UNIVERSIDADE ESTADUAL PAULISTA - UNESP

Dr. Júlio de Mesquita Filho- Câmpus de Presidente Prudente

VANESSA GINES DOS SANTOS OLIVEIRA

O ENSINO DE MATRIZES ATRAVÉS DA CRIPTOGRAFIA: UMA ABORDAGEM CONTEXTUALIZADA NO ENSINO MÉDIO E SUPERIOR

Presidente Prudente

2026

VANESSA GINES DOS SANTOS OLIVEIRA

O ENSINO DE MATRIZES ATRAVÉS DA CRIPTOGRAFIA: UMA ABORDAGEM CONTEXTUALIZADA NO ENSINO MÉDIO E SUPERIOR

Orientador: Profº Dr. José Roberto Nogueira

Presidente Prudente
2026

O48e

Oliveira, Vanessa Gines dos Santos
O Ensino de Matrizes através da Criptografia: Uma abordagem contextualizada no Ensino Médio e Superior / Vanessa Gines dos Santos Oliveira. -- Presidente Prudente, 2026
81 f.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Faculdade de Ciências e Tecnologia, Presidente Prudente
Orientador: Prof.º Dr. José Roberto Nogueira

1. Matemáitca. 2. Educação (Ensino Médio e Superior). 3. Matrizes. 4. Criptografia. 5. Cifra de Hill. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

VANESSA GINES DOS SANTOS OLIVEIRA

O ENSINO DE MATRIZES ATRAVÉS DA CRIPTOGRAFIA: UMA ABORDAGEM CONTEXTUALIZADA NO ENSINO MÉDIO E SUPERIOR

Dissertação apresentada à Universidade Estadual Paulista (UNESP), Júlio de Mesquita Filho, Campus de Presidente Prudente, como parte dos requisitos para obtenção do título de Mestre em Matemática (PROFMAT), da qual a linha de pesquisa é Ensino da Matemática.

Área de concentração: Matemática

Orientador: Prof. Dr. José Roberto Nogueira

Presidente Prudente
2026

VANESSA GINES DOS SANTOS OLIVEIRA

O ENSINO DE MATRIZES ATRAVÉS DA CRIPTOGRAFIA: UMA ABORDAGEM CONTEXTUALIZADA NO ENSINO MÉDIO E SUPERIOR

Dissertação apresentada à Universidade Estadual Paulista (UNESP), Dr. Júlio de Mesquita Filho, Presidente Prudente, para obtenção do título de Mestre em MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT.

Área de Concentração: Matemática

Data de defesa: 04/03/2026

BANCA EXAMINADORA

_____

Profº Dr. José Roberto Nogueira
UNESP – Dr. Júlio de Mesquita Filho – Câmpus de Presidente Prudente

_____

Profª Dra. Marcela Alexandra da Silva
UNIFADRA - Faculdades de Dracena

_____

Profº Dr. Suetônio de Almeida Meira
UNESP – Júlio de Mesquita Filho – Campus de Presidente Prudente

_____

Profª Dra. Cristiane Nespoli de Oliveira
UNESP – Júlio de Mesquita Filho – Campus de Presidente Prudente

_____

Profª Dra. Dayene Miralha de Carvalho Sano
UNOESTE/PP - Universidade do Oeste Paulistta

Dedico este trabalho ao meu marido, Odair Rogério Rodrigues de Oliveira, por toda a paciência e incentivo dispensados aos meus estudos; aos meus filhos, Jhon Róger Gines de Oliveira e Jhordan Rick Gines de Oliveira, que são os maiores motivos para eu sempre querer mais em relação à minha formação; ao meu filho Jhonatan Rogério Gines de Oliveira (in memoriam), meu intercessor diante das inseguranças e provações deste mestrado. Dedico também aos meus pais, Alda Gines dos Santos e Alcides Batista dos Santos (in memoriam), meus maiores exemplos e fonte de inspiração; e aos meus irmãos, Camila Gines dos Santos e Lucas Gines dos Santos, pelo carinho, amizade e constante torcida.

AGRADECIMENTOS

A Deus, em primeiro lugar, pela força, sabedoria e saúde concedidas ao longo dessa jornada. Ao meu orientador, Prof. Dr. José Roberto Nogueira, pelos valiosos ensinamentos, pela orientação dedicada e pelo exemplo de seriedade e profissionalismo que tanto me inspiraram. Agradeço também a todos os professores do curso, que contribuíram de forma significativa para minha formação acadêmica e humana. Aos meus colegas de trabalho da Escola Estadual Dom Bosco, agradeço pelo incentivo e compreensão. Em especial, à diretora Viviane Gonzales de Andrade Risse, à vice-diretora Cristiana Echilla dos Santos Valentim e a coordenadora geral Valéria Anésia Brumatti Jacon, pelo apoio, respeito e consideração nos momentos em que precisei me ausentar. Ao meu amigo e companheiro de mestrado Gustavo Gomes por todo incentivo e por acreditar no meu potencial. Ressaltando meus agradecimentos, visto que, o presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001. A todos, minha sincera gratidão.

‘Compreender matemática é mais importante do que apenas saber fazê-la.’(Skemp, 1976)

RESUMO

Esta dissertação investiga o uso de matrizes no Ensino Médio como uma estratégia para tornar o ensino da Matemática mais dinâmico, aplicado e significativo. O trabalho explora o potencial das matrizes como ferramenta didática para o ensino de Álgebra, com ênfase em suas aplicações no campo da criptografia. O objetivo principal consiste em analisar de que maneira os conceitos matriciais podem ser inseridos no currículo escolar de forma prática e contextualizada, estabelecendo conexões entre a teoria matemática e situações do cotidiano dos estudantes.

A criptografia, historicamente utilizada para a proteção de informações, é apresentada como um contexto pedagógico favorável para a abordagem de conteúdos envolvendo matrizes. A dissertação propõe e discute atividades didáticas baseadas na codificação e decodificação de mensagens por meio da multiplicação de matrizes, possibilitando a exploração de conceitos como determinantes e matrizes inversas. Essa abordagem favorece o desenvolvimento do raciocínio lógico, do pensamento crítico e da capacidade de resolução de problemas.

Trata-se de uma pesquisa de natureza qualitativa, desenvolvida sob a perspectiva da pesquisa-ação, que resultou na elaboração de um produto educacional coerente com os objetivos e fundamentos teórico-metodológicos da dissertação, voltado à contextualização do ensino de matrizes por meio de aplicações como a criptografia.

Os resultados obtidos indicam que a utilização de metodologias contextualizadas, apoiadas em aplicações da Matemática, contribui para a melhoria da aprendizagem dos estudantes em Álgebra, ao promover um elo mais consistente entre os aspectos teóricos e práticos do conteúdo estudado.

Palavras-Chave: matrizes; criptografia; ensino de álgebra; ensino médio; educação matemática.

ABSTRACT

This dissertation investigates the use of matrices in high school education as a strategy to make mathematics teaching more dynamic, applied, and meaningful. The study explores the potential of matrices as a didactic tool for teaching Algebra, with particular emphasis on their applications in the field of cryptography. The main objective is to analyze how matrix concepts can be incorporated into the school curriculum in a practical and contextualized manner, establishing connections between mathematical theory and students' everyday experiences.

Cryptography, historically used to protect information, is presented as a favorable pedagogical context for addressing matrix-related content. The dissertation proposes and discusses teaching activities based on the encoding and decoding of messages through matrix multiplication, enabling the exploration of concepts such as determinants, inverse matrices, and linear transformations. This approach fosters the development of logical reasoning, critical thinking, and problem-solving skills.

The results indicate that the use of contextualized methodologies grounded in mathematical applications contributes to improving students' learning in Algebra by promoting a more consistent link between theoretical and practical aspects of the studied content.

Keywords: matrices; cryptography; algebra teaching; high school; mathematics education.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AIT	Associação Internacional do Trabalho
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
IES	Instituição de Ensino Superior
MEC	Ministério da Educação

LISTA DE SÍMBOLOS

$M_{m\times n}$	Conjunto das matrizes de ordem $m \times n$
A	Matriz genérica
A^{-1}	Matriz inversa da matriz A
$\det(A)$	Determinante da matriz A
I	Matriz identidade
0	Matriz nula
$\equiv$	Relação de congruência
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Z}_n$	Conjunto dos inteiros módulo n
e	Número de Euler
α, β, γ	Letras gregas utilizadas no texto

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO E PROBLEMA DE PESQUISA

Os resultados do SAEB (INEP, 2022) revelam que o desempenho em Matemática no Ensino Médio tem estagnado em níveis críticos, indicando que uma parcela alarmante dos alunos conclui a educação básica sem o aprendizado esperado. Aliado a isso, o relatório do PISA 2022 (OECD, 2023) posicionou o Brasil com um dos maiores déficits de competência matemática entre os países participantes, com cerca de 73% dos estudantes brasileiros abaixo do nível básico de proficiência na disciplina.

Esse panorama estatístico valida a premissa desta dissertação: a necessidade de uma transição de um modelo de ensino puramente mecânico para um modelo contextualizado, capaz de despertar o engajamento através de aplicações reais e tangíveis, como a criptografia e o estudo de matrizes. Nesse sentido, a aprendizagem matemática no ensino básico e superior enfrenta, atualmente, desafios importantes no que diz respeito à motivação e à aplicabilidade dos conteúdos apresentados aos estudantes. Muitas vezes, os estudantes percebem os conceitos matemáticos como abstratos e desconectados da realidade, o que pode levar a uma falta de engajamento e interesse pelo aprendizado. Sendo assim, torna-se necessário buscar estratégias pedagógicas inovadoras que aliem teoria e prática, promovendo a contextualização dos conceitos matemáticos. Além disso, a Base Nacional Comum Curricular (BNCC) para o Ensino Médio destaca a importância de desenvolver, no ensino de Matemática, competências que promovam o pensamento crítico, a resolução de problemas e a aplicação de conceitos matemáticos em diferentes contextos (Brasil, 2025). O documento orienta que os estudantes sejam capazes de utilizar conhecimentos matemáticos para interpretar situações do cotidiano, analisar informações e propor soluções para problemas reais. Nesse sentido, a BNCC enfatiza a necessidade de práticas pedagógicas que favoreçam a investigação, a modelagem e a contextualização dos conteúdos, incentivando o protagonismo do estudante no processo de aprendizagem. Assim, propostas que integrem conceitos matemáticos a aplicações concretas, como a criptografia, alinham-se às diretrizes curriculares nacionais ao promover uma aprendizagem mais significativa e conectada com o mundo contemporâneo.

Diante desse cenário, o problema central da pesquisa consiste em investigar de que maneira o ensino de matrizes, quando contextualizado por meio de aplicações como a criptografia, pode contribuir para uma aprendizagem mais significativa, para o desenvolvimento do raciocínio lógico e para o engajamento dos estudantes do Ensino Médio e Superior.

A matemática é fundamental para a compreensão do mundo e para o desenvolvimento do pensamento lógico. Conforme aponta Skemp (1976), as dificuldades estão frequentemente relacionadas ao caráter abstrato da matemática e à ausência de conexões significativas entre os novos conceitos e os conhecimentos previamente construídos pelos estudantes. Entre esses

conteúdos, o estudo das matrizes destaca-se tanto por sua relevância em diversas áreas do conhecimento quanto pela complexidade conceitual que apresenta aos estudantes.

Uma abordagem prática e contextualizada pode não apenas facilitar o aprendizado de matrizes, mas também gerar maior interesse e engajamento por parte dos estudantes. Neste contexto, propõe-se uso de criptografia como aplicação prática e didática das operações com matrizes.

A criptografia, conhecida por seu papel essencial na segurança digital e na proteção de informações, permite que os estudantes apliquem conceitos de multiplicação de matrizes, matrizes inversas e determinantes de matrizes em atividades de codificação e descodificação de mensagens. Esse enfoque oferece uma introdução interessante aos sistemas de segurança e desperta o interesse dos estudantes ao associar a matemática ao mundo digital, no qual estão imersos, conforme exemplificado por Barichello (s.d.), ao propor o uso de mensagens secretas com matrizes como estratégia para consolidar esses conteúdos matemáticos.

A aplicação de matrizes em criptografia pode ser utilizada como recurso pedagógico para melhorar a compreensão e o interesse dos estudantes pelo estudo das matrizes. Para tanto, são apresentadas e analisadas atividades didáticas que integram essas aplicações práticas, com o intuito de tornar o aprendizado de matrizes mais dinâmico e conectado com o cotidiano dos estudantes. Espera-se que este estudo contribua para uma abordagem mais contextualizada do ensino de matrizes, oferecendo subsídios para educadores utilizarem métodos inovadores que aproximem os estudantes da matemática e promovam uma aprendizagem significativa.

1.2 OBJETIVOS (GERAL E ESPECÍFICOS)

Para enfrentar o desafio de um ensino de matemática frequentemente abstrato e desmotivador, este trabalho estabelece um objetivo geral, que se desdobra em objetivos específicos para a sua realização.

1.2.1 Objetivo Geral

A proposta de uma abordagem para o ensino de matrizes baseada em contextualização e metodologias ativas encontra respaldo em experiências que inserem o conteúdo em situações-problema e em modelagem matemática com apoio de recursos computacionais, promovendo maior engajamento e significado na aprendizagem (Baggio; Schossler; Dullius, 2010).

Busca-se, por meio de um produto educacional composto por uma sequência didática (Criptografia), superar a abordagem puramente algébrica e promover uma aprendizagem significativa, que conecte a teoria matemática a aplicações práticas.

1.2.2 Objetivos Específicos

Para que o objetivo geral seja alcançado, foram delineados os seguintes objetivos específicos:

- Revisar a fundamentação teórica de Matrizes, Determinantes, Matriz Inversa e Aritmética Modular, estruturando este conhecimento de forma a sustentar pedagogicamente as aplicações propostas.
- Desenvolver sequências didáticas (produtos educacionais) como estratégia de intervenção focadas na Criptografia (Cifra de Hill).
- Aplicar as sequências didáticas em turmas da 2ª série do Ensino Médio, bem como em uma turma do curso de Pedagogia, para investigar a eficácia da abordagem em diferentes contextos de aprendizagem.
- Analisar, por meio de uma metodologia de pesquisa-ação de natureza qualitativa, o impacto das atividades no engajamento, na participação e na percepção dos alunos sobre a aplicabilidade da Álgebra Linear.
- Verificar como a contextualização contribui para desmistificar o conteúdo, transformando a relação dos estudantes com a matemática e demonstrando sua relevância interdisciplinar.

1.3 JUSTIFICATIVA E RELEVÂNCIA DO TEMA

Diante do desafio apresentado na contextualização: a dificuldade dos alunos em se conectarem com o ensino abstrato da Álgebra Linear, a presente dissertação justifica-se pela necessidade de desenvolver, aplicar e validar estratégias pedagógicas que superem a mera repetição de cálculos. A relevância deste trabalho reside na seleção de aplicações de alto potencial motivador, a Criptografia, como eixo central para a contextualização do estudo de matrizes.

A escolha da Criptografia, especificamente a Cifra de Hill, justifica-se por sua capacidade de transformar a teoria matricial em uma ferramenta com propósito claro e envolvente. A tarefa de "codificar" e "decodificar" mensagens secretas não é apenas lúdica, mas também pedagogicamente rica, pois exige que os alunos apliquem rigorosamente toda a sequência teórica: a multiplicação de matrizes para a codificação, e os conceitos de determinante, matriz inversa e aritmética modular para a decodificação. A Criptografia, portanto, serve como um fio condutor que dá sentido a cada um dos tópicos teóricos estudados (Araujo; outros, 2024).

O impacto potencial desta pesquisa é, portanto, duplo. No âmbito do estudante, busca-se reconfigurar a sua relação com a matemática, transformando-a de uma disciplina de fórmulas prontas para uma ferramenta lógica, criativa e aplicável. No âmbito do Mestrado Profissional (PROFMAT), o trabalho contribui com um produto educacional validado, as sequências didáticas que podem ser diretamente replicado por outros docentes da Educação Básica que buscam alternativas para um ensino de Álgebra Linear mais significativo e motivador.

1.4 ESTRUTURA DA DISSERTAÇÃO

Com o intuito de apresentar a pesquisa de forma clara e lógica, este trabalho foi estruturado em sete capítulos.

O **Capítulo 1** é esta Introdução, na qual se apresenta a contextualização do problema do ensino de matrizes, a justificativa da pesquisa baseada em aplicações práticas e os objetivos gerais e específicos que norteiam o estudo.

O **Capítulo 2**, Fundamentação Teórica, revisa todo o arcabouço matemático necessário para o desenvolvimento das atividades. A sua sequência foi organizada de forma pedagógica, iniciando-se pelos conceitos fundamentais de matrizes, seguindo para o estudo de Determinantes, o qual é pré-requisito para o capítulo sobre Matriz Inversa, e concluindo com a apresentação da Aritmética Modular, ferramenta essencial para a aplicação em criptografia.

O **Capítulo 3** detalha a Metodologia da pesquisa, enquadrando o trabalho como uma pesquisa-ação de natureza qualitativa e descrevendo o contexto, os sujeitos participantes e os instrumentos de coleta e análise de dados.

O **Capítulo 4**, Aplicações e Propostas Didáticas, apresenta o produto educacional desta dissertação: as sequências didáticas detalhadas sobre Criptografia (Cifra de Hill), prontas para aplicação em sala de aula.

O **Capítulo 5** apresenta a análise dos resultados obtidos com a aplicação das atividades, tecendo as conclusões sobre o impacto da abordagem e sugerindo caminhos para trabalhos futuros.

O **Capítulo 6** traz as Considerações Finais, sintetizando as contribuições do trabalho e o alcance dos objetivos propostos.

Por fim, apresentam-se as **Referências**, que listam o referencial teórico e os documentos norteadores utilizados para a fundamentação desta pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 BREVE HISTÓRICO

O presente trabalho tem como objetivo tornar o ensino de matrizes mais significativo para os estudantes da 2ª série do Ensino Médio, por meio da contextualização com situações do cotidiano e aplicações reais, como a criptografia. A proposta surge da necessidade de superar uma abordagem excessivamente mecânica, ainda recorrente no ensino de Álgebra Linear, na qual os procedimentos algébricos são apresentados de forma desarticulada de seus significados e aplicações.

Historicamente, as ideias associadas às matrizes estão ligadas à resolução de sistemas de equações lineares, cujos registros remontam a civilizações antigas. Há evidências de que os babilônios, por volta de 2000 a.C., já utilizavam métodos sistemáticos para resolver problemas equivalentes a sistemas lineares. De modo semelhante, na China Antiga, o tratado matemático *Os Nove Capítulos sobre a Arte Matemática*, datado de aproximadamente século III a.C., apresentava procedimentos organizados em tabelas que antecipavam conceitos hoje formalizados na teoria das matrizes (Boyer; Merzbach, 1996; Katz, 2009).

Entretanto, foi apenas no século XIX que o conceito de matriz passou a ser formalizado no âmbito da Álgebra Linear. Segundo Boyer (Boyer; Merzbach, 1996), o termo *matriz* foi introduzido por James Joseph Sylvester, em 1850, para designar um arranjo de números a partir do qual outros objetos algébricos, como os determinantes, poderiam ser construídos. Nesse mesmo período, contribuições de matemáticos como Arthur Cayley e Ferdinand Frobenius consolidaram definições, propriedades e operações matriciais, estruturando a teoria das matrizes como um campo fundamental da Matemática.

Ao longo do século XX, o uso das matrizes extrapolou o domínio da Matemática pura, tornando-se essencial em áreas como Física, Engenharia, Economia e Computação. Com o avanço tecnológico e o desenvolvimento dos computadores, as matrizes passaram a ocupar papel central em aplicações como processamento de imagens, modelagem de fenômenos, análise de dados e criptografia (Katz, 2009; Stallings, 2017). Atualmente, constituem a base matemática de algoritmos utilizados em segurança da informação, inteligência artificial e aprendizagem de máquina.

Do ponto de vista educacional, compreender esse percurso histórico contribui para que o estudo das matrizes deixe de ser percebido apenas como um conjunto de técnicas algébricas e passe a ser entendido como uma ferramenta matemática com relevância concreta. Conforme defendem D'Ambrosio (D'Ambrosio, 2004) e Lorenzato (Lorenzato, 2006), quando o estudante reconhece o sentido e a finalidade do conhecimento matemático, a aprendizagem tende a se tornar mais significativa.

Nesse contexto, a criptografia com matrizes, em especial a Cifra de Hill, apresenta-se

como um recurso didático potente, pois articula conceitos como multiplicação de matrizes, determinantes, matriz inversa e aritmética modular em uma atividade com propósito claro: a codificação e a decodificação de mensagens, conforme o método originalmente proposto por Hill Hill (1931). Tal abordagem permite que os estudantes compreendam as matrizes não apenas como arranjos numéricos, mas como instrumentos matemáticos aplicáveis a situações presentes no mundo digital, favorecendo o desenvolvimento do raciocínio lógico, da autonomia intelectual e da resolução de problemas.

Dessa forma, o breve histórico apresentado não tem a finalidade de esgotar o desenvolvimento teórico das matrizes, mas de situar o leitor e, sobretudo, o professor, quanto à relevância desse conteúdo e à pertinência de sua abordagem contextualizada no Ensino Médio. Nos tópicos seguintes, são apresentados os conceitos fundamentais de matrizes e suas principais operações, com foco nos elementos necessários para a compreensão das aplicações didáticas propostas neste trabalho.

2.2 CONCEITOS FUNDAMENTAIS DE MATRIZES

As matrizes constituem uma ferramenta matemática essencial para a organização de dados, a representação de relações e a resolução de problemas envolvendo sistemas de equações lineares. No contexto da Álgebra Linear, seu estudo fornece a base conceitual necessária para diversas aplicações, entre elas a criptografia, foco deste trabalho.

Formalmente, uma matriz é definida como um arranjo retangular de elementos, geralmente números reais, dispostos em linhas e colunas. Cada elemento é identificado por dois índices, sendo o primeiro referente à linha e o segundo à coluna em que o elemento se encontra. Segundo Lay, Lay e McDonald (Lay; Lay; McDonald, 2016), essa forma de organização permite representar informações de maneira sistemática e eficiente, facilitando tanto a manipulação algébrica quanto a interpretação de relações matemáticas.

Definição 1. *Sejam m e n números naturais não nulos. Chama-se matriz M de ordem $m \times n$ todo arranjo retangular formado por números reais distribuídos em m linhas e n colunas. Cada elemento da matriz é indicado por a_{ij}, em que i representa a linha e j a coluna correspondente.*

Uma matriz de ordem $m \times n$ pode ser representada genericamente por

$$M = (a_{ij})_{m \times n},$$

em que $1 \leq i \leq m$ e $1 \leq j \leq n$. Essa notação será utilizada ao longo deste trabalho por sua clareza e adequação às operações matriciais discutidas.

Exemplos de matrizes

$$\begin{bmatrix} 2 & 7 & 3 \\ 1 & \frac{3}{5} & \sqrt{2} \end{bmatrix} \quad \text{é uma matriz de ordem } 2 \times 3.$$

$$\begin{bmatrix} 5 \\ 0 \\ 2 \end{bmatrix} \quad \text{é uma matriz de ordem } 3 \times 1.$$

$$\begin{bmatrix} 1 & 6 \\ 2 & 5 \end{bmatrix} \quad \text{é uma matriz de ordem } 2 \times 2.$$

Esses exemplos ilustram diferentes ordens de matrizes, destacando que, no contexto das aplicações didáticas deste trabalho, as matrizes de ordem 2×2 assumem papel central, especialmente na abordagem da Cifra de Hill. Entretanto, matrizes de outras ordens são apresentadas para garantir consistência conceitual e fundamentação teórica adequada.

Tipos especiais de matrizes

Algumas matrizes apresentam propriedades particulares e, por isso, recebem denominações específicas, relevantes tanto do ponto de vista teórico quanto didático:

- **Matriz linha**: matriz de ordem $1 \times n$, composta por uma única linha.
- **Matriz coluna**: matriz de ordem $m \times 1$, composta por uma única coluna.
- **Matriz nula**: matriz cujos elementos são todos iguais a zero.
- **Matriz quadrada**: matriz de ordem $n \times n$, com o mesmo número de linhas e colunas.
- **Matriz transposta**: matriz obtida ao trocar linhas por colunas.

No caso das matrizes quadradas, destacam-se ainda as noções de diagonal principal e diagonal secundária, conceitos fundamentais para o estudo de determinantes e matrizes inversas, que serão explorados nas seções seguintes.

Definição 2. *A matriz identidade (ou matriz unidade) de ordem n, denotada por I_n, é a matriz quadrada cujos elementos da diagonal principal são iguais a 1 e todos os demais elementos são iguais a zero.*

Por exemplo:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

A matriz identidade desempenha papel fundamental na multiplicação de matrizes, atuando como elemento neutro, e será essencial na definição de matriz inversa, conceito indispensável para a decodificação de mensagens na criptografia de Hill.

Definição 3. *Duas matrizes A e B são ditas iguais se, e somente se, possuem a mesma ordem e se $a_{ij} = b_{ij}$ para todo par de índices (i, j) (Lay; Lay; McDonald, 2016).*

Essa definição estabelece a base para as operações matriciais, uma vez que a adição e a subtração de matrizes só são definidas entre matrizes de mesma ordem.

As operações fundamentais com matrizes incluem a adição, a multiplicação por escalar e a multiplicação entre matrizes. Essas operações são apresentadas a seguir por constituírem o suporte algébrico necessário às aplicações didáticas propostas.

Sejam $A = (a_{ij})$ e $B = (b_{ij})$ matrizes de mesma ordem $m \times n$. A soma $C = A + B$ é definida elemento a elemento por

$$c_{ij} = a_{ij} + b_{ij}.$$

2.3 PROPRIEDADES DA ADIÇÃO DE MATRIZES

A adição de matrizes de ordem $m \times n$ satisfaz as seguintes propriedades:

1. **Associatividade:**
   Para quaisquer matrizes A, B e C de ordem $m \times n$, temos:

$$(A + B) + C = A + (B + C)$$

2. **Comutatividade:**
   Para quaisquer matrizes A e B de ordem $m \times n$, vale:

$$A + B = B + A$$

3. **Elemento Neutro:**
   Existe uma matriz nula O de ordem $m \times n$ tal que, para qualquer matriz A, temos:

$$A + O = A \tag{1}$$

4. **Elemento Simétrico (ou Oposto Aditivo):**
   Para cada matriz A, existe uma matriz A' (ou $-A$) tal que:

$$A + A' = O \tag{2}$$

Seja $k \in \mathbb{R}$ e $A = (a_{ij})$ uma matriz de ordem $m \times n$. O produto kA é a matriz cujos elementos são dados por

$$(kA)_{ij} = k \cdot a_{ij}.$$

Ao definirmos as operações de adição de matrizes e de multiplicação por um escalar, estabelece-se uma estrutura algébrica bem definida. De fato, o conjunto das matrizes reais de ordem $m \times n$, denotado por $M_{m\times n}(\mathbb{R})$, munido dessas duas operações, satisfaz todos os axiomas de um **espaço vetorial** sobre o corpo dos números reais Lay, Lay & McDonald (2016), Anton & Rorres (2012).

Sejam A uma matriz de ordem $m \times n$ e B uma matriz de ordem $n \times p$. O produto AB é a matriz de ordem $m \times p$ definida por

$$(AB)_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}.$$

2.4 PROPRIEDADES DA MULTIPLICAÇÃO DE MATRIZES

Teorema 1. *Sejam $A \in M_{m\times n}(\mathbb{R})$, $B \in M_{n\times p}(\mathbb{R})$ e $C \in M_{p\times q}(\mathbb{R})$, e seja $\lambda \in \mathbb{R}$. Valem as seguintes propriedades:*

- ***Associatividade:*** $(AB)C = A(BC)$.
- ***Distributividade à esquerda:*** $A(B + C) = AB + AC$ *(com $B, C \in M_{n\times p}(\mathbb{R})$).*
- ***Distributividade à direita:*** $(A + B)C = AC + BC$ *(com $A, B \in M_{m\times n}(\mathbb{R})$).*
- ***Compatibilidade com escalar:*** $\lambda(AB) = (\lambda A)B = A(\lambda B)$.
- ***Elemento neutro:*** $AI_n = A$ *e* $I_mA = A$.

Valem as seguintes propriedades (Anton; Rorres, 2012).

É fundamental destacar que a multiplicação de matrizes, em geral, não é comutativa, isto é, $AB \neq BA$, mesmo quando ambos os produtos estão definidos. Essa característica assume papel central na criptografia com matrizes, uma vez que a ordem das operações influencia diretamente o processo de codificação e decodificação das mensagens.

Do ponto de vista didático, a compreensão dessas operações permite ao estudante perceber as matrizes como objetos matemáticos dotados de significado e funcionalidade, e não apenas como tabelas numéricas. Nos tópicos seguintes, esses conceitos serão aprofundados por meio do estudo dos determinantes e das matrizes inversas, fundamentais para a aplicação da Criptografia de Hill desenvolvida neste trabalho.

2.5 DETERMINANTE

Nesse contexto, a criptografia com matrizes, em especial a Cifra de Hill, constitui-se como uma estratégia didática que articula conceitos fundamentais da Álgebra Linear, tais como multiplicação de matrizes, determinantes, matriz inversa e aritmética modular, a partir de um método clássico de codificação e decodificação de mensagens proposto por Hill (1931). Ao empregar esse procedimento em sala de aula, busca-se favorecer a compreensão das matrizes para além de sua definição formal, possibilitando que os estudantes as reconheçam como ferramentas matemáticas aplicáveis a situações associadas ao mundo digital.

Segundo (Anton; Rorres, 2012), o determinante associa a cada matriz quadrada um número real, permitindo analisar se a matriz é inversível e compreender o comportamento das transformações lineares a ela associadas. Dessa forma, o estudo dos determinantes estabelece uma ponte natural entre a teoria matricial e suas aplicações práticas.

Definição e cálculo do determinante

O determinante está definido apenas para matrizes quadradas. Inicialmente, apresenta-se sua definição para matrizes de menor ordem, que são aquelas trabalhadas prioritariamente no Ensino Médio.

Matriz de ordem 1×1

Seja $A = [a]$ uma matriz de ordem 1×1. Define-se o determinante de A como:

$$\det(A) = a.$$

Matriz de ordem 2×2

Seja

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

uma matriz de ordem 2×2. O determinante de A é definido por:

$$\det(A) = ad - bc.$$

Exemplo: Considere a matriz

$$A = \begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix}.$$

Então,

$$\det(A) = (5 \cdot 4) - (2 \cdot 3) = 20 - 6 = 14.$$

Esse cálculo simples é essencial para a aplicação da Cifra de Hill, pois permite verificar rapidamente se uma matriz pode ser utilizada como chave criptográfica.

Determinante de matrizes de ordem 3×3

Embora o foco principal deste trabalho recaia sobre matrizes de ordem 2×2, é importante apresentar o cálculo do determinante de matrizes de ordem 3×3 para garantir consistência teórica e ampliar a compreensão conceitual dos estudantes.

Para matrizes de ordem 3, utiliza-se frequentemente a *Regra de Sarrus*, método prático amplamente difundido no ensino básico (Anton; Rorres, 2012). Seja

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

O determinante de A é dado por:

$$\det(A) = (a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}) - (a_{13}a_{22}a_{31} + a_{11}a_{23}a_{32} + a_{12}a_{21}a_{33}).$$

Exemplo: Considere a matriz

$$B = \begin{bmatrix} 1 & 5 & -2 \\ 4 & 3 & 0 \\ -1 & 8 & 2 \end{bmatrix}.$$

Aplicando a Regra de Sarrus, obtém-se:

$$\det(B) = -104.$$

A apresentação desse método permite ao estudante compreender o cálculo do determinante em ordens superiores, ainda que sua aplicação direta não seja explorada nas atividades didáticas propostas.

Propriedades fundamentais dos determinantes

Os determinantes satisfazem propriedades importantes que auxiliam na análise de matrizes e na simplificação de cálculos. Entre as principais, destacam-se (Anton; Rorres, 2012; Lay; Lay; McDonald, 2016):

- $\det(A^T) = \det(A)$, isto é, o determinante de uma matriz é igual ao determinante de sua transposta;
- $\det(AB) = \det(A)\det(B)$, para matrizes quadradas de mesma ordem;

- Uma matriz quadrada A é inversível se, e somente se, $\det(A) \neq 0$ (Esse tema veremos adiante);
- Se $\det(A) = 0$, a matriz é dita singular e não admite inversa.

Do ponto de vista pedagógico, a propriedade que relaciona o determinante à existência da matriz inversa é a mais relevante para este trabalho, pois permite estabelecer um critério claro para a escolha das matrizes-chave utilizadas na criptografia.

Determinante e aplicações didáticas

Na Criptografia de Hill, o determinante assume papel decisivo, pois apenas matrizes com determinante não nulo possuem inversa e, portanto, permitem a decodificação das mensagens. Essa condição oferece ao professor uma oportunidade didática valiosa para contextualizar o conteúdo, mostrando que o cálculo do determinante não é um procedimento isolado, mas uma etapa necessária para garantir o funcionamento de um sistema criptográfico.

Assim, o estudo dos determinantes, além de aprofundar a compreensão das matrizes quadradas, contribui para atribuir significado às operações matriciais, favorecendo uma aprendizagem mais consciente, aplicada e alinhada às propostas pedagógicas deste trabalho.

2.6 MATRIZ INVERSA

O conceito de matriz inversa está diretamente relacionado ao determinante e desempenha papel central tanto na Álgebra Linear quanto nas aplicações propostas neste trabalho. Em termos teóricos, a existência da matriz inversa permite resolver sistemas lineares e analisar transformações lineares. No contexto didático, sua importância se evidencia na Criptografia de Hill, uma vez que a decodificação das mensagens só é possível quando a matriz utilizada como chave criptográfica admite inversa.

Segundo Anton e Rorres (Anton; Rorres, 2012), uma matriz inversa pode ser compreendida como o análogo matricial do inverso multiplicativo de um número real. Assim como um número real não nulo possui um inverso, uma matriz quadrada só admite inversa quando satisfaz determinadas condições, especialmente a não nulidade do determinante.

Definição de matriz inversa

Definição 4. *Seja A uma matriz quadrada de ordem n. Diz-se que A é inversível se existe uma matriz B de mesma ordem tal que*

$$AB = BA = I_n,$$

em que I_n representa a matriz identidade de ordem n. A matriz B é chamada de matriz inversa de A e é denotada por A^{-1}.

Caso não exista tal matriz B, a matriz A é dita singular. Essa definição estabelece um critério claro para a invertibilidade de matrizes e reforça a conexão direta entre matriz inversa e determinante.

Condição de existência da matriz inversa

Uma matriz quadrada admite inversa se, e somente se, seu determinante é diferente de zero. Ou seja,

$$A \text{ é inversível } \iff \det(A) \neq 0.$$

Essa condição, apresentada em textos clássicos de Álgebra Linear (Lay; Lay; McDonald, 2016; Strang, 2016), é fundamental para as aplicações criptográficas desenvolvidas neste trabalho, pois garante que a operação de decodificação seja possível.

Cálculo da matriz inversa de ordem 2×2

No Ensino Médio e nas atividades propostas nesta dissertação, trabalha-se prioritariamente com matrizes de ordem 2×2, devido à simplicidade dos cálculos e à clareza conceitual. Seja

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

uma matriz quadrada de ordem 2×2 tal que $\det(A) = ad - bc \neq 0$. Usando o método dos cofatores (veremos mais adiante), a matriz inversa de A é dada por:

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Uma matriz quadrada A é denominada inversível quando existe outra matriz A^{-1} tal que $AA^{-1} = A^{-1}A = I$, onde I representa a matriz identidade de mesma ordem. A matriz A^{-1} é chamada de matriz inversa de A (Lay; Lay; McDonald, 2016).

Exemplo: Considere a matriz

$$A = \begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix}.$$

Como $\det(A) = 14 \neq 0$, a matriz é inversível e sua inversa é:

$$A^{-1} = \frac{1}{14} \begin{bmatrix} 4 & -2 \\ -3 & 5 \end{bmatrix}.$$

Esse procedimento é essencial para a Criptografia de Hill, pois a matriz inversa é utilizada no processo de decodificação das mensagens criptografadas.

Propriedades da matriz inversa

A matriz inversa possui propriedades importantes que contribuem para a compreensão de sua estrutura algébrica. Entre as principais, destacam-se (Anton; Rorres, 2012; Lay; Lay; McDonald, 2016):

- $(A^{-1})^{-1} = A$, isto é, a inversa da inversa é a própria matriz;
- $(AB)^{-1} = B^{-1}A^{-1}$, para matrizes inversíveis de mesma ordem;
- $(A^T)^{-1} = (A^{-1})^T$;
- $I_n^{-1} = I_n$.

Essas propriedades reforçam a ideia de que a inversa não é apenas um procedimento de cálculo, mas um objeto matemático com comportamento algébrico bem definido.

2.6.1 O cálculo da inversa de uma matriz

Nesta seção são apresentados alguns métodos clássicos para o cálculo da inversa de uma matriz. Embora existam diferentes abordagens, será enfatizado o **método dos cofatores**, em virtude de sua forte conexão teórica com os determinantes e de sua relevância conceitual no contexto educacional.

O Método dos Cofatores

O método de cálculo da matriz inversa utilizando cofatores, também conhecido como **método da matriz adjunta**, é derivado diretamente da teoria dos determinantes. Para uma matriz quadrada $\mathbf{A}$ de ordem n, a inversa é definida pela relação

$$\mathbf{A}^{-1} = \frac{1}{\det(\mathbf{A})} \cdot \text{adj}(\mathbf{A}), \tag{3}$$

onde $\det(\mathbf{A})$ é o determinante de $\mathbf{A}$ e $\text{adj}(\mathbf{A})$ representa a matriz adjunta de $\mathbf{A}$ (Anton; Rorres, 2012).

A matriz adjunta de uma matriz quadrada A é a matriz obtida pela transposição da matriz formada pelos cofatores dos elementos de A.

Forma matemática

Seja A uma matriz quadrada de ordem n. A matriz adjunta de A, denotada por $\text{adj}(A)$, é definida como a transposta da matriz dos cofatores de A. Assim,

$$\text{adj}(A) = (C_{ij})^T$$

em que C_{ij} representa o cofator do elemento a_{ij} da matriz A.

Algoritmo de Cálculo por Cofatores

Seja $\mathbf{A} = [a_{ij}]$ uma matriz quadrada de ordem n.

Passo 1: Verificação da invertibilidade

Calcula-se inicialmente o determinante $\det(\mathbf{A})$. A matriz $\mathbf{A}$ será invertível se, e somente se, $\det(\mathbf{A}) \neq 0$.

Passo 2: Construção da matriz dos cofatores

O cofator C_{ij} associado ao elemento a_{ij} é definido por

$$C_{ij} = (-1)^{i+j} \cdot \det(\mathbf{M}_{ij}), \tag{4}$$

onde $\mathbf{M}_{ij}$ é a submatriz obtida pela remoção da i-ésima linha e da j-ésima coluna de $\mathbf{A}$.

A **matriz dos cofatores** $\mathbf{C} = [C_{ij}]$ é dada por

$$\mathbf{C} = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix}.$$

Passo 3: Determinação da matriz adjunta

A matriz adjunta $\text{adj}(\mathbf{A})$ é definida como a transposta da matriz dos cofatores:

$$\text{adj}(\mathbf{A}) = \mathbf{C}^T. \tag{5}$$

Passo 4: Cálculo da matriz inversa

A matriz inversa é obtida substituindo os resultados anteriores na Equação (3).

Exemplo 1 (Inversa de uma matriz de ordem 2)**.** *Considere* $A = \begin{bmatrix} 4 & 1 \\ -2 & 3 \end{bmatrix}$. *Como* $\det(A) = 14 \neq 0$*, a matriz é invertível.*

Exemplo 2. *A matriz dos cofatores é*

$$C = \begin{bmatrix} 3 & 2 \\ -1 & 4 \end{bmatrix},$$

e a matriz adjunta é

$$adj(A) = \begin{bmatrix} 3 & -1 \\ 2 & 4 \end{bmatrix}.$$

Assim,

$$A^{-1} = \frac{1}{14} \begin{bmatrix} 3 & -1 \\ 2 & 4 \end{bmatrix}.$$

Exemplo 3 (Inversa de uma matriz 3×3)**.** *Considere a matriz*

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}.$$

Calcula-se inicialmente o determinante, obtendo-se $\det(A) = 1$. *Em seguida, constroem-se os cofatores e a matriz adjunta:*

$$adj(A) = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}.$$

Como $\det(A) = 1$, *a matriz inversa coincide com a matriz adjunta:*

$$A^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}.$$

O cálculo da matriz inversa é particularmente relevante na resolução de sistemas lineares possíveis e determinados. De fato, dado um sistema matricial da forma $A \cdot X = B$, com A invertível, a solução pode ser obtida diretamente por

$$X = A^{-1} \cdot B.$$

Essa abordagem será fundamental para as aplicações desenvolvidas neste trabalho, em especial no contexto da **Criptografia de Hill**.

Matriz inversa e aplicações didáticas

Na Criptografia de Hill, a matriz inversa representa o mecanismo matemático que garante a recuperação da mensagem original. Ao trabalhar esse conceito em sala de aula, o professor pode evidenciar que a existência da inversa não é um detalhe técnico, mas uma condição essencial para o funcionamento do sistema criptográfico.

Do ponto de vista pedagógico, essa abordagem favorece a compreensão do papel do determinante e fortalece a articulação entre os conteúdos de matrizes, determinantes e aritmética modular. Assim, o estudo da matriz inversa deixa de ser um procedimento meramente algébrico e passa a ser compreendido como uma ferramenta matemática com finalidade concreta, alinhada às propostas didáticas deste trabalho.

2.7 O NOVO UNIVERSO MATEMÁTICO: ARITMÉTICA MODULAR

A Aritmética Modular constitui um campo fundamental da Teoria dos Números e desempenha papel central nas aplicações criptográficas abordadas neste trabalho. Diferentemente da aritmética usual, na qual os números crescem indefinidamente, a aritmética modular organiza os inteiros em classes de equivalência, permitindo a análise de operações a partir dos restos da divisão por um número natural fixo, denominado módulo.

Do ponto de vista didático, a aritmética modular é frequentemente associada à chamada *aritmética do relógio*, analogia que facilita a compreensão do conceito por parte dos estudantes. Essa abordagem favorece a introdução de ideias abstratas de forma intuitiva, estabelecendo conexões entre a matemática formal e situações do cotidiano.

Nessa analogia, pode-se considerar um relógio adaptado com 26 posições, correspondentes às 26 letras do alfabeto. Ao avançar além da última posição, a contagem retorna ao início, repetindo o ciclo. Por exemplo, após a 26ª posição, a contagem reinicia na primeira. De modo análogo, na aritmética modular, os números são organizados em ciclos definidos por um módulo — neste caso, 26 — e valores diferentes podem ocupar a mesma posição quando apresentam o mesmo resto na divisão por esse número, ideia fundamental para a codificação e decodificação de mensagens criptográficas.

Exemplo 4. *Considere a congruência* $20 \equiv 6 \pmod 7$. *Usando o algoritmo da divisão:*

$$20 = 7 \cdot 2 + 6, \qquad 6 = 7 \cdot 0 + 6$$

Como ambos têm o mesmo resto, a congruência é verdadeira. Alternativamente, a diferença $(20 - 6) = 14$ *é um múltiplo de 7, o que confirma a congruência.*

Congruência modular

Definição 5. *Sejam* a *e* b *inteiros e* n *um inteiro natural maior que 1. Diz-se que* a *é congruente a* b *módulo* n*, e escreve-se*

$$a \equiv b \pmod n,$$

se n *divide a diferença* $a - b$*.*

Essa relação indica que a e b produzem o mesmo resto quando divididos por n. Por exemplo,

$$17 \equiv 5 \pmod{12},$$

pois $17 - 5 = 12$ é múltiplo de 12. Essa situação é facilmente visualizada em um relógio, no qual, após completar uma volta, a contagem reinicia.

Classes residuais

Dado um módulo n, os inteiros podem ser organizados em n classes residuais distintas, denotadas por:

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Cada classe reúne todos os inteiros congruentes entre si módulo n. Por exemplo, em $\mathbb{Z}_8$, os números 0, 8, 16 e 24 pertencem à mesma classe, pois todos são congruentes a 0 módulo 8.

Essa estrutura é amplamente utilizada na criptografia, pois permite trabalhar com um conjunto finito de símbolos, condição essencial para a codificação de mensagens.

Operações em aritmética modular

As operações de adição, subtração e multiplicação em $\mathbb{Z}_n$ são realizadas de modo semelhante às operações usuais, seguidas da redução do resultado ao módulo n.

Adição modular

Sejam $a, b \in \mathbb{Z}_n$. Define-se:

$$a + b \equiv (a + b) \bmod n.$$

Multiplicação modular

Sejam $a, b \in \mathbb{Z}_n$. Define-se:

$$a \cdot b \equiv (a \cdot b) \bmod n.$$

Exemplo: Em $\mathbb{Z}_8$,

$$5 + 6 = 11 \equiv 3 \pmod 8, \quad 4 \cdot 3 = 12 \equiv 4 \pmod 8.$$

Essas operações permitem construir tabelas de adição e multiplicação, que auxiliam na visualização do funcionamento da aritmética modular e são frequentemente utilizadas como recurso didático introdutório.

As tábuas de $\mathbb{Z}_m$

Vimos anteriormente que o conjunto $\mathbb{Z}_m$ com as operações de adição e multiplicação tem estrutura de anel comutativo com unidade. Em particular se p é primo, $\mathbb{Z}_p$ tem estrutura de corpo. Por se tratar de anéis finitos, a operação de adição e multiplicação podem ser representadas através de tábuas. Para facilitar nossas contas descreveremos o conjunto $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$ ao invés de $\mathbb{Z}_m = \{[0], [1], [2], \cdots, [m-1]\}$.

Exemplo 5. ***Destaque: O conjunto $\mathbb{Z}_2$ e sua importância na computação***

O conjunto $\mathbb{Z}_2$ é formado pelos inteiros módulo 2, isto é,

$$\mathbb{Z}_2 = \{0, 1\}.$$

Nesse sistema aritmético, todas as operações são realizadas módulo 2, o que significa que os resultados possíveis são apenas 0 *ou* 1.

Esse conjunto possui grande importância na computação, pois está diretamente relacionado ao sistema binário utilizado pelos computadores. Nos sistemas digitais, todas as informações são representadas por sequências de bits, que assumem apenas dois estados possíveis: 0 *ou* 1. *Dessa forma, operações matemáticas realizadas em $\mathbb{Z}_2$ servem de base para diversos processos computacionais, como lógica digital, codificação de dados, criptografia e correção de erros em sistemas de comunicação. Por exemplo, na aritmética módulo 2, tem-se*

$$1 + 1 \equiv 0 \pmod 2,$$

resultado que corresponde exatamente à lógica da soma binária utilizada em circuitos digitais.

Exemplo 6. *As operações para $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ podem ser representadas pelas tábuas:*

Tabela 1 – Tábua de adição em $\mathbb{Z}_8$

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Tabela 2 – Tábua da multiplicação em $\mathbb{Z}_8$

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	3	4	2	1

Por meio das tábuas das operações de adição e multiplicação é possível estudar diversas propriedades do conjunto $\mathbb{Z}_m$. Em particular, tais representações permitem identificar o **oposto aditivo** (a partir da tábua da adição) e o **inverso multiplicativo** (a partir da tábua da multiplicação) de um elemento de $\mathbb{Z}_m$ Niven, Zuckerman & Montgomery (2008).

Considerando o caso de $\mathbb{Z}_8$, podemos perguntar qual é o oposto aditivo do elemento $[3]$, isto é, qual elemento $[-3] \in \mathbb{Z}_8$ satisfaz

$$[3] + [-3] = [0].$$

Consultando a tábua da adição módulo 8, observa-se que

$$[3] + [5] = [8] = [0],$$

o que mostra que o oposto aditivo de $[3]$ em $\mathbb{Z}_8$ é a classe $[5]$.

Embora o exemplo em $\mathbb{Z}_8$ seja adequado para ilustrar as propriedades algébricas de um anel finito, no contexto desta pesquisa torna-se particularmente relevante considerar o conjunto $\mathbb{Z}_{26}$, em razão de sua correspondência com as 26 letras do alfabeto latino, amplamente utilizada em aplicações criptográficas. A seguir, apresenta-se um recorte da tábua de adição em $\mathbb{Z}_{26}$, com o objetivo de evidenciar o comportamento cíclico das operações módulo 26.

Tabela 3 – Tábua de adição em $\mathbb{Z}_{26}$ (recorte ilustrativo)

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	8
2	2	3	4	5	6	7	8	9
3	3	4	5	6	7	8	9	10
4	4	5	6	7	8	9	10	11
5	5	6	7	8	9	10	11	12
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
25	25	0	1	2	3	4	5	6

De modo análogo, para determinar o inverso multiplicativo de um elemento $[a] \in \mathbb{Z}_m$, é necessário verificar inicialmente se tal inverso existe. Conforme visto anteriormente, um elemento $[a]$ é inversível em $\mathbb{Z}_m$ se, e somente se, $mdc(a, m) = 1$.

Verificada essa condição, o inverso multiplicativo pode ser identificado na tábua da multiplicação, procurando-se um elemento $[b]$ tal que

$$[a] \cdot [b] = [1].$$

Por exemplo, em $\mathbb{Z}_8$, como $mdc(5, 8) = 1$, o elemento $[5]$ é inversível. Observando a tábua da

multiplicação módulo 8, encontra-se que

$$[5] \cdot [5] = [25] = [1],$$

o que implica que o inverso multiplicativo de $[5]$ em $\mathbb{Z}_8$ é o próprio $[5]$.

Inverso multiplicativo modular

Um conceito fundamental para a criptografia é o de inverso multiplicativo em aritmética modular. Diz-se que um inteiro $a \in \mathbb{Z}_n$ possui inverso multiplicativo módulo n se existe um inteiro $b \in \mathbb{Z}_n$ tal que:

$$a \cdot b \equiv 1 \pmod{n}.$$

Nem todo elemento de $\mathbb{Z}_n$ admite inverso multiplicativo. Tal inverso existe se, e somente se, a e n são coprimos, isto é, $mdc(a, n) = 1$.

Esse conceito será essencial no cálculo da matriz inversa no contexto da Criptografia de Hill, uma vez que as operações envolvem inversos definidos em aritmética modular.

Aritmética modular e criptografia com matrizes

Na Criptografia de Hill, a aritmética modular é utilizada para garantir que os resultados das operações matriciais permaneçam dentro de um conjunto finito de símbolos, geralmente associados a letras do alfabeto. Após a multiplicação da matriz-chave pela matriz que representa a mensagem, os resultados são reduzidos módulo n, assegurando a padronização do sistema criptográfico.

Do ponto de vista pedagógico, essa etapa permite integrar conteúdos de matrizes, determinantes, matriz inversa e aritmética modular em uma única aplicação, conferindo sentido às operações matemáticas estudadas. Assim, a aritmética modular não aparece como um tópico isolado, mas como um elemento estruturante que viabiliza a aplicação concreta da teoria matricial no processo de codificação e decodificação de mensagens.

Dessa forma, o estudo da aritmética modular conclui a fundamentação teórica necessária para o desenvolvimento das atividades didáticas propostas neste trabalho, preparando o leitor para a abordagem prática da Criptografia de Hill apresentada nos capítulos seguintes.

Propriedades Fundamentais

A relação de congruência módulo m é uma **relação de equivalência**, pois satisfaz as propriedades de reflexividade, simetria e transitividade, conforme estabelecido na Teoria dos Números clássica Niven, Zuckerman & Montgomery (2008):

- **Reflexividade:** Todo inteiro é congruente a si mesmo módulo m,

$$a \equiv a \pmod{m}.$$

- **Simetria:** Se a é congruente a b módulo m, então b é congruente a a módulo m,

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}.$$

- **Transitividade:** Se a é congruente a b e b é congruente a c módulo m, então a é congruente a c módulo m,

$$a \equiv b \pmod{m} \text{ e } b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}.$$

Essas propriedades permitem particionar o conjunto dos inteiros em **classes de equivalência**, também chamadas de classes residuais, possibilitando que conjuntos de inteiros com o mesmo resto na divisão por m sejam tratados como um único elemento em operações algébricas.

Sendo a congruência uma relação de equivalência, vamos denotar por $\mathbb{Z}_m$ o conjunto das suas classes de equivalência. Assim, vamos escrever:

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

Vamos agora definir como fazer para somar e multiplicar elementos deste novo conjunto.

Adição e a multiplicação em $\mathbb{Z}_m$

Definição 6. *Sejam $[a]$ e $[b]$ classes de equivalência em $\mathbb{Z}_m$. Definem-se as operações de adição e multiplicação por*

$$[a] + [b] = [a + b] \quad e \quad [a] \cdot [b] = [ab],$$

onde $[a + b]$ e $[ab]$ denotam as classes dos inteiros $a + b$ e ab módulo m, respectivamente. Essas operações estão bem definidas e independem da escolha dos representantes das classes Niven, Zuckerman & Montgomery (2008).

Exemplo 7. *Seja $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$, $[2] + [4] = [1]$, pois 1 é o resto da divisão de $4 + 2 = 6$ por 5.*

Exemplo 8. *Seja $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$, $[2] \times [4] = [3]$, pois 3 é o resto da divisão de $4 \times 2 = 8$ por 5.*

A Estrutura Algébrica de $\mathbb{Z}_m$

O conjunto $\mathbb{Z}_m$, munido das operações de adição e multiplicação definidas por

$$[a] + [b] = [a + b] \quad \text{e} \quad [a] \cdot [b] = [ab],$$

possui a estrutura algébrica de um **anel comutativo com unidade**. O elemento neutro da adição é a classe $[0]$, enquanto o elemento neutro da multiplicação (unidade) é a classe $[1]$ Niven, Zuckerman & Montgomery (2008).

Em particular, quando o módulo m é um número primo, o conjunto $\mathbb{Z}_m$ adquire uma estrutura algébrica ainda mais rica, tornando-se um **corpo**, no qual todo elemento não nulo admite um inverso multiplicativo (Niven; Zuckerman; Montgomery, 2008).

Um conceito fundamental neste estudo é o de **inverso multiplicativo**.

Definição 7. *Dizemos que um elemento $[a] \in \mathbb{Z}_m$ possui inverso multiplicativo se existe $[b] \in \mathbb{Z}_m$ tal que*

$$[a] \cdot [b] = [1].$$

Sendo $\mathbb{Z}_m$ um anel, é natural investigar quais de seus elementos admitem inverso multiplicativo. O resultado a seguir, fundamental na Teoria das Congruências, caracteriza completamente esses elementos.

Proposição 1. *Um $[a] \in \mathbb{Z}_m$ é inversível se, e somente se, $mdc(a, m) = 1$.*

Niven, Zuckerman & Montgomery (2008)

Principais resultados

As congruências são compatíveis com as operações aritméticas básicas, o que as torna poderosas.

Proposição 2. *Sejam $a, b, c, d \in \mathbb{Z}$ e $m > 1$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

(i) $a + c \equiv b + d \pmod{m}$ *e* $a - c \equiv b - d \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

(iii) $a^k \equiv b^k \pmod{m}$ *para qualquer inteiro não negativo* k

(iv) Se $ac \equiv bc \pmod{m}$ *e* $mdc(c, m) = 1$*, então* $a \equiv b \pmod{m}$

2.7.1 Principais Teoremas relacionados a congruência modular

Com base na fundação da congruência modular, diversos teoremas foram desenvolvidos para resolver problemas e revelar propriedades profundas dos números. Eles formam a espinha dorsal de grande parte da teoria dos números moderna.

Aqui estão os principais teoremas que caracterizam a congruência modular:

Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat é um dos resultados mais importantes da Teoria dos Números e constitui a base de diversos algoritmos de criptografia. Ele estabelece uma propriedade fundamental dos números primos relacionada à potenciação modular, conforme apresentado em Niven, Zuckerman & Montgomery (2008).

Teorema 2. *Sejam $a, p \in \mathbb{Z}$ tal que p é primo então*

$$a^p \equiv a \pmod{p}$$

Corolário 1. *Se p é primo e p não divide a, então*

$$a^{p-1} \equiv 1 \pmod{p}$$

Exemplo 9. *Seja $p = 7$ e $a = 2$. Como 7 é primo e $mdc(2, 7) = 1$, o teorema garante que:*

$$2^{7-1} = 2^6 = 64 \equiv 1 \pmod{7}.$$

De fato, o resto da divisão de 64 por 7 é igual a 1.

Teorema de Euler

O Teorema de Euler pode ser visto como uma generalização do Pequeno Teorema de Fermat para módulos compostos. Ele introduz a **função totiente de Euler**, $\varphi(n)$, que conta o número de inteiros positivos menores ou iguais a n que são coprimos com n.

Teorema 3. *Se $n \in \mathbb{N}$ e $mdc(a, n) = 1$, então*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Niven, Zuckerman & Montgomery (2008)

Exemplo 10. *Seja $n = 10$. Os números coprimos com 10 são $\{1, 3, 7, 9\}$. Assim, $\varphi(10) = 4$.*
Seja $a = 3$. Como $mdc(3, 10) = 1$, o teorema garante que

$$3^{\varphi(10)} = 3^4 = 81 \equiv 1 \pmod{10}.$$

Observe que, se $p \in \mathbb{Z}$ é primo, então os números coprimos com p são $\{1, 2, 3, \ldots, p-1\}$ e, portanto, $\varphi(p) = p - 1$. Com essa observação, conclui-se que o Pequeno Teorema de Fermat é um caso particular do Teorema de Euler.

Teorema Chinês do Resto

O Teorema Chinês do Resto tem origem em um problema proposto pelo matemático chinês Sun-Tzu, no século I de nossa era. O problema consiste em determinar um número que deixe resto 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7. A resposta apresentada por Sun-Tzu foi o número 23, o que pode ser facilmente verificado. Na linguagem das congruências, esse problema corresponde a resolver o sistema

$$X \equiv 2 \pmod 3, \quad X \equiv 3 \pmod 5, \quad X \equiv 2 \pmod 7.$$

De modo geral, sistemas de congruências lineares podem ser resolvidos por meio do *Teorema Chinês do Resto*, cujo nome é atribuído a esse problema clássico. A seguir, apresentamos o seu enunciado.

Teorema 4 (Teorema Chinês do Resto)**.** *Se $m_1, m_2, \ldots, m_k$ são inteiros positivos dois a dois coprimos, então o sistema de congruências*

$$X \equiv a_1 \pmod{m_1}, \quad X \equiv a_2 \pmod{m_2}, \quad \ldots, \quad X \equiv a_k \pmod{m_k}$$

possui uma única solução módulo

$$M = m_1 m_2 \cdots m_k.$$

Essa solução pode ser escrita na forma

$$X \equiv M_1 a_1 y_1 + M_2 a_2 y_2 + \cdots + M_k a_k y_k \pmod M,$$

em que $M_i = \dfrac{M}{m_i}$ *e* y_i *é a solução da congruência*

$$M_i y_i \equiv 1 \pmod{m_i}, \quad \textit{para } i = 1, 2, \ldots, k.$$

Niven, Zuckerman & Montgomery (2008)

Exemplo 11. *Para o problema de Sun-Tsu observe que 3,5,7 são dois a dois coprimos. Escrevendo* $M = 3 \cdot 5 \cdot 7 = 105$ *temos que* $M_1 = 35$*,* $M_2 = 21$*,* $M_3 = 15$*,* $c_1 = 2$*,* $c_2 = 3$*,* $c_3 = 2$*, temos que* $y_1 = 2$ *é a solução de* $35y \equiv 1 \pmod 3$*,* $y_2 = 1$ *é a solução de* $21y \equiv 1 \pmod 5$ *e* $y_3 = 1$ *é a solução de* $15y \equiv 1 \pmod 7$*.*

Assim,

$$X = M_1 c_1 y_1 + M_2 c_2 y_2 + \cdots + M_k c_k y_k + M \cdot t = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$$

Observe que $233 \equiv 23 \pmod{105}$

3 METODOLOGIA

3.1 ABORDAGEM DA PESQUISA

A abordagem metodológica desta dissertação é de natureza qualitativa, por buscar a compreensão aprofundada do fenômeno da contextualização da Matemática e dos significados atribuídos pelos sujeitos da pesquisa, em oposição à mera quantificação de dados. Segundo Minayo (2014), a pesquisa qualitativa preocupa-se com o universo dos significados, motivos, aspirações, crenças, valores e atitudes, aspectos que não podem ser reduzidos a variáveis mensuráveis.

A estratégia central adotada é a Pesquisa-Ação, considerada adequada para o desenvolvimento de investigações que visam promover mudanças nas práticas pedagógicas, ao mesmo tempo em que contribuem para a formação continuada dos professores envolvidos. De acordo com Thiollent (2011), a pesquisa-ação caracteriza-se pela interação entre pesquisadores e participantes, com foco na resolução de problemas reais e na transformação da realidade investigada. Destaca-se que essa abordagem se organiza em ciclos reflexivos de planejamento, ação, observação e reflexão, garantindo um processo contínuo de análise e aprimoramento das práticas educativas.

A pesquisa foi estruturada em quatro fases distintas: fase exploratória e documental, implementação das atividades, coleta de dados e análise dos resultados, assegurando a sistematicidade e a coerência metodológica do estudo, conforme orienta Gil (2019).

3.2 CONTEXTO E SUJEITOS

O presente estudo foi desenvolvido em dois contextos distintos, o que permitiu uma análise comparativa da contextualização da Matemática em diferentes níveis de ensino. O primeiro contexto correspondeu a uma Escola Estadual do interior paulista, especificamente na 2ª série do Ensino Médio da E.E. Dom Bosco de Osvaldo Cruz. Participaram dessa etapa estudantes desse nível de ensino, escolhidos por se encontrarem na fase final da Educação Básica, momento considerado estratégico para o desenvolvimento da autonomia intelectual e para a preparação do estudante para a tomada de decisões no cotidiano, conforme orientações da Base Nacional Comum Curricular (Brasil, 2025).

O segundo contexto de aplicação ocorreu no Ensino Superior, envolvendo estudantes do 6º termo do curso de Pedagogia da Faculdade Reges de Osvaldo Cruz, com o objetivo de ampliar a discussão sobre a contextualização e a relevância da Matemática na formação de futuros educadores. Dessa forma, buscou-se analisar como a contextualização matemática pode contribuir tanto para a aprendizagem discente quanto para a prática docente futura.

Os sujeitos participantes do estudo foram constituídos pelos estudantes das turmas mencionadas e pela professora de Matemática responsável pela intervenção pedagógica, totalizando trinta estudantes do Ensino Médio e treze discentes do curso de Pedagogia.

3.3 DESCRIÇÃO DAS ATIVIDADES

A intervenção didática proposta nesta dissertação concentrou-se na contextualização do conteúdo de Matrizes por meio da aplicação da Cifra de Hill no contexto da criptografia, método clássico introduzido por Hill em 1931 Hill (1931). A atividade foi desenvolvida e aplicada tanto aos estudantes da 2ª série do Ensino Médio da E.E. Dom Bosco quanto aos alunos do 6º termo do curso de Pedagogia da Faculdade Reges de Osvaldo Cruz.

O objetivo central foi evidenciar a aplicabilidade prática das operações matriciais, como a multiplicação de matrizes e o cálculo da matriz inversa, na área da segurança da informação, transformando o estudo do conteúdo em uma dinâmica lúdica de "agente secreto". Segundo D'Ambrosio (2004), a contextualização favorece a atribuição de significado aos conteúdos matemáticos, aproximando-os da realidade dos estudantes e ampliando o engajamento no processo de aprendizagem.

A atividade seguiu um fluxo de trabalho que incluiu a conversão de mensagens textuais em códigos numéricos, utilizando uma tabela de correspondência, a codificação da mensagem por meio da multiplicação pela matriz-chave e, posteriormente, a decodificação utilizando a matriz inversa para a recuperação da mensagem original. Essa abordagem buscou superar a visão excessivamente abstrata das matrizes, reforçando a relevância da Álgebra Linear em contextos tecnológicos e no cotidiano contemporâneo.

3.4 INSTRUMENTOS DE COLETA E ANÁLISE

Para a coleta dos dados necessários à pesquisa-ação e para a avaliação do impacto da contextualização no Ensino Médio (E.E. Dom Bosco) e no Ensino Superior (Faculdade Reges de Osvaldo Cruz), foram utilizados diferentes instrumentos de investigação.

O principal instrumento empregado foi o questionário, aplicado nos momentos pré e pós-intervenção, com o objetivo de identificar o conhecimento prévio dos estudantes e suas percepções acerca da utilidade da Matemática. Foram utilizados dois questionários, um diagnóstico (pré-teste) e outro avaliativo (pós-teste), aplicados antes e após a realização das atividades envolvendo matrizes, criptografia (Cifra de Hill). Os instrumentos foram elaborados de forma alinhada, permitindo a comparação item a item dos conhecimentos prévios, percepções e aprendizagens desenvolvidas ao longo da proposta didática.

O pré-teste teve como objetivo identificar o nível inicial de familiaridade dos estudantes com matrizes, criptografia e aplicações geométricas, enquanto o pós-teste buscou verificar a consolidação conceitual, a compreensão das aplicações e a mudança de percepção em relação ao conteúdo. Esse alinhamento possibilitou a obtenção de dados quantitativos de caráter descritivo, utilizados como suporte à análise qualitativa, a qual constituiu o eixo central da interpretação dos resultados.

O quadro 1 apresenta o alinhamento entre o questionário diagnóstico (pré-teste) e o questionário avaliativo (pós-teste), evidenciando a correspondência entre os itens de ambos os

instrumentos e os constructos avaliados. Esse alinhamento foi planejado de forma intencional, permitindo a comparação direta dos conhecimentos prévios dos estudantes com as aprendizagens desenvolvidas ao longo da proposta didática.

No pré-teste, as questões foram elaboradas com o objetivo de identificar a familiaridade inicial dos estudantes com o conceito de matriz, suas possíveis aplicações e o contato prévio com temas como criptografia, mosaicos geométricos e uso de tecnologias educacionais. Já no pós-teste, as questões correspondentes buscaram verificar a consolidação conceitual desses conteúdos, bem como a ampliação da compreensão sobre aplicações específicas, como a Cifra de Hill.

O pareamento item a item entre os questionários possibilitou não apenas uma análise quantitativa dos resultados, por meio da comparação das respostas antes e depois da intervenção, mas também uma análise qualitativa, especialmente nas questões discursivas. Essas questões permitiram identificar mudanças de percepção, maior clareza conceitual e a capacidade dos estudantes de articular a Álgebra Linear com contextos aplicados, tecnológicos e interdisciplinares.

Dessa forma, o uso de instrumentos avaliativos alinhados fortalece a consistência metodológica da pesquisa, uma vez que torna explícito o percurso de aprendizagem dos estudantes. Além disso, esse procedimento contribui para evidenciar o impacto da proposta didática, ao permitir verificar se os objetivos de aprendizagem relacionados ao uso de matrizes em criptografia e mosaicos geométricos foram efetivamente alcançados.

O questionário diagnóstico foi composto por doze questões de múltipla escolha voltadas à avaliação objetiva do conteúdo, e duas questões dissertativas (apêndice E), destinadas à compreensão aprofundada das argumentações e reflexões dos participantes, conforme recomenda Gil (2019).

Já o questionário pós aplicação da atividade foi composto por dez questões de múltipla escolha e quatro questões dissertativas (apêndice F).

De forma complementar, utilizou-se a observação participante, que possibilitou o registro das interações, do envolvimento e das atitudes dos estudantes durante o desenvolvimento das atividades, bem como o diário de campo, no qual a pesquisadora anotou impressões, reflexões e eventos significativos observados ao longo do processo.

Os dados qualitativos obtidos, especialmente as respostas dissertativas e os registros do diário de campo, foram analisados por meio da Análise de Conteúdo, técnica proposta por Bardin (2016), que permite a organização, categorização e interpretação dos dados, favorecendo a identificação de padrões de compreensão, dificuldades recorrentes, avanços conceituais e mudanças de percepção dos estudantes em relação ao uso das matrizes em contextos aplicados.

Ressalta-se que, embora alguns dados numéricos tenham sido utilizados para fins de organização e comparação entre os momentos pré e pós-intervenção, a presente pesquisa não teve como objetivo a generalização estatística dos resultados. A análise concentrou-se na interpretação qualitativa das produções dos estudantes, de suas percepções, argumentações e mudanças conceituais, buscando compreender o impacto pedagógico da proposta didática no processo de

aprendizagem.

4 APLICAÇÕES E PROPOSTAS DIDÁTICAS

Este capítulo apresenta os procedimentos realizados com estudantes da 2ª série do Ensino Médio da E.E. Dom Bosco (GRUPO 1) e com acadêmicos do 6º termo do curso de Pedagogia da Faculdade Reges de Osvaldo Cruz (GRUPO 2). O objetivo do questionário foi investigar o conhecimento prévio, as percepções e as sugestões dos participantes acerca das aplicações de matrizes em criptografia, tomando a Cifra de Hill como eixo de contextualização.

A aplicação de matrizes no domínio da criptografia configura-se como uma estratégia pedagógica relevante para superar a natureza frequentemente abstrata da Álgebra Linear, ao conferir sentido e atratividade ao estudo de operações como multiplicação e inversão de matrizes. Nessa perspectiva, a contextualização favorece a atribuição de significado aos conteúdos matemáticos e pode ampliar o engajamento discente ao aproximar conceitos formais de situações reconhecíveis do cotidiano e da tecnologia (D'Ambrosio, 2004; Lorenzato, 2006). Nesse panorama, a Cifra de Hill emerge como um contexto prático robusto e historicamente relevante por demonstrar, de modo concreto, o uso de matrizes na proteção e ocultação de informações (Hill, 1931). Além disso, por envolver procedimentos operacionais claros (codificação e decodificação), a proposta didática mobiliza conteúdos basilares, notadamente a multiplicação de matrizes para a etapa de cifragem e, de forma crucial, o uso da matriz inversa no processo de decifragem, favorecendo uma aprendizagem mais profunda ao articular técnica, significado e propósito (Hill, 1931; Barichello, s.d.).

4.1 CRIPTOGRAFIA

A criptografia acompanha a evolução da comunicação humana e a necessidade de proteger informações em diferentes contextos (políticos, militares, comerciais e tecnológicos). No cenário contemporâneo, seu papel torna-se ainda mais evidente na realidade digital, em aplicações como transações financeiras, autenticação e comunicações pessoais.

Do ponto de vista conceitual, entende-se criptografia como o conjunto de métodos e técnicas para codificar (cifrar) e decodificar (decifrar) mensagens, de modo que apenas destinatários autorizados consigam recuperar o conteúdo. Em contraste, a criptoanálise dedica-se ao estudo de técnicas de quebra ou recuperação de mensagens sem acesso à chave.

No contexto desta dissertação, a criptografia é abordada como um campo fértil para a contextualização de conteúdos matemáticos, sobretudo por articular operações algébricas, aritmética modular e estruturas algébricas em situações concretas, como ocorre na Cifra de Hill (Hill, 1931; Niven; Zuckerman; Montgomery, 2008).

Cifra de César

A Cifra de César é uma técnica clássica de criptografia por substituição, na qual cada letra do texto original é substituída por outra letra obtida por um deslocamento fixo no alfabeto. Por ser uma cifra simétrica, a mesma chave (o número de deslocamentos) é usada tanto para cifrar quanto para decifrar. Em termos matemáticos, ao representar as letras por números (por exemplo, de 0 a 25), a cifragem pode ser descrita por uma congruência do tipo

$$C \equiv P + k \pmod{26},$$

em que P representa o símbolo do texto claro, k a chave e C o símbolo cifrado, com operações realizadas em aritmética modular (Niven; Zuckerman; Montgomery, 2008).

Cifra de Hill

A Cifra de Hill, proposta por Lester S. Hill, foi uma das primeiras técnicas a empregar explicitamente conceitos de Álgebra Linear na criptografia, por meio do uso de matrizes e operações modulares para cifrar blocos de texto (Hill, 1931). Diferentemente de cifras de substituição simples, a cifra de Hill opera por blocos (pares, trios etc.), o que, em geral, aumenta a difusão dos símbolos e torna a estrutura da transformação menos evidente, especialmente em comparação com deslocamentos letra a letra (Hill, 1931).

Embora historicamente relevante, o método apresenta vulnerabilidades conhecidas em cenários de ataque com texto conhecido, sobretudo para matrizes pequenas, razão pela qual foi substituído por algoritmos mais complexos em aplicações reais. Ainda assim, permanece amplamente utilizado em contextos educacionais, por permitir explorar de modo articulado conteúdos como multiplicação de matrizes, determinante, invertibilidade e matriz inversa, além de congruências modulares (Hill, 1931; Barichello, s.d.).

Codificação

A codificação na Cifra de Hill baseia-se em conceitos de Álgebra Linear, particularmente matrizes e vetores. A ideia central é transformar um bloco de texto em um bloco cifrado a partir da multiplicação de uma matriz-chave por um vetor numérico associado ao texto, reduzindo os resultados módulo 26 (no caso do alfabeto latino) (Hill, 1931; Niven; Zuckerman; Montgomery, 2008).

4.2 A MATEMÁTICA DA CIFRA DE HILL: ARITMÉTICA MODULAR E INVERSÃO EM $\mathbb{Z}_{26}$

Para que o processo de decodificação na Cifra de Hill seja possível, não basta que a matriz chave A seja invertível no conjunto dos Números Reais ($\mathbb{R}$). É necessário que ela possua uma inversa dentro do conjunto das classes de restos módulo 26, denotado por $\mathbb{Z}_{26}$.

4.2.1 Condição de Existência da Inversa

Diferente da álgebra linear convencional, onde basta que $\det(A) \neq 0$, na aritmética modular a matriz A é invertível se, e somente se, o seu determinante é coprimo com o módulo n. No caso do nosso alfabeto ($n = 26$):

$$\text{mdc}(\det(A), 26) = 1 \tag{1}$$

Esta condição implica que $\det(A)$ não pode ser um número par e nem múltiplo de 13. Caso contrário, a função de criptografia não seria bijetora, impossibilitando a recuperação da mensagem original de forma única.

4.2.2 Cálculo da Matriz Inversa Módulo 26

O cálculo da matriz inversa $A^{-1} \pmod{26}$ segue três etapas fundamentais:

1. **Cálculo do Determinante:** Calcula-se $d = \det(A)$ da forma usual.
2. **Cálculo do Inverso Modular do Determinante:** Busca-se um número d^{-1} tal que:

$$d \cdot d^{-1} \equiv 1 \pmod{26} \tag{2}$$

   Este valor pode ser encontrado via Algoritmo de Euclides Estendido ou por inspeção direta para valores pequenos.

3. **Aplicação da Matriz Adjunta:** A inversa é obtida por:

$$A^{-1} = d^{-1} \cdot \text{adj}(A) \pmod{26} \tag{3}$$

Exemplo Prático: Seja a matriz chave $A = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$.

- $\det(A) = (3 \cdot 5) - (3 \cdot 2) = 15 - 6 = 9$.
- Como $\text{mdc}(9, 26) = 1$, a inversa existe.
- O inverso de $9 \pmod{26}$ é 3, pois $9 \cdot 3 = 27 \equiv 1 \pmod{26}$.
- A matriz adjunta (trocando a diagonal principal e invertendo sinais da secundária) é $\begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix}$.
- $A^{-1} = 3 \cdot \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 15 & -9 \\ -6 & 9 \end{pmatrix}$.
- Ajustando os valores negativos para o intervalo $[0, 25]$, temos: $-9 \equiv 17$ e $-6 \equiv 20$.

- Portanto, $A^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \pmod{26}$.

4.3 DESENVOLVIMENTO EDUCACIONAL

De forma geral, procede-se da seguinte maneira:

- convertem-se letras em números (por exemplo, $A \mapsto 0$, $B \mapsto 1$, ..., $Z \mapsto 25$);
- agrupam-se os símbolos em blocos de tamanho n;
- multiplica-se cada bloco (vetor) pela matriz-chave A (matriz $n \times n$);
- reduz-se cada componente do vetor resultante módulo 26;
- convertem-se os números de volta em letras, obtendo o texto cifrado.

Esse encadeamento torna-se especialmente didático por exigir, de maneira situada, o domínio de operações matriciais e de aritmética modular, reforçando a pertinência do conteúdo na segurança da informação (Hill, 1931; Baggio; Schossler; Dullius, 2010).

A matriz codificadora deve ser invertível no anel $\mathbb{Z}_{26}$, condição essencial para que o processo de decodificação seja possível e unívoco. Em particular, exige-se que $\det(A)$ seja coprimo com 26, isto é, $mdc(\det(A), 26) = 1$ (Niven; Zuckerman; Montgomery, 2008). Essa exigência abre espaço para discussões didáticas sobre determinante, inversa e invertibilidade em aritmética modular, consolidando o significado desses conceitos para além da manipulação algébrica (**????**).

Tabela 4 – Tabela de Correspondência.

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
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Elaborada pela autora.

Descrição do método (ordem 2)

Para uma cifra de Hill de ordem 2, procede-se como segue (Hill, 1931; Barichello, s.d.):

1. Escolhe-se uma matriz codificadora

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathbb{Z}^{2\times 2}. \tag{4}$$

2. Divide-se o texto em pares de letras; se o número de letras for ímpar, adiciona-se um *padding* (por exemplo, uma letra neutra).

3. Cada par (p_1, p_2) é convertido para um vetor coluna

$$p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}, \quad p_i \in \{0, 1, \ldots, 25\}. \tag{5}$$

4. Aplica-se a multiplicação matricial e a redução módulo 26

$$q \equiv A\,p \pmod{26}. \tag{6}$$

5. Cada componente de q é convertido de volta em letra usando a Tabela 4.

Essa versão é chamada de *2-cifra de Hill*. O procedimento generaliza naturalmente para matrizes $n \times n$ e blocos de n letras (Hill, 1931).

Exemplo 12. *Vamos codificar a mensagem MATRIZ. Primeiro, separa-se o texto em pares de letras:*

M	A	-	T	R	-	I	Z

Tabela 5 – Separação em pares.

Em seguida, substitui-se cada letra por seu número correspondente (Tabela 4):

12	0	-	19	17	-	8	25

Tabela 6 – Conversão letra–número.

Escreve-se cada par de números como um vetor coluna p e calculam-se os vetores cifrados q por $q \equiv Ap \pmod{26}$ (Hill, 1931; Barichello, s.d.).

Considere a matriz codificadora

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

1. Par MA

$$p = \begin{pmatrix} 12 \\ 0 \end{pmatrix}, \quad q = Ap = \begin{pmatrix} 36 \\ 60 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 8 \end{pmatrix} \pmod{26}. \tag{7}$$

2. Par TR

$$p = \begin{pmatrix} 19 \\ 17 \end{pmatrix}, \quad q = Ap = \begin{pmatrix} 74 \\ 129 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 25 \end{pmatrix} \pmod{26}. \tag{8}$$

3. Par IZ

$$p = \begin{pmatrix} 8 \\ 25 \end{pmatrix}, \quad q = Ap = \begin{pmatrix} 49 \\ 90 \end{pmatrix} \equiv \begin{pmatrix} 23 \\ 12 \end{pmatrix} \pmod{26}. \tag{9}$$

Logo, os pares numéricos cifrados são $(10, 8)$*,* $(22, 25)$*,* $(23, 12)$*, que correspondem às letras* (K, I)*,* (W, Z)*,* (X, M)*. Assim, a mensagem codificada é* ***KIWZXM****.*

Observa-se que a matriz A deve ser invertível em $\mathbb{Z}_{26}$, isto é, deve satisfazer $mdc(\det A, 26) = 1$, para garantir decodificação única (Niven; Zuckerman; Montgomery, 2008). Embora o exemplo utilize o caso 2×2, o procedimento generaliza para $n \times n$ (Hill, 1931). A escolha do *padding* e a verificação de invertibilidade são etapas essenciais do método (Barichello, s.d.).

Decodificação

Para decodificar uma mensagem cifrada via Hill, utiliza-se procedimento análogo ao da codificação, porém aplicando a matriz inversa A^{-1} (módulo 26). Portanto, só é possível decodificar se A for invertível em $\mathbb{Z}_{26}$, ou seja, se $\det(A)$ for coprimo com 26 (Niven; Zuckerman; Montgomery, 2008; Hill, 1931).

Suponha que recebemos o texto cifrado em pares numéricos q. Para cada par, formamos

$$q = \begin{pmatrix} q_1 \\ q_2 \end{pmatrix}, \quad p \equiv A^{-1}q \pmod{26}, \tag{10}$$

em que p é o vetor do texto original. Em seguida, convertem-se os números de p de volta para letras na Tabela 4 (Barichello, s.d.).

Exemplo 13. *Decodificando* ***KIWZXM****. Considerando a matriz inversa (módulo 26)*

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix},$$

decodificaremos os pares $(KI), (WZ), (XM)$*, ou em números* $(10, 8), (22, 25), (23, 12)$ *(Barichello, s.d.; Hill, 1931).*

$$q^{(1)} = \begin{pmatrix} 10 \\ 8 \end{pmatrix}, \quad p^{(1)} = A^{-1}q^{(1)} = \begin{pmatrix} 12 \\ -26 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 0 \end{pmatrix} \pmod{26}. \tag{11}$$

$$q^{(2)} = \begin{pmatrix} 22 \\ 25 \end{pmatrix}, \quad p^{(2)} = A^{-1}q^{(2)} = \begin{pmatrix} 19 \\ -35 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 17 \end{pmatrix} \pmod{26}. \tag{12}$$

$$q^{(3)} = \begin{pmatrix} 23 \\ 12 \end{pmatrix}, \quad p^{(3)} = A^{-1}q^{(3)} = \begin{pmatrix} 34 \\ -79 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 25 \end{pmatrix} \pmod{26}. \tag{13}$$

Convertendo para letras:

$$(12, 0) \to (M, A), \quad (19, 17) \to (T, R), \quad (8, 25) \to (I, Z).$$

Portanto, a mensagem decodificada é ***MATRIZ****.*

Por fim, destaca-se que, ao simular uma situação realista de segurança da informação, a atividade contribui para consolidar a compreensão de matriz inversa como elemento fundamental para reverter a transformação e reestabelecer o significado da mensagem, conectando o conteúdo formal a uma aplicação reconhecível (Hill, 1931; Baggio; Schossler; Dullius, 2010).

Considerações didáticas sobre a escolha da matriz-chave

Na elaboração da atividade prática aplicada aos estudantes, detalhada no Apêndice D, a escolha da matriz-chave utilizada no processo de codificação foi orientada por critérios didáticos e metodológicos. Optou-se, em uma das etapas iniciais da proposta, por uma matriz cujo determinante é igual a 1, de modo a simplificar o cálculo da matriz inversa no contexto da aritmética modular. Essa decisão teve como objetivo evitar uma sobrecarga operacional excessiva, especialmente no primeiro contato dos estudantes com a Cifra de Hill, permitindo que o foco permanecesse na compreensão conceitual das operações matriciais envolvidas e no significado do processo de codificação e decodificação de mensagens.

Ressalta-se, contudo, que tal simplificação não compromete o rigor matemático da atividade, uma vez que a condição fundamental para a invertibilidade da matriz, a coprimalidade do determinante com o módulo 26, é preservada. Ademais, a proposta não se limita a esse caso particular, sendo plenamente possível, em momentos posteriores ou em atividades de aprofundamento, a utilização de matrizes cujo determinante seja diferente de 1, desde que coprimo com 26, como 3, 5 ou 7. Dessa forma, a escolha adotada no Apêndice D configura-se como uma decisão pedagógica intencional, alinhada ao nível dos estudantes e aos objetivos formativos da sequência didática, sem prejuízo da generalidade do método nem da consistência matemática do conteúdo abordado.

Em síntese, a sequência didática apresentada neste capítulo organiza o ensino de matrizes a partir de um percurso progressivo, no qual cada etapa contribui para a consolidação de conceitos matemáticos específicos e para o fortalecimento da prática docente. Inicialmente, a introdução da criptografia e de cifras clássicas favorece a compreensão da aritmética modular e da correspondência letra–número, estabelecendo uma base conceitual acessível. Em seguida, a Cifra de Hill permite integrar, de forma articulada, a multiplicação de matrizes, o cálculo de determinantes e a noção de matriz inversa em um contexto significativo, no qual a codificação e a decodificação de mensagens atribuem sentido às operações algébricas. Para o professor, essa organização proporciona uma alternativa metodológica que supera a abordagem excessivamente abstrata da Álgebra Linear, oferecendo um roteiro estruturado de atividades que favorece o

engajamento discente, a visualização do papel funcional das matrizes e a consolidação dos conceitos ao longo de um processo coerente e contextualizado.

5 MATRIZES COMO FERRAMENTA DIDÁTICA

Este capítulo apresenta a análise dos resultados obtidos a partir da aplicação da sequência didática proposta, fundamentada na contextualização do ensino de matrizes por meio da Criptografia, especificamente da Cifra de Hill. A análise tem caráter qualitativo, conforme definido no Capítulo 3, e busca interpretar os dados coletados à luz dos objetivos da pesquisa e do referencial teórico adotado.

Os dados analisados foram obtidos por meio de questionários aplicados antes e após a intervenção pedagógica, observação do estudante e registros em diário de campo. Esses instrumentos permitiram avaliar não apenas o desempenho dos estudantes, mas também suas percepções, níveis de engajamento e compreensão conceitual acerca das aplicações das matrizes.

5.1 ANÁLISE DOS RESULTADOS DO QUESTIONÁRIO DIAGNÓSTICO E AVALIATIVO

A aplicação do questionário diagnóstico teve como objetivo identificar os conhecimentos prévios dos participantes em relação ao conteúdo de matrizes e suas aplicações, enquanto o questionário avaliativo buscou verificar possíveis mudanças decorrentes da intervenção didática.

Esse aumento não deve ser interpretado apenas como melhora no desempenho pontual, mas como um indício de que a abordagem contextualizada favoreceu a reorganização dos esquemas conceituais dos estudantes. Ao relacionar as operações matriciais a uma situação com propósito definido, a codificação e decodificação de mensagens levam os estudantes a mobilizar os conceitos de forma mais integrada e consciente.

Do ponto de vista pedagógico, esse avanço não pode ser interpretado apenas como um ganho procedimental. A análise das respostas sugere que os alunos passaram a compreender as matrizes como ferramentas matemáticas dotadas de finalidade, e não apenas como tabelas numéricas utilizadas para a execução de cálculos mecânicos. Tal mudança de perspectiva aproxima-se do que Skemp (1976) define como aprendizagem relacional, na qual o estudante entende o porquê dos procedimentos adotados.

5.2 ANÁLISE DAS QUESTÕES DISSERTATIVAS

As questões dissertativas permitiram uma compreensão mais aprofundada das percepções e argumentações dos participantes. A análise dessas respostas foi realizada com base nos pressupostos da Análise de Conteúdo, conforme proposta por Bardin (2016), possibilitando a identificação de categorias emergentes.

Entre as categorias identificadas, destacam-se: (i) compreensão conceitual das matrizes, (ii) percepção de aplicabilidade da Matemática e (iii) engajamento e motivação para a aprendizagem.

No que se refere à compreensão conceitual, observou-se que muitos estudantes passaram a associar diretamente os conceitos de determinante, matriz inversa e aritmética modular ao processo de codificação e decodificação de mensagens. Esse resultado evidencia que a contextualização por meio da criptografia contribuiu para a integração dos conteúdos, evitando a fragmentação frequentemente observada no ensino de Álgebra Linear.

Essa integração sugere que os estudantes deixaram de perceber os conceitos de forma isolada, passando a compreendê-los como partes de um mesmo sistema conceitual. Tal movimento é particularmente relevante no ensino de Álgebra Linear, área em que a fragmentação conceitual frequentemente dificulta a aprendizagem significativa.

Quanto à percepção de aplicabilidade, as respostas indicaram que os participantes passaram a reconhecer a presença das matrizes em contextos tecnológicos do cotidiano, como segurança da informação e comunicação digital. Esse aspecto reforça as contribuições de D'Ambrosio (2004) e Lorenzato (2006), que defendem a contextualização como elemento essencial para a atribuição de significado aos conteúdos matemáticos.

5.3 ANÁLISE DA OBSERVAÇÃO DO ESTUDANTE E DO DIÁRIO DE CAMPO

Os registros obtidos por meio da observação participante e do diário de campo revelaram um aumento significativo no engajamento dos estudantes durante a realização das atividades. Foram observadas maior participação nas discussões, colaboração entre os alunos e interesse em compreender o funcionamento do processo criptográfico.

Esse engajamento pode ser interpretado como resultado direto da atribuição de sentido à atividade matemática. Ao assumir papéis ativos no processo de codificação e decodificação, os estudantes passaram a se reconhecer como agentes do próprio aprendizado, o que favoreceu a autonomia intelectual e a participação efetiva nas discussões.

Essas observações sugerem que o caráter investigativo e lúdico da atividade contribuiu para reduzir a resistência inicial em relação ao conteúdo de matrizes. Ao assumir o papel de "agentes secretos" responsáveis por codificar e decodificar mensagens, os estudantes envolveram-se ativamente no processo de aprendizagem, o que favoreceu a construção do conhecimento de forma mais autônoma.

Do ponto de vista educacional, esse comportamento confirma que propostas pedagógicas contextualizadas podem atuar como mediadoras entre o conhecimento formal e a experiência do aluno, ampliando o interesse e a participação em sala de aula.

5.4 COMPARAÇÃO ENTRE OS CONTEXTOS DE APLICAÇÃO

A aplicação da sequência didática em dois contextos distintos — Ensino Médio e Ensino Superior (curso de Pedagogia) — permitiu uma análise comparativa dos resultados obtidos.

No Ensino Médio, observou-se maior avanço na compreensão operacional dos conceitos matriciais, especialmente no que diz respeito ao uso da matriz inversa e da aritmética modular na

decodificação das mensagens. Já no Ensino Superior, destacou-se a ampliação da percepção dos futuros professores sobre a relevância da Matemática e suas aplicações, bem como a possibilidade de utilização de metodologias contextualizadas em sua prática docente futura.

A diferença de enfoque entre os grupos evidencia que a proposta didática apresenta flexibilidade e potencial de adaptação a diferentes níveis de ensino, reforçando sua pertinência tanto para a aprendizagem discente quanto para a formação de professores.

Essa diferença indica que a mesma sequência didática pode assumir funções pedagógicas distintas conforme o nível de ensino, atuando ora como instrumento de consolidação conceitual, ora como elemento formativo para a prática docente. Tal versatilidade reforça o potencial do produto educacional desenvolvido e sua adequação a diferentes contextos educacionais.

5.5 SÍNTESE INTERPRETATIVA DOS RESULTADOS

De maneira geral, os resultados obtidos indicam que a contextualização do ensino de matrizes por meio da criptografia contribuiu significativamente para a aprendizagem dos estudantes. A integração entre teoria e aplicação favoreceu a compreensão conceitual, o engajamento e a atribuição de significado aos conteúdos matemáticos trabalhados.

Embora a pesquisa não tenha como objetivo a generalização estatística dos resultados, os dados analisados permitem afirmar que a proposta apresentou impacto pedagógico positivo nos contextos investigados. Assim, os resultados corroboram a hipótese de que a utilização de aplicações contextualizadas, como a Criptografia, pode constituir uma estratégia eficaz para superar a abordagem excessivamente abstrata do ensino de matrizes.

Essas conclusões reforçam a relevância do produto educacional desenvolvido e indicam possibilidades de ampliação da proposta em trabalhos futuros, envolvendo outros conteúdos da Matemática e diferentes contextos educacionais.

5.6 CRIPTOGRAFIA COMO FERRAMENTA DIDÁTICA NO ENSINO MÉDIO E NO CURSO DE PEDAGOGIA NO ENSINO SUPERIOR

Foi proposta uma atividade pedagógica voltada à 2ª série do Ensino Médio e ao 6º termo do curso de Pedagogia, cujo objetivo consiste em proporcionar aos estudantes uma compreensão introdutória da criptografia por meio da multiplicação de matrizes e do uso da aritmética modular. Para a aplicação da atividade, adotou-se a metodologia ativa denominada *Sala de Aula Invertida*, na qual os estudantes têm contato prévio com o conteúdo antes do encontro presencial (Bergmann; Sams, 2012).

Inicialmente, a autora realizou uma revisão das operações matriciais e apresentou a congruência módulo 26, associada ao alfabeto latino. Foi disponibilizado aos estudantes um vídeo gravado pela autora deste trabalho, bem como uma atividade (Apêndice A), para que, organizados em grupos, preparassem a apresentação a ser realizada na aula seguinte.

Como produto educacional associado a esta dissertação, foi elaborado um vídeo didático que apresenta a aplicação da atividade proposta como é possível ver na Figura 1 elaborado por Gines (2025).

Figura 1 – Vídeo de orientação.

Fonte: Elaborado pelo autor (2025).

Objetivos da Atividade

- Trabalhar a multiplicação de matrizes 2×2 em um contexto aplicado;
- Aplicar conceitos de aritmética modular (módulo 26);
- Introduzir noções básicas de criptografia e codificação de mensagens;
- Estimular o raciocínio lógico, crítico e interdisciplinar;
- Promover o engajamento dos estudantes por meio de um tema contemporâneo.

Um exemplo de aplicação de atividade

Enunciado

Considere a matriz-chave a seguir utilizada para codificar pares de letras:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Deseja-se codificar a palavra **"HI"**, utilizando a Cifra de Hill. Para isso:

1. Converta as letras da palavra para números (A=0, B=1, ..., Z=25);
2. Escreva a palavra como um vetor coluna;
3. Multiplique a matriz K pelo vetor e aplique o módulo 26;
4. Converta os números resultantes de volta para letras.

Resolução da Codificação

Conversão das letras

- H $\rightarrow$ 7
- I $\rightarrow$ 8

Mensagem em forma vetorial:

$$M = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$$

Multiplicação matricial:

$$C = K \cdot M = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 45 \\ 54 \end{bmatrix}$$

Aplicando módulo 26:

$$C = \begin{bmatrix} 19 \\ 2 \end{bmatrix}$$

Mensagem criptografada:

- 19 $\rightarrow$ T
- 2 $\rightarrow$ C

Resultado: a palavra "HI" é codificada como **"TC"**.

Resolução da Decodificação

Para recuperar a mensagem original, é necessário utilizar a matriz inversa de K no módulo 26.

Cálculo do determinante

$$\det(K) = (3 \cdot 5) - (3 \cdot 2) = 9$$

Como $9^{-1} \equiv 3 \pmod{26}$, a matriz é invertível em $\mathbb{Z}_{26}$.

Matriz inversa

$$K^{-1} = 3 \cdot \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \equiv \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \pmod{26}$$

Aplicando à mensagem cifrada:

$$M = K^{-1} \cdot C = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$$

Mensagem original: “HI”.

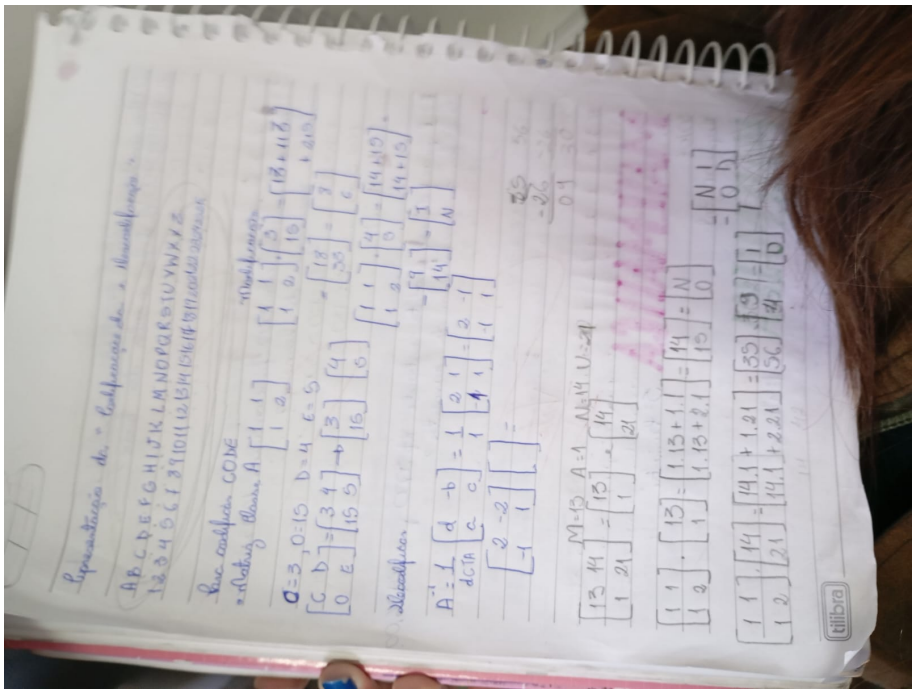
Considerações Didáticas

A atividade apresentada constitui uma estratégia eficaz para explorar, de forma prática e contextualizada, conteúdos da Álgebra Matricial e da aritmética modular. Além disso, a utilização de recursos computacionais pode potencializar a compreensão conceitual e favorecer a validação dos resultados obtidos (Borba; Silva; Gadanidis, 2014).

5.7 GRUPO 1

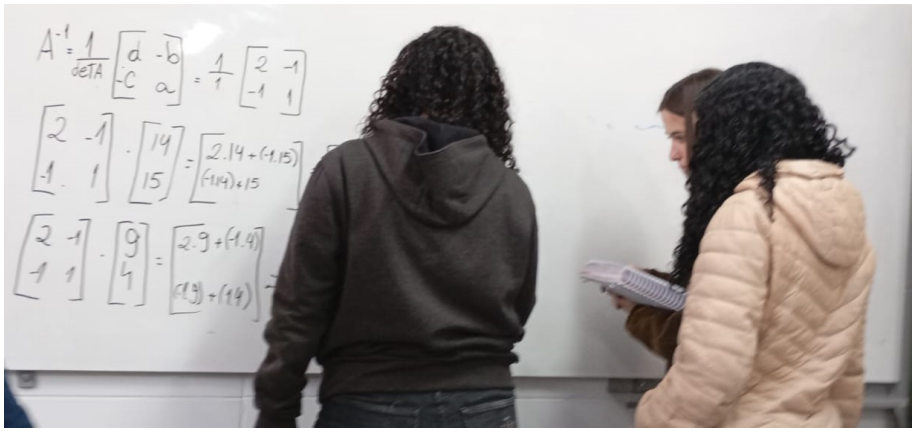
A turma foi composta por 24 estudantes, organizados em quatro grupos. A dinâmica adotada evidenciou o protagonismo estudantil, favorecendo autonomia, colaboração e comunicação matemática, aspectos centrais das metodologias ativas (Bergmann; Sams, 2012). É possível ver a aplicação na Figura 2, Figura 3 e Figura 4

Figura 2 – Registro da atividade na 2ª série do Ensino Médio.



Fonte: Elaborado pelo autor (2025).

Figura 3 – Seminário do primeiro grupo de alunos.



Fonte: Elaborado pelo autor (2025).

Figura 4 – Seminário do segundo grupo de alunos.

Fonte: Elaborado pelo autor (2025).

5.8 GRUPO 2

A atividade foi aplicada a 13 estudantes do 6º termo do curso de Pedagogia. Observou-se que a contextualização por meio da criptografia contribuiu para ressignificar a relação dos licenciandos com a Matemática, tradicionalmente marcada por experiências negativas (Lorenzato, 2006).

6 CONSIDERAÇÕES FINAIS

O presente trabalho de dissertação propôs e avaliou a aplicação da Cifra de Hill como estratégia metodológica para o ensino de Matrizes. A abordagem teve como objetivo primordial não apenas a transmissão do conhecimento técnico, mas também a promoção do **engajamento** e da **compreensão contextualizada** dos conceitos de Álgebra Linear.

6.1 SÍNTESE DOS RESULTADOS E IMPACTO PEDAGÓGICO

A intervenção demonstrou a eficácia da Cifra de Hill como ferramenta lúdica e interdisciplinar. Os resultados apontaram para:

- **Aumento da Motivação:** Foi observável um crescimento significativo no interesse e na participação dos estudantes, transformando o estudo de Matrizes de uma série de cálculos mecânicos em um **desafio intelectual** e um jogo de decodificação.
- **Melhoria na Compreensão Conceitual:** A necessidade de decodificar mensagens forçou os alunos a internalizar a lógica por trás de operações complexas, como a **multiplicação de matrizes** e, crucialmente, o cálculo da **matriz inversa** e **determinantes**, elementos fundamentais para a criptografia.
- **Conexão Prática:** A aplicação da Criptografia estabeleceu uma ponte clara entre a Matemática abstrata e a **segurança de dados** no mundo real, reforçando a relevância do conteúdo.

6.2 CONTRIBUIÇÕES DO TRABALHO

Esta dissertação oferece contribuições significativas para o campo do Ensino de Matemática:

- **Metodologia validada:** proposição de um material didático e de um plano de aula que integram **Álgebra Linear e Criptografia**, validados em contexto escolar.
- **Inovação pedagógica:** o trabalho configura-se como um referencial para o uso de **metodologias ativas** no ensino de Matrizes, promovendo a interdisciplinaridade e o desenvolvimento de habilidades de raciocínio lógico-matemático.
- **Alinhamento curricular:** demonstra como o conteúdo de Matrizes pode ser abordado de forma **contextualizada**, em consonância com as diretrizes curriculares nacionais.

6.3 MATRIZES E A BASE NACIONAL COMUM CURRICULAR (BNCC)

O modelo de ensino proposto atende diretamente aos preceitos da Base Nacional Comum Curricular (BNCC) para a área de Matemática e suas Tecnologias no Ensino Médio.

- **Enquadramento Curricular:** O estudo de **Matrizes, Determinantes e Sistemas Lineares** integra o rol de Objetos de Conhecimento da **Formação Geral Básica (FGB)**. Embora a BNCC não os fixe em uma série específica, o trabalho demonstra como o conteúdo pode ser desenvolvido no 1º ou 2º ano do Ensino Médio Brasil (2025).
- **Desenvolvimento de Competências:** A atividade criptográfica estimula a **Competência Geral 5** (Cultura Digital), ao lidar com o conceito de códigos e algoritmos de segurança. Além disso, fomenta a habilidade de **representar e resolver problemas** utilizando a linguagem matricial.
- **Contextualização:** O trabalho reforça o princípio da BNCC de que a Matemática deve ser ensinada em conexão com a **realidade social e tecnológica** dos estudantes, conferindo sentido prático ao aprendizado.

Além da articulação com a Competência Geral 5 da BNCC, que enfatiza a Cultura Digital e o uso crítico e ético das tecnologias, a proposta desenvolvida neste trabalho dialoga de forma direta com a habilidade EM13MAT315, que prevê a utilização de conceitos matemáticos na construção, análise e interpretação de modelos, bem como na elaboração e compreensão de algoritmos. Ao explorar a Cifra de Hill como estratégia didática, os estudantes são levados a modelar matematicamente o processo de codificação e decodificação de mensagens, compreendendo a lógica algorítmica subjacente à criptografia por meio de operações matriciais e da aritmética modular. Dessa forma, a atividade promove não apenas o domínio técnico de conteúdos de Álgebra Linear, mas também o desenvolvimento do pensamento computacional e da capacidade de analisar algoritmos em contextos significativos, alinhando-se aos objetivos formativos do Ensino Médio e reforçando o caráter aplicado e profissional da proposta pedagógica.

6.4 LIMITAÇÕES DO ESTUDO

Apesar dos resultados positivos, é imperativo reconhecer as limitações da pesquisa:

- **Escopo Amostral:** O estudo foi circunscrito a duas unidades escolares, o que pode limitar a generalização dos achados para outros contextos socioeconômicos e pedagógicos.
- **Complexidade Matemática:** A Cifra de Hill exige o domínio da **Aritmética Modular** e o cálculo da **matriz inversa** em $\mathbb{Z}_{26}$, tópicos que, embora trabalhados na intervenção, representaram desafios conceituais iniciais para alguns grupos.

6.5 SUGESTÕES PARA TRABALHOS FUTUROS

Com base nas conclusões e limitações, sugerem-se as seguintes frentes de pesquisa:

- **Expansão Interdisciplinar:** Explorar a integração da Cifra de Hill com os **Itinerários Formativos** do Novo Ensino Médio, especialmente em trilhas de **Computação e Algoritmos** ou **Ciências Humanas** (História da Criptografia).
- **Outras Cifras:** Aplicar outras cifras criptográficas baseadas em Matrizes, como a Cifra de Vigenère, para introduzir conceitos adicionais de Álgebra Linear ou Teoria dos Números.
- **Estudo Longitudinal:** Acompanhar os estudantes que participaram da intervenção por um período mais longo para avaliar o **grau de retenção** dos conceitos de Matrizes e o impacto da metodologia em seu desempenho em outras áreas da Matemática.

Acreditamos que a utilização da Criptografia na educação matemática representa um caminho promissor para construir um aprendizado mais significativo e engajador, preparando os estudantes não apenas para o exame, mas para o pensamento lógico no século XXI.

REFERÊNCIAS

ANTON, H.; RORRES, C. **Álgebra Linear e Aplicações**. 10. ed. Porto Alegre: Bookman, 2012.

ARAUJO, W. V. d.; OUTROS. A cifra de hill como aplicação lúdica no ensino de matrizes no ensino médio. In: **Fundamentos e inovações nas Ciências Exatas**. Ponta Grossa: Atena Editora, 2024.

BAGGIO, G.; SCHOSSLER, D.; DULLIUS, M. M. Utilizando diferentes metodologias para o ensino de matrizes: uso de modelagem matemática e recursos computacionais em dois ambientes escolares. **Revista Destaques Acadêmicos**, Lajeado, v. 2, n. 4, p. 9–16, 2010.

BARDIN, L. **Análise de conteúdo**. 1. ed. São Paulo: Edições 70, 2016.

BARICHELLO, L. **Mensagens secretas com matrizes**. Campinas: [s.n.], s.d. Coleção Matemática Multimídia. Acesso em: 17 dez. 2025. Disponível em: https://m3.ime.unicamp.br/arquivos/1020/TELA-mensagens_secretas_com_matrizes---o_experimento.pdf.

BERGMANN, J.; SAMS, A. **Flip Your Classroom**. [S.l.]: ISTE, 2012.

BORBA, M. d. C.; SILVA, R. S. R. d.; GADANIDIS, G. **Fases das Tecnologias Digitais em Educação Matemática: Sala de Aula e Internet em Movimento**. Belo Horizonte: Autêntica Editora, 2014.

BOYER, C. B.; MERZBACH, U. C. **História da Matemática**. São Paulo: Edgard Blücher, 1996.

Brasil. **Base Nacional Comum Curricular: Educação Infantil e Ensino Fundamental – versão final**. 2025. Disponível em: https://www.gov.br/mec/pt-br/escola-em-tempo-integral/BNCC_EI_EF_110518_versaofinal.pdf.

D'AMBROSIO, U. **Educação Matemática: da teoria à prática**. 12. ed. Campinas: Papirus, 2004.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 7. ed.. ed. São Paulo: Atlas, 2019.

GINES, V. Vídeo online, **Matrizes: Codificar e Descodificar**. YouTube, 2025. Duração: 22 min 02 s. Disponível em: https://youtu.be/PJq6BApgXqw?feature=shared.

HILL, L. S. Cryptography in an algebraic alphabet. **The American Mathematical Monthly**, v. 38, n. 6, p. 306–312, 1931.

INEP. Relatório de resultados do saeb 2021. **Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira**, Brasília, 2022. Disponível em: https://www.gov.br/inep.

KATZ, V. J. **A History of Mathematics: An Introduction**. 3. ed. Boston: Addison-Wesley, 2009.

LAY, D. C.; LAY, S. R.; MCDONALD, J. J. **Álgebra Linear e Suas Aplicações**. 5. ed. Rio de Janeiro: LTC, 2016.

LORENZATO, S. **Para aprender Matemática**. Campinas: Autores Associados, 2006.

MINAYO, M. C. d. S. **O desafio do conhecimento: pesquisa qualitativa em saúde**. 14. ed. São Paulo: Hucitec, 2014.

NIVEN, I.; ZUCKERMAN, H. S.; MONTGOMERY, H. L. **An Introduction to the Theory of Numbers**. 5. ed. New York: John Wiley & Sons, 2008.

OECD. **PISA 2022 Results (Volume I): The State of Learning and Equity in Education**. Paris: PISA, OECD Publishing, 2023.

SKEMP, R. R. Relational understanding and instrumental understanding. **Mathematics Teaching**, n. 77, p. 20–26, 1976.

STALLINGS, W. **Criptografia e segurança de redes**. 6. ed. [S.l.]: Pearson, 2017.

STRANG, G. **Introduction to Linear Algebra**. 5. ed. Wellesley: Wellesley-Cambridge Press, 2016.

THIOLLENT, M. **Metodologia da pesquisa-ação**. 18. ed. São Paulo: Cortez, 2011.

APÊNDICE A – ATIVIDADE COM CRIPTOGRAFIA DE HILL

Atividade – Matemática – 2ª Série do Ensino Médio

Tema: Criptografia com Matrizes – Decodificando Segredos com Números

Nome do(a) estudante: _____ **Data:** _____
Professor(a): _____

Contextualização

A criptografia é um conjunto de técnicas utilizadas para proteger informações, garantindo que apenas pessoas autorizadas tenham acesso ao conteúdo de mensagens. No cotidiano, ela está presente em transações bancárias, aplicativos de mensagens, redes sociais e sistemas de segurança digital.

Nesta atividade, será explorada a criptografia por meio do uso de matrizes, permitindo aplicar conteúdos matemáticos como multiplicação matricial e matriz inversa em uma situação contextualizada.

TABELA DE CONVERSÃO

A	B	C	D	E	F	G	H	I	J	K	L	M
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

ETAPA 1 – PREPARANDO A MENSAGEM

1. Escolha uma palavra ou frase curta.
2. Converta cada letra em seu número correspondente, utilizando a tabela acima.
3. Organize os números obtidos em uma matriz coluna. Caso necessário, complete com zero.

Mensagem escolhida: _____

Mensagem em números: _____

ETAPA 2 – CODIFICAÇÃO DA MENSAGEM

Considere a matriz-chave:

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

1. Multiplique a matriz A pela matriz coluna que representa a mensagem.
2. O resultado corresponde à mensagem codificada.

Espaço para cálculos:

Mensagem codificada (números): _____

ETAPA 3 – DECODIFICAÇÃO DA MENSAGEM

Para recuperar a mensagem original, utiliza-se a matriz inversa de A:

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

1. Multiplique a matriz A^{-1} pela matriz codificada.
2. Converta os números obtidos novamente em letras, utilizando a tabela de conversão.

REFLEXÃO FINAL

1. Foi possível decodificar corretamente a mensagem?
   Sim Não Parcialmente
2. Como você avalia a atividade desenvolvida?

3. Cite situações do cotidiano em que a criptografia pode ser aplicada.

DESAFIO (OPCIONAL)

Pesquise: o que é criptografia RSA e em quais contextos ela é utilizada atualmente.

Atividade elaborada por: Prof.ª Vanessa Gines dos Santos Oliveira – Mestrado Profissional em Matemática (UNESP).

APÊNDICE B – DESAFIO DE CRIPTOGRAFIA COM MATRIZES

OBJETIVO

Nesta atividade, você aplicará o que aprendeu sobre codificação de mensagens com matrizes para **decifrar uma mensagem secreta** e **criar a sua própria**.

MENSAGEM CODIFICADA (USANDO MATRIZ DESCONHECIDA)

Mensagem: `ULFJQZTQ`
Dica: a matriz usada foi:

$$K = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$$

1. Converta a mensagem em blocos de duas letras.
2. Converta os blocos em números.
3. Use a matriz inversa de $K \mod 26$ para decodificar.

(Sugestão: o professor pode fornecer a matriz inversa já pronta.)

CRIE SUA MENSAGEM

Agora é sua vez de criar uma mensagem codificada.

1. Escreva uma palavra ou frase curta (sem espaços, letras maiúsculas).
2. Escolha uma matriz-chave:
$$K = \begin{bmatrix} 5 & 2 \\ 7 & 3 \end{bmatrix}$$
3. Codifique a mensagem e troque com um colega.
4. Desafiem-se para decodificar as mensagens usando a matriz inversa.

Mensagem original: _____
Mensagem codificada: _____

Dica: lembre-se de aplicar o módulo 26 após as multiplicações.

APÊNDICE C – ATIVIDADE CONTEXTUALIZADA COM CRIPTOGRAFIA DE HILL

PROPOSTA DE ATIVIDADE COM CRIPTOGRAFIA DE HILL

Título da Atividade:*"Explorando a Matemática da Cifra de Hill: Mensagens Codificadas"*

Enunciado: A criptografia está presente em nosso dia a dia, protegendo informações importantes. Um exemplo famoso é a Cifra de Hill, que utiliza conceitos matemáticos, como matrizes e álgebra linear, para codificar mensagens. Apesar de parecer complexo, esse método é uma forma interessante de explorar como a matemática e a segurança de dados estão conectadas.

Nesta atividade, você usará a Cifra de Hill para codificar uma mensagem e, em seguida, decodificar uma mensagem enviada por um colega. Vamos colocar a matemática em prática!

Passos da Atividade

1. Introdução ao Método:

Revise os conceitos de matrizes (adição, multiplicação, determinante e matriz inversa) que serão usados na Cifra de Hill. Entenda como uma matriz chave k é utilizada para transformar letras em números e codificar mensagens.

2. Preparação:

Escolha uma mensagem curta com número de caracteres múltiplo de 2. **Converta as letras em números baseado na tabela à seguir:**

A	B	C	D	E	F	G	H	I	J	K	L	M
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

Use uma matriz chave k (2×2). Certifique-se de que k é invertível no módulo 26, ou seja, o determinante seja 1.

3. Codificação:

Divida a mensagem em blocos e use a matriz k para multiplicar pelos vetores numéricos correspondentes à mensagem. Transforme o resultado da multiplicação em letras novamente, considerando o módulo 26. Como os estudantes ainda não estudaram a congruência modular, a tabela de conversão será explicada como se fosse um relógio, por exemplo, se o resultado for 2 equivale a letra c, se o resultado for 28 também equivale a letra c, se for 54 também, e assim por diante. Podemos chamar a tabela de "O relógio de 26 casas". Compartilhe a mensagem codificada com um colega.

4. Descodificação:
Receba a mensagem codificada de outro colega. Use a matriz inversa k^{-1}, também no módulo 26 ou no "relógio de 26 casas", para decifrar a mensagem. Verifique se conseguiu recuperar o texto original.

5. Discussão:
Em grupo, discuta os desafios encontrados no processo de codificação e decodificação. Reflitam sobre a segurança da Cifra de Hill e como ela pode ser quebrada se a matriz chave for descoberta.

Objetivos da Atividade:

Aplicar conceitos de matrizes na prática, relacionando a matemática com situações reais. Entender o funcionamento básico da Cifra de Hill como exemplo de criptografia simétrica. Desenvolver habilidades de raciocínio lógico e trabalho colaborativo.

Materiais Necessários:

Papel e caneta. Calculadora científica (ou software que suporte operações com matrizes, como Excel ou photomat).

Entrega:

Responda às seguintes perguntas em um relatório curto:

Qual foi a matriz chave utilizada? Como foi o processo de codificação e decodificação? Que dificuldades você encontrou? Qual a importância da criptografia no dia a dia?

Duração da Atividade: 1 aula (45 minutos) para rever operações com matrizes. 1 aula (45 minutos) para codificar e decodificar mensagens.

20 minutos para discussão e entrega do relatório.

APÊNDICE D – INTRODUÇÃO À CRIPTOGRAFIA COM MATRIZES (CIFRA DE HILL)

OBJETIVO

Nesta atividade, os estudantes aprenderão como a Matemática — em especial as matrizes — pode ser usada para criptografar mensagens. Utilizaremos a **Cifra de Hill**, um método de codificação baseado em multiplicação de matrizes modulares.

ALFABETO NUMÉRICO

A tabela abaixo associa letras a números de 0 a 25:

A=0	B=1	C=2	D=3	E=4	F=5	G=6	H=7
I=8	J=9	K=10	L=11	M=12	N=13	O=14	P=15
Q=16	R=17	S=18	T=19	U=20	V=21	W=22	X=23
Y=24	Z=25						

PASSOS DA CODIFICAÇÃO

1. Divida a mensagem em blocos de duas letras. Exemplo: `AULA → AU, LA`
2. Converta cada letra para seu valor numérico.
3. Utilize uma matriz-chave 2×2. Exemplo:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

4. Multiplique cada vetor da mensagem por essa matriz:
Se `AU = [0, 20]`, então:

$$K \cdot \begin{bmatrix} 0 \\ 20 \end{bmatrix} = \begin{bmatrix} 60 \\ 100 \end{bmatrix} \mod 26 = \begin{bmatrix} 8 \\ 22 \end{bmatrix} \Rightarrow IW$$

EXERCÍCIO 1 — CODIFIQUE VOCÊ MESMO

Use a matriz-chave abaixo para codificar a palavra: **“REDE”**

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

1. Divida a palavra: ____ , ____

2. Converta para números: ____, ____
3. Multiplique pela matriz K (mod 26)
4. Mensagem codificada: _____

DESAFIO

Qual será a mensagem criptografada de “FIM” com a matriz:

$$K = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

(Se necessário, adicione uma letra extra para completar o par.)

APÊNDICE E – QUESTIONÁRIO DIAGNÓSTICO – MATRIZES E APLICAÇÕES

Este questionário foi aplicado **antes da realização das atividades envolvendo matrizes e criptografia (Cifra de Hill)**. Seu objetivo é identificar os conhecimentos prévios, experiências anteriores e percepções iniciais dos estudantes sobre o conteúdo.

Instruções: Responda às questões de acordo com seu conhecimento atual. Para as questões objetivas, assinale apenas uma alternativa. Para as questões abertas, escreva de forma clara e objetiva.

1. Você já estudou matrizes em Matemática?
   (a) Sim, com bastante profundidade
   (b) Sim, apenas noções básicas
   (c) Já ouvi falar, mas não estudei formalmente
   (d) Não conheço matrizes
2. Uma matriz pode ser definida como:
   A. Um conjunto de gráficos matemáticos.
   B. Um arranjo de números organizados em linhas e colunas.
   C. Uma tabela usada apenas para textos.
   D. Uma figura geométrica plana.
3. Você já utilizou matrizes para resolver algum problema matemático?
   (a) Sim
   (b) Não
   (c) Não me lembro
4. Antes desta aula, você já ouviu falar em **criptografia**?
   (a) Sim, sei o que é
   (b) Já ouvi falar, mas não sei explicar
   (c) Não conhecia
5. Você sabia que a criptografia pode utilizar conceitos matemáticos como matrizes?
   (a) Sim
   (b) Não

(c) Nunca pensei sobre isso

6. Você já ouviu falar na **Cifra de Hill**?

   (a) Sim

   (b) Não

7. Em sua opinião, o estudo de matrizes costuma ser:

   (a) Muito abstrato

   (b) Interessante

   (c) Difícil

   (d) Útil para resolver problemas

8. Você acredita que aprender Matemática por meio de aplicações práticas pode facilitar a compreensão dos conteúdos?

   (a) Sim

   (b) Não

   (c) Talvez

9. Você já estudou ou sabe que é possível utilizar **matrizes** para **codificar e decodificar mensagens**, como ocorre em alguns métodos de **criptografia**, por exemplo, a **Cifra de Hill**?

   (a) Sim

   (b) Não

   (c) Muito pouco

10. Antes desta atividade, você já utilizou matrizes para outros fins ?

    (a) Sim

    (b) Não

    (c) Nunca ouvi falar

11. Você já utilizou algum software matemático (como GeoGebra, por exemplo) para estudar Álgebra?

    (a) Sim

    (b) Não

12. Na sua opinião, qual dessas áreas parece mais interessante para aplicar matrizes?

(a) Criptografia

(b) Especificamente a Cifra de Hill

(c) Ambas

(d) Não sei opinar

13. O que você espera aprender ao estudar matrizes por meio de atividades envolvendo criptografia?

14. Você acredita que a Matemática pode estar relacionada à tecnologia e à segurança da informação? Explique brevemente.

APÊNDICE F – QUESTIONÁRIO PÓS APLICAÇÃO – MATRIZES E CRIPTOGRAFIA

Este questionário foi disponibilizado após a aplicação das atividades.

Instruções: Responda às questões de acordo com seu conhecimento e opinião. Para as questões objetivas, assinale apenas uma alternativa. Para as questões abertas, redija suas respostas de forma clara e objetiva.

1. O que é uma matriz?

   A. Um gráfico que representa funções polinomiais.

   B. Um arranjo retangular de números dispostos em linhas e colunas.

   C. Uma tabela usada apenas para armazenar textos.

   D. Um diagrama para representar apenas figuras geométricas.

2. Para decodificar uma mensagem na cifra de Hill, a matriz-chave deve:

   A. Ter determinante igual a zero.

   B. Ser triangular superior.

   C. Ter determinante invertível módulo 26.

   D. Ter todos os elementos pares.

3. Uma vantagem de usar matrizes para representar mensagens é:

   A. Elas sempre simplificam qualquer cálculo.

   B. Permitem manipulação de dados e aplicação de conteúdos como codificar e decodificar códigos.

   C. Funcionam apenas para criptografia.

   D. Não exigem cálculos com determinantes.

4. Aprender criptografia no estudo das matrizes pode:

   A. Tornar o estudo mais interessante, pois conecta teoria e aplicações reais.

   B. Tornar o estudo mais difícil sem benefícios.

   C. Ser útil apenas para estudantes de História.

   D. Substituir a necessidade de aprender multiplicação de matrizes.

5. Você já estudou aplicações de matrizes fora do contexto puramente algébrico (ex.: além da resolução de sistemas lineares)?

(a) Sim

(b) Não

(c) Pouco

6. Avalie seu conhecimento sobre criptografia clássica baseada em matrizes (ex.: cifra de Hill).

   (a) Nunca ouvi falar

   (b) Conheço superficialmente

   (c) Conheço bem a teoria

   (d) Já apliquei em projetos ou pesquisas

7. Você já estudou ou sabe que é possível utilizar **matrizes** para **codificar e decodificar mensagens**, como ocorre em alguns métodos de **criptografia**, por exemplo, a **Cifra de Hill**?

   (a) Sim

   (b) Não

   (c) Parcialmente

8. Na sua opinião, qual dessas áreas oferece maior aplicabilidade real para o uso de matrizes? (escolha apenas uma ou justifique)

   (a) Criptografia

   (b) Mensagem não criptografada

   (c) Ambas igualmente

   (d) Outra: _____

9. Você considera que o ensino de matrizes deveria incluir mais exemplos de aplicações como criptografia?

   (a) Sim, com certeza

   (b) Talvez, depende do nível do aluno

   (c) Não, o foco deve ser teórico

   (d) Sem opinião

10. Você já desenvolveu (ou conhece) algum projeto prático ou didático que utilizou matrizes para codificar e decodificar códigos (ex.: usando software como GeoGebra)?

    (a) Sim

(b) Não

(c) Já vi, mas nunca desenvolvi

11. Na sua visão, qual é o maior desafio ao aplicar matrizes em criptografia, como na cifra de Hill?

12. Como você descreveria o papel das matrizes para resolver problemas diversos da matemática

13. Você vê potencial em integrar criptografia baseada em álgebra linear no currículo da educação básica ou média como forma de interdisciplinaridade com tecnologia e história? Por quê?

14. Quais softwares ou ferramentas você recomenda para explorar o uso de matrizes em aplicações criptográficas?

APÊNDICE G – ALINHAMENTO ENTRE OS QUESTIONÁRIOS

Nesta seção apresenta-se o alinhamento entre o questionário diagnóstico (pré-teste) e o questionário avaliativo (pós-teste), de modo a evidenciar a correspondência entre os constructos investigados, as questões aplicadas e os objetivos de comparação.

Quadro 1 – Alinhamento entre o questionário diagnóstico (pré-teste) e o questionário avaliativo (pós-teste)

Constructo	**Questão no Pré-teste**	**Questão no Pós-teste**	**Objetivo da Comparação**
Conceito de matriz	Q2 – Definição de matriz	Q1 – O que é uma matriz?	Verificar consolidação do conceito formal
Uso de matrizes	Q3 – Uso prévio de matrizes	Q3 – Vantagens do uso de matrizes	Identificar ampliação da percepção de aplicabilidade
Conhecimento em criptografia	Q4 – Conhecimento prévio sobre criptografia	Q6 – Avaliação do conhecimento em criptografia matricial	Verificar evolução do conhecimento específico
Matrizes e criptografia	Q5 – Relação entre matrizes e criptografia	Q2 – Condições da matriz-chave na Cifra de Hill	Analisar compreensão técnica da aplicação
Cifra de Hill	Q6 – Conhecimento prévio da Cifra de Hill	Q2 – Processo de decodificação	Avaliar aprendizagem do conteúdo específico
Percepção sobre matrizes	Q7 – Opinião inicial sobre o estudo de matrizes	Q4 – Interesse ao aprender com criptografia	Identificar mudança atitudinal
Aprendizagem por aplicações	Q8 – Expectativa sobre aplicações práticas	Q9 – Opinião sobre inclusão de aplicações no ensino	Avaliar validação pedagógica da proposta
Criptografia	Q9 – Contato prévio com a Criptografia	Q7 – Uso de matrizes para codificar e decodificar códigos	Verificar ampliação conceitual
Engajamento	Q10 – Conhecimento prévio sobre interações e formação de grupos para estudos	Q12 – Papel das metodologias ativas em sala de aula	Consolidar compreensão dos conteúdos
Tecnologia e software	Q11 – Uso prévio de software matemático	Q10 / Q14 – Projetos e softwares recomendados	Analisar transferência do aprendizado para ferramentas
Interdisciplinaridade	Q12 – Área mais interessante para aplicar matrizes	Q8 / Q13 – Aplicabilidade e integração curricular	Avaliar visão interdisciplinar
Expectativas e reflexões	Q13 / Q14 – Expectativas iniciais	Q11 / Q13 – Desafios e potencial curricular	Comparar expectativas e aprendizagens