliações nacionais em larga escala: análises e propostas. **Estudos em avaliação educacional**, v. 25, n. 60, p. 41–76, 2003.

5 O Uso de Recursos Digitais por Alunos do Ensino Médio no Estudo de Operações Com Frações

Me. José Marcos de Lima Barbosa[1]
Dr. Elisângela Bastos de Mélo Espindola[2]

Resumo: Neste artigo buscamos analisar o uso de recursos digitais para a aprendizagem de alunos do Ensino Médio sobre operações com frações. Utilizamos como suporte teórico, dentre outros, as orientações curriculares sobre o uso de tecnologias para o estudo de conteúdos matemáticos. A pesquisa ocorreu em duas escolas com a participação de trinta e quatro alunos. Foram propostas cinco atividades envolvendo o manuseio de recursos digitais, sendo três da plataforma PheT e duas do GeoGebra. Em seguida aplicamos um questionário de avaliação sobre tais atividades. Dentre os resultados, verificamos que na multiplicação e divisão de frações, ocorre uma maior falta de compreensão dessas operações sem o uso de regras. Além disso, entendemos que o uso das representações interativas contribuíram para um avanço na compreensão dos alunos sobre este tema, bem como sobre o conceito de fração, número misto, adição e subtração de fração com denominadores diferentes.

Palavras-chave: Ensino Médio. Operações com frações. Recursos digitais.

5.1 Introdução

Este trabalho é parte de uma dissertação do Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT) da Universidade Federal Rural de Pernambuco (UFRPE) sobre o uso de recursos digitais por alunos do ensino médio no estudo de operações com frações.

Na análise de (RIBEIRO, 2014, p.14):

> Tecnologia digital é um conjunto de tecnologia que permite, principalmente, a transformação de qualquer linguagem ou dado em números, isto é, em zeros e uns (0,1). Uma imagem, um som, um texto, ou a convergência de todos eles, que aparecem para nós na forma final da tela de um dispositivo digital na linguagem que conhecemos (imagem fixa ou em movimento, som, texto verbal), são traduzidos em números, que são lidos por dispositivos variados, que podemos chamar, genericamente, de computadores.

O uso da tecnologia digital é uma realidade na nossa sociedade e nesse processo de mudanças constantes dos avanços tecnológicos, temos visto cada vez mais pessoas utilizá-

[1] UFRPE, jmarcosrcd@gmail.com
[2] UFRPE, elisangela.melo@ufrpe.br

las, em particular, nossos alunos. Neste cenário, buscamos desenvolver uma sequência de atividades sobre frações em virtude das dificuldades apresentadas pelos alunos quando se deparam com esse conteúdo. Por exemplo, "quando estes transferem as propriedades do conjunto dos Números Naturais para as frações, não compreendendo as características particulares de cada conjunto numérico" (MONTEIRO;GROENWALD, 2014, p.8).

Na sequência, apresentamos algumas considerações sobre o uso de tecnologias digitais e sobre como desenvolvemos as atividades para o estudo de operações com frações usando recursos da Plataforma da Physics Educacional Technology (PhEt) e do Geogebra. Por fim expomos os resultados deste trabalho e alguns comentários sobre o que dele podemos perceber em termos de avanços na aprendizagem dos alunos sobre o tema em tela.

5.2 Fundamentos Teóricos e Metodológicos

A mais recente Resolução nº 3, de 21 de novembro de 2018, que atualiza as Diretrizes Curriculares Nacionais para o Ensino Médio, orienta:

> Art. 8º. As propostas curriculares do Ensino Médio devem: I - Garantir o desenvolvimento das competências gerais e específicas da Base Nacional Comum Curricular (BNCC); II - Garantir ações que promovam: [.] b) cultura e linguagens digitais, pensamento computacional, a compreensão do significado da ciência, das letras e das artes, das tecnologias da informação, da matemática, bem como a possibilidade de protagonismo dos estudantes para a autoria e produção de inovação (EDUCAÇÃO BRASIL, 2018, p.11).

A Base Nacional Comum Curricular (BNCC) propõe nas Competências Gerais da Educação Básica o uso de tecnologias digitais, como podemos observar:

> 5. Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva (BRASIL, 2018, p.9).

A BNCC destaca as constantes transformações trazidas pela tecnologia digital e os impactos dessas transformações na vida dos alunos. Para o Ensino Médio, podemos observar nas Competências Específicas para área de Matemática:

> 5. Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando estratégias e recursos, como observação de padrões, experimentações e diferentes tecnologias, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas (BRASIL, 2018, p.540).

O Currículo de Pernambuco enfatiza que os jovens que estão, atualmente, no Ensino Médio são considerados nativos digitais. Ou seja, nasceram num contexto em que o uso da tecnologia é elemento básico no cotidiano. Sendo assim, "a escola também tem a responsabilidade de contribuir na formação dos estudantes de forma que eles façam uso crítico e consciente das tecnologias" (PERNAMBUCO, 2021, p.49).

Observa-se que a importância atribuída ao uso das tecnologias na Educação Básica é fruto da percepção de estarmos vivendo em um mundo digital, do qual fazem parte nossos alunos, bem como das potencialidades oferecidas por essas tecnologias para a aprendizagem de conteúdos escolares. Consideramos que muitos softwares têm se apresentado como ótimas ferramentas para o estudo de várias áreas, em especial, para a Matemática. Diante do exposto, tomamos como suporte para o desenvolvimento do presente trabalho o GeoGebra e a Plataforma da Physics Educacional Technology (PhEt) (COLORADO, 2021).

O GeoGebra é um software gratuito e de fácil acesso. Sendo assim, cada vez mais professores e alunos fazem uso desse recurso digital. Esse software reúne a possibilidade de explorarmos, dentre outros conteúdos, Geometria, Álgebra e Estatística.

> O GeoGebra possui uma comunidade de milhões de usuários em praticamente todos os países [.] Seu nome deriva da junção de Geometria e Álgebra, deste modo, o software tem uma grande capacidade para resolver problemas envolvendo conceitos de geometria plana, analítica, espacial, conceitos de funções, dentre outros [.] O GeoGebra foi criado em 2001 como tese de Markus Hohenwarter e a sua popularidade tem crescido desde então. Atualmente, o GeoGebra é usado em 190 países, traduzido para 55 idiomas, são mais de 300.000 downloads mensais, 62 Institutos GeoGebra em 44 países para dar suporte para o seu uso (**pereira**).

Com um conhecimento básico sobre o funcionamento do GeoGebra, que pode ser adquirido por meio de uma infinidade de vídeos disponíveis na internet, pode-se criar atividades para o estudo de diversos temas na área de Matemática. No nosso caso, utilizamos atividades para multiplicação e divisão de frações.

Já a Plataforma da Physics Educacional Technology (PhEt), desenvolvida pela Universidade do Colorado, explora o conceito de simulações aplicáveis ao campo das Ciências da Natureza e da Matemática, permitindo trabalhar, a partir de recursos digitais, conceitos para os quais a experimentação possa contribuir para o processo de aprendizagem. É importante ressaltar que, como qualquer simulação, o PhET também apresenta limitações, e seu uso deve ser mediado pelo professor durante todo o processo de utilização.

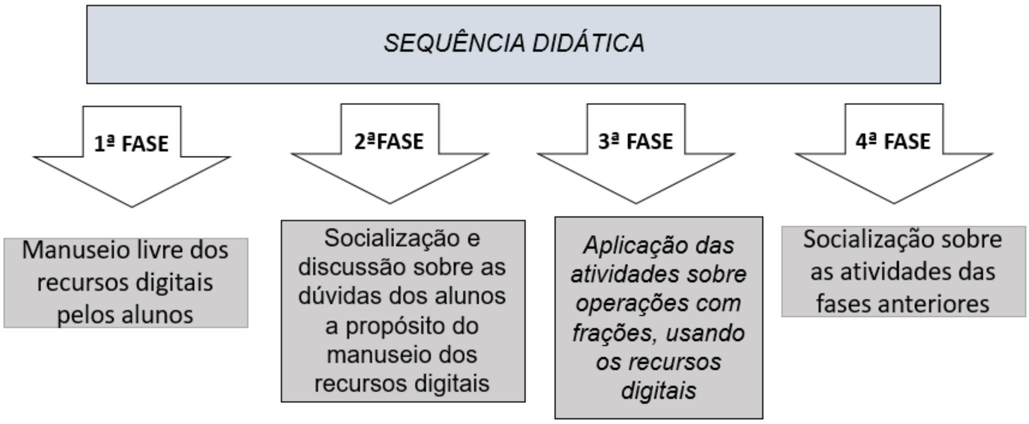
A plataforma PhET, segundo informações de seu site, oferece simulações de Matemática e Ciências divertidas, interativas, grátis, baseadas em pesquisas com testes e avaliações para assegurar a sua eficácia educacional. Essa plataforma foi desenvolvida para: 1. Incentivar a investigação científica; 2. Fornecer interatividade; 3. Tornar visível o invisível; 4. Mostrar modelos mentais visuais; 5. Incluir várias representações (por exemplo, objeto de movimento, gráficos, números, etc.); 6. Usar conexões com o mundo real; 7. Dar aos usuários a orientação implícita (por exemplo, através de controles de limite) na exploração produtiva; 8. Criar uma simulação que possa ser flexivelmente usada em muitas situações educacionais.

Os recursos digitais da PhET são de fácil acesso, bastando acessá-lo através do site: https://phet.colorado.edu/pt_br

5.2.1 A sequência de atividades proposta aos alunos

Na Figura 23, apresentamos as fases em que desenvolvemos a pesquisa com o objetivo de analisar o uso de recursos digitais para a aprendizagem de alunos do Ensino Médio sobre operações com frações.

Figura 23 – Sequência das atividades



Fonte: Produzido pelo autor.

A pesquisa ocorreu durante o período de ensino remoto com alunos de uma escola da rede pública estadual de Pernambuco (PE) (identificada por Escola A), localizada em Recife – PE e uma escola da rede privada (Escola B) em Vitória de Santo Antão - PE. Para tanto, contamos com a colaboração de dois professores das respectivas escolas e trinta e quatro alunos do Ensino Médio, sendo esses do 1º ano (12 alunos) e do 2º ano (22 alunos).

Na **primeira fase** enviamos aos alunos apenas os links de acesso aos recursos digitais, da Physics Educacional Technology (PhEt) e do GeoGebra, para que eles tentassem manuseá-los livremente (durante uma semana). Os links foram enviados para os grupos de cada escola que formamos no WhatsApp. Entendemos que essa abordagem poderia contribuir ao senso criativo e crítico dos alunos sobre os recursos, a saber:

- Introdução de Frações: https://phet.colorado.edu/pt_\BR/simulation/fractions-intro
- Frações - Números Mistos: https://phet.colorado.edu/pt_\BR/simulation/fractions-mixed-numbers;
- Igualdade de Frações: https://phet.colorado.edu/pt_\BR/simulation/fractions-equali
- Multiplicação de Frações: https://www.geogebra.org/m/drFAJzXh;
- Frações e Inteiros: https://www.geogebra.org/m/gn5cpjfd.

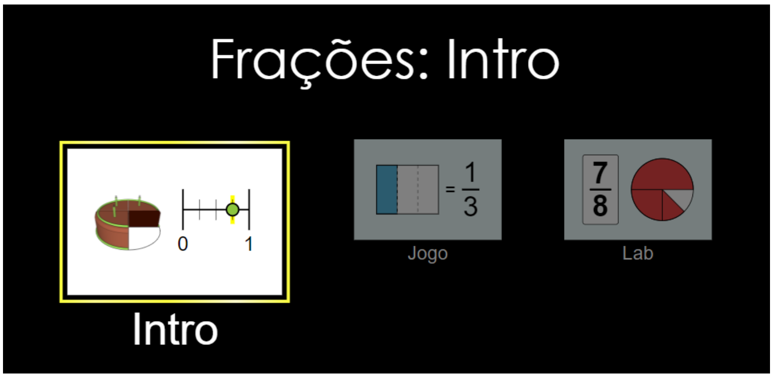
Na **segunda fase** realizamos dois encontros utilizando o Google Meet, um com os alunos da escola A e outro com os alunos da escola B. Esses encontros tiveram como finalidade discutir as dúvidas dos alunos sobre o uso dos já mencionados recursos digitais.

Na **terceira fase** enviamos aos alunos cinco atividades, nas quais eles deveriam manusear os recursos digitais. Cada atividade conteve orientações e questões sugeridas sobre operações com frações.

Atividade 1

A Figura 24 mostra a tela inicial do recurso digital usado na primeira atividade. Clicando no ícone **INTRO**, temos acesso à tela principal desse recurso.

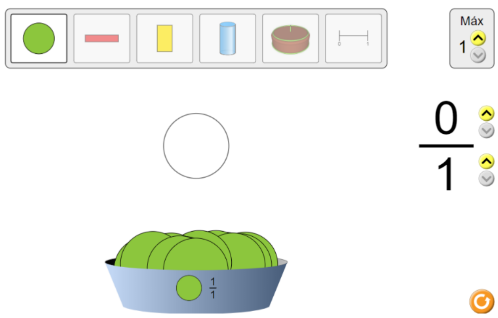
Figura 24 – Tela inicial do recurso digital usado na Atividade 1



Fonte: Phet (2021).

Na Figura 25, podemos perceber cinco tipos de figuras diferentes e mais a representação na reta numérica, de acordo com as opções que estão na parte superior esquerda da tela. O ícone que fica do lado direito da parte superior da tela controla o número de figuras que podem ser representadas no centro. Na parte central inferior, existe uma cesta com representações figurais das frações unitárias $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}$ etc., de acordo com o denominador sugerido para a fração. Assim, determinado um denominador para a fração, podemos representar frações na figura central, arrastando as frações unitárias da cesta.

Figura 25 – Tela principal do recurso digital usado na Atividade 1



Fonte: Phet (2021).

As orientações aos alunos sobre a Atividade 1 (Quadro 1) tiveram duas finalidades, a primeira, tem o objetivo de fazer o aluno compreender o significado do numerador e do denominador de uma fração, levando-os a perceber que frações com denominadores iguais representam quantidades da mesma "parte" (ex.: quantidades de meios, quantidades de terços, quantidades de quartos, etc.) e, assim, concluir que, para somar ou subtrair frações com denominadores iguais basta somar ou subtrair os numeradores, que representam as quantidades dessas "partes"iguais. Enquanto a segunda, visa fazer o aluno perceber que os números naturais podem ser escritos na forma de fração e que, na reta numérica, podemos representar qualquer fração.

Quadro 1 - Orientações para Atividade 1

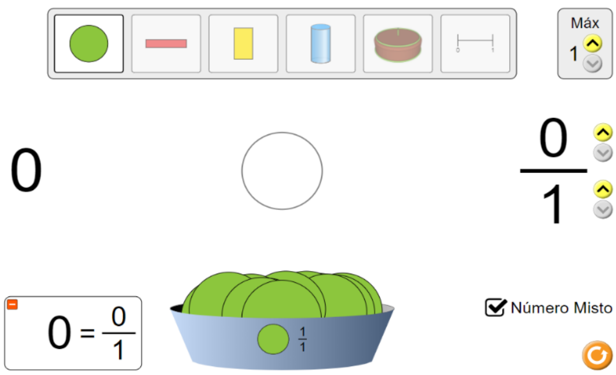
1	Clique no ícone **INTRO** para começar esta Atividade.
2	Você deve representar as seguintes frações: a) Frações com numeradores e denominadores iguais; b) Frações com numeradores maiores do que os denominadores; c) Frações com numeradores menores do que os denominadores.
Observação: Para cada caso, faça várias representações. Use mais de uma figura e não deixe de usar a reta numérica. Observe o que acontece com a figura à medida que você muda o denominador e o numerador da fração. Observe o que acontece com a fração quando você muda a figura.	

Fonte: Produzido pelo autor.

Atividade 2

Na tela inicial do recurso usado na segunda atividade, clicando no ícone **INTRO**, temos acesso à tela principal que se encontra presente na figura abaixo (26). Essa tela é semelhante à tela do recurso digital da Atividade 1, tendo como diferença o número misto, que fica do lado esquerdo e a igualdade entre o número misto e a fração, localizada do lado esquerdo inferior da tela. A representação do número misto e a igualdade entre o número misto e a fração são acessadas pelo ícone "número misto" que fica na parte inferior direita da tela.

Figura 26 – Tela principal do recurso digital usado na Atividade 2



Fonte: Phet (2021).

As orientações que elaboramos sobre a Atividade 2 (Quadro 2) tiveram como objetivo fazer o aluno compreender que: 1. Toda fração, cujo numerador é maior do que o denominador, pode ser representada pela soma de um número inteiro com uma fração menor do que um; 2. Essa representação, sem o sinal da adição, é o que chamamos de número misto.

Quadro 2 - Orientações para Atividade 2

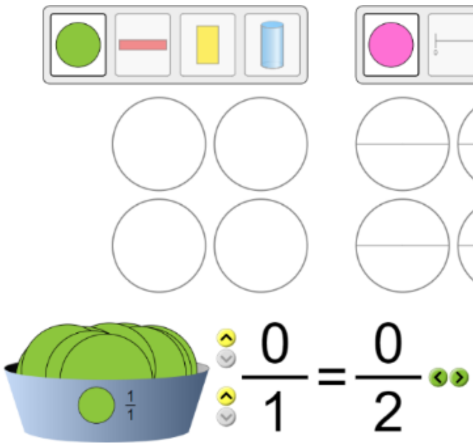
1	Para começar esta Atividade clique no ícone **INTRO**. Em seguida, marque o quadrinho do número misto.
2	Na tela aparecerá: A fração, a representação do número misto e a transformação do número misto em fração.
3	Represente várias frações com numeradores e denominadores iguais e diferentes. Observe para cada caso a representação da figura, do número misto e da transformação do número misto em fração.
4	Represente as frações $\frac{1}{3}$, $\frac{2}{3}$, $\frac{3}{3}$, $\frac{4}{3}$ e $\frac{7}{3}$. Para cada fração, observe a representação do número misto.

Fonte: Produzido pelo autor.

Atividade 3

Na tela inicial do recurso digital usado na Atividade 3, clicando no ícone Lab da Igualdade, acessamos a tela principal desse recurso conforme disposto na Figura 27. Na parte inferior da tela, podemos escolher uma fração usando as setas amarelas.

Figura 27 – Tela principal do recurso digital usado na Atividade 3



Fonte: Phet (2021).

Para cada fração escolhida, o recurso apresenta duas frações equivalentes, que podem ser vistas, clicando nas setas verdes. No centro da tela, há dois conjuntos de figuras, o da esquerda representa a fração escolhida (primeira fração) e o da direita representa a fração equivalente à primeira. A cesta que se encontra na parte inferior, do lado esquerdo da tela, funciona da mesma forma que a do recurso digital da Atividade 1.

Para a Atividade 3 (Quadro 3) tomamos como objetivo levar os alunos a compreenderem que: 1. Existem infinitas frações com numeradores e denominadores diferentes, que representam a mesma parte do todo; 2. Para achar uma fração equivalente a uma fração dada, basta multiplicar ou dividir o numerador e o denominador da fração pelo mesmo número natural diferente de zero; 3. Usar as frações equivalentes para somar e subtrair frações com denominadores diferentes.

Quadro 3 - Orientações para Atividade 3

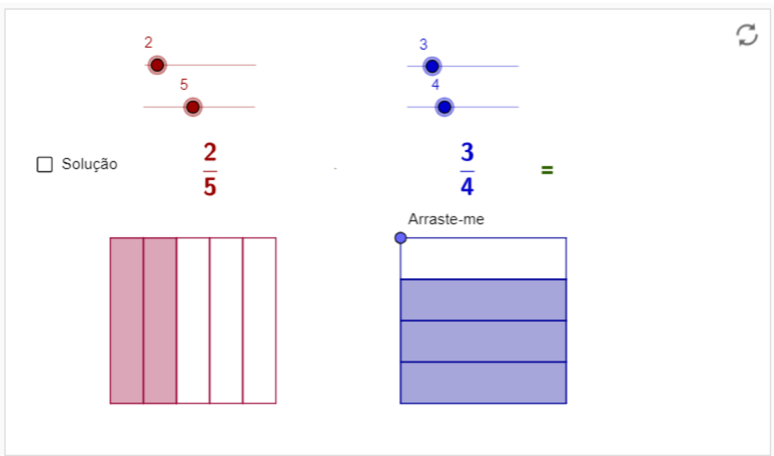
1	Clique no ícone LAB DA IGUALDADE para começar esta Atividade.
2	Manipulando o numerador e o denominador da fração represente algumas frações e, para cada uma delas, verifique as duas frações que são iguais (equivalentes) à fração que você representou.
3	Observe para cada caso do item 2 a representação das frações na figura.

Fonte: Produzido pelo autor.

Atividade 4

Na Figura 28 apresentamos a tela do GeoGebra usada na Atividade 4. No centro da tela encontramos duas frações que devem ser multiplicadas. Para alterar as frações, podemos utilizar os controles deslizantes, que ficam na parte superior da tela. Na parte inferior, temos duas figuras congruentes, a da esquerda representa a primeira fração e a da direita representa a segunda, cada representação usa uma cor diferente. Para achar o resultado da multiplicação das frações, deve-se sobrepor a figura da direita à figura da esquerda e observar a parte destacada com uma cor diferente das cores representadas nas figuras iniciais. O resultado pode ser conferido, clicando no ícone solução, que está representado do lado esquerdo central da tela.

Figura 28 – Tela do recurso digital usado na atividade 4



Fonte: (ARAUJO, 2021).

As orientações para a Atividade 4 (Quadro 4) tiveram como objetivo levar os alunos a perceberem que quando as figuras se sobrepõem, estamos encontrando a fração de outra fração e como o resultado da figura sobreposta pode ser conferido algebricamente, no recurso, o aluno é levado a compreender que multiplicar duas frações é o mesmo que achar uma fração de outra fração.

Quadro 4 - Orientações para a Atividade 4

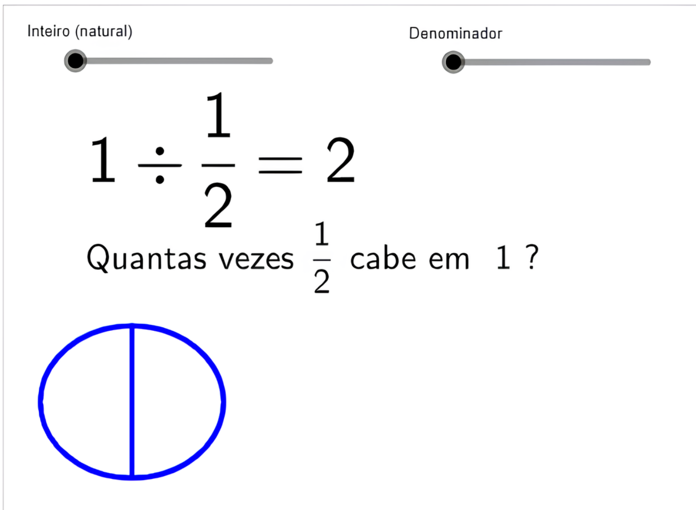
1	Usando os controles deslizantes de cada fração, escreva as frações que você quer multiplicar.
2	Em seguida, observe como cada fração está representada abaixo;
3	Clicando no ponto azul e arraste a figura da esquerda até que ela se sobreponha à figura da direita.
4	Aperte no botão solução e compare o resultado da multiplicação com o resultado da figura sobreposta.
5	Repita a sequência para várias frações.
Observação: não use frações com numeradores maiores do que os denominadores (esta Atividade não contempla estes resultados).	

Fonte: Produzido pelo autor.

Atividade 5

O recurso do GeoGebra utilizado na Atividade 5 Figura 29 propõe a divisão de um número inteiro por uma fração unitária (fração de denominador igual a 1). Na parte superior da tela deste existem dois controles deslizantes que podem alterar o número inteiro e o denominador da fração. O resultado dessa divisão aparece assim que manipulamos os controles deslizantes. A resposta também aparece na representação figural, que fica na parte inferior da tela. A ideia desse recurso é calcular a divisão, usando a noção de quantas vezes o divisor cabe no dividendo.

Figura 29 – Tela da primeira parte do recurso digital usado na Atividade 5



Fonte: (SOUSA, 2021)

As orientações acerca da primeira parte da Atividade 5 tiveram como objetivo proporcionar aos alunos perceberem que a fração $\frac{1}{a}$ cabe “a” vezes no número 1, “2a” vezes no número 2 e assim, sucessivamente. Dessa forma, esperávamos que eles concluíssem que a fração b/a cabe a vezes no número b.

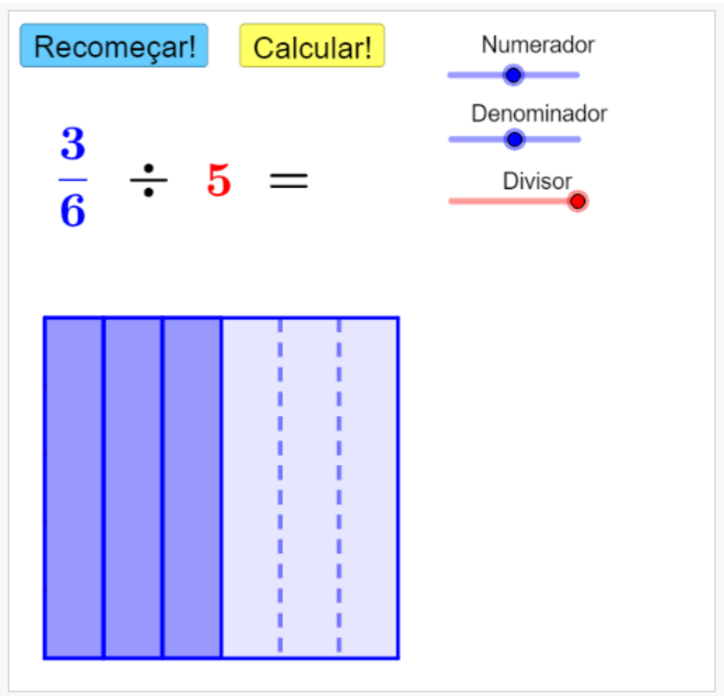
Quadro 5 - Orientações para o primeira parte do recurso da Atividade 5

1	Na primeira parte da Atividade, vamos dividir um número inteiro por uma fração de numerador igual a 1.
2	Vamos usar uma das ideias de divisão, que é saber quantas vezes o divisor cabe no dividendo.
3	Com os controles deslizantes, escreva o número inteiro e o denominador da fração.
4	Observe o resultado da divisão e a figura que corresponde ao resultado.
5	Repita a sequência para várias frações e vários números inteiros.

Fonte: Produzido pelo autor.

Na parte superior da tela (Figura 30) existem dois ícones, um para recomeçar a operação de divisão e outro para calcular o valor da divisão. À direita, existem três controles deslizantes que alteram o numerador da fração, o denominador da fração e o divisor da operação. Na parte inferior da tela temos uma figura que representa a fração proposta na divisão. Quando clicamos no ícone calcular, a figura é dividida horizontalmente pelo divisor da operação proposta, e passa a representar o resultado final da divisão, através de retângulos pintados de cor diferente das cores iniciais (azul claro e azul escuro).

Figura 30 – Tela da segunda parte do recurso digital usado na Atividade 5



Fonte: (SOUSA, 2021).

As orientações dadas na segunda parte da Atividade 5 tiveram a finalidade de tornar compreensível que na divisão de uma fração por um número inteiro, se ele inverter o número inteiro, o procedimento é igual ao de multiplicar duas frações.

Quadro 6 - Orientações para o segundo recurso da Atividade 5

1	Agora vamos dividir uma fração por um número inteiro.
2	Para este caso, usaremos a seguinte ideia de divisão: dividir o dividendo em partes iguais.
3	Usando os controles deslizantes, escolha a fração e o número inteiro para realizar a divisão.
4	Aperte em calcular e observe como a figura se desenha e compare com o resultado da divisão.
5	Aperte em recomeçar e repita a sequência para várias frações.

Fonte: Produzido pelo autor.

Na **quarta fase**, houve a socialização e discussão das atividades realizadas pelos alunos, com a finalidade de corrigir as questões sugeridas e tentar alcançar com eles aos objetivos traçados. Para isso, realizamos um encontro com alunos da escola A e outro, com aqueles da escola B, via Google Meet. Esses encontros foram gravados pela mesma plataforma, a fim de posterior transcrição das falas dos estudantes.

5.2.2 Socialização com os alunos das Escolas A e B

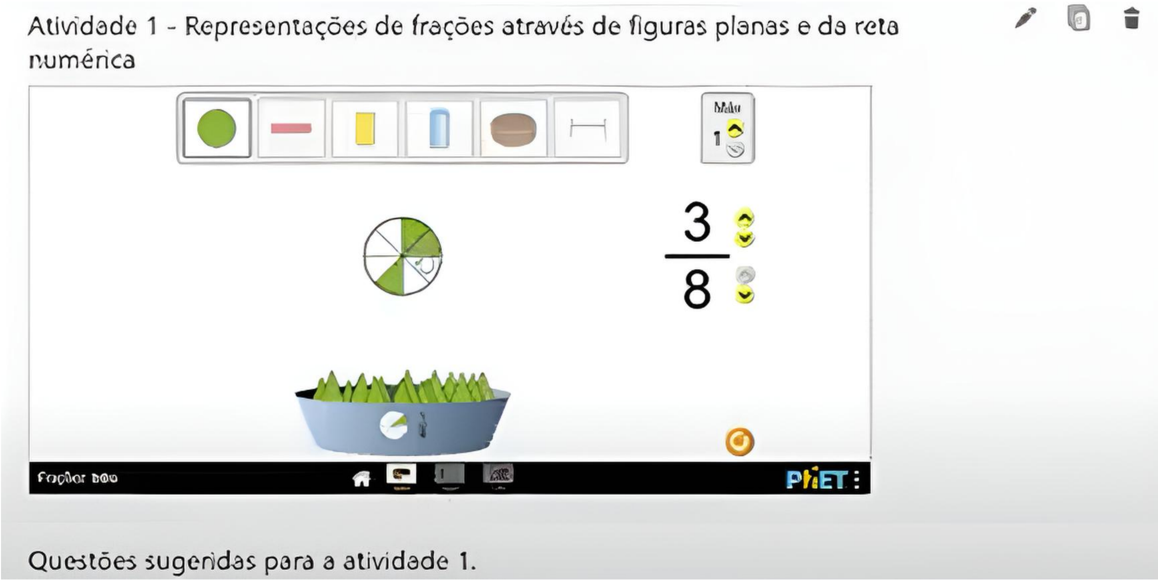
O uso do recurso digital "Frações Intro - PhET"mostrou-se eficaz na construção das bases conceituais. A clareza dos alunos ao definir o denominador como o número de partes iguais em que o todo é dividido e o numerador como a quantidade de partes consideradas demonstra que a visualização proporcionada pela simulação auxiliou na ancoragem desses significados .

Na adição e subtração com denominadores iguais, os estudantes compreenderam a regra (somar/subtrair numeradores e repetir o denominador) com base em um raciocínio lógico e concreto: "Como as partes eram iguais a gente poderia somar e subtrair coisas iguais e o resultado seria essa mesma coisa."Essa justificativa confirmou que eles viam a operação como a contagem de unidades fracionárias idênticas (ex.: $\frac{1}{8} + \frac{2}{8} = \frac{3}{8}$).

O desafio seguinte, a operação com denominadores diferentes (ex.: $\frac{1}{2} + \frac{1}{4}$), expôs a limitação da regra anterior. Os alunos, coerentes com o aprendizado, hesitaram e verbalizaram a dificuldade: "Aqui as partes não são iguais, então não posso somar a metade com um quarto, porque são pedaços diferentes. Teria que ser tudo do mesmo tamanho primeiro."

Essa reflexão crítica revelou a assimilação do conceito de unidades fracionárias homogêneas. O foco pedagógico passou, então, a ser o uso do PhET para guiar os alunos, de forma autônoma, à descoberta da necessidade de frações equivalentes e do denominador comum para que pudessem aplicar a regra de adição já dominada.

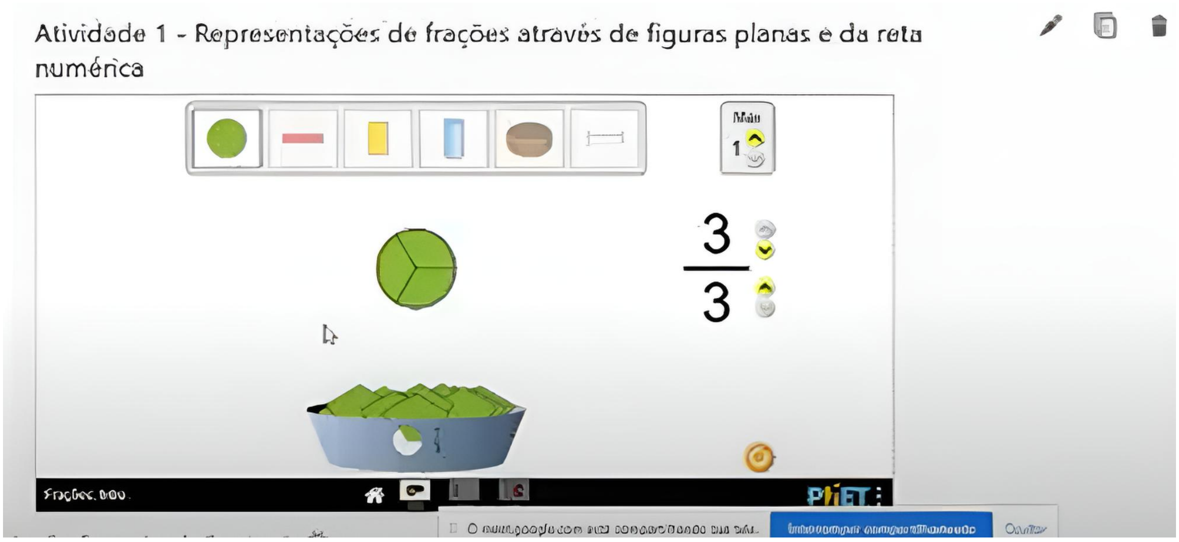
Figura 31 – Exemplo da representação de $\frac{1}{8} + \frac{2}{8}$



Fonte: Protocolo da pesquisa.

Quando perguntado se foi percebido algo que merecesse destaque na Atividade 1, uma das alunas respondeu que: “Quando representava a fração 1/1, 2/2 e 3/3 a bolinha ficava completa, mesmo que as divisões fossem diferentes, eles representavam a mesma coisa” Figura 32.

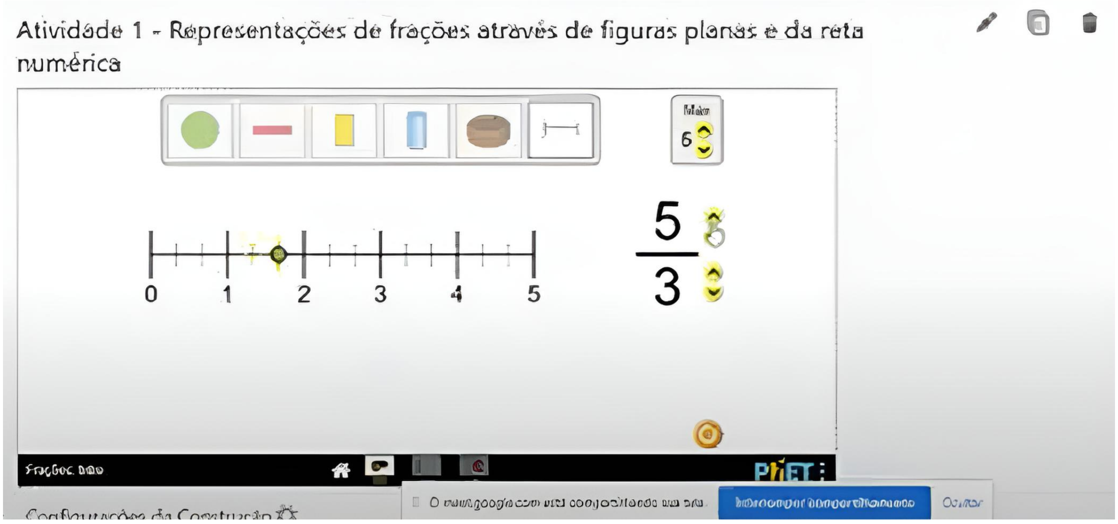
Figura 32 – Representação da fração $\frac{3}{3}$



Fonte: Protocolo da pesquisa.

Sobre as frações serem números, uma aluna respondeu: “Sim, porque quando dividimos o numerador pelo denominador vamos encontrar um número, mesmo que seja decimal ou decimal infinito”. Na Figura 33, usamos a reta numérica disponível na plataforma Phet para ajudar na compreensão sobre as frações como números.

Figura 33 – Representação da fração $Fonte : Produzidopeloautor.\frac{5}{3}$ na reta numérica

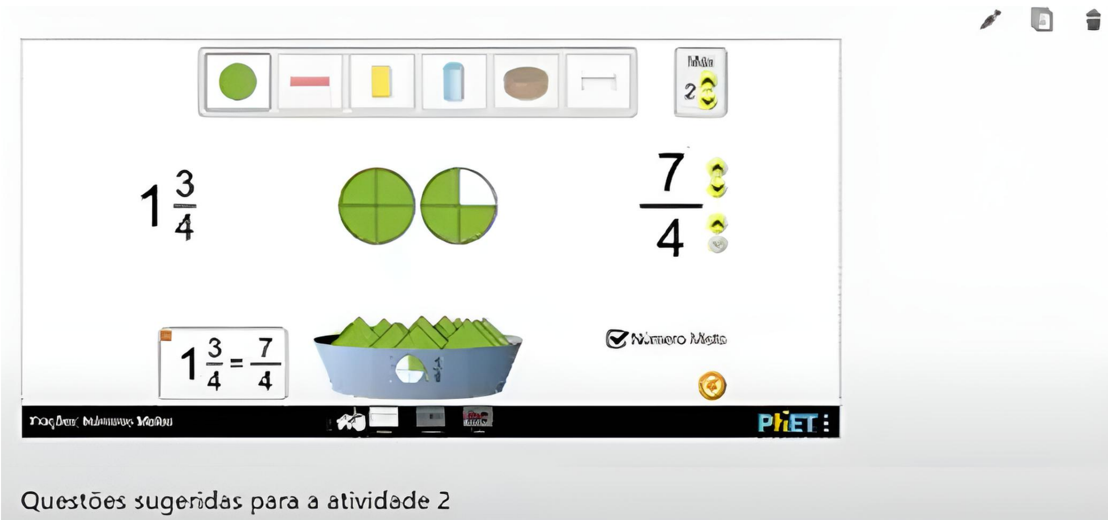


Fonte: Protocolo da pesquisa.

Após esse momento, os alunos disseram que as frações são números diferentes de 1, 2, 3. Mas uma uma das alunas questionou que esses números também são frações e exemplificou: $\frac{2}{2} = 1$. O que trouxe à tona a relação entre a representação de um número natural na forma de fração.

Sobre a Atividade 2, iniciamos perguntando aos alunos se eles conseguiram responder às questões usando o recurso digital (PhET - Frações Números Mistos). Uma das alunas respondeu Figura 34 que para achar a fração correspondente a $1\ \frac{3}{4}$ ela fez da seguinte maneira: "Eu usei duas bolas, coloquei o denominador quatro na fração e preenchi uma das bolas, a outra eu só coloquei três partes, que era o que faltava" .

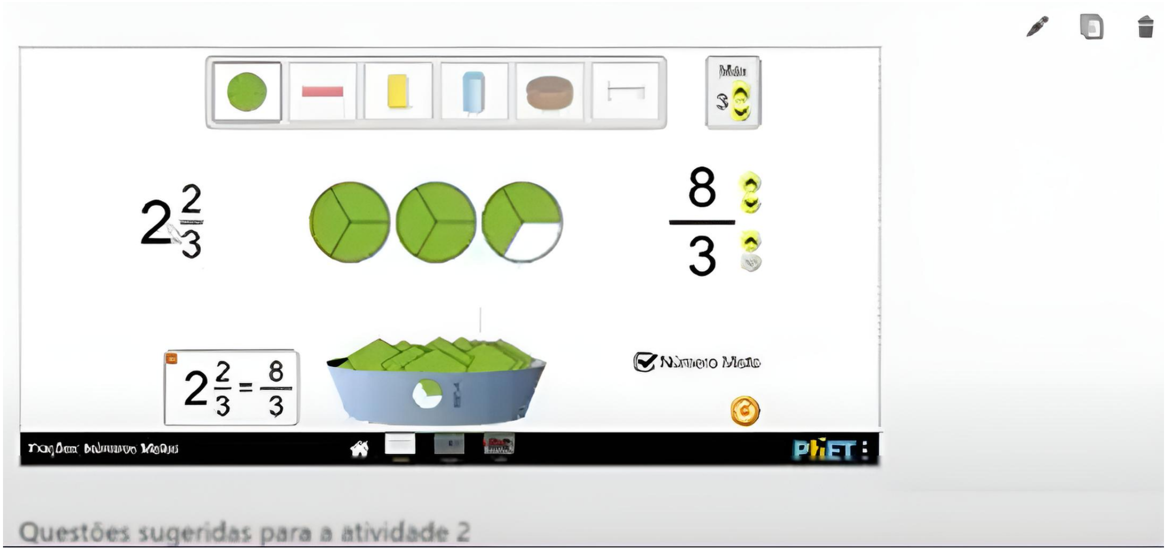
Figura 34 – Representação do número misto $1\ \frac{3}{4}$, proposta pela aluna



Fonte: Protocolo da pesquisa.

Quando perguntamos qual a operação que deveríamos usar para transformar um número misto em fração, os alunos disseram que era a multiplicação e depois a adição. A partir de então trabalhamos a compreensão do número misto deles, usando o recurso digital. Após as intervenções, os alunos disseram que a parte inteira do número misto é representada pela figura completa e a parte da fração representava o que faltava. A Figura 35 mostra um exemplo de transformação de número misto em fração, usando o recurso digital da PhET).

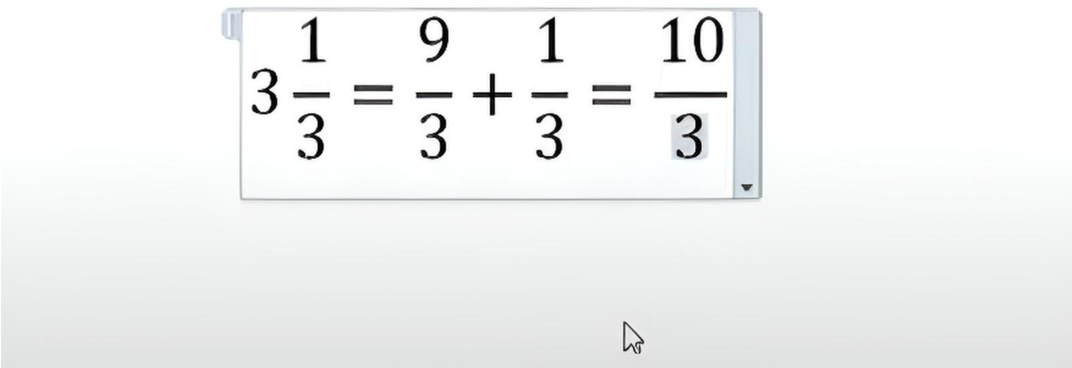
Figura 35 – Exemplo de transformação de número misto em fração



Fonte: Protocolo da pesquisa.

Os alunos não conseguiram concluir que para transformar um número misto numa fração bastava somar a parte inteira do número misto com a parte fracionária. Então resolvemos a seguinte questão: $3\,\frac{1}{3} = \frac{9}{3} + \frac{1}{3} = \frac{10}{3}$ Figura 36.

Figura 36 – Exemplo de transformação de número misto em fração

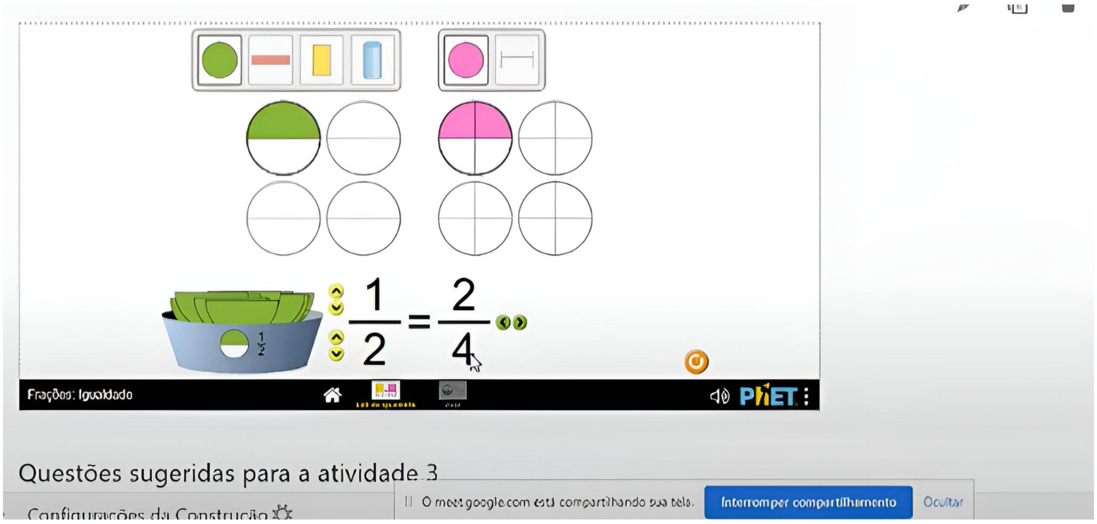


Fonte: Protocolo da pesquisa.

Um aluno perguntou se era sempre possível achar denominadores iguais. Deixamos a resposta para a Atividade 3. Quando perguntamos se fazia sentido representar uma fração própria por um número misto, uma aluna respondeu que não, porque essa fração não tem a parte inteira.

Quanto à Atividade 3, começamos questionando como faríamos para somar ou subtrair frações com denominadores diferentes. Uma aluna respondeu: "Tirando o MMC." Então, trabalhamos no recurso digital as frações equivalentes. Os alunos não tiveram dificuldades para perceber que podemos ter mais de uma fração representando a mesma parte do todo, visto que o recurso dispunha de dois casos para cada fração representada. A Figura 37 mostra a representação no recurso digital para a equivalência $\frac{1}{2} = \frac{2}{4}$.

Figura 37 – Exemplo de fração equivalente no recurso digital



Fonte: Protocolo da pesquisa.

A partir da Atividade 3, os alunos entenderam que a parte representada na figura era a mesma nos dois casos, metade do todo. Chegamos a fazer a seguinte pergunta: Dada uma fração, quantas frações equivalentes a ela existem. Uma aluna respondeu: "Infinitas" - todos concordaram. Voltamos à questão de como somar e subtrair frações com denominadores diferentes. Os alunos apresentaram dificuldades para encontrar as frações equivalentes a $\frac{5}{6}$ e $\frac{1}{8}$ com um mesmo denominador. Depois de trabalhar esse exemplo eles chegaram a $\frac{20}{24}$ e $\frac{3}{24}$, respectivamente. Vejamos a Figura 38.

Figura 38 – Exemplo de resposta – fração equivalente

$$\frac{5}{6} = \frac{20}{24}$$

$$\frac{1}{8} = \frac{3}{24}$$

Fonte: Protocolo da pesquisa.

Uma aluna perguntou se poderia relacionar de alguma forma o 6 e o 8 com algum número que fosse comum Figura 39. De imediato outra aluna disse que “tinha o número 24”. Questionamos sobre o que o 24 tinha em comum com 6 e 8. Uma aluna respondeu que “era o MMC”. Eles não conseguiram dizer que 24 é múltiplo de 6 e 8. Depois de trabalharmos alguns exemplos para mostrar que qualquer múltiplo de 6 e 8 podia ser o denominador das frações equivalentes a $\frac{5}{6}$ e $\frac{1}{8}$ Figura 39, eles opinaram que havia um padrão, que era multiplicar o numerador e o denominador pelo mesmo número.

Figura 39 – Exemplo de resposta – fração equivalente a $\frac{5}{6}$ e $\frac{1}{8}$

$$\frac{5}{6} = \frac{40}{48}$$

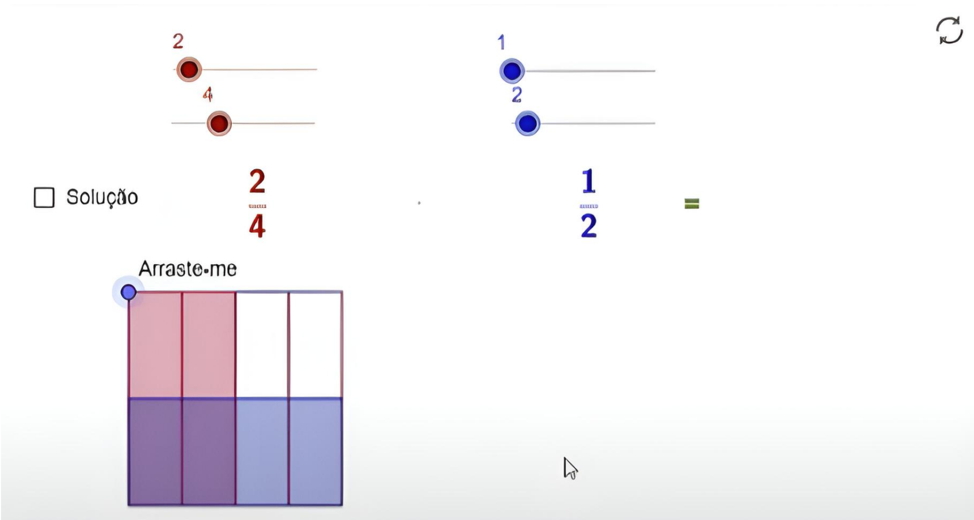
$$\frac{1}{8} = \frac{6}{48}$$

Fonte: Protocolo da pesquisa.

A partir de então fizemos mais alguns exemplos sem dificuldades. Os alunos chegaram à conclusão de que, para somar e subtrair frações de denominadores diferentes, bastava achar frações equivalentes com o mesmo denominador e usar o aprendizado da Atividade 1. Perguntados sobre o resultado de $\frac{5}{6} + \frac{1}{8}$, eles foram rápidos em dizer que era $\frac{23}{24}$. Para resolver $\frac{1}{3} - \frac{1}{4}$, eles também chegaram ao resultado sem dificuldades, $\frac{1}{12}$. Um aluno questionou sobre simplificação de frações, o que nos deu a oportunidade de trabalhar frações equivalentes dividindo o numerador e o denominador pelo mesmo número, abrindo outra possibilidade para achar frações equivalentes.

A propósito da Atividade 4, os alunos não mostraram muita dificuldade para multiplicar frações, mas não sabiam explicar por que multiplicavam os numerados e os denominadores. Eles disseram que não trabalharam o recurso digital (GeoGebra - Multiplicação de Frações), porque não entenderam como ele funcionava. Então começamos a utilizar o recurso da seguinte forma: propomos a multiplicação de $\frac{2}{4}$ por $\frac{1}{2}$ e mostramos que quando a figura que representava $\frac{1}{2}$ era sobreposta à figura que representa $\frac{2}{4}$, ocorria a divisão dessa figura em duas partes. Mas a figura que representava $\frac{2}{4}$ já estava dividida em 4 partes, o que fez o todo ficar dividido em 8 partes. Ou seja, os denominadores eram multiplicados. Para encontrar o numerador deveríamos pegar uma parte da divisão Figura 40, como cada parte estava dividida por dois, estávamos pegando 2 partes do total, o que também mostrava a multiplicação dos denominadores.

Figura 40 – Exemplos da multiplicação de $\frac{2}{4}$ por $\frac{1}{2}$

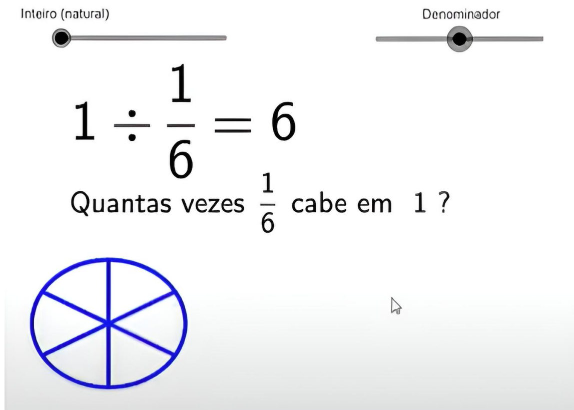


Fonte: Protocolo da pesquisa.

Trabalhamos vários exemplos, inclusive, com frações com denominadores iguais e chegamos à mesma conclusão. Questionamos qual o cuidado que deveríamos ter quando somamos e subtraímos frações que não precisamos ter quando multiplicamos frações. Vejamos a resposta de uma aluna: "Na multiplicação não importa se os denominadores são iguais ou diferentes". Apesar de termos avançado no propósito da Atividade 4, entendemos que se os alunos tivessem trabalhado com o recurso digital antes, os ganhos seriam muito maiores. Perguntamos o que eles acharam do recurso, os estudantes disseram que ficou mais fácil com o ele, porque ajudava a visualizar melhor as frações.

Como aconteceu na Atividade 4, os alunos disseram que não conseguiram usar o recurso da Atividade 5 (GeoGebra - Frações e Inteiros), à exceção de uma aluna que relatou que tentou mexer, mas não entendeu. Começamos a trabalhar o primeiro recurso da Atividade 5, que tinha a finalidade de mostrar que qualquer fração da forma $\frac{1}{a}$, caberia "a" vezes na unidade. Eles não tiveram dificuldade para perceber esse fato, pois sempre respondiam corretamente quando perguntados quantos $\frac{1}{3}$ caberiam em 3, quantos $\frac{1}{2}$ caberiam em 2 e assim sucessivamente. A Figura 19, mostra um dos exemplos trabalhados.

Figura 41 – Exemplo da divisão de 1 por $\frac{1}{6}$

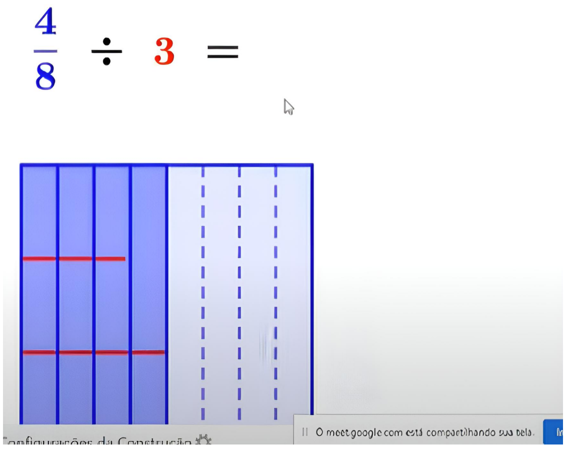


Fonte: Protocolo da pesquisa.

Sugerimos que os estudantes resolvessem a operação $1 \div \frac{1}{3}$. Não houve dificuldade. Quando pedimos para que eles achassem o valor de $1 \div \frac{2}{3}$, eles não conseguiram achar a resposta usando o recurso. Explicamos que $\frac{2}{3}$ cabia 3 vezes em 2, portanto cabia $\frac{3}{2}$ vezes em 1. Para outros exemplos desse tipo, eles conseguiram chegar às respostas corretas.

Ainda utilizando o recurso da Atividade 5 que teve como finalidade levar os alunos a dividir frações por números inteiros, tal recurso mostrava que quando dividimos uma fração por um número inteiro o denominador da fração fica multiplicado por esse número. Os alunos tiveram menos dificuldade com ele e, ao solicitarmos que eles resolvessem outros exemplos por esse método, não houve problemas. A Figura 42 mostra um dos exemplos mostrados apresentados.

Figura 42 – Exemplo da operação $\frac{4}{8} \div 3$



Fonte: Protocolo da pesquisa.

Questionamos como eles faziam as divisões, quando tinha um número inteiro. Um dos alunos respondeu que: "Coloco o 1 debaixo do número inteiro e inverto a segunda fração, depois multiplico as duas frações". De modo geral, eles não conseguiram usar os recursos para fazer divisão de frações por frações.

Ao final, perguntamos qual desses recursos eles acharam mais interessante. Os alunos foram unânimes em apontar o recurso usado na multiplicação. Um fato muito comentado por eles foi que quando eles aprendem os conceitos, os professores só dizem como fazer e não explicam porque estão fazendo daquela forma. Outro comentário dos alunos que merece destaque foi que com o recurso e a ajuda do professor fica mais fácil aprender.

5.2.3 Resultado do Questionário

Para avaliar o uso da plataforma PhET na Atividade 1 e a percepção dos estudantes, utilizamos a pergunta: "Você utilizou o recurso plataforma da PhET ao responder a Atividade 1? O que você achou dessa atividade?". As respostas estão detalhadas a seguir:

A7: Sim. Foi chato de fazer, mas gostei.
A3: Não; achei tranquila.
A12: Na primeira Atividade não foi preciso. Achei a Atividade compreensível.
A29: Interativa e interessante.
A9: Sim. Achei legal, consegui fazer.
A24: Usei, achei muito boa a Atividade.
A17: Bastante intuitiva e fácil de usar.
A6: Sim. Achei um pouco fácil, já que podíamos representar na figura a fração.
A8: Eu gostei muito da tarefa, foi a que eu consegui fazer com mais facilidade, apenas as questões 4 e 5 me deixaram um pouco confusa, por causa do denominador, o máximo

suportado na interface era até 8.
A26: Sim. Gostei, foi fácil de utilizar.
A5: Achei interessante, me ajudou a entender mais sobre a formação de uma fração e visualizar ela.
A41: Sim. A princípio achei complicado o uso, mas depois de entender e ver como usar ficou muito mais fácil e deu pra entender muito melhor o assunto.
A36: Achei que me ajudou melhor a entender sobre como funcionam as funções e como eu posso representá-las com uma figura.
A10: eu achei dinâmica, prática e divertida.

Verificamos que apenas dois alunos não usaram o recurso digital na Atividade 1, pois, segundo eles, essa atividade foi tranquila e compreensível. A maioria dos estudantes demonstrou satisfação com o uso do recurso PhET, descrevendo-o como simples, interativo e dinâmico. Destaca-se que três alunos (A5, A41 e A36) mencionaram explicitamente que o recurso foi fundamental para a compreensão do tema estudado.

Em seguida, para a Atividade 2, a seguinte questão foi apresentada: "Você utilizou o recurso plataforma da PhET ao responder a Atividade 2? O que você achou dessa atividade?"As respostas obtidas foram:

A7: Sim. Gostei, mostrou de forma simples como fazer os cálculos.
A3: Nessa eu utilizei. Achei dinâmica e mais fácil, achou muito a entender as questões.
A12: As Atividades em geral são interativas.
A29: Achei legal, muito útil pra eu conseguir entender os números mistos.
A9: Sim. Foi fácil de fazer.
A24: Consegui aprender sobre um número misto que não tinha conhecimento antes.
A17: Sim. Também consegui fazer.
A6: Esse aqui também me ajudou na compreensão do assunto.
A8: Sim. Um pouco mais complicado a forma de representação, mas depois que o professor explicou ficou melhor.
A26: A mais intuitiva, ao mexer nas setas e figura eu consegui entender a lógica. A questão visual facilitou demais.
A5: Sim, deu ainda mais para entender como funcionam as frações. A41: Usei não, mas a Atividade eu gostei.
A36: achei a mesma linha de raciocínio da primeira, uma boa metodologia.
A10: Não, achei tranquila.

Dois alunos não usaram o recurso digital, tendo um deles alegado que a Atividade 2 era tranquila. Os outros alunos usaram o recurso e disseram que ajudava a resolver os cálculos (A7), entender o tema (A3, A29, A24, A6, A26 e A5).

Em relação à Atividade 3, a seguinte questão foi utilizada para coletar feedback sobre o uso da plataforma PhET: "Você utilizou o recurso plataforma da PhET ao responder a Atividade 3? O que você achou dessa atividade?". As respostas obtidas foram as seguintes:

A7: Sim. Gostei, também foi divertido de mexer.
A3: Utilizei. Também ajudou a entender as questões e foi dinâmica. A questão em si também dava pra resolver sem.
A12: Achei boa.
A29: Ótima Atividade.
A9: Sim. Foi fácil de fazer.
A24: Tudo normal consegui aprender.
A17: Sim. Essa eu também consegui fazer.
A6: Sim, esse aqui foi melhor pois eu tinha dificuldade na hora de reduzir uma fração para outra de numerador e denominador menor, mas que fossem equivalentes.
A8: Não. Essa não cheguei a fazer, mas entendi após o explicando do professor.
A26: Acredito que, em questões visuais, foi a mais intuitiva, em todas as perguntas você pode descobrir a resposta analisando a imagem, isso aconteceu mais facilmente que nas outras Atividades. A5: Não fiz a Atividade, mas após explicação na aula remota achei também consegui entender bem como funciona as resoluções das frações.
A41: Usei, achei tranquila.
A36: A terceira tbm, as três estimulam q continuemos usando para uma aprendizagem mais divertida.
A10: Não, achei tranquila.

Na Atividade 3, três alunos disseram não ter usado o recurso digital, mas dois deles afirmaram que depois do encontro que fizemos para correção das questões eles conseguiram entender (A8 e A5). Os outros alunos conseguiram usar o recurso digital. Destacamos a resposta dos alunos A6 e A26:

A6: Sim, esse aqui foi melhor pois eu tinha dificuldade na hora de reduzir uma fração para outra de numerador e denominador menor, mas que fossem equivalentes.
A26: Acredito que, em questões visuais, foi a mais intuitiva, em todas as perguntas você pode descobrir a resposta analisando a imagem, isso aconteceu mais facilmente que nas outras Atividades.

Em relação à Atividade 4, a pergunta "Você utilizou o recurso plataforma da PhET ao responder a Atividade 4? O que você achou dessa atividade?"foi aplicada. As respostas dos alunos foram as seguintes:

A7: Sim. Essa eu achei um pouco mais complicada.

A3: A partir da 4° Atividade eu travei.
A12: Interativa e divertida.
A29: Foi bom pra entender a multiplicação entre as frações.
A9: Sim. Foi chato de fazer, mas até que foi legal.
A24: Um jeito mais divertido e dinâmico de ver as frações.
A17: Sim. Essa eu também consegui fazer.
A6: Utilizei, mas esse assunto eu já entendendo, exceto quando uma das frações tem número inteiro.
A8: Sim. Multiplicação de frações eu considero o mais fácil, e através desse site foi possível aprender outra forma de explicar o porquê de se calcular assim.
A26: Demorei para entender, porém quando eu finalmente entendi achei a Atividade maravilhosa, ficar deslocando os quadrados que representam as frações foi bem criativo e interessante. Embora no começo achei as questões difíceis, depois da explicação ficou fácil. Acredito que para dar certo, a interação com um professor orientador seja essencial.
A5: Também foi muito fácil de entender.
A41: Não usei o aplicativo, mas achei a Atividade interessante e boa de fazer.
A36: Eu n cheguei a utilizar essa.
A10: Sim; achei interessante, mas não entendi bem a proposta da terceira questão.

Sobre a Atividade 4, três alunos não usaram o recurso digital (GeoGebra), um deles disse que apesar de não ter usado, achou a atividade interessante e boa de fazer (A41). Todos os outros alunos disseram usar o recurso e acharam interativa e divertida (A12), divertido e dinâmico (A24). Destacamos as respostas dos alunos A8 e A26:

A8: Sim. Multiplicação de frações eu considero o mais fácil, e através desse site foi possível aprender outra forma de explicar o porquê de se calcular assim.
A26: Demorei para entender, porém quando eu finalmente entendi achei a Atividade maravilhosa, ficar deslocando os quadrados que representam as frações foi bem criativo e interessante. Embora no começo achei as questões difíceis, depois da explicação ficou fácil. Acredito que para dar certo, a interação com um professor orientador seja essencial.

A fim de avaliar o uso do recurso GeoGebra e a percepção dos estudantes sobre a Atividade 5, foi aplicada a pergunta: "Você utilizou o recurso GeoGebra ao responder a Atividade 5? O que você achou dessa Atividade?", as respostas estão detalhadas a seguir:

A7: Sim. Essa também achei um pouco mais difícil que as outras.
A3: Não fiz também.
A12: Um pouco complicada de entender mais dps q entende fica legal.
A29: Foi bom pra entender como funciona a divisão de duas frações.
A9: Sim. Foi bem fácil de fazer.

A24: Básico, me ajudou pela facilidade de fazer.
A17: Não. Não consegui fazer porque eu lembro como faz, mas não consegui entender o porquê.
A6: Esse eu também usei e denomino o assunto, exceto quando uma das frações tem número inteiro.
A8: Não cheguei a fazer, mas consegui entender um pouco com a explicação do professor. Divisão com fração é um pouco chato mesmo.
A26: Definitivamente a mais confusa de todas, mexer nessa interface foi complicado e nada intuitivo, mesmo após a explicação na aula acabei ficando com um pé atrás nessa Atividade. A5: Não fiz a Atividade, mas vi através da aula remota e também consegui entender como resolver a questão. A41: Não usei nessa Atividade, achei tranquila, mas demorei para fazer.
A36: nem essa.
A10: Não; achei tranquila.

Esse foi o recurso digital menos usado pelos alunos, um total de 7. Também foi alegado que o recurso era complicado de mexer (A7, A12 e A26). Alguns alunos disseram que o recurso ajudou a entender (A29 e A24). Merece destaque a resposta do aluno A26:

A26: Definitivamente a mais confusa de todas, mexer nessa interface foi complicado e nada intuitivo, mesmo após a explicação na aula acabei ficando com um pé atrás nessa Atividade.

5.3 Considerações Finais

Por meio deste trabalho, podemos constatar como os alunos chegam ao Ensino Médio sem compreender o conceito de fração e por consequência com muita dificuldade em realizar suas operações. Dessa forma, acreditamos que o aprendizado sobre como operar frações não foi realizado de forma eficaz, no Ensino Fundamental. Na maioria dos casos o que se conseguiu foi decorar regras.

A experiência vivida na socialização das atividades através das colocações dos alunos e as respostas apresentadas por eles no questionário avaliativo nos levaram a uma perspectiva positiva sobre o uso de recursos digitais para trabalharmos temas na área de Matemática. Diante do exposto, recomendamos o uso de recursos digitais para o aprendizado de operações com frações. Haja vista, que isto ainda é pouco oferecido na escola, mesmo para o estudo de outros temas, sabendo-se do mundo digital no qual nossos alunos estão inseridos.

Acreditamos que a experiência com recursos digitais propõe ao aluno efeitos de compreensão que o método tradicional centrado “em decorar regras e fórmulas” não possibilita. Entendemos que os recursos digitais proporcionam aprendizagens, por exemplo, no que concerne aos diferentes tipos de registros de representação semiótica (numérica, figural.), que seriam mais difíceis sem o uso desses recursos.

Nosso estudo nos levou a acreditar que se fizermos uso de recursos digitais propondo situações que visem a construção do conhecimento e a compreensão dos alunos este é um meio que pode favorecer o ensino e a aprendizagem de frações e de outros temas matemáticos.

Referências

ARAUJO. **Multiplicação de frações – GeoGebra**. São Paulo, 2021. Disponível em: <https://www.geogebra.org/m/drFAJzXh>.

BRASIL. **Resolução nº 3, de 21 de novembro de 2018**. Ministério da Educação. Brasília, 2018. Disponível em: <https://www.in.gov.br/materia/-%20/asset_publisher/Kujrw0TZC2Mb/content/id/51281622>.

COLORADO, UNIVERSIDADE DO. **Physics Educacional Technology. Matemática**. [S.l.], 2021. Disponível em: <https://phet.colorado.edu/pt/simulations/filter?subjects=math&type=html&sort=alpha&view=grid>.

EDUCAÇÃO BRASIL, Ministério de. **Secretaria de Educação Básica. Base Nacional Comum curricular**. Brasília: MEC, 2018. P. 11.

MONTEIRO;GROENWALD, A. B. **Sistemas Operacionais Modernos**. São Paulo: GROENWALD, C. L. O. Dificuldades na Aprendizagem de Frações: Reflexões a partir de uma Experiência Utilizando Testes Adaptativos, ALEXANDRIA Revista de Educação em Ciência e Tecnologia, v.7, n.2, 2014. P. 103–135.

PERNAMBUCO, Crrículo de. **Ensino Médio**. Recife: Secretaria de Educação, 2021.

RIBEIRO, A. E. **Tecnologia digital**. São Paulo, 2014. Disponível em: <https://www.ceale.fae.ufmg.br/glossarioceale/verbetes/tecnologia-digital>.

SOUSA, A. C. B. **Frações, inteiros**. São Paulo, 2021. Disponível em: <https://www.geogebra.org/m/aVbhn2W5>.

O Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) constitui um programa de pós-graduação stricto sensu de abrangência nacional, seguindo a modalidade semipresencial. Seu principal objetivo é promover o aprimoramento da formação profissional de professores que atuam na educação básica. No volume III desta coletânea, apresentamos uma compilação de contribuições originárias de dissertações defendidas ao longo dos últimos anos neste programa exclusivamente para o polo da UFRPE. Esta obra serve como um indicativo palpável da excelência do programa como instrumento eficaz de formação continuada para os professores de Matemática.

www.editora.ufrpe.br

O Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) constitui um programa de pós-graduação stricto sensu de abrangência nacional, seguindo a modalidade semipresencial. Seu principal objetivo é promover o aprimoramento da formação profissional de professores que atuam na educação básica. No volume III desta coletânea, apresentamos uma compilação de contribuições originárias de dissertações defendidas ao longo dos últimos anos neste programa exclusivamente para o polo da UFRPE. Esta obra serve como um indicativo palpável da excelência do programa como instrumento eficaz de formação continuada para os professores de Matemática

EX SEMINE SEGES
UFRPE

Editora Universitária da UFRPE

ISBN DIGITAL nº 978-65-86466-01-0

9 786586 466010