UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DE BRAGANÇA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

ENIGMÁTICA: uma proposta metodológica para o ensino de alguns objetos matemáticos usando a criptografia

Dayziane do Socorro Epifanio da Silva

BRAGANÇA-PA
2023

ENIGMÁTICA: uma proposta metodológica para o ensino de alguns objetos matemáticos usando a criptografia

Dayziane do Socorro Epifanio da Silva

Dissertação apresentada ao programa de Pós-Graduação de mestrado profissional em Matemática em Rede Nacional – PROFMAT, da Universidade Federal do Pará, como parte dos requisitos necessários para obtenção do Título de Mestre em Matemática.

Orientadora: Prof. Dra Marly dos Anjos Nunes

Coorientadora: Prof. Dra Edilene Farias Rozal

BRAGANÇA-PA

2023

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

S586e Silva, Dayziane do Socorro Epifanio da.
ENIGMÁTICA: uma proposta metodológica para o ensino de alguns objetos matemáticos usando a criptografia / Dayziane do Socorro Epifanio da Silva. — 2023.
76 f. : il. color.

Orientador(a): Profª. Dra. Marly dos Anjos Nunes
Coorientação: Profª. Dra. Edilene Farias Rozal
Dissertação (Mestrado) - Universidade Federal do Pará, Campus Universitário de Bragança, Programa de Mestrado Profissional em Ensino da Matemática, Bragança, 2023.

1. Criptografia, ensino de matrizes e funções. I. Título.

CDD 513.6

ENIGMÁTICA: uma proposta metodológica para o ensino de alguns objetos matemáticos usando a criptografia

Dayziane do Socorro Epifanio da Silva

Dissertação apresentada ao programa de Pós-Graduação de mestrado profissional em Matemática em Rede Nacional – PROFMAT, da Universidade Federal do Pará, como parte dos requisitos necessários para obtenção do Título de Mestre em Matemática.

Bragança, 19 de agosto de 2023

BANCA EXAMINADORA

Marly dos Anjos Nunes.

Prof. Dra Marly dos Anjos Nunes

Orientadora - UFPA

Edilene Farias Rozal

Prof. Dra Edilene Farias Rozal

Coorientadora - UFPA

Edson Jorge de Matos

Prof. Dr Edson Jorge de Matos

Examinador Interno - UFPA

Andréia Gomes Pinheiro

Prof. Dra Andréia Gomes Pinheiro

Examinador Interno - IFPA

Sandro do N. da Costa

Prof. Dr Sandro do Nascimento da Costa

Examinador Externo - IFPA

Dedico este trabalho a todas as pessoas que contribuíram direta ou indiretamente com a sua concretização. Em especial aos meus pais, que sempre foram grandes incentivadores dos meus estudos, mesmo sem terem tido as mesmas oportunidades para estudos formais.

Agradecimentos

A Deus, por iluminar meus caminhos, proporcionando condições para vencer todos os obstáculos e dificuldades enfrentadas ao longo do curso.

A meus familiares, em especial, meus pais, Raimundo e Maria José e meu esposo Lucivaldo pela dedicação, amor e carinho que sempre tiveram por mim, principalmente, quando eu mesma não mais acreditava ser capaz, eles estavam ali me apoiando.

Aos meus colegas de curso, que hoje posso verdadeiramente chamar pelo adjetivo, amigos, pois eles me auxiliaram nos momentos de dificuldades oferecendo sempre um ombro amigo, além é claro, de seus conhecimentos matemáticos.

A minha orientadora Profa. Dra. Marly dos Anjos, que não à toa tem esse sobrenome, pois foi um anjo que surgiu em minha vida em meio à turbulência e pressão que é este curso. Minha gratidão pela paciência, sabedoria, carinho e pelo seu incansável e permanente encorajamento destacados sempre em nossos processos dialéticos.

A minha co-orientadora Profa. Dra. Edilene Farias por sua grande contribuição, dedicação e sugestões que foram preciosas para a concretização desta dissertação.

Aos professores que passaram pelo curso PROFMAT contribuindo significativamente para o nosso crescimento intelectual, em especial ao professor Dr. Edson Matos que tenho como um grande mestre e exemplo de ser humano e ao professor Dr. Carlos Baldez que não mediu esforços para auxiliar nossa turma nessa grandiosa caminhada formativa, disponibilizando seu precioso tempo para que pudéssemos obter um bom desempenho no ENQ.

Aos meus alunos que contribuíram com a pesquisa, eles foram fundamentais para o enriquecimento do trabalho.

Enfim, quero agradecer a todos que contribuíram de alguma forma para que eu chegasse ao final desta jornada.

Resumo

Um grande desafio enfrentado pelos professores de matemática, na contemporaneidade, é desenvolver atividades que sejam atrativas e aos mesmo tempo consigam desenvolver o cognitivo do aluno. É neste contexto que este trabalho foi desenvolvido, objetivando apresentar a criptografia como um recurso didático para estimular a aprendizagem de alguns objetos do conhecimento matemático. Tendo em vista que, a criptografia é bastante utilizada por nossa sociedade de um modo geral, em especial, com o avanço e modernização das tecnologias. Esse trabalho foi desenvolvido com o objetivo de apresentá-la como um recurso didático no ensino de conteúdos da educação básica, mais precisamente na disciplina Matemática, uma vez que, ela é a principal ferramenta utilizada hoje para criptografar mensagens de forma segura e eficaz por meio do uso de chaves. Para isso, realizou-se uma pesquisa qualitativa para aprofundamento da fundamentação teórica, descreveu-se a importância da criptografia no cotidiano. Posteriormente, tem-se um exemplo de recurso metodológico que utiliza a criptografia como fonte facilitadora do ensino de funções por meio de histórias em quadrinhos. Adiante, temos a apresentação do jogo ENIGMÁTICA que utiliza o QR CODE para criptografar as questões, além de ter uma boa dosagem de tecnologia, tornando o jogo ainda mais atrativo. Por fim, tem-se uma pesquisa de campo para verificar as deficiências no aprendizado, mas também averiguar o nível de aceitação e consequentemente, efetividade do jogo. Com base nos resultados da pesquisa, conseguimos certificar que a utilização de jogos aliando criptografia a conteúdos básicos matemáticos desperta o interesse, estimulando a aprendizagem significativa.

Palavras-chave: Criptografia, Matemática, ENIGMÁTICA, ensino.

Abstract

A major challenge faced by mathematics teachers today is to develop activities that are attractive and at the same time manage to develop the student's cognitive skills. It is in this context that this work was developed, aiming to present cryptography as a teaching resource to stimulate the learning of some objects of mathematical knowledge. Considering that encryption is widely used by our society in general, especially with the advancement and modernization of technologies. This work was developed with the aim of presenting it as a didactic resource in teaching basic education content, more precisely in the Mathematics discipline, since it is the main tool used today to encrypt messages securely and effectively through the use of keys. To this end, qualitative research was carried out to deepen the theoretical foundation, describing the importance of encryption in everyday life. Subsequently, there is an example of a methodological resource that uses cryptography as a source to facilitate the teaching of functions through comic books. Next, we have the presentation of the ENIGMÁTICA game that uses QR CODE to encrypt questions, in addition to having a good dose of technology, making the game even more attractive. Finally, there is field research to verify learning difficulties, but also to determine the level of acceptance and, consequently, effectiveness of the game. Based on the research results, we were able to certify that the use of games combining cryptography with basic mathematical content arouses interest, stimulating meaningful learning.

Keywords: Cryptography, Mathematics, ENIGMATICA, teaching.

Lista de Figuras

Sumário

Capítulo 1

Introdução

O presente trabalho é moldado através de uma pesquisa qualitativa que aborda o poder que a criptografia exerce em sala de aula no processo de ensino e aprendizagem de alguns conteúdos matemáticos, proporcionando ao aluno o contexto histórico, a revisão de alguns objetos do conhecimento matemático, dando a ele um novo sentido ao que é apresentado em sala de aula com a sua realidade, sobretudo, através do uso da tecnologia para ocultar algumas informações confidenciais. É importante destacar que, a pesquisa qualitativa se preocupa com o nível de realidade que não pode ser quantificado, ou seja, ela trabalha com o universo de significados, de motivações, aspirações, crenças, valores e atitudes (MINAYO, 2014).

A humanidade, desde seus primórdios, sempre teve a necessidade de se comunicar e ao mesmo tempo de manter uma grafia secreta, uma vez que o sigilo na comunicação deve acompanhar o surgimento da escrita. Esse tipo de escritura fez-se indispensável, pelo comércio, espionagem e guerras que sempre estiveram presentes em nossa sociedade.

Dessa forma, a criptografia faz parte da história humana e é definida como sendo o estudo de métodos para "esconder" o conteúdo original de mensagens, tornando as informações ilegíveis para pessoas não autorizadas. Nesse processo de ocultar as informações, a matemática é uma grande aliada da criptografia.

Diante desse quadro, considera-se relevante desenvolver um estudo sobre o papel imprescindível que a matemática básica exerce sobre o sigilo de senhas, transações bancárias, mensagens instantâneas entre outros.

De acordo com Cantoral et al (2000) a Criptografia pode ser um elemento motivador para o processo de ensino da Matemática. Nesta perspectiva, existe uma necessidade

de apresentar a criptografia como um instrumento pedagógico aos alunos de qualquer nível de ensino, desde que, sejam feitas as devidas adequações, a fim de instigar e potencializar o conhecimento matemático de alguns objetos tão importante no campo da referida disciplina.

Embora a criptografia possa ser largamente explorada em disciplinas envolvendo a segurança da informação para proteção de dados, pesquisas na área da educação indicam que os alunos não se sentem motivados neste tema devido, principalmente, ao número limitado de horas de aula, dificuldades matemáticas e a falta de ferramentas para obter prática na criptografia (SONG; DENG, 2009; OLEJAR; STANEK, 1999).

Pesquisas como a de Pacheco e Andreis (2018) e Holanda, Freitas e Rodrigues (2020) apontam que as principais dificuldades em aprender matemática podem estar relacionadas ao fato de o aluno criar barreira em si mesmo após ter os primeiros contatos com a disciplina, onde não obteve uma experiência positiva em sala de aula, e assim, passa a acreditar que não será capaz de aprender.

A criptografia possibilita interligar os conteúdos matemáticos a situações do mundo real, e ajuda a desenvolver habilidades e competências na resolução de problemas, a criar estratégias de resolução, a ter autonomia durante o processo de aprendizagem (GROENWALD e FRANKE, 2008), o que possibilita uma melhor compreensão dos objetos matemáticos envolvidos nesta técnica.

Durante esses quinze anos de docência transitando em escola pública e privada, sempre percebi as dificuldades que a maioria dos alunos têm em construir um pensamento matemático, principalmente se tratando de álgebra. Sempre existiu dentro de mim uma grande inquietude que me instigava a buscar métodos que pudessem minimizar essas dificuldades. Tendo isso em mente, fiz cursos que possibilitavam melhorar minhas práticas docentes. Em 2018 fui apresentada ao curso Google for education, onde utilizávamos recursos tecnológicos para deixar as aulas mais interativas. Motivada pelo curso, em 2019 resolvi fazer uma especialização nessa área, podendo me aprofundar melhor no conhecimento sobre as metodologias ativas, que muito contribuíram para a descentralização do meu trabalho enquanto professora, deixando um espaço mais amplo para o protagonismo do aluno.

Em 2020, a pandemia aumentou ainda mais o abismo existente no nosso sistema educacional. Neste mesmo ano terminava a especialização e um curso de tecnologia ofer-

tado pela universidade do Ceará. Esses cursos me auxiliaram a montar as aulas remotas de modo mais dinâmico e também a perceber que era possível ir mais longe, tanto que enveredei para o PROFMAT, que me ajudou a sistematizar os conhecimentos matemáticos, além de me colocar novamente na situação de aluna, fazendo com que eu pudesse exercer com mais empatia o papel de professora, uma vez que estava vivenciando os dois lados ao mesmo tempo. Tal egresso fez com que muitas situações fossem por mim refletidas, uma delas foi minha prática docente, uma vez que, como professora, muitas vezes repliquei o modo tradicional outrora trabalhado por meus professores e que muitas vezes no papel de aluna questionei. Desta maneira Delors coloca que:

> A qualidade de ensino é determinada tanto ou mais pela formação contínua dos professores, do que pela sua formação inicial... A formação contínua não deve desenrolar-se, necessariamente, apenas no quadro do sistema educativo: um período de trabalho ou de estudo no setor econômico pode também ser proveitoso para aproximação do saber e do saber-fazer (DELORS, 2003, p. 160)

Diante disso, é necessário desenvolver atividades que estimulem e aumentem a confiança do aluno em aprender matemática e ao mesmo tempo destacar suas aplicações práticas. Dessa maneira, o uso da criptografia como recurso didático pode ser a válvula propulsora para o ensino da matemática, permitindo o aprofundamento da compreensão dos conceitos apresentados em sala de aula.

Perante esse desafio e das experiências que ele nos proporcionará é válido nos questionarmos: será que a criptografia aliada aos conteúdos matemáticos pode estimular a aprendizagem matemática? É possível despertar o interesse dos alunos relacionando a prática que envolve criptografia e a matemática?

Assim, temos como objetivo deste trabalho apresentar a criptografia como um recurso didático para estimular a aprendizagem de alguns objetos do conhecimento matemático. De modo específico: 1. conceituar os objetos matemáticos que auxiliam o funcionamento da criptografia; 2. destacar a relação da matemática e suas sutilezas no processo de criptografar informações; e 3. desenvolver atividades para codificar e decodificar mensagens usando alguns objetos matemáticos.

O trabalho está dividido em seis capítulos, o primeiro apresenta-se a introdução, que é o "cartão de visita" da dissertação. O segundo capítulo aborda a fundamentação teórica, o capitulo três fala sobre a importância da Criptografia no cotidiano. Já o quarto capítulo é dedicado as Histórias Criptografadas: um recurso metodológico para aplicação

da criptografia no contexto escolar, este apresenta uma atividade desenvolvida em sala de aula, trazendo alguns exemplos. O capítulo cinco apresenta o Jogo ENIGMÁTICA, detalhando o uso dele como recurso no processo de ensino e aprendizagem de uma turma de terceiro ano do ensino médio de uma escola estadual localizada em Capanema-Pa. Por sua vez, o capítulo seis vem mostrando o resultado da pesquisa de campo e, na sequência, as considerações finais.

Capítulo 2

Fundamentação Teórica

A matemática do ensino médio assim como toda matemática ensinada na educação básica, tem por finalidade na formação do raciocínio lógico do aluno, além de ajudá-lo na resolução de problemas do cotidiano. Porém, a forma engessada que muitos professores utilizam para compreender esse conhecimento, faz com que, essa disciplina seja considerada por muitos como difícil e inacessível, tornando o aluno como um sujeito passivo dentro do seu processo de aprendizagem.

Freudenthal (1991) destaca que, na prática, professores se apegam ao livro didático para desenvolver o conteúdo curricular e essa postura, muitas vezes, impede o docente de se apropriar do contexto escolar e improvisar sua prática pedagógica. De fato, é preciso ensinar uma matemática mais associada a realidade do aluno. D'Ambrósio (1999) enfatiza a importância em recuperar a presença de ideias matemáticas em todas as ações humanas devido à necessidade de descobrir que há uma forma matemática de estar no mundo.

Trazendo a discussão para o campo da álgebra, pode-se dizer que o objetivo do ensino da mesma, se dá na possibilidade de fazer com que o discente aumente sua capacidade de abstrair e generalizar, no entanto, o que acontece muitas vezes é que essa disciplina é ministrada de forma mecanizada e sem importância para além dos muros da escola. Sobre o assunto, Lins (2004) explica que há:

> Um grande estranhamento entre a matemática da escola, dita oficial e a matemática da rua, da vida real, o que justifica o fracasso de tantos em relação à matemática escolar, não por não conseguirem aprender, mas por apresentarem como que um sintoma de recusa em se aproximar das coisas estranhas da sala de aula. (LINS, 2004, p. 109)

Hoje em dia, uma das grandes dificuldades retratadas pelos alunos é o uso de letras nos cálculos matemáticos. Nas palavras de Santomé (2002, p. 161): "Em muitas ocasiões os conteúdos são contemplados pelo alunado como fórmulas vazias, sem sequer a compreensão de seu sentido". Neste contexto, temos o estudo da álgebra que parece não ter nenhuma correlação com o cotidiano do aluno, ocasionando muitas vezes o insucesso no aprendizado.

Levando em consideração esse panorama, compreende-se que é necessário tencionar e selecionar metodologias de ensino que levem em conta não tão somente a natureza do assunto, mas ao mesmo tempo a forma como os discentes aprendem e conseguem aplicar no mundo que o cerca, mostrando que não é aprender somente por aprender, mas que existe uma aplicabilidade funcional em seu cotidiano.

Nesta perspectiva, é necessário que os professores procurem incentivar a criatividade de seus alunos através de atividades que realmente os estimulem e que façam parte de sua vivência, como é o caso, do ensino das funções, matrizes, critérios de divisibilidade e congruência modular usando a criptografia.

2.1 Aplicando a criptografia nos objetos de conhecimento do ensino médio.

A criptografia utiliza muitos conhecimentos matemáticos, como matrizes e funções, para garantir uma maior segurança ao ocultar uma mensagem, por isso é uma excelente opção de recurso didático. Para tanto, iremos justificar a importância de lecionar esses objetos no ensino médio.

As matrizes fazem parte da vida do aluno, ainda que ele não perceba, devido muitas vezes a descontextualização a qual se trabalha o assunto, pois a tabela de jogos feita no campeonato estudantil, ou simplesmente, seu boletim escolar, são exemplos clássicos de matrizes. É importante ressaltar o fato que muitas vezes é desprezado, que matriz é um importante instrumento para a compreensão de outros conceitos. Afirma Dante (2005, p.240) que "é importante que se domine um instrumento matemático para poder utilizá-lo como ferramenta nas diversas aplicações possíveis".

De acordo com Saches, 2002 (apud SALATESKI, 2008, p. 5):

> A álgebra das matrizes tem importância significativa para várias ciências e encontram, cada vez mais, aplicações em diversos setores como a Economia, a Engenharia e Tecnologia, etc. Se não ocorrer uma aprendizagem significativa e relevante dos conceitos de matrizes, os estudantes poderão apresentar dificuldades, em níveis mais avançados, para compreender e aplicar outros conceitos relacionados, tais como conceitos de programação, computação gráfica, custos de produção, teoria dos grafos, circuitos elétricos, modelos econômicos lineares, entre centenas de outros.

De tal modo, diante do exposto, fica corroborada a importância do estudo do objeto do conhecimento, matrizes, mostrando a sua aplicabilidade para o aluno, através do uso da criptografia, situação que está diretamente ligada a sua vida, para que seja possibilitado uma aprendizagem significativa.

Por outro lado, temos também um outro objeto matemático muito importante, para ser apresentado ao aluno de forma mais contextualizada com o mundo em que ele vive, as funções.

O conceito de função é um dos mais importantes dentro da matemática, além de ter uma grande aplicabilidade no cotidiano.

Brasil (2002, 2006) destacam o poder de alcance do conceito de função e a importância do mesmo para a Matemática e outros campos do conhecimento:

> O estudo das funções permite ao aluno adquirir a linguagem algébrica como a linguagem das ciências, necessária para expressar a relação entre grandezas e modelar situações-problema, construindo modelos descritivos de fenômenos e permitindo várias conexões dentro e fora da própria matemática. (BRASIL, 2006, p.121)

Desse modo, fica evidente que tal conteúdo não deve de modo algum ser ministrado de forma desassociada da realidade, pois situações do cotidiano não podem ser consideradas apenas importantes. Elas são indispensáveis! Ou então, a formação para a cidadania não terá sua completude.

2.1.1 Matrizes

Segundo Lopes (2008), podemos encontrar matrizes em diversos setores sociais. Sua importância é bastante significativa dentro da Matemática, especialmente na Álgebra Linear e computação gráfica, assim como também no cotidiano do ser humano. Um

exemplo bastante relevante a ser ressaltado são os pixels da tela de um computador, além de ser uma poderosa ferramenta bastante usada na criptografia.

Sendo assim, esta seção apresenta os conteúdos de matrizes que serão utilizados na criptografia.

Definicão 2.1.1. *Uma matriz é uma tabela com m linhas e n colunas (indicamos por $m \times n$), com m e n números inteiros positivos.*

Exemplos 2.1.1. *Veja um exemplo de matriz:*

$$A = \begin{pmatrix} 1 & 3 & 0 \\ 2 & 5 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

Dizemos que A é uma matriz 3×3, pois possui 3 linhas e 3 colunas.

Em uma matriz A, indicamos cada elemento por a_{ij}. Onde o índice i indica a linha e o índice j a coluna às quais o elemento pertence. Veja como podemos representar uma matriz com m linhas e n colunas.

$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix}$$

Chamamos de matriz quadrada de ordem n toda matriz do tipo $n \times n$, isto é, toda matriz que possui n linhas e n colunas e representamos:

$$A_{n\times n} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}$$

Uma matriz A_n é dita nula se $a_{ij} = 0$ para todo i e todo j.

Em uma matriz quadrada A de ordem n, os elementos a_{ij} tais que $i = j$ formam a diagonal principal e os elementos tais que $i + j = n + 1$ formam a diagonal secundária.

Quando os elementos da diagonal principal de uma matriz quadrada são iguais a 1 e os demais elementos iguais a zero, temos uma matriz chamada matriz identidade. A matriz I_n é o elemento neutro da multiplicação de matrizes quadradas de mesma ordem.

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$$

Multiplicação de matrizes

Dada as matrizes $A = (a_{ij})$ de tipo $m \times n$, e uma matriz $B = (b_{jk})$, de tipo $n \times p$, o produto de A por B (indica-se AB) a matriz $C = (c_{ik})$, de tipo $m \times p$, em que cada elemento c_{ik} é obtido multiplicando ordenadamente os elementos da linha i da matriz A pelos elementos da coluna k da matriz B e somando os produtos obtidos. Simbolicamente, podemos escrever

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}$$

Matriz Inversa

Seja A uma matriz quadrada de ordem n. Quando existir uma matriz B de ordem n tal que $A \cdot B = I_n$ e $B \cdot A = I_n$, dizemos que B é a matriz inversa de A. Quando B existe, dizemos que A é invertível. Indicamos a matriz inversa de A por A^{-1} e ela é única.

De fato, suponha que B e C sejam, inversas de A. Então

$$C = CI = C(AB) = (CA)B = IB = B$$

Proposição 2.1.1. *A matriz quadrada A é invertível se, e somente se,* $\det A \neq 0$.

Exemplos 2.1.2. *Encontre a matriz inversa de A*

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

Pela definição de matriz inversa, vem que

$$\begin{aligned} A \cdot A^{-1} &= I_n \\ \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Ao realizar a multiplicação entre as matrizes, temos

$$\begin{aligned} A \cdot A^{-1} &= I_n \\ \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} a+2c & b+2d \\ 3a+4c & 3b+4d \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Resolvendo os sistemas, obtemos a seguinte matriz inversa

$$A^{-1} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

Utilizando matrizes inversas para criptografar mensagem

A tabela 2.1 a seguir apresenta a correspondência para converter as letras em números, usaremos o símbolo #, que indica espaço.

Tabela 2.1: Alfabeto com seus respectivos valores numéricos

#	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

A correspondência da tabela 2.1 deve ser conhecida tanto pelo remetente da mensagem criptografada quanto o destinatário. Além do mais, uma matriz invertível deve ser definida, pois ela será a chave de codificação e decodificação da mensagem.

Exemplos 2.1.3. *Usaremos como chave a matriz invertível* $A = \begin{pmatrix} 2 & 3 \\ 5 & 8 \end{pmatrix}$ *para criptografar a seguinte palavra PROFMAT#.*

Como a chave para criptografar a mensagem é uma matriz quadrada de ordem 2, organizaremos a matriz que forma a palavra em uma sequência numérica obtida em uma matriz D com duas linhas, por isso, justifica-se o uso # para completar a matriz.

P	R	O	F	M	A	T	#
16	18	15	6	13	1	20	0

Observe que a palavra tem 8 elementos. Os 4 primeiros serão dispostos na primeira linha e os outros 4 na segunda

$$D = \begin{pmatrix} 16 & 18 & 15 & 6 \\ 13 & 1 & 20 & 0 \end{pmatrix}$$

Devemos multiplicar a matriz chave (A) pela matriz mensagem (D) encontrando $B = A \cdot D$, obtendo a mensagem criptografada.

$$B = A \cdot D = \begin{pmatrix} 2 & 3 \\ 5 & 8 \end{pmatrix} \cdot \begin{pmatrix} 16 & 18 & 15 & 6 \\ 13 & 1 & 20 & 0 \end{pmatrix} = \begin{pmatrix} 71 & 39 & 90 & 12 \\ 184 & 98 & 235 & 30 \end{pmatrix}$$

Logo, a matriz $B = \begin{pmatrix} 71 & 39 & 90 & 12 \\ 184 & 98 & 235 & 30 \end{pmatrix}$

Ao receber a mensagem criptografada, o destinatário deverá multiplicá-la pela matriz inversa de A, isto é, $A^{-1} = \begin{pmatrix} 8 & -3 \\ -5 & 2 \end{pmatrix}$.

$$D = A^{-1} \cdot B = \begin{pmatrix} 8 & -3 \\ -5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 71 & 39 & 90 & 12 \\ 184 & 98 & 235 & 30 \end{pmatrix} = \begin{pmatrix} 16 & 18 & 15 & 6 \\ 13 & 1 & 20 & 0 \end{pmatrix}$$

Dessa forma, o destinatário usando a tabela referência consegue chegar na palavra original.

2.1.2 Funções

No que diz respeito ao conteúdo "Funções", segundo os PCNEM (BRASIL, 1997) observa-se que o ensino isolado desse tema não permite a exploração do caráter integrador que ele possui e que este conteúdo pode integrar vários assuntos como a Trigonometria sendo vista como as funções trigonométricas e seus gráficos, as sequências, em especial progressões aritméticas e progressões geométricas, nada mais são que particulares funções,

as propriedades de retas e parábolas estudadas em Geometria Analítica são propriedades dos gráficos das funções correspondentes e os aspectos do estudo de polinômios e equações algébricas podem ser incluídos no estudo de funções polinomiais. (BRASIL,1997)

O objeto de conhecimento função tem um papel extremamente fundamental, pois além de atrelar vários temas matemáticos ainda possibilita estudar por meio da leitura e interpretação de gráficos, o desempenho de alguns fenômenos do dia a dia, assim como de outras áreas do conhecimento, como Geografia ou Física.

Tendo sua importância justificada, abordaremos neste tópico um conciso estudo sobre funções e como ela pode ser aplicada na criptografia.

Definicão 2.1.2. *Dados dois conjuntos X e Y definimos uma função f de X em Y, denotado por $f : X \to Y$, uma regra que associa a cada $x \in X$ um único $y \in Y$.*

A definição citada acima é uma das mais popularizadas principalmente, em livros didáticos, porém, existem outras definições. Uma delas está ligada diretamente com a Teoria dos Conjuntos de Cantor, que permitiu a Riemann (século XIX) definir uma função f como uma relação dada por um conjunto de pares ordenados que obedecem à seguinte condição: se os pares (x_1, y_1) e (x_2, y_2) pertencem a f, e $x_1 = x_2$, logo $y_1 = y_2$. O conjunto dos primeiros elementos dos pares ordenados é o domínio da função, e o conjunto de todos os segundos elementos dos pares ordenados se diz imagem da função. Assim, uma função é simplesmente um tipo particular de subconjunto do produto cartesiano de dois conjuntos. (EVES, 2011, p. 660-661).

Função Afim

Uma aplicação de $\mathbb{R}$ em $\mathbb{R}$ recebe o nome de função afim quando a cada $x \in \mathbb{R}$ associa o elemento $(ax + b) \in \mathbb{R}$ com $a \neq 0$ em que a e b são números reais dados.

$$f(x) = ax + b \quad (a \neq 0)$$

Função Inversa

Se f é uma função bijetora de A em B, a relação inversa de f é uma função de B em A que denominamos função inversa de f e indicamos por f^{-1}, tal que $f^{-1} : B \to A$, $y \in B$ é tal que $f^{-1}(y) = x$, onde x é o único elemento em A que satisfaz $f(x) = y$.

Teorema 2.1.1. *Seja $f : A \to B$. A função f admite inversa f^{-1} de B em A se, e somente se, f é bijetora.*

Demonstração: A função afim $f(x) = ax + b$ com $a \neq 0$, é injetora.

De fato, para todos x_1 e x_2 em $\mathbb{R}$, temos

$$f(x_1) = f(x_2) \quad \Leftrightarrow \quad ax_1 + b = ax_2 + b \quad \Leftrightarrow \quad ax_1 = ax_2 \Leftrightarrow$$
$$ax_1 - ax_2 = 0 \quad \Leftrightarrow \quad a(x_1 - x_2) = 0$$

Como $a(x_1 - x_2) = 0$, $a \neq 0$, então $(x_1 - x_2) = 0$ e portanto $x_1 = x_2$.

A função afim $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax + b \quad (a \neq 0)$ é sobrejetora.

Dado $y \in \mathbb{R}$, exibiremos $x \in \mathbb{R}$ tal que $f(x) = y$. Se $y \in \mathbb{R}$ então $x = \frac{y-b}{a}$ é um número real tal que

$$f(x) = a(\tfrac{y-b}{a}) + b = y$$

Portanto, a função afim é bijetora.

Demonstração:

i. Se f^{-1} é uma função de B em A, então f é bijetora.

- Para todo $y \in B$ existe um $x \in A$ tal que $f^{-1}(y) = x$, isto é $(y, x) \in f^{-1}$, ou ainda $(x, y) \in f$. Assim f é sobrejetora.

- Dados $x_1 \in A$ e $x_2 \in A$, com $x_1 \neq x_2$, se tivermos $f(x_1) = f(x_2) = y$ resultará em $f^{-1}(y) = x_1$ e $f^{-1}(y) = x_2$, que é absurdo pois y só tem uma imagem em f^{-1}. Assim, $f(x_1 \neq f(x_2))$ é injetora.

ii. Se f é bijetora, então f^{-1} é uma função de B em A.

- Como f é sobrejetora, para todo $y \in B$ existe um $x \in A$ tal que $(x, y) \in f$ portanto, $(y, x) \in f^{-1}$.

- Se $y \in B$, para duas imagens x_1 e x_2 em f^{-1}, vem $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$ portanto, $(x_1, y) \in f$ e $(x_2, y) \in f$. Como f é injetora, resulta $x_1 = x_2$.

A função afim será o objeto de estudo no processo de criptografia, por isso, é preciso provar que ela é bijetora, logo admite uma inversa, pois é baseado neste conceito que usamos as chaves para esconder as informações de pessoas não autorizadas a vê-las.

Utilizando os conceitos de função afim e inversa para criptografar mensagens.

Assim como utilizado nas matrizes, devemos também ter uma tabela de conversão que deve ser conhecida tanto pelo emissor quanto pelo receptor. Para efeito de demonstração do processo de criptografia usando função, usaremos a tabela 2.1 para converter as letras em números.

Iremos criptografar a mensagem: EU GOSTO DE ESTUDAR

E	U	#	G	O	S	T	O	#	D	E	#	E	S	T	U	D	A	R
5	21	0	7	15	19	20	15	0	4	5	0	5	19	20	21	4	1	18

Usando a função afim $f(x) : 2x + 5$ como chave para criptografar a mensagem escolhida, temos

$$
\begin{aligned}
f(15): &\quad 2 \cdot 5 + 5 &&= 15 \\
f(21): &\quad 2 \cdot 21 + 5 &&= 47 \\
f(0): &\quad 2 \cdot 0 + 5 &&= 5 \\
f(7): &\quad 2 \cdot 7 + 5 &&= 19 \\
f(15): &\quad 2 \cdot 15 + 5 &&= 35 \\
f(19): &\quad 2 \cdot 19 + 5 &&= 43 \\
f(20): &\quad 2 \cdot 20 + 5 &&= 45 \\
f(15): &\quad 2 \cdot 15 + 5 &&= 35 \\
f(0): &\quad 2 \cdot 0 + 5 &&= 5 \\
f(4): &\quad 2 \cdot 4 + 5 &&= 13 \\
f(5): &\quad 2 \cdot 5 + 5 &&= 15 \\
f(0): &\quad 2 \cdot 0 + 5 &&= 5 \\
f(5): &\quad 2 \cdot 5 + 5 &&= 15 \\
f(19): &\quad 2 \cdot 19 + 5 &&= 43 \\
f(20): &\quad 2 \cdot 20 + 5 &&= 45
\end{aligned}
$$

$$
\begin{aligned}
f(21): \quad 2 \cdot 21 + 5 &= 47 \\
f(4): \quad 2 \cdot 4 + 5 &= 13 \\
f(1): \quad 2 \cdot 1 + 5 &= 7 \\
f(18): \quad 2 \cdot 18 + 5 &= 41
\end{aligned}
$$

A mensagem criptografada é: 15 47 5 19 35 43 45 35 5 13 15 5 15 43 45 47 13 7 41.

Ao receber a mensagem criptografada o destinatário deve descriptografá-la utilizando a função inversa, no caso, $f^{-1}(y) : \frac{y-5}{2}$, da seguinte forma

$$
\begin{aligned}
f^{-1}(y): \quad \tfrac{y-5}{2} & \\
f^{-1}(15): \quad \tfrac{15-5}{2} &= 5 \\
f^{-1}(47): \quad \tfrac{47-5}{2} &= 21 \\
f^{-1}(5): \quad \tfrac{5-5}{2} &= 0 \\
f^{-1}(19): \quad \tfrac{19-5}{2} &= 7 \\
f^{-1}(35): \quad \tfrac{35-5}{2} &= 15 \\
f^{-1}(43): \quad \tfrac{43-5}{2} &= 19 \\
f^{-1}(45): \quad \tfrac{45-5}{2} &= 20 \\
f^{-1}(35): \quad \tfrac{35-5}{2} &= 15 \\
f^{-1}(5): \quad \tfrac{5-5}{2} &= 0 \\
f^{-1}(13): \quad \tfrac{13-5}{2} &= 4 \\
f^{-1}(15): \quad \tfrac{15-5}{2} &= 5 \\
f^{-1}(5): \quad \tfrac{5-5}{2} &= 0 \\
f^{-1}(15): \quad \tfrac{15-5}{2} &= 5 \\
f^{-1}(43): \quad \tfrac{43-5}{2} &= 19 \\
f^{-1}(45): \quad \tfrac{45-5}{2} &= 20 \\
f^{-1}(47): \quad \tfrac{47-5}{2} &= 21 \\
f^{-1}(13): \quad \tfrac{13-5}{2} &= 4
\end{aligned}
$$

$$f^{-1}(7): \ \frac{7-5}{2} = 1$$
$$f^{-1}(41): \ \frac{41-5}{2} = 18$$

A mensagem descriptografada é: 5 21 0 7 15 19 20 15 0 4 5 0 5 19 20 21 4 1 18, isto é, a mensagem original.

2.1.3 Aritmética Modular

Mesmo que de forma inconsciente, muitas pessoas usam constantemente a aritmética modular, em especial, quando realizam divisões cujo resto é a resposta para seus questionamentos ou necessidades.

O conceito de aritmética modular passa pela teoria da divisibilidade de números inteiros e pode ser contemplada nos mais diversos campos da matemática, principalmente na teoria dos números, além de possuir um vasto campo de aplicabilidade.

Ponte, Brocado e Oliveira (2009) advertem quanto à importância do desenvolvimento do pensamento aritmético ao colocá-lo como objetivo principal do processo de ensino e aprendizagem da Matemática:

> O conceito de número ocupa um lugar de destaque na matemática escolar. Desenvolver o sentido do número, ou seja, adquirir uma compreensão global dos números e das operações e usá-la de modo flexível para analisar situações e desenvolver estratégias úteis para lidar com os números e as operações é um objetivo central da aprendizagem matemática (PONTE, BROCADO e OLIVEIRA, 2009, p. 55).

Em concordância com o que foi relatado, é importante ressaltar que um dos principais objetivos do ensino da aritmética é compreender os números, as operações, o sistema numérico e as relações entre eles, assim como ampliar a habilidade de cálculo, usando artefatos adequados a cada situação na resolução de problemas.

Congruência Modular

Antes de analisarmos os teoremas que fundamentam a criptografia, é preciso definir a congruência modular. Começaremos com uma notação que designa elementos com mesmo resto na divisão por um mesmo natural.

Definicão 2.1.3. *Seja $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Se $a = mq_1 + r$ e $b = mq_2 + r$, com $0 \leq r < m$, então diremos que a e b são congruentes entre si módulo m, ou, se o contexto deixar m*

claro, simplesmente congruentes. Denotaremos, quando isso ocorrer, por

$$a \equiv b \, mod \, (m)$$

Perceba que nesse caso, quando os restos na divisão por m são iguais, temos

$$a - b = mq_1 + r - mq_2 - r = m(q_1 - q_2).$$

Ou seja, a diferença entre elementos congruentes módulo m é um múltiplo de m. E, supondo dois inteiros $a = mq_1 + r_1$ *e* $b = mq_2 + r_2$ *cuja diferença é um múltiplo de m, teremos*

$$a - b = mk \; \rightarrow \; m(q_1 - q_2) + (r_1 - r_2) = mk.$$

Mas $0 \leq r_1 - r_2 < m$ *e* $m|r_1 - r_2$*, o que implica em* $r_1 - r_2 = 0$ *e portanto* $r_1 = r_2$*.*

Acabamos de provar a primeira propriedade dessa relação entre inteiros, que pode ser enunciada como se segue.

Lema 2.1.1. $a \equiv b \, mod \, (m) \Leftrightarrow m|(a - b)$.

Usando este lema, temos que:

1. $a \equiv a \, mod \, (m)$ pois $a - a = 0$ e $m|0$;
2. $a \equiv b \, mod \, (m)$ implica em $b \equiv a \, mod \, (m)$, pois se $m|a-b$ então $m|-(a-b)$, ou seja, $m|b - a$;
3. e se $a \equiv b \, mod \, (m)$ e $b \equiv c \, mod \, (m)$, então $a \equiv c \, mod \, (m)$, pois $m|a - b$ e $m|b - c$, logo $m|(a - b) + (b - c)$, ou seja, $m|(a - c)$

Em outras palavras, as três propriedades listadas acima mostram que a congruência módulo m é respectivamente reflexiva, simétrica e transitiva, ou seja, é uma **relação de equivalência**.

A aritmética modular permite a criação de sistemas de criptografia mais robustos ao abordar conceitos de divisibilidade e congruência que são trabalhados com conjunto dos números inteiros, dando ênfase ao uso de números primos grandes que permitem uma codificação simples, porém uma decodificação bem mais complexa, como exemplo, temos o sistema de criptografia RSA, iniciais de seus desenvolvedores Rivest, Shamir e Adleman surgiu em 1976. Para isso, deve-se conhecer os Teoremas que são fundamentais nesse processo, os quais veremos a seguir:

Teorema 2.1.2. *(**Teorema Fundamental da Aritmética**). Todo inteiro $a \geq 2$ pode ser escrito como produto de números primos. Esta decomposição é única exceto pela ordem dos fatores primos.*

Prova: Ver [Hefez], p. 122

Teorema 2.1.3. *(**Divisão Euclidiana**). Sejam a e b dois números inteiros com $a > 0$. Existem dois únicos números inteiros q e r que são chamados o quociente e resto da divisão de b por a, tais que: $b = a.q + r$, com $0 \leq r < a$.*

Prova: Ver [Hefez], p. 46

Algoritmo Euclidiano

Dados dois números inteiros positivos a e b tais que $a \geq b$, divide-se a por b, encontrando resto r_1. Se $r_1 \neq 0$, dividimos b por r_1, obtendo resto r_2. Se $r_2 \neq 0$, dividimos r_1 por r_2 e assim por diante. O último resto diferente de zero dessa sequência de divisões é o $mdc\,(a, b)$.

Teorema 2.1.4. *(**Algoritmo Euclidiano Estendido**). Sejam a e b inteiros positivos e seja d o máximo divisor comum entre a e b. Existem inteiros α e β tais que $\alpha a + \beta b = d$.*

Definicão 2.1.4. *Seja n um inteiro positivo. A função de Euler $\phi(n)$ é definida como o número de inteiros positivos não excedendo n que são relativamente primos com n.*

Definicão 2.1.5. *Diremos que d é um máximo divisor comum mdc de a e b se possuir as seguintes propriedades:*

- *d é um divisor comum de a e de b, sendo a e b não simultaneamente nulos;*
- *d é divisível por todo divisor comum de a e b.*

Teorema 2.1.5. *(Função de Euler). Se m, n são inteiros positivos tais que $mdc\,(m, n) = 1$, então $\phi(mn) = \phi(m-1) \cdot \phi(n-1)$*

Se $n = p_1^{k1} \cdots p_r^{kr}$, onde os p_j são os fatores primos de n, então, pode-se determinar o valor da função em n, por: $\phi(n) = (p1-1)p_1^{k1-1} \cdots (pr-1)p_r^{kr-1}$.

Teorema 2.1.6. *(**Teorema de Euler**). Se n é um inteiro positivo e a é um inteiro tal que $mdc\,(a, n) = 1$, então $a^{\phi(n)} \equiv 1 (mod\, n)$.*

Processo de cifragem por meio de RSA

1. Atribuímos valores numéricos as letras do alfabeto;

2. Escolhemos dois primos distintos p e q e definimos seu produto por $n = p.q$, que pelo Teorema 2.1.2, garante-se que é único;

3. Aplicamos o Teorema 2.1.5 em n para obter $\phi(n)$;

4. Escolhemos um número r em que $1 < r < \phi(n)$, de forma que $mdc\,(\phi(n), r) = 1$. Neste passo, criamos a chave-pública, que permite cifrar a mensagem;

5. Aplicando a fórmula $m^r \equiv c\,(mod\, n)$, onde m é o valor numérico de cada letra. Assim, ciframos a mensagem.

Processo de decifragem

Para decifrar a mensagem utiliza-se a chave privada que obtêm-se por meio de:

1. Encontrar o inverso multiplicativo de r. Ou seja, $\alpha \cdot r = 1(mod\, \phi(n))$. Para isso, aplica-se o Teorema 2.1.4, para encontrar α, tal que $\alpha \cdot r + \beta(\phi(n)) = mdc\,(\phi(n), r) = 1$.

2. Por fim, aplicamos a seguinte equação: $m \equiv c^{\alpha}(mod\, n)$

Com o objetivo de ilustrar o Sistema RSA, mostraremos o exemplo a seguir, onde começaremos por traduzir as mensagens (sequência de letras) em sequências de números inteiros

Tabela 2.2: Conversão de letras para números

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

Usando a tabela 2.2, iremos pré codificar a palavra FERIAS, obtendo

F	E	R	I	A	S
15	14	27	18	10	28

Tomando $p = 5$, $q = 7$ e $r = 7$. Neste caso $n = 5 \times 7 = 35$. Como $r = 7$ é primo, $mdc\,(7, 4\times6) = 1$. Codificando a palavra FERIAS e sabendo que cada bloco da mensagem 151427181028 deve ser menor que o valor de n, temos as seguintes congruências:

$$\begin{aligned} 15^7 &\equiv 15\, mod\, 35 \\ 14^7 &\equiv 14\, mod\, 35 \\ 27^7 &\equiv 13\, mod\, 35 \\ 18^7 &\equiv 32\, mod\, 35 \\ 10^7 &\equiv 10\, mod\, 35 \\ 28^7 &\equiv 7\, mod\, 35 \end{aligned}$$

Os restos encontrados resultam na mensagem codificada: 151413321007.

Quando esta mensagem for recebida, o receptor deve decodificá-la da seguinte maneira:

Deve-se encontrar $\phi(n)$, isto é, $(p-1) \times (q-1)$, no caso do exemplo apresentado o $\phi(n) = 4 \times 6 = 24$.

Assim, para determinar a chave privada α temos que resolver a congruência

$$\begin{aligned} r\alpha &\equiv 1 mod\, \phi(n) \\ 7\alpha &\equiv 1 mod\, \phi(n), \end{aligned}$$

aplicando o inverso multiplicativo, temos que $\alpha = 7$.

Agora resolveremos as congruências para reverter a mensagem, voltando ao seu

formato original.

$$\begin{aligned} c^{\alpha} &\equiv b \, mod \, n \\ 15^7 &\equiv 15 \, mod \, 35 \\ 14^7 &\equiv 14 \, mod \, 35 \\ 13^7 &\equiv 27 \, mod \, 35 \\ 32^7 &\equiv 18 \, mod \, 35 \\ 10^7 &\equiv 10 \, mod \, 35 \\ 7^7 &\equiv 28 \, mod \, 35 \end{aligned}$$

A mensagem descriptografada é 151427181028.

É muito importante perceber que no processo de codificação e decodificação de uma mensagem são acionados alguns teoremas e resultados importantes da aritmética. Isso faz com que, o ensino desses conteúdos utilizando a criptografia seja repensado pelos docentes, pois se torna uma poderosa ferramenta motivadora no processo de ensino e aprendizagem.

Capítulo 3

A importância da Criptografia no cotidiano

Vinda da palavra grega *kryptos*, que significa "escondido, oculto", a criptografia é a área de conhecimento que busca desenvolver técnicas e métodos de modificar uma mensagem tornando-a compreensível apenas aqueles a quem ela se destina, gerando assim sigilo e segurança na troca de informações.

O uso demasiado dessa técnica desde os primórdios, dar-se-á pela seguinte característica: admitir que duas pessoas partilhem entre si mensagens de modo secreto, sem que elas sejam acessadas por algum indivíduo indesejado.

De modo geral, para se criptografar algo, é usado um texto cifrado para esconder o texto original, com base em uma chave.

De acordo com (ORDONEZ; PEREIRA; CHIARAMONTE, 2005), a criptografia é uma técnica que existe há milênios, sendo utilizada até mesmo no hieróglifo, antiga forma de escrita dos egípcios. Isso nos mostra que essa técnica de esconder informações é algo que perdura por muitos anos, mas que vem evoluindo ao longo do tempo, em especial, com o avanço tecnológico.

Por meio dela, cada vez mais, ocorrem atividades do dia-a-dia, como transações financeiras, logar no e-mail, usar o cartão de crédito, receber e enviar criptomoedas, enviar mensagens instantâneas, entre outros. Porém as vezes esse uso passa despercebido, porque muitos utilizam esse processo de forma passiva.

A criptografia desempenha um papel social muito significativo na contemporaneidade, pois assegura ao indivíduo sigilo de suas informações pessoais, principalmente,

porque a Internet não é um ambiente seguro. Além disso, vale ressaltar que a importância dela no meio digital vai para além do sigilo das informações, mas também para a estabilidade e continuidade da oferta de produtos e serviços neste meio, mostrando assim, sua importância econômica.

3.1 Cifras

Para ocultar mensagens de pessoas indesejadas, existem dois modos operantes: por meio de códigos ou de cifras.

O estudo do referido trabalho está concentrado nas cifras, um processo na qual o teor da mensagem original é cifrado através da permuta e/ou substituição das letras da mensagem original. Para descriptografar a mensagem é preciso fazer o processo inverso ao ciframento.

Segundo (ORDONEZ; PEREIRA; CHIARAMONTE, 2005), as cifras mais utilizadas são as de transposição, que consistem de embaralhar os caracteres da informação contida no texto original. Por outro lado, as cifras de substituição utilizam-se de tabelas de substituição predefinidas, que trocam ou substituem um ou mais caracteres da informação original.

3.1.1 Cifra Afim

Para a utilização da cifra afim, assim como outras técnicas já supracitadas, deve-se fazer a substituição das letras e símbolos por números inteiros entre 0 e 26, usando a tabela 2.1 do capítulo 2, seção 2.1.1 e logo depois aplicando a seguinte função

$$y_i = c(x_i) \equiv (ax_i + b)\, mod\, 26$$

em que a e b são números em $\mathbb{Z}_{26}$ x_i e a i-ésima letra do alfabeto original, y_i é a i- ésima letra do texto cifrado e $c(x_i)$ corresponde à codificação da letra x_i.

Vale ressaltar, que a função em questão deve ser injetiva em $\mathbb{Z}_{26}$, pois se assim não o for, poderá haver uma duplicação das letras do alfabeto original que corresponderiam a uma mesma letra ao ser cifrada.

Para que a função $y_i = ax_i + b$ seja injetiva em $\mathbb{Z}_{26}$ devemos ter que a e 26 sejam primos entre si. Quando isso ocorre, podemos criptografar a mensagem sem nos preocuparmos com a repetição de letradas cifradas repetidas.

Exemplificando o uso da cifra afim para função $y_i \equiv (7x_i + 5)\, mod\, 26$. Observe que 7 e 26 são primos entre si, logo essa função é injetiva, assim é possível criptografar a mensagem.

- Para a letra A temos que $x_i = 1$ logo:
  $y_i \equiv (7 \cdot 1 + 5)\, mod\, 26 \quad \rightarrow \quad y_i \equiv 12\, mod\, 26 \quad \rightarrow \quad y_i = L$

- Para a letra B temos que $x_i = 2$ logo:
  $y_i \equiv (7 \cdot 2 + 5)\, mod\, 26 \quad \rightarrow \quad y_i \equiv 19\, mod\, 26 \quad \rightarrow \quad y_i = S$

- Para a letra C temos que $x_i = 3$ logo:
  $y_i \equiv (7 \cdot 3 + 5)\, mod\, 26 \quad \rightarrow \quad y_i \equiv 26\, mod\, 26 \quad \rightarrow \quad y_i = Z$

e assim sucessivamente.

Para decodificar a mensagem, deve-se utilizar a seguinte função

$$x_i = d(y_i) \equiv a^{-1}(y_i - b)\, mod\, 26$$

em que a^{-1} indica o inverso multiplicativo módulo 26 de a.

Utilizando a cifra afim em $y_i = c(x_i) \equiv (3x_i + 8)\, mod\, 26$ e sabendo que essa função é injetiva, pois 3 e 26 são primos entre si, vamos codificar a frase:

Ouse arriscar.

Pela tabela 2.1, fazendo a mudança das letras pelos números, temos

O	U	S	E	#	A	R	R	I	S	C	A	R
15	21	19	5	0	1	18	18	9	19	3	1	18

Aplicando a técnica de afim, vem que

$$
\begin{aligned}
y_i \equiv (3 \cdot 15 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 1\, mod\, 26 \rightarrow \quad y_i = A \\
y_i \equiv (3 \cdot 21 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 19\, mod\, 26 \rightarrow \quad y_i = S \\
y_i \equiv (3 \cdot 19 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 13\, mod\, 26 \rightarrow \quad y_i = M \\
y_i \equiv (3 \cdot 5 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 23\, mod\, 26 \rightarrow \quad y_i = W \\
y_i \equiv (3 \cdot 0 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 8\, mod\, 26 \rightarrow \quad y_i = H \\
y_i \equiv (3 \cdot 1 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 11\, mod\, 26 \rightarrow \quad y_i = K \\
y_i \equiv (3 \cdot 18 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 10\, mod\, 26 \rightarrow \quad y_i = J \\
y_i \equiv (3 \cdot 18 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 10\, mod\, 26 \rightarrow \quad y_i = J \\
y_i \equiv (3 \cdot 9 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 9\, mod\, 26 \rightarrow \quad y_i = I \\
y_i \equiv (3 \cdot 19 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 13\, mod\, 26 \rightarrow \quad y_i = M \\
y_i \equiv (3 \cdot 3 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 17\, mod\, 26 \rightarrow \quad y_i = Q \\
y_i \equiv (3 \cdot 1 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 11\, mod\, 26 \rightarrow \quad y_i = K \\
y_i \equiv (3 \cdot 18 + 8)\, mod\, 26 &\rightarrow \quad y_i \equiv 10\, mod\, 26 \rightarrow \quad y_i = J
\end{aligned}
$$

A mensagem cifrada é: ASMWHKJJIMQKJ e usando mais uma vez a tabela 2.1 para fazer a conversão, temos o seguinte valor: 1 19 13 23 8 11 10 10 9 13 17 11 10.

Para decodificar a mensagem, devemos encontrar o inverso multiplicativo de 3, pois ele é a constante ao lado de x_i módulo 26, que neste caso, é 9, pois $3 \cdot 9 \equiv 1\, mod\, 26$. Portanto, a função que convém usar para voltar a mensagem à seu formato original é

$$x_i = d(y_i) \equiv 9(y_i - 8)\, mod\, 26$$

que é equivalente a

$$x_i = d(y_i) \equiv (9y_i + 6)\, mod\, 26$$

$$
\begin{aligned}
x_i = d(\ 1\ ) \equiv (9 \cdot\ 1\ + 6)\, mod\, 26 \quad &\equiv 15\, mod\, 26 \rightarrow \quad x_i = O \\
x_i = d(19) \equiv (9 \cdot 19 + 6)\, mod\, 26 \quad &\equiv 21\, mod\, 26 \rightarrow \quad x_i = U \\
x_i = d(13) \equiv (9 \cdot 13 + 6)\, mod\, 26 \quad &\equiv 19\, mod\, 26 \rightarrow \quad x_i = S \\
x_i = d(23) \equiv (9 \cdot 23 + 6)\, mod\, 26 \quad &\equiv 5\, mod\, 26 \rightarrow \quad x_i = E \\
x_i = d(\ 8\ ) \equiv (9 \cdot\ 6\ + 6)\, mod\, 26 \quad &\equiv 0\, mod\, 26 \rightarrow \quad x_i = \# \\
x_i = d(11) \equiv (9 \cdot 11 + 6)\, mod\, 26 \quad &\equiv 1\, mod\, 26 \rightarrow \quad x_i = A \\
x_i = d(10) \equiv (9 \cdot 10 + 6)\, mod\, 26 \quad &\equiv 18\, mod\, 26 \rightarrow \quad x_i = R \\
x_i = d(10) \equiv (9 \cdot 10 + 6)\, mod\, 26 \quad &\equiv 18\, mod\, 26 \rightarrow \quad x_i = R \\
x_i = d(\ 9\ ) \equiv (9 \cdot\ 9\ + 6)\, mod\, 26 \quad &\equiv 9\, mod\, 9 \rightarrow \quad x_i = I \\
x_i = d(13) \equiv (9 \cdot 13 + 6)\, mod\, 26 \quad &\equiv 19\, mod\, 26 \rightarrow \quad x_i = S \\
x_i = d(17) \equiv (9 \cdot 17 + 6)\, mod\, 26 \quad &\equiv 3\, mod\, 26 \rightarrow \quad x_i = C \\
x_i = d(11) \equiv (9 \cdot 11 + 6)\, mod\, 26 \quad &\equiv 1\, mod\, 26 \rightarrow \quad x_i = A \\
x_i = d(10) \equiv (9 \cdot 10 + 6)\, mod\, 26 \quad &\equiv 18\, mod\, 26 \rightarrow \quad x_i = R
\end{aligned}
$$

Terminado o processo, teremos a mensagem original descriptografada com sucesso.

3.1.2 Cifra de Hill

Conforme Godinho et al (2011), a cifra de Hill surge por volta de 1929 inventada por Lester S. Hill. Ela consiste em, inicialmente, tomar uma matriz quadrada invertível $n \times n$ módulo 26 da forma

$$
M = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}
$$

onde cada elemento a_{ij} é um número inteiro em $\mathbb{Z}_{26}$, essa é a matriz chave do processo.

Para a utilização do processo de Hill, precisaremos de alguns resultados importantes.

Proposição 3.1.1. *O conjunto* $[a] = \{x \in \mathbb{Z}; x \equiv a\, mod\, m\} \in \mathbb{Z}_m$ *e invertível se, e somente se,* a *e* m *não têm fatores primos comuns, isto é,* $mdc\,(a, m) = 1$

Prova: Ver [Costa et al], p. 15

Teorema 3.1.1. *Uma matriz* 2×2 *com entradas em* $\mathbb{Z}_m$ *e invertível modulo* m *se, e somente se, o resíduo de* $det\,(A)$ *modulo* m *tem um inverso multiplicativo módulo* m.

Prova: Ver [Costa et al], p. 16

Corolário 3.1.1. *Uma matriz quadrada* A *com entradas em* $\mathbb{Z}_m$ *e invertível módulo* m *se, e somente se,* m *e o resíduo de* $det\,(A)$ *módulo* m *não tem fatores primos comuns.*

Prova: Ver [Costa et al], p. 16

Uma mensagem para ser criptografada usando a técnica de Hill, deve ser primeiramente quebrada em partes contendo n caracteres, sendo n a ordem da matriz dada. Seja X o texto a ser criptografado e

$$x_1 x_2 x_3 \cdots x_n$$

cada letra do bloco partido em n caracteres. Para cada letra do alfabeto, deve-se atribuir um valor numérico pré-estabelecido. Usaremos a tabela 1 para trocar as letras pelos números. Terminado essa etapa, efetua-se o produto matricial

$$\begin{pmatrix} y_{11} \\ y_{12} \\ \vdots \\ y_{n1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{n1} \end{pmatrix}$$

onde as operações são efetuadas módulo 26, para obter-se o bloco criptografado

$$y_1 y_2 y_3 \cdots y_n$$

Para decodificar a mensagem é necessário encontrar a matriz inversa da chave M.

Uma matriz quadrada A com elementos em $\mathbb{Z}_{26}$ é invertível em $\mathbb{Z}_{26}$ se existir outra matriz B com elementos em $\mathbb{Z}_{26}$ tal que $AB = I$, onde I é a matriz identidade de ordem n em $\mathbb{Z}_{26}$.

$$\begin{pmatrix} y_{11} \\ y_{12} \\ \vdots \\ y_{n1} \end{pmatrix} = M \cdot \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{n1} \end{pmatrix}$$

$$M^{-1} \begin{pmatrix} y_{11} \\ y_{12} \\ \vdots \\ y_{n1} \end{pmatrix} = M^{-1}M \cdot \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{n1} \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{n1} \end{pmatrix}$$

assim,

$$\begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{n1} \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} y_{11} \\ y_{12} \\ \vdots \\ y_{n1} \end{pmatrix}$$

sendo que $y_1y_2y_3 \cdots y_n$ corresponde ao texto codificado inicial e $x_1x_2x_3 \cdots x_n$ corresponde ao texto original.

Veremos agora, uma aplicação prática da cifra de Hill. Seja M uma matriz

$$M = \begin{pmatrix} 2 & 3 \\ 5 & 8 \end{pmatrix}$$

da forma 2×2, por isso, irá ser utilizado de 2 em 2, y_1y_2, depois y_3y_4

Suponhamos que se queira criptografar a palavra **FLOR**, fazendo a substituição conforme a tabela 2.1, temos que FLOR= (6 12 15 18). Utilizando M como chave e efetuando as operações módulo 26 tem-se.

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 5 & 8 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 12 \end{pmatrix}$$

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 48 \\ 126 \end{pmatrix} = \begin{pmatrix} 22 \\ 22 \end{pmatrix} = \begin{pmatrix} V \\ V \end{pmatrix}$$

$$\begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 5 & 8 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 18 \end{pmatrix}$$

$$\begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 84 \\ 219 \end{pmatrix} = \begin{pmatrix} 6 \\ 11 \end{pmatrix} = \begin{pmatrix} F \\ K \end{pmatrix}$$

A mensagem criptografa é VVFK

Usa-se a matriz inversa de M para decodificar a mensagem.

$$M^{-1} = \begin{pmatrix} 8 & -3 \\ -5 & 2 \end{pmatrix}$$

Pela tabela 2.1, VVFK= (22 22 6 11), desta maneira, para voltar ao valor original $x_1x_2x_3 \cdots x_n$, deve-se

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 8 & -3 \\ -5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 22 \\ 22 \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 110 \\ -66 \end{pmatrix} = \begin{pmatrix} 6 \\ 12 \end{pmatrix} = \begin{pmatrix} F \\ L \end{pmatrix}$$

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 8 & -3 \\ -5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 15 \\ -8 \end{pmatrix} = \begin{pmatrix} 15 \\ 18 \end{pmatrix} = \begin{pmatrix} O \\ R \end{pmatrix}$$

Ao finalizar o processo retornamos a mensagem inicial FLOR.

3.1.3 Cifra de Cesar

A cifra de César, um dos mais famosos destes métodos, usada na Roma antiga, por Júlio César, de onde vem seu nome, consistia em substituir cada letra do alfabeto pela terceira letra na sequência a ela, como mostra a figura 3.1. Este método, porém, é frágil por usar de simples substituição que é facilmente "quebrável"a partir da análise da frequência das letras. Na língua portuguesa, por exemplo, a letra de maior ocorrência em um código de substituição, possui altas chances de ser a substituta da letra A, já que sua ocorrência em nosso idioma é de 14,63%, sendo maior que a de qualquer outra.

Figura 3.1: Cifra de Cesar

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

Fonte: Recanto do Dragão (https://recantododragao.com.br/ acesso em março 2023)

Usando a cifra de Cesar, vamos codificar a frase: **MESTRADO PROFISSIONAL EM MATEMÁTICA**

Dessa forma, a frase cifrada é: PHVWUDGR SURILVVLRQDO HP PDWHPDWLFD . Percebe-se que é um processo bem simples, apenas de substituição, sem haver a necessidade de nenhum cálculo matemático para isso. Porém, essa simplicidade apresenta também uma fragilidade na frase/palavra criptografada, principalmente, pelo que foi transcorrido anteriormente. Por isso, o uso de chaves, através de mecanismos matemáticos faz-se necessário, em especial, para dificultar a quebra da mensagem original.

Capítulo 4

Histórias Criptografadas: um recurso metodológico para aplicação da criptografia no contexto escolar

Para abordar o tema criptografia dentro de sala de aula, foi usado um modelo diretamente de interesse educacional, pois as criptografias utilizadas por órgão do governo, por exemplo, empregam uma complexidade bem superior a apresentada no contexto escolar. Vale ressaltar, que o interesse maior é dinamizar o ensino de Matemática fazendo com que o aluno aprimore seus conhecimentos, em especial, o de função afim, que foi o objeto usado para esconder as informações. Tendendo alcançar esses resultados, buscou-se elaborar atividades com alunos do 2º ano do Ensino Médio, que consistiram em criar histórias em quadrinhos utilizando a criptografia associada a função afim.

4.1 Motivação

A partir de pesquisas feitas para escrever essa dissertação, deparei-me com o artigo: Potencializando o Estudo de Criptografia Com a Utilização de HQD no Ensino de Matemática, dos autores: Silva, Evangelista e Evangelista (2022), que foi extremamente relevante para desenvolver esse trabalho.

O desenvolvimento do trabalho deu-se em três etapas, sendo elas:

1° etapa: apresentação dos conceitos básicos sobre criptografia e função polinomial do 1° grau;

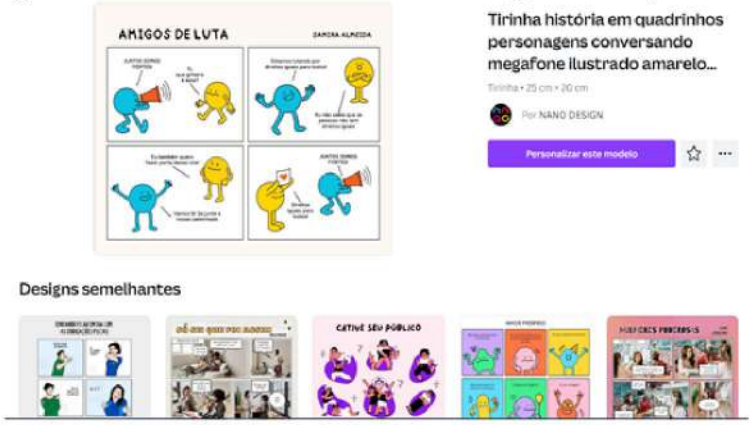
2° etapa: fazer vários exemplos para criptografar e descriptografar mensagens usando sempre a mesma chave e depois mudando a chave para reforçar o entendimento;

3° etapa: elaboração no papel do roteiro da história que seria apresentada.

4.2 Elaboração das histórias em quadrinhos

Para elaborar as histórias foi utilizado o CANVA, uma plataforma online de *designer* e comunicação visual que traz algumas tirinhas pré- definidas prontas para serem editadas de forma gratuita.

Figura 4.1: Interface do CANVA com sugestão de quadrinhos



Fonte: Própria da autora (2023)

Nesta etapa, contou-se com a ajuda do professor de Língua Portuguesa que auxiliou os alunos na questão ortográfica das histórias.

Figura 4.2: Processo de criação das histórias

Fonte: Própria da autora (2023)

Figura 4.3: Auxílio do professor de Língua Portuguesa

Fonte: Própria da autora (2023)

Apesar da criptografia ser um recurso bastante utilizado em nosso cotidiano, ainda é pouco explorado dentre de sala de aula, embora seu uso permita relacionar situações do dia a dia com diversos objetos matemáticos. Reforçando

> A inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, onde o professor, através de atividades práticas, poderá mostrar a aplicabilidade dos conceitos trabalhados em sala de aula, relacionando-os a fatos importantes ocorridos na atualidade (OLIVEIRA e KRIPKA, 2011, p.12)

Dessa forma, a criação de histórias em quadrinhos auxilia o aluno a melhorar a compreensão do assunto apresentado, de modo diferenciado e divertido, além de melhorar também sua escrita e o seu processo de criação, tornado assim o aluno protagonista do seu conhecimento, isto é, mais autônomo e mais produtivo.

A seguir será apresentado uma história em quadrinhos elaborada por um grupo de alunos, a intenção é apresentar uma conversar entre dois paraenses, ressaltando a linguagem regional através das gírias.

Figura 4.4: História elaborada por uma dupla participante

Fonte: Própria da autora (2023)

Para codificar a mensagem foi utilizada a seguinte chave$f(x) : 3x-1$. Descriptografando o balão que contém a mensagem escondida utilizando a função inversa $f^{-1}(y) : \frac{y+1}{3}$, temos

$$
\begin{aligned}
f^{-1}(y) : &\quad \tfrac{y+1}{3} \\
f^{-1}(50) : &\quad \tfrac{50+1}{3} &&= 17 \\
f^{-1}(62) : &\quad \tfrac{62+1}{3} &&= 21 \\
f^{-1}(2) : &\quad \tfrac{2+1}{3} &&= 1 \\
f^{-1}(56) : &\quad \tfrac{56+1}{3} &&= 19 \\
f^{-1}(14) : &\quad \tfrac{14+1}{3} &&= 5 \\
f^{-1}(-1) : &\quad \tfrac{-1+1}{3} &&= 0 \\
f^{-1}(14) : &\quad \tfrac{14+1}{3} &&= 5 \\
f^{-1}(62) : &\quad \tfrac{62+1}{3} &&= 21 \\
f^{-1}(-1) : &\quad \tfrac{-1+1}{3} &&= 0 \\
f^{-1}(35) : &\quad \tfrac{35+1}{3} &&= 12 \\
f^{-1}(14) : &\quad \tfrac{14+1}{3} &&= 5 \\
f^{-1}(65) : &\quad \tfrac{65+1}{3} &&= 22 \\
f^{-1}(44) : &\quad \tfrac{44+1}{3} &&= 15
\end{aligned}
$$

$$
\begin{aligned}
f^{-1}(-1): &\ \tfrac{-1+1}{3} &&= 0\\
f^{-1}(44): &\ \tfrac{44+1}{3} &&= 15\\
f^{-1}(-1): &\ \tfrac{-1+1}{3} &&= 0\\
f^{-1}(17): &\ \tfrac{17+1}{3} &&= 6\\
f^{-1}(2): &\ \tfrac{2+1}{3} &&= 1\\
f^{-1}(53): &\ \tfrac{53+1}{3} &&= 18\\
f^{-1}(14): &\ \tfrac{14+1}{3} &&= 5\\
f^{-1}(35): &\ \tfrac{35+1}{3} &&= 12\\
f^{-1}(44): &\ \tfrac{44+1}{3} &&= 15
\end{aligned}
$$

A mensagem descriptografada é 17 21 1 19 5 0 5 21 0 12 5 22 15 0 15 0 6 1 18 5 12 15, usando novamente a tabela 2.1 do capítulo 2, seção 2.1.1, logo, "o mano tremeu na base porque": "quase eu levo o farelo".

As histórias criadas pelos alunos foram reunidas em um livro chamado: Minhas histórias criptografadas e disponibilizadas entre os participantes para que eles possam se deleitar nessa grandiosa aventura e ao mesmo tempo verificar se seus colegas fizeram a criptografia corretamente.

Figura 4.5: Capa do livro

Fonte: Própria da autora (2023)

Capítulo 5

O jogo - ENIGMÁTICA

A Matemática escolar, de acordo com Grillo (2012, p. 55), é sustentada por uma cultura de aula que a considera como ciência perfeita, infalível e técnica, estruturada em "[...] números, axiomas, fórmulas e técnicas padronizadas, sobretudo, que demonstrem uma certeza no que concerne ao produto final". Essa crença é levada em consideração por muitos docentes, que acreditam não ser possível que a Matemática seja ensinada de outra forma, se não de maneira tradicional, através do quadro e pincel e com inúmeras listas de exercícios.

É perceptível por muitos, que um dos grandes problemas no ensino básico, em relação a Matemática é a falta de ligação dos conteúdos ministrados com a vivência do aluno. Com o intuito de amenizar essa problemática, o educador deve fazer uso de novos recursos metodológicos que possibilitem essa aproximação, sendo uma delas, os jogos.

As inúmeras barreiras enfrentadas dentro da sala de aula, em especial, a dificuldade de prender a atenção do aluno em um mundo tão modernizado, deve levar o professor a repensar o seu papel. Neste sentido, foi que surgiu a ideia da criação de um jogo de tabuleiro que utiliza a criptografia, além de recursos tecnológicos para seu funcionamento. Tendo em vista, que a educação mais eficaz é aquela que instiga o desejo do ser em explorar, observar, trabalhar, jogar e acreditar.

O jogo possibilita ao discente ter audácia de pensar, de se comunicar, de argumentar, e de elaborar estratégias, muitas vezes, únicas, além de desenvolver habilidades matemáticas. O jogo deve ser visto como um agente cognitivo que ajuda o aluno a agir com mais dependência sobre suas ações e decisões, pois em alguns momentos ele será provocado a posicionar-se criticamente frente a uma situação problema, a qual deverá ser

capaz de solucionar.

O principal objetivo de introduzir o uso de jogos no Ensino da Matemática é fazer com que os alunos sintam prazer em aprender essa área da ciência, mudando a forma tradicional de ensino e aguçando o interesse do principal ator do processo, o aluno. Um jogo bem elaborado e aplicado é um poderoso recurso metodológico de ensino. Sobre isso, afirma Lara (2003 p. 57) que:

> A aprendizagem através de jogos, como dominó, palavras cruzadas, memória e outros permite que o aluno faça da aprendizagem um processo interessante e até divertido. Para isso, eles devem ser utilizados ocasionalmente para sanar as lacunas que se produzem na atividade escolar diária. Neste sentido verificamos que há três aspectos que por si só justificam a incorporação do jogo nas aulas. São estes: o caráter lúdico, o desenvolvimento de técnicas intelectuais e a formação de relações sociais.

5.1 Processo de estruturação do ENIGMÁTICA

O jogo teve sua concepção a partir da necessidade de confeccionar um recurso que materializasse alguns objetos matemáticos que são fundamentais, mas que demandam muitas dificuldades pelos alunos, em especial, os da 3° série do Ensino Médio. O principal propósito do jogo é de contribuir com um aprendizado significativo para os educandos que tiverem contato com ele e disponibilizar mais um recurso para os docentes utilizarem nas diversas subáreas da matemática.

O jogo enigmática é um resultado que foi alcançado pela professora Dayziane[1] na estruturação que se encontra hoje, mas que outrora foi pensado e apresentado pelos alunos que se encontravam na época no 1º ano do ensino médio como produto para apresentação de um seminário integrado que tinha como orientadora a referida professora.

A priori foi confeccionado um tabuleiro e as cartas pelos próprios alunos. Em seguida, a professora solicitou aos educandos uma pesquisa para a escolha das questões de matemática que seriam utilizadas no jogo de acordo com cada nível e as armazenou em um banco de dados online, que funciona de maneira randômica liberado para uso quando os alunos estão utilizando o jogo. Para o armazenamento dessas questões foi utilizado o programa QuizGlobal, que funciona de forma online e gratuita.

Foram criados três bancos de dados com diferentes níveis de dificuldades e divididos

[1]Professora da turma pesquisada e também autora da dissertação.

por cores no tabuleiro: nível fácil (cor verde), nível médio (cor amarelo) e nível difícil (cor vermelho). As questões são de múltipla escolha, com apenas duas opções de resposta. Caso ele erre, será mostrado a alternativa correta, com o objetivo de fazer o aluno fixar o conteúdo.

5.1.1 Jogos de tabuleiro

Os jogos de tabuleiro instigam e ampliam habilidades efetivas para quem os joga, como comunicação verbal, o raciocínio lógico, a atenção, a concentração e a interação social. Eles auxiliam também na elevação do nível de paciência e do respeito, características necessárias para o desenrolar da atividade, além de serem associados a diversão e entretenimento. Um exemplo de jogos de tabuleiro bastante usado e conhecido é o xadrez que segundo alguns historiadores, foi criado na Índia há cerca de 1.400 anos (SÉRGIO, 2004).

Os tabuleiros podem ser de madeira, plástico, papel, tecido ou marcações no chão. Esse tipo de jogo pode requerer apenas sorte ou conhecimento, estratégia ou memória. No caso, do jogo tratado nesta dissertação, além dos conhecimentos matemáticos, os outros fatores citados também implicam fortemente para chegar ao fim do tabuleiro.

5.1.2 Escolha do Conteúdo

Dados do IDEB mostram que o Estado do Pará tem o segundo pior ensino médio do Brasil. No que diz respeito ao aprendizado em matemática, o Pará ficou na quarta pior colocação, com nota 3,98, à frente apenas dos estados do Amazonas (3,97), Bahia (3,96) e Maranhão (3,92). Levando em consideração esse cenário, surge a necessidade de pensar recursos metodológicos que despertassem o interesse dos alunos, afim de motivá-los no processo de aprendizagem e, consequentemente melhorar esses indicadores. .

Os objetos matemáticos escolhidos para fazerem parte do jogo são aqueles que dão base para o desenvolvimento da criptografia, tema central da dissertação, mas, que também apresentam enorme complexidade de compreensão por parte dos alunos. Em especial, as funções e matrizes, pois apresentam a álgebra como fundamento principal. Esses conteúdos além de serem básicos, são bastante cobrados na prova do SAEB.

Outro conteúdo contemplado no jogo foram os critérios de divisibilidade, este é ensinado no ensino fundamental, e logo é esquecido por grande parte dos alunos. Para a aplicação do jogo, foi feito uma revisão sobre esse tópico, exatamente porque muitos

alunos não lembravam se um dia haviam estudado. De posse desse conhecimento é possível solucionar de maneira mais rápida muitos problemas de divisão.

Ao estudar a disciplina Aritmética no curso PROFMAT, o aluno tem o privilégio de ser apresentado ao tópico de Criptografia. Tal encontro, fez com que o interesse em pesquisar e aprofundar ainda mais sobre o tema fosse destertado, até descobrir que ele poderia auxiliar na mudança do cenário caótico que se encontra o Estado do Pará nas provas de larga escala, em especial, na área matemática.

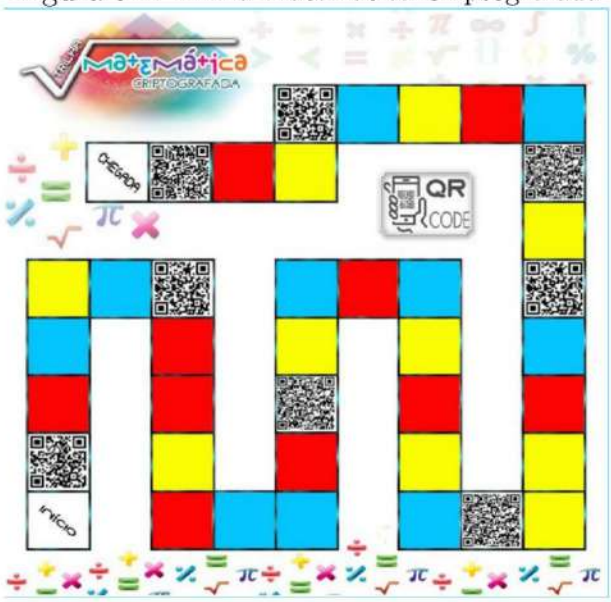
5.1.3 ENIGMÁTICA

Para elaborar o jogo ENIGMÁTICA, foi usado como referência o jogo Trilha Matemática Criptografada, das professoras Solange Mariano da Silva Santos e Zenaide de Fátima Dante Correia Rocha. O jogo apresentado pelas professoras utiliza 120 cartas de perguntas e respostas, um tabuleiro e um celular com leitor de Qrcode, sem necessidade de estar conectado à Internet. Porém, ao se jogar várias vezes a Trilha Matemática é possível "decorar" as perguntas das cartas, pois estas serão sempre as mesmas. Com o objetivo de diminuir o número de cartas e também as repetições frequentes de perguntas, foi que o Enigmática surgiu. Ele possui somente três cartas, isto porque está conectado a um banco de dados online e randômico.

O tabuleiro usado no ENIGMÁTICA é bem parecido com o criado pelas professoras, mudando apenas algumas cores e também algumas regras que nele estão criptografadas.

Depois do jogo pronto veio o momento de escolher seu nome, e esse é claro, deveria fazer jus ao que estava sendo proposto na temática. Pensando nisso, o nome contemplado para o jogo foi ENIGMÁTICA, uma mistura de enigma (por conta da criptografia) e matemática (disciplina base para a aprimorar essa técnica).

Figura 5.1: Trilha Matemática Criptografada



Fonte: Universidade Tecnológica Federal do Paraná (https://repositorio.utfpr.edu.br/jspui/bitstream/1/4562/2/LD_PPGMAT_M_Santos%2C_Solange_Mariano_da_Silva_2019_1.pdf, acesso em novembro 2022)

5.2 O protótipo do jogo

O primeiro protótipo foi baseado na Trilha Matemática Criptografada e chamava-se Saberes Criptografados. Porém, as cores e as regras criptografadas no tabuleiro foram desenvolvidas pelos alunos, distinguindo algumas da versão original. Vale ressaltar, que para a apresentação do primeiro protótipo as perguntas foram pesquisadas e sugeridas também por eles.

Figura 5.2: Apresentação do protótipo

Fonte: Própria da autora (2023)

5.3 Validação

O jogo foi elaborado para ser apresentado em um seminário integrado de uma escola estadual. O teste foi feito com os alunos do 1° ano que elaboraram o jogo, e depois disponibilizado para a turma do 2° ano da referida escola. A ideia de criar o banco de dados, surgiu quando o jogo foi apresentado, pois um dos avaliadores questionou o fato de ao se jogar várias vezes, o jogador teria a possibilidade de decorar as cartas de perguntas e respostas, uma vez que eram enumeradas, embora fossem criptografadas. Começava então, uma nova articulação no intuito de solucionar esse obstáculo. Depois de uma vasta pesquisa, o problema foi solucionado e os testes foram retomados, agora com os alunos do 3° ano, para verificar a funcionalidade, onde foi constatado que a solução adotada foi válida.

5.4 As regras do Jogo

5.4.1 Composição

O jogo é composto por 1 carta verde criptografada, 1 carta amarela criptografada, 1 carta vermelha criptografada, 2 carrinhos com cores diferentes, 1 dado e 1 tabuleiro, além disso utiliza-se o programa Quizglobal para armazenar as questões no banco de dados e o QR Code Generator para gerar os QR codes tanto das cartas quanto do tabuleiro. As cores das cartas e do tabuleiro foram baseadas no semáforo.

5.4.2 Preparação

Em uma superfície, posicione o tabuleiro. Os jogadores deverão formar 02 duplas, escolherem o carrinho de sua preferência e posicioná-los na casa INÍCIO. Baixar o aplicativo QR CODE em seus aparelhos celulares, além de estarem conectados à Internet.

5.4.3 As regras do Jogo

As cartas nas cores verde, amarela e vermelha, são colocadas ao lado do tabuleiro e denotam questões de nível: fácil, médio e difícil, respectivamente. Escolhe-se um dos integrantes da dupla para jogar o dado, a dupla que tirar o número maior inicia o jogo, lançando novamente o dado, o número tirado no dado será a quantidade de casas que

irão andar. Se o carrinho parar em uma casa do tabuleiro que possui uma mensagem criptografada, a dupla deverá fazer a leitura da mensagem utilizando o aplicativo QR CODE baixado no celular e seguir as instruções; se parar em uma casa colorida (verde, amarelo ou vermelha), a dupla adversária deve pegar a carta de acordo com a cor da casa, e então com o aplicativo QR CODE irão fazer a leitura da mensagem criptografada, onde constará o problema matemático que deverá ser respondido pela dupla que está na vez, vale ressaltar que o banco de questão é randômico (aleatório). Se acertarem, devem avançar uma casa, se errarem, devem voltar uma casa. Para as próximas jogadas, a outra dupla deve realizar os mesmos procedimentos. Ganha o jogo a dupla que percorrer as 40 casas e atingir a casa de CHEGADA em primeiro lugar.

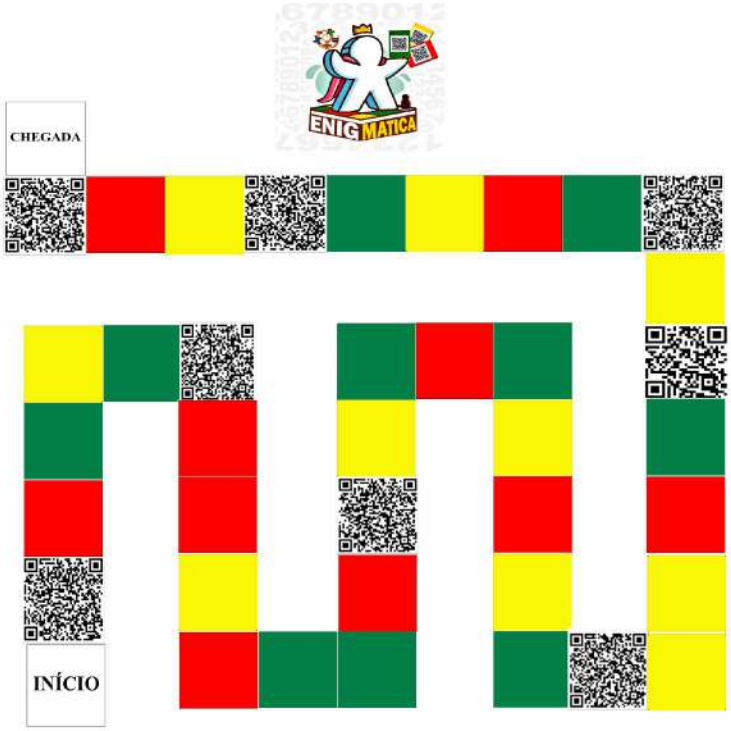
5.5 O Designer do Jogo

Os jogos de tabuleiro são uma forma lúdica de ensinar e aprender, além disso, por meio dele, o discente amplia tanto o intelecto como a parte afetiva, pois exige a interação entre os jogadores requerendo fundamentalmente a capacidade de parar, concentrar, elaborar pensamentos e, sobretudo saber respeitar o tempo do outro e as regras pré-estabelecidas. Podendo ser definido como aqueles competidos, por uma ou mais pessoas, em uma superfície plana, que pode ser de madeira, metal, papelão, entre outros, com marcações e movimentações que obedecem as regras predefinidas.

Esse tipo de jogo oferece uma gama de benefícios, pois intensifica o entendimento das regras de convívio, além de estimular e desenvolver importantes capacidades como a criação de estratégias para vencer o jogo. Promove entre os alunos o respeito, a paciência, as diferenças existentes entre eles e da sociedade a qual vivemos. Tais benefícios foram um grande estímulo na hora de montar o ENIGMÁTICA.

Para montar o tabuleiro do jogo para distribuição entre os alunos foi utilizado o programa paint.net.

Figura 5.3: Tabuleiro do jogo



Fonte: Própria da autora (2023)

5.5.1 A Logo do Jogo

A logo do jogo foi desenvolvida no programa chamado paint.net, que é um editor de imagens. Ela foi pensada para representar de maneira fidedigna o jogo, trazendo elementos como: um boneco que possui uma coroa que representa o campeão do jogo, em uma das mãos o boneco traz as três cartas do jogo e na outra uma bola com os símbolos das operações matemáticas, além de estar localizado em cima de um tabuleiro no formato de um paralelepípedo que contém as cores do tabuleiro original.

Figura 5.4: Logo do Jogo

Fonte: Própria da autora (2023)

5.5.2 As cartas do jogo

As cartas do jogo possuem as cores que se encontram no tabuleiro, além de trazerem um apelo visual em seu verso, o QR CODE, que tem como função principal linkar o jogador com o banco de dados referente ao nível da questão. Para a confecção do modelo base foram utilizados papel cartão dupla face.

Figura 5.5: Cartas do Jogo

Fonte: Própria da autora (2023)

O jogo foi pensado para unir teoria e prática, bem como, tornar o processo de ensino e aprendizagem mais dinamizado e prazeroso aos discentes, que são indivíduos imersos na tecnologia, uma vez que fazem parte dos nativos digitais. Assim sendo, procurou- se desenvolver uma das competências indicadas por Brasil (2019) que é:

> Produzir, avaliar e utilizar tecnologias digitais de informação e comunicação de modo crítico, ético e responsável, compreendendo seus significados para os diferentes grupos ou estratos sociais (BRASIL, 2019, p. 404).

Deste modo, tendo como referência a competência acima citada e tendo como desenvolver um ensino voltado para o uso das novas tecnologias, foi que surgiu o ENIGMÁTICA, com uma proposta inovadora utilizando-se dos recursos tecnológicos disponíveis.

Capítulo 6

Metodologia da aplicação em sala de aula

O presente capítulo descreve como se deu a aplicação do ENIGMÁTICA em uma turma do terceiro ano de uma escola estadual de tempo integral, localizada no município de Capanema-Pa, cujo os objetos matemáticos contemplados foram: critérios de divisibilidade, função polinomial do 1° grau e matrizes.

6.1 O planejamento

Por se tratar de conteúdos ministrados em anos anteriores, em especial, o objeto de conhecimento relacionado aos critérios de divisibilidade que é um tópico abordado no 6° ano do ensino fundamental e que raramente é explorado nos anos subsequentes, antes da aplicação do jogo foi necessária uma revisão, para isso foram utilizadas 4 horas-aulas. Era esperado que algumas dificuldades relacionadas aos tópicos matemáticos fossem encontradas, tais como: dificuldade em montar um esquema para resolver as questões, não lembrar algumas fórmulas, entre outros. E, inicialmente, seria necessário descobrir uma forma de identificá-las para organizar a aplicação do jogo, definindo objetivos que pudessem minimizar essas questões.

Para tal, optou-se por aplicar um questionário que ajudasse mapear a problemática enfrentada pelos alunos a respeito dos tópicos propostos no jogo (ver anexo). Ele foi aplicado antes das revisões acontecerem, visto que a finalidade do momento era ter uma visão generalizada da situação quanto às lacunas em relação ao conteúdo e também suas

expectativas sobre a metodologia a ser aplicada.

Ao término das revisões, ocorreu uma apresentação mais aprofundada do material didático que seria utilizado junto à turma, mostrando as regras e objetivos da aplicação, oportunizando o contato e familiarização com a proposta. Em seguida, a turma foi dividida em equipes de quatro integrantes, podendo assim ter a primeira experiência com o jogo.

6.2 Questionário

A utilização de questionários nesta pesquisa torna-se indispensável para coletar os dados, eles foram aplicados em dois momentos distintos, início e fim da utilização do jogo (ver modelos nos anexos). O maior objetivo, de tais questionamentos é quantificar a origem acerca das deficiências apresentadas pelos participantes no processo de ensino e aprendizagem no que tange aos objetos matemáticos destacados na pesquisa.

Em contrapartida, existem também indagações a respeito da compreensão do indivíduo sobre si. Sendo de extrema importância, uma vez que este trabalho busca o altruísmo dos atores envolvidos (pesquisador e entrevistados) e, a partir da ciência das dificuldades existentes, é que intervenções mais eficientes serão concebidas.

É notório que a dificuldade de compreensão dos objetos matemáticos vão além dos tópicos abordados na pesquisa, uma vez que o processo de ensino e aprendizagem acrescenta uma complicação que envolve o ensinar e aprender, passando pelas particularidades dos contextos educacionais aos quais se apresentam as ações pedagógicas.

Com as informações das variáveis qualitativas e quantitativas do questionário aplicado, obteve-se uma visão mais ampla sobre o cenário de atuação da pesquisa, podendo assim, realizar a análise dos dados com consistência com o intuito de obter resultados eficazes para o estudo. A aplicação do questionário deu-se de maneira cortês e sem muitas complicações, uma vez que a pesquisadora também é professora da turma. O questionário apresentava uma quantidade razoável de perguntas, o que tornou o processo de aplicação ainda mais fácil, pois não era algo monótono aos alunos, além do que, a pesquisadora-professora já havia explicado detalhadamente o objetivo da pesquisa e os benefícios que ela traria para ambas as partes.

6.2.1 Primeiro questionário

Foi realizada a pesquisa de campo para obter o resultado do estudo, com intuito de verificar as dificuldades e ao mesmo tempo as expectativas dos alunos com relação aos tópicos que seriam apresentados. Foram aplicados 28 (vinte e oito) questionários aos alunos que estão cursando o terceiro ano do ensino médio em tempo integral, tendo um retorno de 100% das respostas, o resultado da análise dos questionários aplicado em entrevistas, serão demonstrados nos tópicos a seguir.

Nessa seção serão analisados os dados do perfil cognitivo dos sujeitos da pesquisa de campo, onde foram procedidos com perguntas abertas, dando assim, mais liberdade para o entrevistado expor suas opiniões.

A primeira pergunta já instiga essa temática, pois é necessário saber quais as perspectivas dos alunos sobre o que será apresentado a ele.

Figura 6.1: Expectativa dos alunos em relação ao jogo e aos tópicos abordados

Fonte: Dados da pesquisa (2023)

O gráfico da figura 6.1 nos mostra que 78% dos pesquisados esperam que a metodologia apresentada facilite seu aprendizado, enquanto que 18% não conseguem esboçar nenhuma expectativas alguns, por nunca terem visto os assuntos e outros por pura frustração com a disciplina matemática.

Foi questionado aos alunos quais dos objetos do conhecimento que fazem parte da pesquisa (Funções, Matrizes e Critérios de divisibilidade) eles têm mais dificuldade em compreender. O resultado está sendo mostrado no gráfico 6.2.

Figura 6.2: Dificuldade na compreensão da teoria dos conteúdos que integram a pesquisa.

Fonte: Dados da pesquisa (2023)

Pelo gráfico da figura 6.2, tem-se que, 21% dos educandos responderam não compreender nenhum dos objetos da pesquisa. Alguns relatos retirados dos questionários, nos mostram que a maioria não lembra do que se trata determinado assunto, logo respondem não saber. Por outro lado, 14% dos entrevistados não dominam funções e 21% não compreendem ao mesmo tempo funções e os critérios de divisibilidade. Já 11% disseram não ter nenhuma dificuldade na compreensão dos objetos propostos e 29% responderam que não conseguem manusear as fórmulas (equações) existentes nestes tópicos e, por isso, não alcançam sucesso na resolução dos problemas.

Com relação ao uso de equações para resolver problemas matemáticos, Crease (2011, p.236) ressalta:

> Nós também aprendemos que as equações não são simples ferramentas científicas, mas possuem "vidas sociais", por assim dizer. Estamos inclinados a vê-las como instrumentos mudos e inertes, capazes de afetar o mundo somente quando empunhadas por cientistas e engenheiros. Mas elas são ativas e podem exercer uma força educacional e cultural, nos instruindo sobre o mundo e ocasionalmente reformulando a percepção humana a respeito dele.

Quando questionados sobre qual dos três assuntos eles se sentiam mais seguros em afirmar que aprenderam, temos o resultado apresentado no gráfico (figura 6.3).

Figura 6.3: Qual dos assuntos você pode afirmar que aprendeu?

Fonte: Dados da pesquisa (2023)

Para 46% dos entrevistados o assunto que eles mais se sentem seguros em dizer que aprenderam é sobre matrizes, mas isso pode ser justificado pelo fato de ter sido um assunto ministrado ano passado e ainda estar presente em suas memórias. Já para um número considerável de 43% dos pesquisados dizem não dominar nenhum desses assuntos. Outros 7% afirmam saber sobre funções, enquanto apenas 4% afirmam ter aprendido sobre critérios de divisibilidade.

O relato do aluno 1, evidencia a dificuldade em critérios: "nunca fui bom na divisão, principalmente pelo fato de não saber multiplicação e pela falta de concentração e foco".

Ao finalizar a análise dos resultados do primeiro questionário com base na investigação de campo, foi possível refletir sobre o conhecimento dos alunos e, propor reflexões sobre uma possibilidade de metodologia para que seus conhecimentos possam ser ampliados, aprimorados, assegurados e sejam significativos.

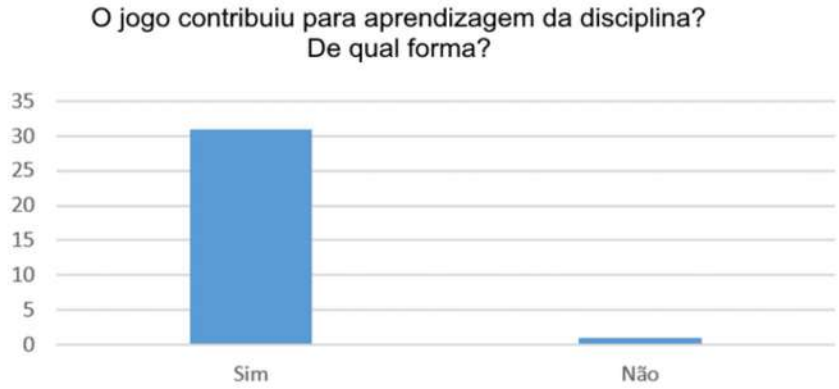
6.2.2 Segundo questionário

Este por sua vez, está mais centrado no jogo, isto é, na forma como essa metodologia pode contribuir no aprendizado dos alunos e na evolução deles em relação aos conteúdos propostos. O número de alunos que responderam este questionário foi maior que o primeiro, 32 alunos. Isto é, tivemos quatro alunos que não responderam o primeiro questionário, mas não poderiam ser privados de forma alguma de experimentarem o jogo.

A figura 6.4 nos mostra que dos 32 participantes da pesquisa, 31 responderam

que o ENIGMÁTICA contribuiu com sua aprendizagem, em especial, por estimular a competitividade saudável, na forma de diversão.

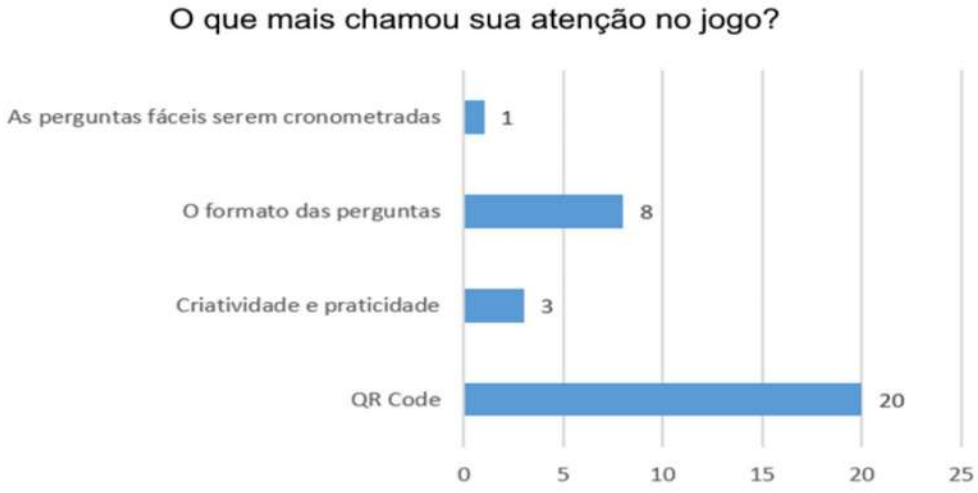
Figura 6.4: Contribuição do jogo para aprendizagem



Fonte: Dados da pesquisa (2023)

Sobre a questão da competição no Ensino Médio, Vivaldi (2014), esclarece que, competir, vencer e perder são experiências indispensáveis ao desenvolvimento humano. Vencer pelo trabalho e dedicação, faz com que a pessoa se sinta mais confiante, e não como o melhor, o que, por conseguinte, é uma poderosa arma para exercer a humildade. Por outro lado, perder é uma ótima chance para aprender a passar com dignidade pelas frustrações de não conseguir obter o resultado almejado, procurando reavaliar os métodos usados. É preciso, portanto, percebe que há lugar para uma experiência ética positiva, tanto em circunstâncias de competição quanto nas de cooperação.

Figura 6.5: Qual é a maior atratividade do jogo?

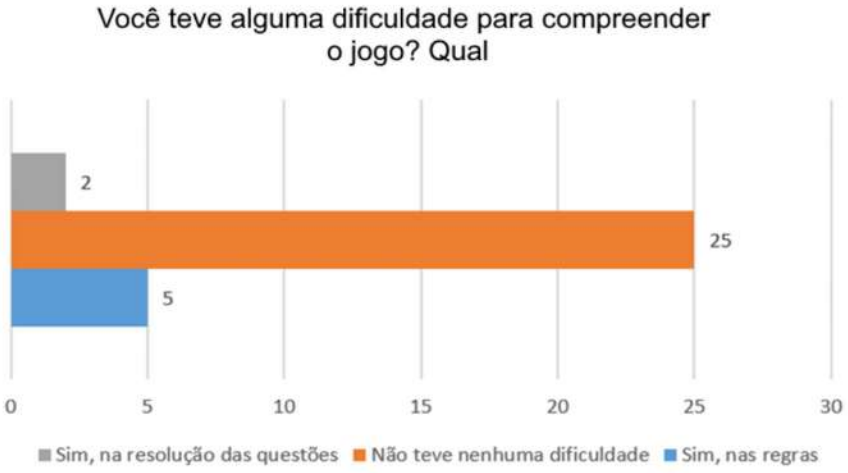


Fonte: Dados da pesquisa (2023)

Pelo gráfico (figura 6.5), temos o fator que mais chamou a atenção dos alunos em relação ao jogo foi o uso do QR Code, onde 20 alunos responderam esse quesito. Já para oito alunos o que mais despertou a atenção foi o formato das perguntas, enquanto três responderam ser a criatividade e praticidade do jogo. Já um aluno disse ter sido o fato de as perguntas de caráter fácil terem um tempo a serem respondidas.

Segundo Moran, (2007, p.21), "A educação tem de surpreender, cativar, conquistar os estudantes a todo momento, A educação precisa encantar, entusiasmar, seduzir, apontar possibilidades e realizar novos conhecimentos e práticas."

Figura 6.6: Dificuldade em compreender o jogo



Fonte: Dados da pesquisa (2023)

O gráfico (figura 6.6), vem mostrando que uma maioria considerável de alunos, isto é, 25 educandos, não tiverem nenhuma dificuldade em compreender a forma de como o jogo funcionava. Outros cinco alunos tiveram dificuldades em compreender as regras, mesmo tendo o manual em mãos e para outros dois alunos a maior dificuldade se concentrou na resolução das questões, onde algumas eram bem longas, em especial, as de caráter difícil. É importante destacar que quanto mais complexo é o jogo, maior a tensão entre os que dele participam. Segundo Grando (2000) este fator dentro do jogo é essencial no processo de aprendizagem pois favorece a construção e a verificação de hipóteses.

O gráfico (figura 6.7), mostra que o objeto de conhecimento que foi mais compreendido pelos pesquisados ao jogarem o ENIGMÁTICA foram os critérios de divisibilidade, uma vez que 13 alunos responderam que absorveram melhor esse conteúdo após o jogo. Já nove alunos responderam não terem compreendido nenhum objeto. Dentre os que deram essa resposta, a maior alegação para esse fato, deu-se pelo pouco tempo de uso do

jogo. Uma pessoa respondeu ter compreendido todos, quatro compreenderam matrizes e critérios ao mesmo tempo, três pessoas compreenderam matrizes e duas pessoas disseram terem compreendido outras coisas, como, por exemplo, a interpretação das questões.

Figura 6.7: O conteúdo mais compreendido ao se jogar o Enigmática

Fonte: Dados da pesquisa (2023)

6.3 O contato com o jogo

Depois da revisão e aplicação do primeiro questionário, era chegada a hora do contato direto com o jogo. Para isso, houve uma explanação acerca das regras que seriam utilizadas e, em seguida, cada equipe recebeu o kit para aplicação do jogo, contendo um tabuleiro de papel, dois carrinhos de cores diferentes, um dado e as três cartas de cores distintas criptografadas, além disso, cada equipe deveria ter um celular conectado à internet.

Figura 6.8: Entrega dos kits

Fonte: Própria da autora (2023)

Após os devidos esclarecimentos e dúvidas retiradas, os alunos foram divididos em equipes de quatro integrantes, totalizando seis equipes bastante heterogêneas. Para facilitar a interação dos alunos e um melhor rendimento, eles foram colocados em duas salas, uma do lado da outra, sendo uma supervisionada pela autora da pesquisa e a outra pelo professor de filosofia, que teve participação apenas na observação das turmas para manter a ordem. Vale ressaltar que, a pesquisadora visitava a outra sala para verificar se estava transcorrendo tudo dentro do previsto.

Figura 6.9: Utilização do jogo

Fonte: Própria da autora (2023)

As jogadas foram supervisionadas atentamente pelos colaboradores da pesquisa. Dos vários pontos positivos observados durante a aplicação, vale destacar alguns: a concentração dos alunos, o companheirismo com o parceiro (uma vez que, a dinâmica se deu em dupla), e seriedade com que eles encararam o jogo. Por outro lado, existiram também os pontos negativos, em especial, com as questões de caráter difícil, pois os alunos se sentiam acanhados em tentar começar a resolver. Porém com incentivo eles foram se envolvendo com o jogo e encarando todas as etapas.

Como o jogo está também associado ao fator sorte, fica bem difícil criar uma estratégia para vencê-lo, pois é possível que a dupla vencedora chegue ao fim do tabuleiro sem ter respondido nenhuma pergunta difícil.

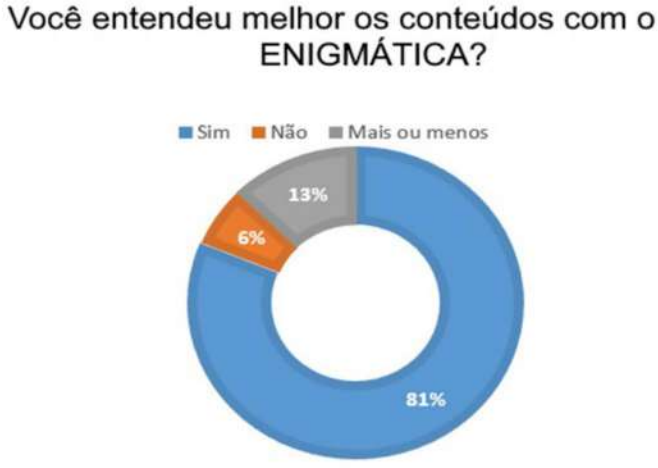
Com o fim das jogadas, houve uma socialização para que os alunos expusessem suas opiniões sobre o jogo. Dos quais destacaram: uma melhor "memorização" dos conteúdos e fórmulas, facilidade em compreender a leitura e interpretação de algumas questões. Além disso, a motivação em aprender os conteúdos de um modo inovador e divertido.

6.4 Aprimorando os objetos de conhecimento matemático

É visível que os alunos ficaram bem focados em solucionar os problemas que lhes foram propostos pelo jogo, sem enrolação ou preguiça, fazendo com que seus conhecimentos ficassem mais aflorados. A introdução desta metodologia foi satisfatória que ela está sendo usada ao término dos conteúdos ministrados pela professora para fazer revisões, abrangendo outros objetos matemáticos. O resultado veio não somente refletido nas notas, mas também no anseio do aluno em aprender, muitas vezes motivado pela vontade de vencer as partidas. O ENIGMÁTICA será utilizado no segundo semestre na escola por professores de outras áreas, comprovando ainda mais seu sucesso.

O gráfico (figura 6.10), vem revelar o que foi relatado acima, pois nos mostra que 81% dos alunos responderam ter entendido melhor os conteúdos após ter usado o ENIGMÁTICA, enquanto 6% disseram não ter entendido e 13% dizem ter entendido mais ou menos.

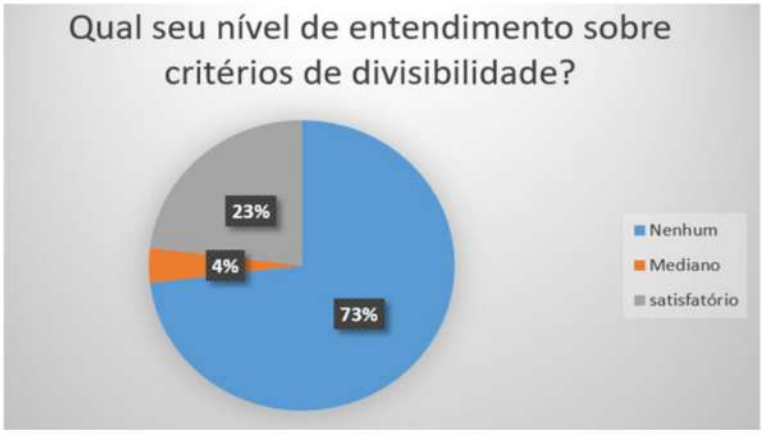
Figura 6.10: Eficácia do ENIGMÁTICA



Fonte: Dados da pesquisa (2023)

Quando solicitado pela autora da pesquisa que os alunos comentassem no questionário sobre a eficácia do jogo, houve uma unanimidade em dizer que a utilização dele nas aulas potencializou o conhecimento dos participantes, pois segundo eles: ajuda a relembrar os conteúdos já vistos, estimula a aprendizagem de maneira dinâmica e descontraída, além de envolver uma disputa de maneira saudável.

Figura 6.11: Como é seu entendimento sobre critérios de divisibilidade?



Fonte: Dados da pesquisa (2023)

O gráfico 6.11, referente a uma pergunta feita no primeiro questionário, evidencia que 73% dos entrevistados não tinham nenhum entendimento sobre critérios de divisibilidade, enquanto 23% tinham um entendimento satisfatório e 4% era mediano.

Figura 6.12: O conteúdo mais compreendido ao se jogar o Enigmática

Fonte: Dados da pesquisa (2023)

O gráfico 6.12, mostra que o objeto de conhecimento mais compreendido pelos pesquisados depois do uso do ENIGMÁTICA foi os critérios de divisibilidade, uma vez que 41% dos alunos responderam que absorveram melhor esse conteúdo após usarem o jogo. Além de 13% que responderam ter compreendido Matrizes e critérios, somando assim um percentual de 54% de alunos que entenderam melhor os critérios de divisibilidade. Comparando os gráficos (7 e 8) percebe-se que as revisões e posteriormente a inserção do jogo auxiliou a melhorar o aprendizado dos alunos neste objeto do conhecimento matemático que era o mais o deficitário entre os pesquisados.

Nesse sentido, o jogo mostrou-se como um instrumento pedagógico eficiente, pro-

porcionando resultados satisfatórios no processo de ensino e aprendizagem em Matemática.

> Os jogos e brincadeiras são elementos muito valiosos no processo de apropriação do conhecimento. Permitem o desenvolvimento de competências no âmbito da comunicação, das relações interpessoais, da liderança e do trabalho em equipe, utilizando a relação entre cooperação e competição em um contexto formativo. O jogo oferece o estímulo e o ambiente propícios que favorecem o desenvolvimento espontâneo e criativo dos alunos e permite ao professor ampliar seu conhecimento de técnicas ativas de ensino, desenvolver capacidades pessoais e profissionais para estimular nos alunos a capacidade de comunicação e expressão, mostrando-lhes uma nova maneira, lúdica, prazerosa e participativa de relacionar-se com o conteúdo escolar, levando a uma maior apropriação dos conhecimentos envolvidos (BRASIL, 2006, p. 28).

6.5 Análise e discussão de dados

A aplicação dos questionários aliado a observação da utilização do ENIGMÁTICA possibilitou o alcance de resultados aceitáveis para a pesquisa, pois permitiu uma análise do processo antes, durante e depois do contato com proposta metodológica introduzida. No primeiro momento, procurou-se conhecer os déficits de aprendizagem dos conteúdos por parte dos alunos, para então fazer um planejamento que contribuísse para potencializar esse conhecimento.

As indagações mostraram que um número considerável de alunos não tinha o menor conhecimento sobre critérios de divisibilidade, conteúdo extremamente básico e importante para solucionar diversos problemas de divisão. Outro ponto de bastante carência, foi o conhecimento sobre função. Embora, esse último possa ser justificado pelo fato de ter sido trabalhado no período de pandemia, onde a maioria das atividades eram de forma remota e alcançava um número mínimo de alunos, pois não existia uma obrigatoriedade de se realizar as tarefas propostas.

Além desses, houve identificação de outras dificuldades como: problemas em memorizar as fórmulas, falta de conhecimento da matemática básica (as quatro operações) e complicações com a álgebra. Estes fatores contribuem significativamente para o insucesso dos alunos em relação ao campo do conhecimento da matemática.

Depois de minimizados esses fatores, é importante salientar que as expectativas com relação ao ENIGMÁTICA foram extremamente positiva. O fascínio pelo jogo deu-se pela possibilidade de diversão e ao mesmo tempo aprendizado. Além do que, o uso da

tecnologia através do QR Code aguçou ainda mais a curiosidade e interesse dos alunos em utilizar esse recurso.

Outro ponto que deve ser destacado, foi a interação entre as duplas, que produziam os cálculos juntos sem medo de errarem e sem julgamentos se isso acontecesse, pois era algo que estava sendo construído de comum acordo. Isso contribuiu muito para termos um aprendizado compartilhado.

Com tudo, ficou evidente que o planejamento feito a partir do relatos vivenciados pelos entrevistados sobre suas necessidades foi um dos principais ingredientes para obtenção do sucesso do jogo, pois ele foi elaborado visando preencher as lacunas existentes.

Capítulo 7

Considerações Finais

O ensino da matemática a partir da criptografia é vantajoso por apresentar esta área de conhecimento associada a um tópico que ao mesmo tempo é comum ao cotidiano e desperta o interesse e a curiosidade. Porém, algumas ponderações precisam ser destacadas para obtenção do sucesso no desenvolvimento dessa metodologia, como a de que é de suma importância que o professor avalie o conhecimento prévio da turma para que as atividades sejam condizentes a esses conhecimentos e haja uma transposição didática adequada.

Tais atividades devem ser criadas de modo a motivar a construção do conhecimento para que não se torne apenas mais um tópico abordado de maneira tradicional. A utilização da criptografia se mostrou satisfatória como recurso metodológico, como foi o caso da atividade desenvolvida sobre as histórias criptografadas, onde houve uma melhor compreensão do alunos sobre funções, além de algumas duplas participantes, terem escrito suas histórias enaltecendo uso da linguagem regional, perpassando as barreiras para além da matemática, havendo a interação com as outras áreas do conhecimento.

Os discentes codificaram e decodificaram as mensagens em quadrinhos, fizeram uma análise dos resultados adquiridos e assim puderam tirar suas próprias conclusões. Tal atividade promoveu a curiosidade dos alunos, proporcionando o desenvolvimento de suas próprias ideias e pensamentos, ajudando também na evolução de seus conhecimentos matemáticos.

Outro ponto que deve ser destacado foi o uso dos jogos como método de ensino da Matemática, pois ele é uma opção vantajosa para fugir do tradicionalismo. Isso porque, prende a atenção dos alunos, ajudando-os a absorver de maneira mais satisfatória os conteúdos.

No entanto, deve-se também destacar que a preparação do docente é primordial, pois a criptografia não é um assunto que faz parte da grade curricular do ensino básico e precisa ser trabalhada de forma a ser entendida sem complicações e com suas aplicações e usos em foco.

Nesta perspectiva, apresentamos uma proposta didática, através do uso da criptografia, oportunizando a prática dos discentes, potencializando o aprendizado sobre funções, matrizes e critérios de divisibilidade para além da teoria e colocando o aluno em foco, o tirando de sua posição de coadjuvante do processo educacional e aumentando, assim, suas ferramentas para sua existência no mundo real.

Diante de tudo que foi referenciado no trabalho, acreditamos que ele atingiu seu objetivo primordial de apresentar a criptografia como um recurso didático para estimular a aprendizagem de alguns objetos do conhecimento matemático. Indiscutivelmente, a proposta proporcionou aos participantes uma forma de aprender matemática de um jeito que foge ao tradicional.

Por fim, como trabalhos futuros, pensamos na possibilidade de que banco de questões do jogo ENIGMÁTICA seja alimentado com questões das diversas áreas do conhecimento, buscando envolver todos os professores do ambiente da pesquisa, favorecendo assim, o processo de ensino e aprendizagem como um todo.

Referências

BICUDO, Maria Aparecida Viggiani e BORBA, Marcelo de Carvalho (Orgs.). **Educação Matemática: pesquisa em movimento**. São Paulo: Cortez, 2004.

BRASIL, Ministério da Educação. Secretaria da Educação Básica. **Base Nacional Comum Curricular**. Brasília, DF, 2019. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC˙EI˙EF˙110518˙versaofinal˙site.pdf. Acesso em: 20 julho. 2023.

BRASIL, **Parâmetros Curriculares Nacionais Ensino Médio. Ministério da Educação** , 1997.

BRASIL, Secretaria da educação Básica. **Orientações Curriculares para o Ensino Médio: Ciências da Natureza, Matemática e suas Tecnologias**. Brasília, MEC, 2006.

BEHRENS, M. ALCÂNTARA, P..R., VIENS, J.: **Implementaçao de Uma Tecnología Inovadora no Ensino Superior**: Prometo PACTO (1999-2000). Colabora – Revista Digital da CVA-RICESU. V.1, n. 2, nove. 2001, 37 p

CANTORAL, Ricardo; et. Al. **Desarrollo Del Pensamento Matemático**. México: Trillas, 2000.

COSTA, Edson Marques; CAETANO, Natalia Gonçalves. **Criptografia com utilização de cifra de Hill e cifra afim**. REVISTA ELETRÔNICA MATEMATICA E ESTATÍSTICA EM FOCO, Minas Gerais, v. 5, n.1, p. 14- 21, julho 2017.

CREASE, Robert. (2011). **As grandes equações**. Rio de Janeiro: editora Zahar.

DANTE, Luiz Roberto. **Didática da Resolução de Problemas de Matemática.** 12 ed. São Paulo: Ática, 2003.

D'AMBROSIO, Ubiratan. **Educação para uma sociedade em transição**. Campinas. Papirus. 1999.

DELORS, J. **Educação: um tesouro a descobrir.** 8. ed. - São Paulo: Cortez; Brasília, DF: MEC: UNESCO, 2003.

Ensino médio do Pará é o mais fraco do Braisl, aponta IDEB. **ZE DUDU**, 2022. Disponível em: https://www.zedudu.com.br/ensino-medio-do-para-e-o-mais-fraco-do-brasil-aponta-ideb/. Acesso em 22 de mar. de 2023.

EVES, Howard. **Introdução à História da Matemática.** Tradução de Hygino Domingues. 5ª ed. – Campinas: Editora da Unicamp, 2011.

FREUDENTHAL, Hans. **Revisiting Mathematics Education: China Lectures**. Kluwer Academic Publishers. Mathematics Education Library.1991.

GODINHO, D. S. **Criptografia: a importância da álgebra linear para decifrá-la**. Revista iTEC, v. II, n° 2, p. 26-31, jul. 2011.

GRANDO, R. C. **O conhecimento matemático e o uso de jogos na sala de aula.** 239 f. Tese de doutorado – Faculdade de Educação, UNICAMP, São Paulo, 2000.

GRILLO, R. de M. **O Xadrez Pedagógico na Perspectiva da Resolução de Problemas em Matemática no Ensino Fundamental**. 2012. 280f. Dissertação (Mestrado em Educação) - Universidade São Francisco, Itatiba.

GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber. **Currículo de**

Matemática e o tema Criptografia no Ensino Médio. Educação Matemática em Revista, Rio Grande do Sul, p. 51-57, 2008.

HEFEZ, Abramo. **Elementos de Aritmética**. SBM, Rio de Janeiro, 2006.

HEFEZ, Abramo. **Aritmética**. SBM, Rio de Janeiro, 2016.

LARA, Isabel Cristina M. **Jogando com a matemática de 5ª a 8ª série**. São Paulo: Rêspel, 2003.

LINS, Romulo Campos. **Matemática, monstros, significados e Educação Matemática**. In: PONTE, J. P; BROCADO, J.; OLIVEIRA, H. **Investigações matemáticas na sala de aula**. Belo Horizonte: Autêntica: 2009.

MINAYO, M. C. de S. (Org.). **O desafio do conhecimento: pesquisa qualitativa em saúde.** 14ª ed. Rio de Janeiro: Hucitec, 2014. 408 p.

MORAN, José Manuel. **A educação que desejamos: Novos desafios e como chegar lá.** (Livro eletrônico) /José Manuel Moran. - Campinas, SP. Papirus, 2013- (Coleção Papirus Educação) 2.702Kb; PDF.

OLIVEIRA, D.; KRIPKA, R. M. L. **O uso da criptografia no ensino de matemática**. In: Conferência Interamericana de Educação Matemática, XIII, 2011. Acesso em: 23 de Abr. de 2014. Disponível em: Acesso em 25 out. 2021.

ORDONEZ, E.; PEREIRA, F.; CHIARAMONTE, R. **Criptografia em Software e Hardware**. 1st edition. ed. São Paulo: Novatec, 2005. ISBN 85-7522-069-1.

PACHECO, M. B.; ANDREIS, G. da S. L. **Causas das dificuldades de aprendizagem em Matemática: percepção de professores e estudantes do 3º ano do Ensino Médio**. Revista Principia, n. 38. João Pessoa, PB. 2018.

SALATESKI, Cleonice. **A webquest valorizando matrizes no contexto da educação matemática**. Disponível em:

http://www.diaadiaeducacao.pr.gov.br/portals/pde/arquivos/1951-6.pdf. Acesso em 24 mar 2023.

SANTOMÉ, Jurjo Torres. As culturas negadas e silenciadas no currículo. In: SILVA, Tomaz Tadeu da (Org.). **Alienígenas na sala de aula: uma introdução aos estudos culturais em educação.** 4. ed. Petrópolis: Vozes, 2002.

SÉRGIO, Pedro. **O que é xadrez (Primeiros Passos)**. 2004. Vol. 271. Editora Brasiliense, 2017.

SILVA, Marta Vieira da; EVANGELISTA, Cristiane Johann; EVANGELISTA, Dilson Henrique Ramos. **Potencializando o Estudo de Criptografia com a Utilização de HQD no Ensino De Matemática.** Disponível em: https://editorarealize.com.br/editora/anais/conedu/2021/TRABALHO˙EV150˙MD1˙SA113˙ID5753˙05112021145144.pdf . Acesso em: 19 fev. 2023.

SONG, X.; DENG, H. **Taking flexible and diverse approaches to get undergraduate students interested in cryptography course. In: First International Workshop on Education Technology and Computer Science.** 2009. v. 2, p. 490-494. Disponível em: https://ieeexplore.ieee.org/document/4959085. Acesso em: 09 fev. 2023.

VIVALDI, Flávia. **Refletindo sobre a competitividade**. Nova Escola – Gestão Escolar. Out.-2014. Disponível em: https://gestaoescolar.org.br/conteudo/977/refletindo-sobre-a-competitividade. Acesso em: 20/06/2023.

Apêndices A

1º Questionário de aplicação do ENIGMÁTICA

Universidade Federal do Pará

Campus Universitário de Bragança

Docente: Dra Marly dos Anjos Nunes

Discente: Dayziane Silva

1º Questionário de aplicação do ENIGMÁTICA]

1. Qual a sua expectativa em relação a um jogo relacionado as funções, matrizes e critérios de divisibilidade?

2. Você tem dificuldades em trabalhar com as funções de 1º grau? Quais?

3. Você tem dificuldade em compreender a teoria que envolve os conteúdos já citados? Se sim, em qual parte?

4. E em relação a teoria que envolve matrizes? Quais?

5. Quanto a parte4 da teoria ligada ao conceito de critérios de divisibilidade, comente como está seu entendimento?

6. Qual dos três assuntos você se sente seguro em afirmar que aprendeu?

Apêndices B

2º Questionário de aplicação do ENIGMÁTICA

Universidade Federal do Pará

Campus Universitário de Bragança

Docente: Dra Marly dos Anjos Nunes

Discente: Dayziane Silva

2º Questionário de aplicação do ENIGMÁTICA]

1. O jogo do Enigmática contribuiu para a sua aprendizagem da disciplina? De que forma?

2. O que mais chamou sua atenção no jogo?

3. Qual/quais conteúdos você conseguiu compreender melhor com o jogo?

4. Você teve alguma dificuldade para compreender o jogo? Qual?

5. Você entendeu melhor os conteúdos com o Enigmática? De que forma?

6. Comente em poucas palavras a eficácia do jogo para o ensino da disciplina Matemática?