Rodrigo Rodrigues Garcia

A CIFRA DE HILL COMO ESTRATÉGIA NA APRENDIZAGEM DE MATRIZES

Rondonópolis

2026

Rodrigo Rodrigues Garcia

A CIFRA DE HILL COMO ESTRATÉGIA NA APRENDIZAGEM DE MATRIZES

Dissertação de mestrado apresentada ao PROFMAT como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática

UNIVERSIDADE FEDERAL DE RONDONÓPOLIS

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Orientadora: Profa. Dra. Joelma Ananias de Oliveira

Rondonópolis

2026

Dados Internacionais de Catalogação na Fonte
Ficha Catalográfica elaborada de forma automática com os dados fornecidos pelo(a) autor(a).
Permitida a reprodução parcial ou total, desde que citada a fonte.

G216c Garcia, Rodrigo Rodrigues.
A CIFRA DE HILL COMO ESTRATÉGIA NA APRENDIZAGEM DE MATRIZES [recurso eletrônico] / Rodrigo Rodrigues Garcia. – Dados eletrônicos (1 arquivo : 88 f., il. color., pdf). – 2026.

Orientador(a): Joelma Ananias de Oliveira.
Dissertação (mestrado) – Universidade Federal de Rondonópolis, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Matemática em Rede Nacional, Rondonópolis, 2026.
Inclui bibliografia.

1. Matrizes. 2. Criptografia. 3. Cifra de Hill. 4. Estratégias didáticas. I. Oliveira, Joelma Ananias de, *orientador*. II. Título.

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DE RONDONÓPOLIS-UFR.

PRÓ-REITORIA DE ENSINO DE PÓS-GRADUAÇÃO E PESQUISA - PROPGP/UFR.

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT/UFR.

FOLHA DE APROVAÇÃO

TÍTULO: "A cifra de Hill como estratégia na aprendizagem de matrizes"

AUTOR: MESTRANDO **RODRIGO RODRIGUES GARCIA.**

Dissertação submetida ao programa de pós-graduação do Mestrado Profissional em Matemática em Rede Nacional, PROFMAT, da Universidade Federal de Rondonópolis-UFR, como requisito parcial para obtenção do grau de Mestre em Matemática.

Dissertação defendida e aprovada em **26** de **Junho** de **2026**.

Seguem as assinaturas dos membros titulares da banca examinadora.

COMPOSIÇÃO DA BANCA EXAMINADORA

1. **Profa. Dra. Joelma Ananias de Oliviera** (Presidente da Banca/Orientadora);
2. **Profa. Dra. Priscila Friedemann Cardoso** (Membro interno titular/UFR);
3. **Profa. Dra. Lia Corrêa da Costa** (Membro externo titular, IFMT/Cuiabá).

Rondonópolis-MT, **26/06/2026**.

Documento assinado eletronicamente por **Lia registrado(a) civilmente como Lia Corrêa da Costa** , **Usuário Externo**, em 26/06/2026, às 16:31, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539, de 8 de outubro de 2015 .

Documento assinado eletronicamente por **Joelma Ananias de Oliveira**, **Docente - UFR**, em 26/06/2026, às 16:32, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Priscila Friedemann Cardoso**, **Docente - UFR**, em 26/06/2026, às 16:33, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufr.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0716717** e o código CRC **92179B84**.

Referência: Processo nº 23853.005471/2026-16 SEI nº 0716717

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por me conceder força, sabedoria e perseverança ao longo desta caminhada. Nos momentos de dificuldade e incerteza, foi a fé que me sustentou e deu coragem para continuar e seguir em frente.

Aos meus pais, Milton (*in memoriam*) e Benedita, expresso minha mais profunda gratidão por todo amor, apoio e incentivo incondicional. Obrigado pelos ensinamentos, valores transmitidos e inúmeros sacrifícios realizados para que eu pudesse chegar até aqui. Esta conquista também é de vocês, que sempre acreditaram em mim e estiveram ao meu lado em todos os momentos.

Aos meus irmãos, Rafael e Fernando, agradeço pelo carinho, apoio e presença constante ao longo desta jornada. Ter vocês ao meu lado foi fundamental para enfrentar os desafios e celebrar cada conquista.

Ao PROFMAT, agradeço pela oportunidade de crescimento acadêmico e profissional, bem como pela excelência do programa e pela contribuição para o fortalecimento da educação matemática.

Aos professores que fizeram parte desta trajetória, registro meu sincero agradecimento pelos ensinamentos, dedicação e generosidade em compartilhar conhecimentos. Cada orientação, incentivo e aprendizado contribuiu de forma significativa para minha formação acadêmica e profissional.

Aos colegas de turma, agradeço pela parceria, trocas de experiências e companheirismo ao longo dessa jornada. Em especial, meu agradecimento ao Diogo, Fernando, Gustavo (*in memoriam*), Mário e Juliana, pelo apoio mútuo e momentos compartilhados, que tornaram essa caminhada mais leve e enriquecedora.

Por fim, agradeço a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho e para esta importante etapa da minha vida.

“ Se você não consegue explicar algo de forma simples, você não entendeu o assunto o suficiente. ”

(Richard Feynman)

RESUMO

As matrizes constituem um dos tópicos centrais da Álgebra Linear e desempenham papel relevante em diversas aplicações científicas e tecnológicas. Entretanto, sua abordagem no contexto escolar frequentemente se restringe à execução de procedimentos algébricos, o que pode dificultar a construção de significados pelos estudantes e comprometer a aprendizagem conceitual. Esta dissertação investiga a utilização da *Cifra de Hill* como estratégia didática para o ensino de matrizes no Ensino Médio. A pesquisa fundamenta-se na necessidade de propor alternativas metodológicas que promovam maior contextualização e engajamento discente. Nesse sentido, a criptografia apresenta-se como um campo interdisciplinar promissor ao relacionar conceitos matemáticos com situações reais envolvendo segurança da informação e comunicação digital. Entre os métodos criptográficos clássicos, destaca-se a *Cifra de Hill*, baseada em operações com matrizes e aritmética modular. O estudo desenvolve-se por meio de uma abordagem qualitativa, de caráter bibliográfico, apoiada em referenciais teóricos da Educação Matemática, especialmente aqueles relacionados à aprendizagem significativa e à contextualização do ensino. Além da revisão teórica, foi elaborada uma proposta pedagógica estruturada em atividades que exploram a codificação e a decodificação de mensagens por meio da *Cifra de Hill*, evidenciando a aplicação prática de conceitos como multiplicação de matrizes, determinante, matriz inversa e operações no sistema modular. Como produto educacional, foi desenvolvida uma sequência didática destinada ao ensino de matrizes no Ensino Médio, contendo orientações metodológicas, sugestões de atividades e fundamentação teórica. Espera-se que a integração entre criptografia e ensino de matrizes contribua para práticas pedagógicas mais contextualizadas e significativas. Conclui-se que a *Cifra de Hill* constitui um recurso pedagógico com potencial para evidenciar aplicações da Álgebra Linear e favorecer a aprendizagem conceitual. Dessa forma, esta dissertação busca contribuir para o aprimoramento das práticas pedagógicas na Educação Básica.

Palavras-chave: Matrizes; Criptografia; Cifra de Hill; Estratégias didáticas.

ABSTRACT

Matrices constitute one of the central topics of Linear Algebra and play a relevant role in various scientific and technological applications. However, their approach in the school context is often restricted to the execution of algebraic procedures, which may hinder the construction of meaning by students and compromise conceptual learning. This dissertation investigates the use of the *Hill Cipher* as a didactic strategy for teaching matrices in Secondary Education. The research is grounded in the need to propose methodological alternatives that promote greater contextualization and student engagement. In this regard, cryptography presents itself as a promising interdisciplinary field by relating mathematical concepts to real-world situations involving information security and digital communication. Among classical cryptographic methods, the *Hill Cipher* stands out, as it is based on matrix operations and modular arithmetic. The study is developed through a qualitative approach of bibliographic nature, supported by theoretical frameworks from Mathematics Education, particularly those related to meaningful learning and the contextualization of teaching. In addition to the theoretical review, a pedagogical proposal was elaborated, structured around activities that explore the encoding and decoding of messages through the *Hill Cipher*, highlighting the practical application of concepts such as matrix multiplication, determinants, inverse matrices, and operations within the modular system. As an educational product, a didactic sequence was developed for the teaching of matrices in Secondary Education, containing methodological guidelines, suggested activities, and theoretical foundations. It is expected that the integration of cryptography and matrix instruction will contribute to more contextualized and meaningful pedagogical practices. It is concluded that the *Hill Cipher* constitutes a pedagogical resource with the potential to highlight applications of Linear Algebra and foster conceptual learning. Thus, this dissertation seeks to contribute to the improvement of pedagogical practices in Basic Education.

Keywords: Matrices; Cryptography; Hill Cipher; Teaching Strategies.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O ensino de Matemática na Educação Básica apresenta desafios recorrentes, especialmente no que se refere à aprendizagem de conteúdos que exigem elevado nível de abstração. Entre esses, destacam-se as matrizes, introduzidas geralmente no Ensino Médio e retomadas no Ensino Superior, desempenhando papel fundamental em diversas áreas do conhecimento, como Física, Computação, Economia e Engenharia. Apesar de sua relevância teórica e aplicada, observa-se que muitos estudantes demonstram dificuldades na compreensão desse tema, o que se reflete no baixo engajamento em uma aprendizagem predominantemente mecânica.

Em muitos dos materiais didáticos, o ensino de matrizes ainda é conduzido de forma predominantemente formal, com ênfase em definições, propriedades e procedimentos algébricos. Essa abordagem, muitas vezes dissociada de aplicações concretas, pode limitar a compreensão conceitual e dificultar a percepção da utilidade desse conteúdo (SKOVSMOSE, 2000). Como consequência, o estudo das matrizes tende a ser percebido como um conjunto de regras a serem aplicadas, e não como uma ferramenta matemática dotada de sentido e aplicabilidade.

Diante desse cenário, torna-se necessário repensar práticas pedagógicas que promovam maior envolvimento dos discentes e favoreçam a construção de aprendizagens significativas. Segundo Charlot (2013), a educação não consiste em transmitir conhecimentos acabados, mas em propor aos alunos situações e problemas que desencadeiem uma atividade intelectual que, com a mediação do professor, os conduza à construção do conhecimento.

A contextualização do conhecimento matemático configura-se, nesse sentido, como um elemento central para a aprendizagem. Ao articular os conteúdos curriculares com situações concretas e socialmente relevantes, o professor pode criar ambientes de aprendizagem mais dinâmicos, nos quais os estudantes são incentivados a mobilizar saberes prévios, formular hipóteses e resolver problemas. Essa perspectiva está alinhada às concepções de aprendizagem significativa e ao papel ativo do aluno no processo educativo.

Nesse contexto, a criptografia apresenta-se como um campo interdisciplinar promissor. Desde a Antiguidade até a era digital, a necessidade de proteger informações impulsionou o desenvolvimento de métodos de codificação e decodificação de mensagens, muitos dos quais fundamentados em conceitos matemáticos. Entre os métodos clássicos,

destaca-se a *Cifra de Hill*, desenvolvida em 1929 por *Lester Sanders Hill* (HILL, 1929), cujo funcionamento baseia-se diretamente em operações com matrizes e aritmética modular. Essa característica a torna especialmente adequada para fins didáticos, pois permite explorar, de forma articulada, conceitos como multiplicação de matrizes, determinante e matriz inversa em um contexto aplicado.

Diante do exposto, este trabalho parte da seguinte questão norteadora: *quais fundamentos teóricos e matemáticos sustentam a viabilidade da Cifra de Hill como estratégia didática para o ensino de matrizes no Ensino Médio?* A partir dessa indagação, o estudo tem como objetivo geral elaborar uma proposta didática fundamentada na Cifra de Hill para o ensino de matrizes no Ensino Médio, articulando fundamentos teóricos da Educação Matemática e da Álgebra Linear com o desenvolvimento de uma sequência de atividades contextualizadas.

Para alcançar esse objetivo, foram estabelecidas as seguintes metas específicas: analisar as principais dificuldades relacionadas ao ensino e à aprendizagem de matrizes no Ensino Médio; estudar os fundamentos matemáticos da *Cifra de Hill*, destacando sua relação com os conceitos da Álgebra Linear, especialmente multiplicação de matrizes, determinante, matriz inversa e aritmética modular; identificar o potencial pedagógico da criptografia como recurso de contextualização no ensino de matrizes; e elaborar uma sequência didática fundamentada na *Cifra de Hill* para o ensino de matrizes no Ensino Médio.

Esta pesquisa caracteriza-se como um estudo de natureza qualitativa de caráter bibliográfico, fundamentado em referenciais teóricos da Educação Matemática e na literatura específica sobre criptografia e Álgebra Linear, como os artigos de Brandão (2018) e Barbosa e Cornelissen (2017). Não se contempla, neste trabalho, uma aplicação empírica sistemática da sequência elaborada, concentrando-se a investigação na análise teórica e na construção do produto educacional. Ao propor a utilização da *Cifra de Hill* como recurso pedagógico, pretende-se contribuir para o desenvolvimento de práticas mais investigativas e contextualizadas, nas quais os estudantes possam perceber as matrizes não apenas como estruturas algébricas formais, mas como ferramentas matemáticas com aplicações concretas na sociedade contemporânea.

Este trabalho está organizado da seguinte forma: os Capítulos 2 e 3 discutem os conceitos de matrizes e os principais desafios relacionados ao seu ensino; os Capítulos 4 e 5 abordam a criptografia e a Cifra de Hill, destacando sua relação com a Matemática; os Capítulos 6 e 7 apresentam os fundamentos matemáticos necessários e o processo de codificação e decodificação; o Capítulo 8 apresenta a proposta didática elaborada; e o Capítulo 9 traz as considerações finais do trabalho.

Declaração de uso de Inteligência Artificial Generativa: a elaboração deste trabalho contou com o auxílio de ferramentas de Inteligência Artificial Generativa em diferentes fases e finalidades, conforme detalhado a seguir: (1) a ferramenta Claude (Anthropic) foi utilizada para conversão de expressões e notações matemáticas para a linguagem LaTeX, para revisão ortográfica e de concordâncias verbais e nominais do texto, e para organização e estruturação do produto educacional apresentado no Capítulo 8; (2) a ferramenta ChatGPT (OpenAI) foi utilizada para levantamento de indicações de autores e referências bibliográficas relacionados à *Cifra de Hill*, posteriormente verificadas e validadas pelo autor; e (3) a plataforma Canva foi utilizada para a criação das imagens e elementos visuais presentes no produto educacional. O uso dessas ferramentas ocorreu nas fases de redação, formatação e elaboração do material didático, em conformidade com a Portaria CNPq n.º 2.664, de 6 de março de 2026. A responsabilidade integral pelo conteúdo, escolhas teóricas e metodológicas, verificação das referências bibliográficas e revisão crítica de todas as informações é do autor.

2 O CONCEITO DE MATRIZ

2.1 Introdução

O presente capítulo tem por objetivo apresentar os fundamentos históricos e conceituais das matrizes, estabelecendo a base teórica necessária para o desenvolvimento da proposta didática apresentada posteriormente. Embora o foco desta dissertação esteja na utilização da *Cifra de Hill* como estratégia pedagógica, torna-se indispensável explicitar os principais conceitos matemáticos envolvidos, garantindo rigor formal e coerência conceitual.

A abordagem aqui desenvolvida fundamenta-se em obras clássicas da Álgebra Linear amplamente utilizadas na formação inicial e continuada de professores de Matemática, tais como *Álgebra Linear com Aplicações*, de Anton e Rorres (2001), *Álgebra Linear*, de Steinbruch e Winterle (1987) e *Álgebra Linear*, de Boldrini et al. (1986). Também dialoga com manuais e livros didáticos adotados no Ensino Médio, como *Matemática Completa*, de Giovanni, Bonjorno e Júnior (2005), e *A matemática do ensino médio*, de Lima (2012), buscando estabelecer uma ponte entre o tratamento formal do conteúdo e sua abordagem no contexto escolar.

Além das referências matemáticas, este capítulo considera contribuições da Educação Matemática que discutem a importância da contextualização e da atribuição de significado aos objetos matemáticos, como Ausubel (2003) e D'Ambrosio (1996), compreendendo que a aprendizagem se fortalece quando o conhecimento escolar se relaciona com experiências e contextos socialmente significativos.

Dessa forma, procura-se apresentar as matrizes não apenas sob o ponto de vista estrutural e algorítmico, mas também sob a perspectiva de sua construção histórica e de suas possibilidades pedagógicas.

A organização do capítulo contempla inicialmente aspectos históricos do desenvolvimento do conceito de matriz, seguidos da definição formal, notação, principais operações e elementos fundamentais, como determinante e matriz inversa. Ao final, estabelece-se a articulação desses conceitos com a proposta didática baseada na Cifra de Hill, evidenciando sua pertinência para o Ensino Médio.

A definição de matriz, tal como compreendida atualmente, é resultado de um processo histórico de formalização que envolveu diferentes matemáticos ao longo dos séculos. Embora hoje seja apresentada como um objeto algébrico estruturado, sua origem está

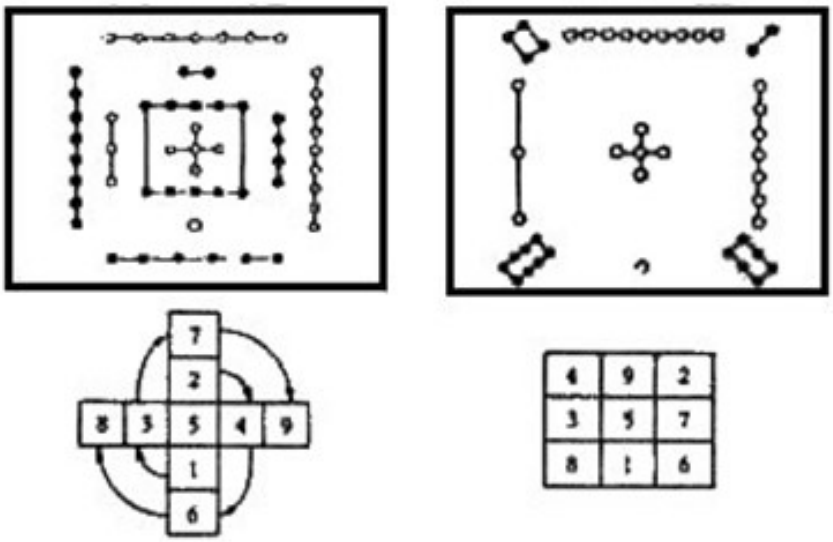
associada à necessidade de organizar e resolver sistemas de equações lineares. Inicialmente, esses arranjos numéricos eram utilizados apenas como ferramentas auxiliares de cálculo.

A consolidação das matrizes como entidade matemática autônoma ocorreu apenas no século XIX, quando passaram a ser estudadas dentro de uma estrutura teórica própria, especialmente no contexto da Álgebra Linear, permitindo o desenvolvimento sistemático de conceitos como determinantes, autovalores e transformações lineares (MEYER, 2000).

2.2 Origens Históricas

Registros antigos indicam que métodos semelhantes à organização matricial já eram utilizados na China antiga, especialmente na obra *Nove Capítulos sobre a Arte da Matemática*, como pode ser observado na Figura 1, onde sistemas de equações eram organizados em tabelas retangulares para facilitar cálculos (EVES, 2004). Contudo, tais representações ainda não eram concebidas como objetos matemáticos independentes.

Figura 1 – Representação de sistemas lineares em *Nove Capítulos sobre a Arte da Matemática*

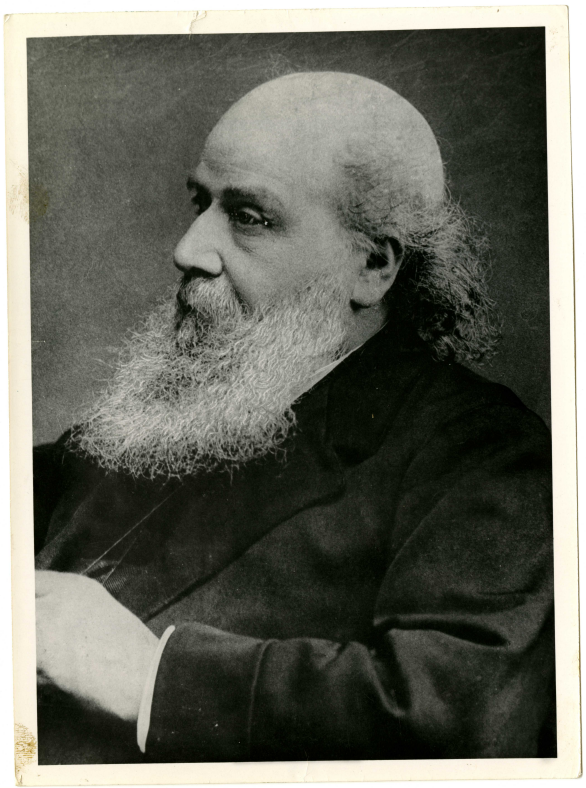


Fonte: https://arbitrarilyclosecom.wordpress.com/2020/08/01/mathartchallenge-95-magic-squares/. Acesso em: 21 fev. 2026.

No século XVII, o desenvolvimento da álgebra simbólica e dos métodos para resolução de sistemas lineares criou bases mais sólidas para o surgimento das matrizes. Um passo importante ocorreu com o trabalho de *Gottfried Wilhelm Leibniz* (1646-1716), que investigou determinantes e estruturas relacionadas à resolução de sistemas lineares (KLINE, 1972). Posteriormente, no século XVIII, *Gabriel Cramer* (1704-1752) apresentou a Regra de Cramer, utilizando determinantes para resolver sistemas lineares (KLINE, 1972). Ainda que o termo "matriz" não estivesse formalmente estabelecido, o tratamento algébrico dessas estruturas começava a se consolidar.

A formalização do conceito de matriz ocorreu efetivamente no século XIX. O termo *"matrix"* foi introduzido por *James Joseph Sylvester* (1814 – 1897) em 1850, conforme retratado na Figura 2, para designar um arranjo retangular de números que daria origem aos determinantes (EVES, 2004).

Figura 2 – James Joseph Sylvester

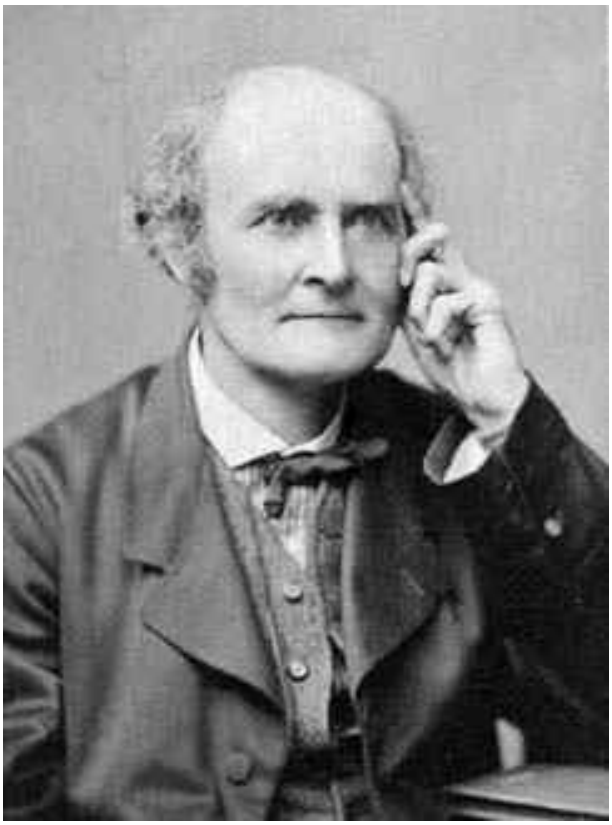


Fonte: https://digital.library.jhu.edu/islandora/photograph-james-joseph-sylvester-1. Acesso em: 21 fev. 2026.

Pouco depois, *Arthur Cayley* (1821-1895), retratado na Figura 3, desenvolveu a teoria algébrica das matrizes em sua obra *A Memoir on the Theory of Matrices*, publicada em 1858 nos *Philosophical Transactions of the Royal Society of London* (CAYLEY, 1858). Nesse trabalho, Cayley partiu da observação de que sistemas de transformações lineares, como $X = ax + by + cz$, podiam ser representados de forma abreviada por meio de arranjos retangulares de coeficientes, os quais ele passou a tratar como objetos algébricos autônomos, e não apenas como uma notação auxiliar para sistemas de equações. A partir dessa representação, Cayley estabeleceu as regras de adição, multiplicação por escalar e, principalmente, de multiplicação entre matrizes, definindo essa última operação de modo consistente com a composição de transformações lineares sucessivas: multiplicar duas matrizes correspondia a aplicar, em sequência, as transformações que cada uma representava. Um aspecto central de sua formulação foi a constatação de que essa multiplicação não é comutativa, isto é, o resultado depende da ordem em que as matrizes

são multiplicadas, uma propriedade que distinguia as matrizes da aritmética usual e as aproximava, nesse sentido, da álgebra dos quatérnios, com a qual Cayley também estabeleceu comparações. Com isso, demonstrou que as matrizes poderiam ser tratadas como objetos matemáticos dotados de propriedades próprias, incluindo a existência de inversas, consolidando as bases da álgebra matricial moderna.

Figura 3 – Arthur Cayley



Fonte: https://mathshistory.st-andrews.ac.uk/Biographies/Cayley/pictdisplay/. Acesso em: 21 fev. 2026.

A seguir, apresenta-se uma definição de caráter introdutório e informal, suficiente para a compreensão inicial do conceito de matriz; a formalização matemática mais rigorosa será apresentada em capítulo posterior.

Definição 2.2.1 (Informal)**.** Uma matriz pode ser entendida como uma forma organizada de dispor números em linhas e colunas, semelhante a uma tabela.

Exemplo 2.2.1. Considere uma turma com três alunos e duas provas. Podemos organizar as notas em uma tabela, conforme a Tabela 1.

Tabela 1 – Exemplo contextualizado de matriz

Aluno	Prova 1	Prova 2
Ana	8,0	7,5
Bruno	6,5	9,0
Carlos	7,0	8,5

Fonte: Elaborado pelo autor (2026)

De forma matemática, a Tabela 1 pode ser representada pela seguinte matriz, onde cada linha corresponde a um estudante e cada coluna a uma prova.

$$A = \begin{bmatrix} 8,0 & 7,5 \\ 6,5 & 9,0 \\ 7,0 & 8,5 \end{bmatrix}$$

A compreensão histórica e conceitual das matrizes é fundamental para situar esse objeto matemático não apenas como conteúdo formal da Álgebra Linear, mas também como ferramenta com potencial de aplicação em diferentes contextos. Entretanto, para que esse potencial se efetive no espaço escolar, torna-se necessário discutir como as matrizes são abordadas no Ensino Médio e quais dificuldades emergem nesse processo, aspecto que será tratado no capítulo seguinte.

3 O ENSINO DE MATRIZES E OS DESAFIOS NA APRENDIZAGEM

3.1 Introdução

Após a apresentação do conceito de matriz e de seu desenvolvimento histórico no capítulo anterior, torna-se pertinente discutir como esse conteúdo é abordado no contexto da Educação Básica, bem como os principais desafios relacionados à sua aprendizagem. Este capítulo tem como objetivo analisar o ensino de matrizes na Educação Básica, discutindo os principais obstáculos identificados na literatura da área e as perspectivas teóricas que fundamentam propostas de superação. A análise apoia-se em referenciais da Educação Matemática que problematizam o ensino mecanizado e defendem práticas orientadas pela construção de significado, pela articulação entre diferentes registros de representação e pela contextualização do conhecimento escolar.

3.2 As Matrizes no Currículo do Ensino Médio

O conteúdo de matrizes integra o currículo do Ensino Médio e costuma ser apresentado em articulação com sistemas lineares e determinantes. Nos documentos curriculares oficiais, como a Base Nacional Comum Curricular (BNCC), o estudo desse tema está associado ao desenvolvimento do raciocínio algébrico, à modelagem de situações e à resolução de problemas (BRASIL, 2018). Na área de Matemática e suas Tecnologias para o Ensino Médio, a habilidade mais diretamente relacionada ao estudo de sistemas lineares e, indiretamente, ao trabalho com matrizes, é a de código EM13MAT301, que orienta os estudantes a *"resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais"* (BRASIL, 2018, p. 536).

É preciso reconhecer, contudo, que essa habilidade aborda as matrizes apenas de forma indireta, no contexto da resolução de sistemas lineares, sem contemplar explicitamente operações matriciais, determinantes ou matrizes inversas como objetos de estudo autônomos. Tal ausência evidencia uma lacuna curricular relevante, uma vez que as matrizes possuem aplicações próprias e significativas em diferentes contextos matemáticos e tecnológicos, muito além da resolução de sistemas. Essa marginalização curricular pode contribuir para que professores e materiais didáticos tratem o tema de forma apressada ou excessivamente instrumental, reforçando uma abordagem procedimental em detrimento

da compreensão conceitual. Pesquisas voltadas ao ensino de Álgebra Linear no contexto brasileiro, como as desenvolvidas por Dorier et al. (2000) e Sierpinska (2000), apontam que a dificuldade com conceitos matriciais não é exclusiva do Ensino Médio, estendendo-se ao Ensino Superior. Esses estudos identificam que a principal barreira não está na execução dos algoritmos em si, mas na ausência de compreensão do significado das operações e de sua articulação com outros conceitos matemáticos. Tal perspectiva reforça a necessidade de repensar a abordagem do conteúdo desde a Educação Básica.

3.3 O Ensino Procedimental e seus Limites

Observa-se que, em muitas práticas pedagógicas, o ensino de matrizes tende a privilegiar procedimentos operatórios, como a aplicação de regras de cálculo para adição, multiplicação e determinação de inversa, em detrimento da compreensão conceitual do objeto matemático. Tal abordagem pode contribuir para que os estudantes associem o conteúdo apenas à execução mecânica de algoritmos, sem compreender seu significado ou suas possibilidades de aplicação.

Esse fenômeno não é exclusivo do ensino de matrizes. Skovsmose (2000) denomina de *"educação matemática como exercício"* a prática escolar centrada na repetição de procedimentos descontextualizados, na qual o estudante aprende a operar símbolos sem construir relações de sentido com o que está fazendo. Nessa perspectiva, o conhecimento matemático torna-se um conjunto de regras a serem memorizadas e aplicadas em situações padronizadas, o que compromete tanto a motivação quanto a retenção duradoura dos conceitos.

Freudenthal (1991), ao desenvolver os princípios da Educação Matemática Realística, argumenta que a matemática deve ser aprendida como uma atividade humana de organização da realidade, e não como um sistema fechado de regras prontas. Aplicando essa perspectiva ao ensino de matrizes, seria esperado que os estudantes encontrassem situações nas quais a organização de dados em linhas e colunas surgisse como uma necessidade natural, antes de receberem a definição formal do objeto. Isso raramente ocorre nos materiais didáticos tradicionais, que costumam apresentar a definição formal de matriz antes de qualquer motivação contextual.

Nessa mesma direção, Duval (2003) destaca que a aprendizagem matemática exige a capacidade de transitar entre diferentes registros de representação, ou seja, o numérico, o algébrico, o gráfico e o verbal. No caso das matrizes, o ensino frequentemente se restringe ao registro algébrico, sem explorar representações visuais, situações-problema ou conexões com outros campos do conhecimento. Essa limitação dificulta a construção de uma compreensão multidimensional do conceito, tornando-o frágil diante de situações que

fujam ao formato dos exercícios habituais.

3.4 Dificuldades Identificadas na Literatura

As dificuldades de aprendizagem em matrizes foram identificadas e categorizadas em diferentes pesquisas da área de Educação Matemática. Kuhn (2022) aponta que tais dificuldades estão frequentemente associadas à fragilidade de conhecimentos anteriores, especialmente em operações algébricas básicas e raciocínio lógico, o que compromete a assimilação de conceitos mais elaborados e o desenvolvimento do pensamento matemático abstrato.

Entre as dificuldades mais recorrentes identificadas na literatura, destacam-se: a dificuldade em interpretar a organização dos elementos em linhas e colunas e compreender o que representa cada posição da matriz; a confusão entre a multiplicação de matrizes e a multiplicação de números reais, especialmente no que diz respeito à comutatividade; a dificuldade em compreender por que a multiplicação de matrizes é definida da forma que é, sem perceber a relação com transformações lineares ou sistemas de equações; a incompreensão do significado do determinante como grandeza associada à invertibilidade e à área ou volume em contextos geométricos; e a dificuldade em operar com a matriz inversa sem entender para que ela serve ou em que condições existe.

Essas dificuldades são agravadas quando o professor não dispõe de um repertório diversificado de aplicações e contextos que possibilitem selecionar ou elaborar situações adequadas às características de sua turma. Conforme argumenta Maioli (2012), a contextualização não consiste na aplicação de um procedimento padronizado, mas em um processo que exige do docente domínio do conteúdo e sensibilidade pedagógica para identificar quais conexões são significativas para seus estudantes.

Pesquisas desenvolvidas no âmbito do PROFMAT e de outros programas de pós-graduação em Educação Matemática têm explorado diferentes estratégias para superar essas dificuldades, como o uso de jogos, softwares de geometria dinâmica, modelagem matemática e situações-problema interdisciplinares. Em comum, essas propostas reconhecem que a superação do ensino procedimental exige não apenas a substituição de atividades, mas uma mudança na concepção do que significa ensinar e aprender matemática.

3.5 A Aprendizagem Significativa como Referencial Orientador

Ausubel (2003) propõe que a aprendizagem torna-se significativa quando novas informações se relacionam, de maneira não arbitrária e não literal, com conhecimentos prévios já existentes na estrutura cognitiva do estudante, aos quais denomina *subsunçores*.

Quando essa relação não ocorre, o aprendizado tende a assumir caráter mecânico, superficial e pouco duradouro.

Aplicando esse referencial ao ensino de matrizes, é possível identificar que os subsunçores necessários para uma aprendizagem significativa do conteúdo incluem: a compreensão de operações aritméticas e algébricas básicas; a familiaridade com a organização de dados em tabelas; a noção de função como relação entre conjuntos; e, em nível mais avançado, a compreensão de sistemas de equações lineares. Quando esses conhecimentos prévios não estão consolidados, a introdução formal de matrizes encontra uma estrutura cognitiva pouco receptiva, o que favorece a memorização mecânica em detrimento da compreensão.

Nesse sentido, Ausubel (2003) sugere o uso de organizadores avançados, ou seja, materiais introdutórios que estabelecem pontes entre o que o aluno já sabe e o novo conteúdo como estratégia para preparar a estrutura cognitiva antes da apresentação formal dos conceitos. A *Cifra de Hill* pode cumprir exatamente essa função: ao apresentar uma situação concreta e motivadora que requer o uso de matrizes, ela cria um contexto no qual o estudante percebe a necessidade do conceito antes de aprendê-lo formalmente, favorecendo uma ancoragem mais sólida e significativa.

D'Ambrosio (1996) complementa essa perspectiva ao argumentar que a matemática deve ser compreendida como construção cultural e social, sendo fundamental estabelecer vínculos entre o conhecimento escolar e contextos significativos para os sujeitos da aprendizagem. Nessa direção, a utilização de situações relacionadas à segurança da informação e à comunicação digital, realidades presentes no cotidiano dos estudantes contemporâneos, pode conferir maior relevância ao estudo das matrizes, aproximando o conteúdo escolar de questões que fazem sentido fora da sala de aula.

3.6 A Contextualização como Princípio Pedagógico

A contextualização configura-se como uma estratégia com grande potencial para favorecer a aprendizagem dos estudantes. Para Maioli (2012):

> trata-se de um princípio pedagógico potencialmente rico para melhorar a aprendizagem de matemática dos alunos, mas que precisa ser compreendido em seus propósitos e usos pelos diferentes atores do processo de ensino e aprendizagem.[p. 31]

Essa observação é importante porque a contextualização não deve ser confundida com a simples inserção de enunciados com personagens ou situações do cotidiano, prática

que muitas vezes não passa de uma contextualização superficial, sem alterar a natureza procedimental da atividade.

Uma contextualização efetiva, segundo Skovsmose (2000), é aquela que coloca o estudante diante de uma situação na qual o uso da matemática é genuinamente necessário para compreender ou transformar um aspecto da realidade. Nesse sentido, a criptografia apresenta-se como um campo particularmente fértil: a necessidade de proteger informações é uma demanda real e contemporânea, e os métodos criptográficos que envolvem matrizes permitem que o estudante experiencie o uso do conteúdo em uma situação com finalidade clara e socialmente reconhecível.

Além disso, a criptografia tem a vantagem pedagógica de tornar visíveis as consequências dos erros matemáticos: uma multiplicação incorreta produz uma mensagem indecifrável, o que cria um incentivo natural para a verificação e a correção dos procedimentos. Esse aspecto está alinhado ao que Brousseau (1997) denomina situações de validação, nas quais o próprio contexto do problema oferece ao estudante meios de verificar a correção de suas respostas, reduzindo a dependência exclusiva da autoridade do professor como fonte de verdade matemática.

A análise desenvolvida neste capítulo permite identificar que as dificuldades no ensino e na aprendizagem de matrizes decorrem de fatores interligados: uma abordagem curricular que trata o conteúdo de forma marginal e instrumental; práticas pedagógicas centradas na execução mecânica de algoritmos; ausência de conexões entre o objeto matemático e situações que confiram sentido às operações; e fragilidade de conhecimentos prévios que sustentariam uma aprendizagem mais consistente.

Diante desse quadro, a *Cifra de Hill* surge como um campo de aplicação capaz de articular o ensino de matrizes a situações concretas, motivadoras e matematicamente ricas. Ao exigir o uso integrado de multiplicação matricial, determinantes, matrizes inversas e aritmética modular em um contexto com finalidade clara, a *Cifra de Hill* oferece condições para que a aprendizagem ocorra de forma mais significativa, conforme os referenciais discutidos. O capítulo seguinte apresenta uma discussão sobre criptografia que aprofunda essa articulação, estabelecendo os fundamentos necessários para a compreensão da proposta didática desenvolvida nesta dissertação.

4 CRIPTOGRAFIA

As dificuldades identificadas no ensino de matrizes indicam a necessidade de contextos que favoreçam a significação desse conteúdo. Entre tais possibilidades, destaca-se a criptografia, cuja relação com a matemática justifica sua exploração neste trabalho. Dessa forma, este capítulo objetiva apresentar o conceito de criptografia e discutir seu desenvolvimento histórico, destacando os principais marcos que contribuíram para sua consolidação como área de estudo. Inicialmente, será apresentado um panorama histórico geral da criptografia, situando seu surgimento e evolução. Em seguida, o texto será organizado em quatro momentos principais: a criptografia na Antiguidade, com ênfase nos métodos clássicos de substituição; os avanços ocorridos na Idade Média, especialmente no campo da criptoanálise; o desenvolvimento da criptografia moderna, impulsionado pelos conflitos mundiais e a criptografia na era da computação.

Segundo Singh (2001), a Criptografia (*kripto* = escondido, oculto e *grápho* = grafia, escrita) pode ser compreendida como o conjunto de técnicas destinadas a transformar mensagens em códigos, de modo que apenas os destinatários autorizados sejam capazes de interpretá-las. Seu principal objetivo é garantir a confidencialidade e a segurança das informações transmitidas, protegendo-as contra acessos indevidos. Embora suas origens remontem à Antiguidade, a criptografia tornou-se essencial na sociedade contemporânea, estando presente em diversas atividades cotidianas, como transações bancárias, compras online e aplicativos de mensagens, evidenciando sua relevância na proteção da comunicação digital.

De acordo com Stinson e Paterson (2019), a criptografia pode ser classificada em dois grandes tipos: *simétrica* e *assimétrica*. Embora ambos tenham como objetivo comum a proteção da informação, distinguem-se principalmente pela forma de utilização das chaves e pelo nível de segurança oferecido. Enquanto a criptografia simétrica é mais simples e eficiente em termos de velocidade, a criptografia assimétrica se destaca pela maior robustez na proteção das mensagens. A Tabela 2 sintetiza as principais diferenças entre esses dois tipos de criptografia, apresentando suas características, vantagens, limitações e exemplos.

Tabela 2 – Comparação entre criptografia simétrica e assimétrica

Aspecto	**Criptografia Simétrica**	**Criptografia Assimétrica**
Uso das chaves	Utiliza a mesma chave para codificação e decodificação.	Utiliza duas chaves distintas: uma pública (codificação) e uma privada (decodificação).
Velocidade de processamento	Geralmente mais rápida, pois envolve operações matemáticas menos complexas.	Mais lenta, devido à utilização de algoritmos baseados em operações matemáticas avançadas.
Distribuição das chaves	Requer que a chave seja compartilhada previamente de forma segura entre as partes.	A chave pública pode ser distribuída livremente, sem comprometer a segurança.
Segurança	Menor segurança em caso de interceptação da chave, já que é a mesma.	Maior segurança, pois a chave privada não é compartilhada.
Exemplos	Cifra de César, Cifra de Hill, DES, AES.	RSA, ECC (Criptografia de Curvas Elípticas).
Aplicações comuns	Sistemas de criptografia em massa, armazenamento de dados, criptografia de discos.	Certificados digitais, assinaturas eletrônicas, protocolos de internet (HTTPS, SSL/TLS).

Fonte: Elaborado pelo autor (2026).

A comparação evidencia que a escolha entre criptografia simétrica e assimétrica depende diretamente do contexto de aplicação. Em situações que exigem rapidez e processamento de grandes volumes de dados, como no armazenamento de informações ou na proteção de arquivos locais, os métodos simétricos se mostram mais adequados. Por outro lado, quando a prioridade é garantir maior segurança na troca de informações em ambientes abertos, como a internet, os métodos assimétricos são preferíveis, ainda que demandem maior custo computacional. Dessa forma, compreender as diferenças entre essas abordagens é essencial tanto para aplicações práticas em segurança digital quanto para fins pedagógicos, já que possibilita uma associação de conceitos matemáticos abstratos com o uso de problemas práticos e concretos na sociedade contemporânea.

4.1 Panorama Histórico da Criptografia

4.1.1 Criptografia na Antiguidade

A criptografia tem suas origens associadas à necessidade humana de proteger informações estratégicas, especialmente em contextos políticos e militares. Desde as primeiras

civilizações organizadas, a transmissão segura de mensagens constituiu elemento essencial para a manutenção do poder e da segurança. Ao longo da história, diferentes métodos de codificação de mensagens foram criados e aperfeiçoados em função das necessidades políticas, militares e sociais de cada época (SINGH, 2001).

Entre os registros mais antigos de técnicas criptográficas encontra-se a *escítala espartana*, utilizada na Grécia Antiga. Esse dispositivo consistia em um bastão cilíndrico em torno do qual se enrolava uma tira de couro ou pergaminho; a mensagem era escrita longitudinalmente e só podia ser lida corretamente por quem possuísse um bastão de mesmo diâmetro, caracterizando um mecanismo de transposição conforme a Figura 4.

Figura 4 – Escítala Espartana

Fonte: https://www.mj2artesanos.es/blog/category/replicas/. Acesso em: 21 fev. 2026.

No Império Romano, destaca-se a chamada *Cifra de César*, atribuída a Júlio César, que de acordo com Faleiros (2011), empregava um método de substituição simples ao deslocar o alfabeto três casas adiante para codificar suas mensagens, como pode ser visualizado na Tabela 3.

Tabela 3 – A cifra de César

Letra Original	**Letra Modificada**
A	D
B	E
C	F
D	G
E	H
⋮	⋮

Fonte: Elaborado pelo autor (2026).

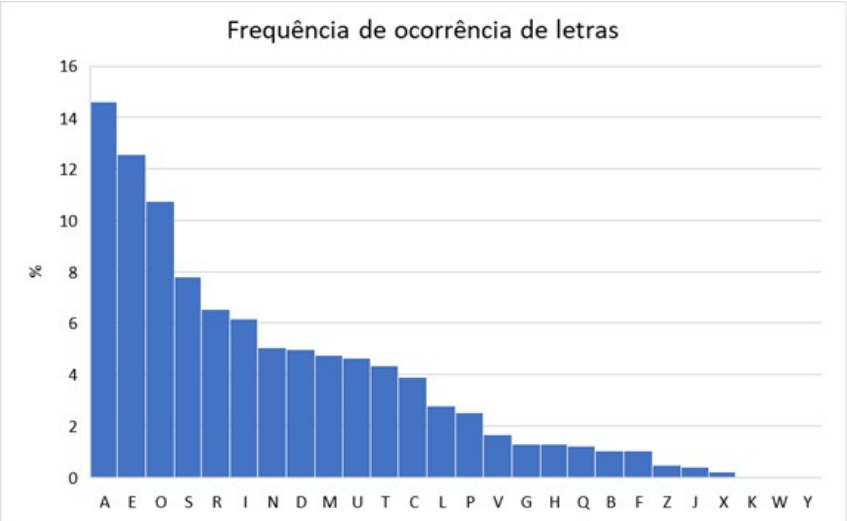
Esses métodos antigos eram, em geral, monoalfabéticos e relativamente vulneráveis à análise de frequência, técnica que começaria a ser formalmente explorada séculos depois. Ainda assim, constituíram os fundamentos da criptografia clássica, ao estabelecerem os princípios de substituição e transposição que perdurariam por muitos séculos (SINGH, 2001).

4.1.2 Idade Média e Avanços na Criptoanálise

Durante a Idade Média, o desenvolvimento da criptografia esteve fortemente ligado às comunicações diplomáticas e religiosas. No mundo islâmico, estudiosos realizaram contribuições decisivas para a criptoanálise. Entre eles, destaca-se *Al-Kindi* (801-873), que, no século IX, sistematizou o método de análise de frequência para quebrar cifras de substituição monoalfabética (BROEMELING, 2011).

A análise de frequência constitui uma ferramenta básica para a criptoanálise de cifras clássicas de substituição, uma vez que tais cifras preservam as características estatísticas do idioma original. Esse método, também denominado ataque estatístico, baseia-se no princípio de que quanto maior o texto cifrado, mais representativos tornam-se os padrões de repetição, facilitando a identificação de letras e palavras de uso frequente na língua. De acordo com Quaresma e Pinho (2007), para se obter um estudo estatístico confiável de uma língua, é necessário selecionar um conjunto amplo e representativo de textos, cobrindo diferentes autores, contextos históricos e estilos literários. Os autores analisaram 95 textos de 38 autores da língua portuguesa contemporânea, totalizando mais de 5 milhões de letras, cujos resultados permitem representar a frequência relativa das letras do alfabeto português, conforme o histograma organizado pelo autor a partir desse estudo na Figura 5.

Figura 5 – Histograma por ordem de frequência



Fonte: Elaborado pelo autor (2026).

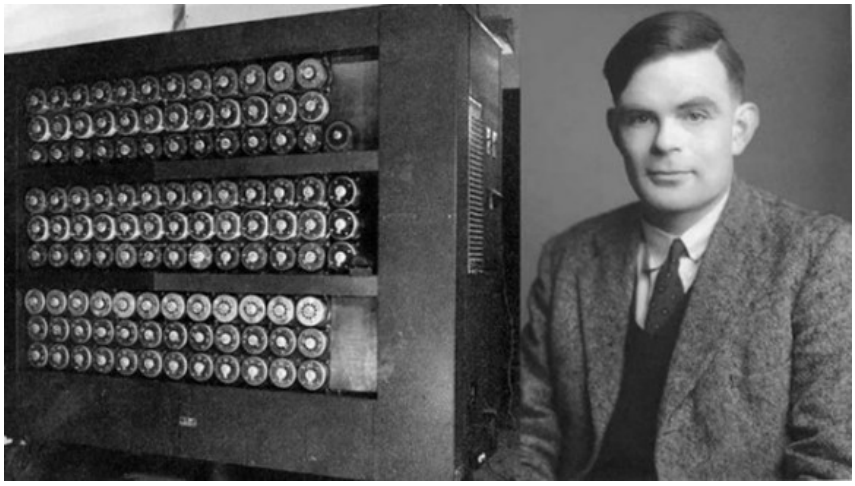
A partir desse período, a necessidade de sistemas mais seguros levou ao desenvolvimento das cifras polialfabéticas, que buscavam dificultar a identificação de padrões estatísticos. Entre os métodos mais conhecidos está a Cifra de Vigenère, amplamente utilizada entre os séculos XVI e XIX, considerada por muito tempo indecifrável.

4.1.3 Criptografia Moderna e os Conflitos Mundiais

O século XX marcou uma transformação profunda na história da criptografia, impulsionada principalmente pelos conflitos mundiais. Durante a Primeira e a Segunda Guerra Mundial, a segurança das comunicações militares tornou-se questão estratégica de grande relevância.

Nesse contexto, ganhou notoriedade a máquina *Enigma*, utilizada pela Alemanha nazista para cifrar mensagens. O esforço para decifrar seus códigos envolveu matemáticos e criptógrafos, entre os quais se destacou *Alan Turing* (1912 – 1954), cujo trabalho foi fundamental para o desenvolvimento de técnicas sistemáticas de quebra de cifras. Na Figura 6, apresentam-se a máquina alemã ENIGMA e o retrato do matemático Alan Turing respectivamente, cujos esforços não apenas contribuíram para o desfecho da guerra, mas também impulsionaram o avanço da computação e da teoria da informação.

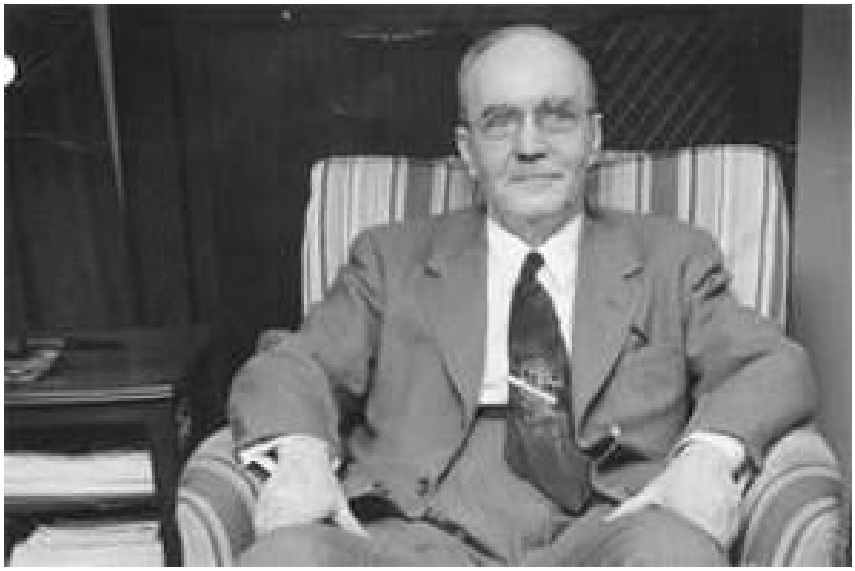
Figura 6 – A máquina ENIGMA e Alan Turing



Fonte: https://outraspalavras.net/outrasmidias/o-desafio-de-alan-turing-a-inteligencia-humana/. Acesso em: 21 fev. 2026.

Paralelamente, em 1929, *Lester Sanders Hill* (1891 – 1961), retratado na Figura 7, propôs a *Cifra de Hill*, que introduziu formalmente o uso de matrizes e álgebra linear em sistemas criptográficos. Essa proposta representou um marco ao aproximar explicitamente a criptografia da matemática abstrata, especialmente das estruturas algébricas.

Figura 7 – Lester Sanders Hill



Fonte: https://alchetron.com/Lester-S-Hill. Acesso em: 21 fev. 2026.

4.1.4 A Criptografia na Era da Computação

Com o advento dos computadores na segunda metade do século XX, a criptografia passou por uma profunda transformação conceitual e tecnológica. Métodos que anteriormente dependiam de dispositivos mecânicos ou procedimentos manuais foram gradualmente substituídos por algoritmos matemáticos executados em ambientes computacionais. Essa mudança ampliou significativamente a complexidade e a eficiência dos sistemas criptográficos, permitindo o processamento de grandes volumes de dados em tempos cada vez menores. Nesse contexto, a criptografia passou a apoiar-se de maneira mais intensa em áreas da matemática como a teoria dos números, a álgebra abstrata, a teoria da complexidade computacional e a probabilidade (STINSON; PATERSON, 2019).

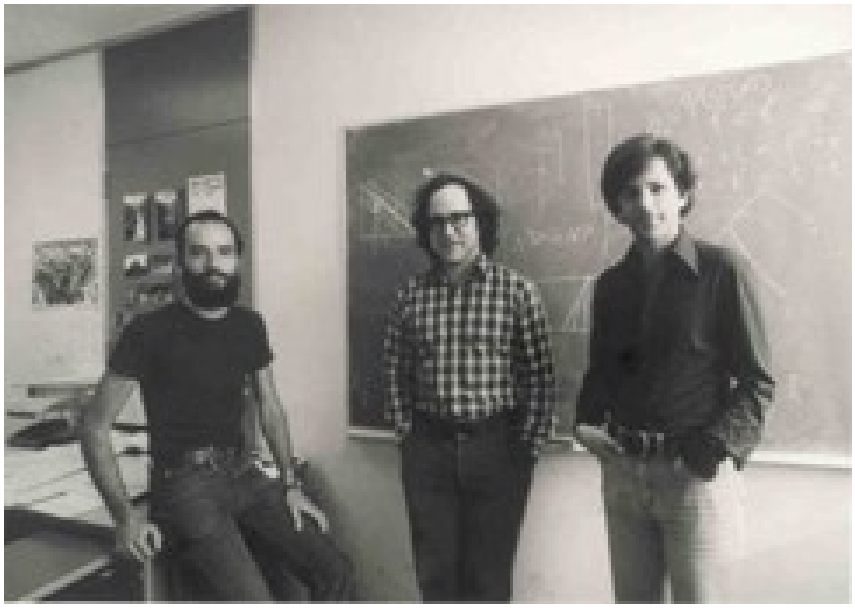
A crescente utilização de computadores em ambientes militares, governamentais e posteriormente comerciais intensificou a necessidade de métodos seguros de proteção da informação. Durante a Guerra Fria, muitos dos avanços na área de criptografia foram conduzidos por instituições governamentais e centros de pesquisa ligados à segurança nacional. Com o avanço da tecnologia digital e a expansão das redes de comunicação, tornou-se evidente que os métodos criptográficos clássicos, baseados em substituições e transposições simples, já não eram suficientes para garantir a confidencialidade das informações transmitidas.

Um marco importante nesse processo ocorreu na década de 1970 com o desenvolvimento da criptografia de chave pública. Até então, os sistemas criptográficos eram predominantemente de chave simétrica, isto é, utilizavam a mesma chave tanto para

criptografar quanto para decodificar uma mensagem. Esse modelo apresentava um desafio logístico significativo: a necessidade de compartilhar previamente a chave secreta entre os participantes da comunicação de forma segura.

Nesse contexto, em 1977, os pesquisadores *Ron Rivest*, *Adi Shamir* e *Leonard Adleman*, retratados na Figura 8, desenvolveram o algoritmo RSA (abreviatura de seus sobrenomes), considerado um dos marcos fundamentais da criptografia moderna.

Figura 8 – Da esquerda para a direita: Ron Rivest, Adi Shamir e Leonard Adleman



Fonte: https://mathshistory.st-andrews.ac.uk/Biographies/Adleman/pictdisplay/. Acesso em: 15 mar. 2026.

O sistema RSA introduziu o conceito de criptografia assimétrica, no qual são utilizadas duas chaves distintas: uma chave pública, que pode ser divulgada livremente, e uma chave privada, mantida em segredo pelo destinatário da mensagem. A segurança do algoritmo baseia-se em propriedades matemáticas relacionadas à dificuldade computacional da fatoração de números inteiros muito grandes, problema que, até o momento, não possui solução eficiente conhecida para computadores clássicos (**??**).

A introdução da criptografia de chave pública representou uma mudança paradigmática na forma como as informações poderiam ser protegidas. Esse modelo permitiu resolver o problema da distribuição de chaves, possibilitando que usuários que nunca tiveram contato prévio pudessem estabelecer comunicações seguras por meio de canais abertos. Tal avanço foi essencial para o desenvolvimento de aplicações modernas como o comércio eletrônico, as assinaturas digitais e os protocolos de segurança utilizados na internet.

Além do RSA, diversos outros algoritmos criptográficos foram desenvolvidos ao longo das décadas seguintes. Entre eles destacam-se os sistemas de criptografia simétrica, como o DES (*Data Encryption Standard*), adotado como padrão pelo governo dos Estados Unidos na década de 1970, e posteriormente o AES (*Advanced Encryption Standard*), que passou a substituí-lo no início do século XXI devido às suas propriedades de segurança mais robustas. Esses algoritmos são amplamente utilizados para a criptografia de grandes volumes de dados devido à sua alta eficiência computacional.

Outro avanço significativo ocorreu com o desenvolvimento das funções de *hash criptográficas*, que transformam dados de tamanho arbitrário em sequências de tamanho fixo. Essas funções desempenham papel fundamental em diversos mecanismos de segurança digital, como a verificação de integridade de arquivos, autenticação de usuários e construção de assinaturas digitais.

Com a expansão da internet a partir da década de 1990, a criptografia passou a desempenhar papel central na proteção das comunicações digitais. Protocolos de segurança como SSL/TLS tornaram-se essenciais para garantir a confidencialidade e a integridade das informações transmitidas em redes públicas. Atualmente, praticamente todas as transações realizadas na internet — desde o acesso a serviços bancários até compras em plataformas digitais — utilizam algum tipo de sistema criptográfico.

Nos últimos anos, novas áreas de pesquisa têm emergido no campo da criptografia, como a criptografia baseada em curvas elípticas, que oferece níveis elevados de segurança com chaves menores, e a chamada criptografia pós-quântica, que busca desenvolver algoritmos resistentes a possíveis ataques provenientes de computadores quânticos. Essas pesquisas demonstram que a criptografia continua sendo uma área dinâmica, profundamente conectada aos avanços tecnológicos e científicos (KATZ; LINDELL, 2021).

Dessa forma, a criptografia na era da computação consolidou-se como um campo interdisciplinar que integra matemática, ciência da computação e engenharia da informação. Seu desenvolvimento não apenas transformou os mecanismos de proteção de dados, mas também se tornou elemento fundamental para o funcionamento seguro das infraestruturas digitais que sustentam a sociedade contemporânea.

Nesse amplo panorama histórico e conceitual da criptografia, destaca-se a *Cifra de Hill*, método que evidencia de modo particular a articulação entre criptografia e conceitos da Álgebra Linear. Por essa razão, o capítulo seguinte dedica-se à apresentação desse método, destacando seus fundamentos, seu funcionamento e seu potencial como estratégia didática para o ensino de matrizes.

5 A CIFRA DE HILL

Este capítulo tem como objetivo compreender o conceito da *Cifra de Hill*, desenvolvida graças aos avanços nos campos da Álgebra e da Teoria dos Números, como matrizes e operações em sistemas numéricos, possibilitando novas formas de tratamento matemático da informação. De acordo com Singh (2001), a história da criptografia está profundamente ligada ao progresso da matemática e da ciência da computação, sendo marcada por sucessivas tentativas de proteger mensagens contra interceptações e interpretações não autorizadas.

Nesse cenário de desenvolvimento científico, em 1929 o matemático norte-americano *Lester S. Hill* apresentou um método criptográfico que ficaria conhecido como *Cifra de Hill*. Esse sistema baseia-se na transformação de blocos de letras em vetores numéricos e na aplicação de multiplicações matriciais em aritmética modular, geralmente considerando o conjunto dos inteiros módulo 26 quando se utiliza o alfabeto latino. Tal procedimento introduziu um nível de complexidade superior aos métodos criptográficos clássicos, ampliando a segurança das mensagens e evidenciando a possibilidade de aplicar conceitos da álgebra linear em problemas de comunicação e proteção de informações (KAHN, 1996).

Além de seu caráter inovador, a *Cifra de Hill* destacou-se por incorporar explicitamente estruturas algébricas formais ao processo de criptografia, permitindo que propriedades de matrizes, como determinante, invertibilidade e operações sobre o anel $\mathbb{Z}_{26}$, desempenhassem papel fundamental na segurança do método. Essa característica representou um avanço importante em relação às cifras clássicas baseadas apenas em substituições simples ou transposições. Conforme destacam Stinson e Paterson (2019), a utilização de ferramentas algébricas em sistemas criptográficos constitui um passo importante para o desenvolvimento da criptografia moderna.

Outro aspecto relevante da *Cifra de Hill* está relacionado à sua capacidade de operar com blocos maiores de caracteres. Ao realizar transformações simultâneas em grupos de símbolos, o método reduz a eficácia de ataques baseados exclusivamente na análise de frequência de letras individuais, técnica frequentemente utilizada na criptoanálise de cifras clássicas. Dessa forma, o sistema dificulta a identificação de padrões linguísticos e exige do atacante um conhecimento matemático mais elaborado para a quebra da cifra.

Do ponto de vista educacional, o estudo da *Cifra de Hill* apresenta grande potencial pedagógico, especialmente no ensino de matrizes, aritmética modular e transformações lineares. Seu funcionamento possibilita a visualização de aplicações concretas de conceitos

matemáticos frequentemente considerados abstratos pelos estudantes. Segundo Ausubel (2003), a aprendizagem significativa ocorre quando novas informações são incorporadas à estrutura cognitiva do sujeito por meio de relações substantivas com conhecimentos previamente existentes. Nesse processo, os conhecimentos prévios desempenham papel fundamental, pois possibilitam a atribuição de significado ao novo conteúdo, favorecendo a retenção e a compreensão duradoura do conhecimento.

A compreensão da *Cifra de Hill* como método criptográfico exige o domínio de alguns conceitos matemáticos fundamentais, especialmente aqueles relacionados às matrizes, à invertibilidade e à aritmética modular. Por esse motivo, o capítulo seguinte apresenta os fundamentos matemáticos que sustentam o funcionamento do método e sua utilização como estratégia didática para o ensino de matrizes.

6 BASES MATEMÁTICAS

Neste capítulo, serão apresentadas definições e resultados relacionados às matrizes, com base em Álgebra Linear com Aplicações de Anton e Rorres (2001), Álgebra Linear de Boldrini et al. (1986) e Álgebra Linear de Steinbruch e Winterle (1987). Também serão apresentados conceitos de aritmética modular, fundamentados em Santos (2020), Lima (2012) e Evaristo e PERDIGÃO (2002), os quais constituem a base necessária para a compreensão do método de Hill.

6.1 Definições e Proposições

Definição 6.1.1 (Formal)**.** Uma matriz de ordem $m \times n$ é uma disposição retangular de elementos a_{ij}, pertencentes a um conjunto numérico K (em geral $\mathbb{R}$), organizada em m linhas e n colunas. Denota-se por

$$A = [a_{ij}]_{m\times n}, \quad \text{com } 1 \leq i \leq m,\ 1 \leq j \leq n \text{ e } m, n \in \mathbb{N},$$

onde a_{ij} representa o elemento localizado na i-ésima linha e na j-ésima coluna. O conjunto de todas as matrizes de ordem $m \times n$ com entradas em K é denotado por $M_{m\times n}(K)$.

Exemplo 6.1.1. A matriz do Exemplo 2.2.1 pode ser escrita como

$$A = [a_{ij}]_{3\times 2}, \quad \text{com } 1 \leq i \leq 3 \text{ e } 1 \leq j \leq 2,$$

ou seja,

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 8,0 & 7,5 \\ 6,5 & 9,0 \\ 7,0 & 8,5 \end{bmatrix}.$$

Definição 6.1.2. Uma matriz quadrada é uma matriz de ordem $n \times n$, isto é, uma matriz que possui o mesmo número de linhas e de colunas, ou seja,

$$A = [a_{ij}]_{n\times n}, \quad \text{com } 1 \leq i, j \leq n.$$

Nesse caso, dizemos que A é uma matriz quadrada de ordem n.

Exemplo 6.1.2. As matrizes

$$A = \begin{bmatrix} 2 & -1 \\ 0 & 3 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 1 & 1 & -1 \\ 0 & 3 & 2 \\ -2 & 4 & 5 \end{bmatrix}$$

são matrizes quadradas de ordem 2 e 3, respectivamente.

Definição 6.1.3. Dadas duas matrizes $A = [a_{ij}]_{m\times n}$ e $B = [b_{jk}]_{n\times p}$, definimos o produto $A \cdot B = C = [c_{ik}]_{m\times p}$ como a matriz de ordem $m \times p$ cujos elementos são obtidos por

$$c_{ik} = \sum_{j=1}^{n} a_{ij} \cdot b_{jk}, \quad \text{para } 1 \leq i \leq m \text{ e } 1 \leq k \leq p.$$

Em outras palavras, cada elemento c_{ik} resulta do somatório dos produtos entre os elementos da i-ésima linha de A e da k-ésima coluna de B. Essa operação está bem definida somente quando o número de colunas de A coincide com o número de linhas de B.

Exemplo 6.1.3. Sejam as matrizes

$$A = \begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix}.$$

Como a matriz A tem 2 colunas e a matriz B tem 2 linhas, o produto está definido e pode ser obtido pela matriz

$$C = A \cdot B = \begin{bmatrix} 1\cdot 0 + 2\cdot 2 & 1\cdot(-1) + 2\cdot 1 & 1\cdot 3 + 2\cdot 0 \\ -3\cdot 0 + 4\cdot 2 & -3\cdot(-1) + 4\cdot 1 & -3\cdot 3 + 4\cdot 0 \end{bmatrix} = \begin{bmatrix} 4 & 1 & 3 \\ 8 & 7 & -9 \end{bmatrix}.$$

Observação 6.1.1. Em geral, a multiplicação de matrizes não é comutativa, isto é, existem matrizes quadradas A e B de mesma ordem tais que

$$A \cdot B \neq B \cdot A.$$

Para ilustrar esse fato, basta apresentar um contraexemplo. Considere as matrizes

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix}.$$

Inicialmente, calculemos o produto:

$$A \cdot B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ 3 & 1 \end{bmatrix}.$$

Agora, calculando $B \cdot A$, temos:

$$B \cdot A = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}.$$

Observa-se que $A \cdot B \neq B \cdot A$, portanto a multiplicação de matrizes não é comutativa em geral.

Proposição 6.1.1. A multiplicação de matrizes é associativa, isto é, se A, B e C são matrizes de ordens compatíveis (de modo que os produtos envolvidos estejam definidos), então

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

Demonstração. Sejam $A = (a_{ij})$ uma matriz de ordem $m \times n$, $B = (b_{jk})$ uma matriz de ordem $n \times p$ e $C = (c_{kl})$ uma matriz de ordem $p \times q$. Vamos mostrar que o elemento genérico da linha i e coluna l de $(A \cdot B) \cdot C$ é igual ao elemento correspondente de $A \cdot (B \cdot C)$.

Primeiramente, o elemento (i, k) da matriz $A \cdot B$ é dado por

$$(A \cdot B)_{ik} = \sum_{j=1}^{n} a_{ij}\, b_{jk}.$$

Logo, o elemento (i, l) da matriz $(A \cdot B) \cdot C$ é

$$\Big[(A \cdot B) \cdot C\Big]_{il} = \sum_{k=1}^{p} (A \cdot B)_{ik}\, c_{kl} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} a_{ij}\, b_{jk} \right) c_{kl} = \sum_{k=1}^{p} \sum_{j=1}^{n} a_{ij}\, b_{jk}\, c_{kl}.$$

Por outro lado, o elemento (j, l) da matriz $B \cdot C$ é dado por

$$(B \cdot C)_{jl} = \sum_{k=1}^{p} b_{jk}\, c_{kl}.$$

Assim, o elemento (i, l) da matriz $A \cdot (B \cdot C)$ é

$$\Big[A \cdot (B \cdot C)\Big]_{il} = \sum_{j=1}^{n} a_{ij}\, (B \cdot C)_{jl} = \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{p} b_{jk}\, c_{kl} \right) = \sum_{j=1}^{n} \sum_{k=1}^{p} a_{ij}\, b_{jk}\, c_{kl}.$$

Como as somas finitas podem ser reordenadas livremente (comutatividade e associatividade da adição de números reais), segue que

$$\sum_{k=1}^{p} \sum_{j=1}^{n} a_{ij}\, b_{jk}\, c_{kl} = \sum_{j=1}^{n} \sum_{k=1}^{p} a_{ij}\, b_{jk}\, c_{kl},$$

ou seja, $\Big[(A \cdot B) \cdot C\Big]_{il} = \Big[A \cdot (B \cdot C)\Big]_{il}$ para todo i e todo l. Portanto,

$$(A \cdot B) \cdot C = A \cdot (B \cdot C),$$

como queríamos demonstrar. □

Definição 6.1.4. A matriz identidade, denotada por I_n, é a matriz quadrada de ordem n cujos elementos da diagonal principal são iguais a 1 e todos os demais iguais a 0, ou seja,

$$a_{ij} = \begin{cases} 1, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases}$$

Exemplo 6.1.4. As matrizes

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{e} \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

são as matrizes identidades de ordem 2 e 3, respectivamente.

Proposição 6.1.2. Seja A uma matriz quadrada de ordem n e seja I_n a matriz identidade de mesma ordem. Então

$$A \cdot I_n = I_n \cdot A = A,$$

isto é, a matriz identidade comuta com qualquer matriz quadrada de mesma ordem, funcionando como elemento neutro da multiplicação de matrizes.

Demonstração. Seja $A = (a_{ij})$ uma matriz quadrada de ordem n e seja $I_n = (\delta_{ij})$ a matriz identidade de ordem n, em que δ_{ij} é o delta de Kronecker, definido por

$$\delta_{ij} = \begin{cases} 1, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases}$$

Vamos mostrar inicialmente que $A \cdot I_n = A$. O elemento (i, j) do produto $A \cdot I_n$ é dado por

$$(A \cdot I_n)_{ij} = \sum_{k=1}^{n} a_{ik}\, \delta_{kj}.$$

Como $\delta_{kj} = 0$ para todo $k \neq j$ e $\delta_{jj} = 1$, apenas o termo em que $k = j$ é não nulo na soma, restando

$$(A \cdot I_n)_{ij} = a_{ij}.$$

Logo, $A \cdot I_n = A$.

Analogamente, mostremos que $I_n \cdot A = A$. O elemento (i, j) do produto $I_n \cdot A$ é dado por

$$(I_n \cdot A)_{ij} = \sum_{k=1}^{n} \delta_{ik}\, a_{kj}.$$

Novamente, como $\delta_{ik} = 0$ para todo $k \neq i$ e $\delta_{ii} = 1$, apenas o termo em que $k = i$ é não nulo, restando

$$(I_n \cdot A)_{ij} = a_{ij}.$$

Logo, $I_n \cdot A = A$.

Portanto,

$$A \cdot I_n = I_n \cdot A = A,$$

como queríamos demonstrar. □

Definição 6.1.5. Seja $A \in M_{n\times n}(\mathbb{R})$. Dizemos que A é invertível ou não singular quando existe uma matriz $B \in M_{n\times n}(\mathbb{R})$ tal que

$$A \cdot B = B \cdot A = I_n.$$

Nesse caso, B é denominada matriz inversa de A e denotamos $B = A^{-1}$.

Proposição 6.1.3. Se $A \in M_{n\times n}(\mathbb{R})$ possui inversa, então essa inversa é única.

Demonstração. Suponha que A possua duas matrizes inversas, B e C, isto é,

$$A \cdot B = B \cdot A = I_n$$

e

$$A \cdot C = C \cdot A = I_n.$$

Escrevendo $B = B \cdot I_n$ e substituindo $I_n = A \cdot C$, obtemos

$$B = B \cdot (A \cdot C).$$

Pela associatividade da multiplicação de matrizes,

$$B = (B \cdot A) \cdot C.$$

Como $B \cdot A = I_n$, segue que

$$B = I_n \cdot C = C.$$

Portanto, a inversa, quando existe, é única. □

Definição 6.1.6. Seja $A = (a_{ij}) \in M_{n\times n}(\mathbb{R})$. O determinante de A, denotado por $\det(A)$, é definido recursivamente por:

- Se $n = 1$, então $\det(A) = a_{11}$.
- Se $n \geq 2$, então, fixado j com $1 \leq j \leq n$,

$$\det(A) = \sum_{i=1}^{n} a_{ij}(-1)^{i+j} \det(A(i|j)),$$

onde $A(i|j)$ é a matriz obtida de A pela supressão da i-ésima linha e da j-ésima coluna.

Proposição 6.1.4. Seja $A \in M_{n\times n}(\mathbb{R})$ e seja B a matriz obtida de A trocando-se duas linhas entre si. Então

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

Demonstração. **Passo 1: Fórmula de Leibniz.**

Por definição, o determinante de $A = (a_{ij})$ é dado por

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)},$$

onde S_n é o conjunto de todas as permutações de $\{1, 2, \ldots, n\}$ e $\operatorname{sgn}(\sigma)$ é o sinal da permutação σ ($+1$ se σ é par, -1 se é ímpar).

Passo 2: Trocando duas linhas.

Suponha que B seja obtida de A trocando as linhas p e q (com $p \neq q$). Isso significa que as entradas de B satisfazem

$$b_{pj} = a_{qj}, \qquad b_{qj} = a_{pj}, \qquad b_{ij} = a_{ij} \quad \text{para } i \neq p, q.$$

Aplicando a fórmula de Leibniz a B:

$$\det(B) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, b_{p,\sigma(p)}\, b_{q,\sigma(q)} \prod_{\substack{i=1 \\ i \neq p,q}}^{n} b_{i,\sigma(i)} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, a_{q,\sigma(p)}\, a_{p,\sigma(q)} \prod_{\substack{i=1 \\ i \neq p,q}}^{n} a_{i,\sigma(i)}.$$

Passo 3: Mudança de variável na soma.

Seja $\tau = (p\ q)$ a transposição que troca p e q, e defina $\sigma' = \sigma \circ \tau$. Como τ é uma bijeção de S_n em si mesmo, quando σ percorre todo S_n, σ' também percorre todo S_n. Note que:

$$\sigma'(p) = \sigma(\tau(p)) = \sigma(q), \qquad \sigma'(q) = \sigma(\tau(q)) = \sigma(p), \qquad \sigma'(i) = \sigma(i) \quad \text{para } i \neq p, q.$$

Reescrevendo a expressão do Passo 2 em termos de σ':

$$a_{q,\sigma(p)}\, a_{p,\sigma(q)} \prod_{\substack{i=1 \\ i \neq p,q}}^{n} a_{i,\sigma(i)} = a_{p,\sigma'(p)}\, a_{q,\sigma'(q)} \prod_{\substack{i=1 \\ i \neq p,q}}^{n} a_{i,\sigma'(i)} = \prod_{i=1}^{n} a_{i,\sigma'(i)}.$$

Além disso, como τ é uma transposição (permutação ímpar),

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma' \circ \tau^{-1}) = \operatorname{sgn}(\sigma') \operatorname{sgn}(\tau^{-1}) = -\operatorname{sgn}(\sigma').$$

Passo 4: Conclusão.

Substituindo no Passo 2 e somando agora sobre $\sigma' \in S_n$ (a soma é a mesma, pois $\sigma \mapsto \sigma'$ é uma bijeção de S_n):

$$\det(B) = \sum_{\sigma' \in S_n} \Big(-\operatorname{sgn}(\sigma') \Big) \prod_{i=1}^{n} a_{i,\sigma'(i)} = -\sum_{\sigma' \in S_n} \operatorname{sgn}(\sigma') \prod_{i=1}^{n} a_{i,\sigma'(i)} = -\det(A). \qquad \square$$

Proposição 6.1.5. Seja $A \in M_{n\times n}(\mathbb{R})$. Se A possui duas linhas iguais ou duas colunas iguais, então $\det(A) = 0$.

Demonstração. Vamos demonstrar o caso de linhas iguais; o caso de colunas é análogo, bastando aplicar o resultado a A^T e usar que $\det(A) = \det(A^T)$.

Passo 1: Propriedade da troca de linhas.

Uma propriedade fundamental do determinante é que, se B é obtida de A trocando-se duas linhas entre si, então

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

Passo 2: Aplicando a hipótese.

Suponha que as linhas i e j de A (com $i \neq j$) sejam iguais, isto é, $A_i = A_j$, onde A_k denota a k-ésima linha de A.

Seja B a matriz obtida de A trocando-se as linhas i e j. Como $A_i = A_j$, essa troca não altera a matriz, ou seja,

$$B = A.$$

Passo 3: Conclusão.

Por um lado, pelo Passo 1,

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

Por outro lado, como $B = A$,

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

Igualando as duas expressões:

$$\det(A) = -\det(A) \quad \Longrightarrow \quad 2\det(A) = 0 \quad \Longrightarrow \quad \det(A) = 0.$$

Isso prova o resultado para linhas. Para colunas, se A tem duas colunas iguais, então A^T tem duas linhas iguais, e pelo caso já demonstrado, $\det(A^T) = 0$. Como $\det(A) = \det(A^T)$, segue que

$$\det(A) = 0. \qquad \square$$

Proposição 6.1.6 (Teorema de Binet)**.** Sejam A e B matrizes quadradas de mesma ordem n. Então

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Demonstração. A demonstração é feita em duas etapas: primeiro para o caso em que A é uma matriz elementar, e depois para o caso geral, utilizando o fato de que toda matriz pode ser escrita como produto de matrizes elementares e, eventualmente, de uma matriz com uma linha nula.

Caso 1: A é uma matriz elementar.

Recordemos que uma matriz elementar é obtida a partir da matriz identidade I_n por meio de uma única operação elementar sobre linhas. Há três tipos possíveis:

(i) Multiplicação de uma linha por um escalar não nulo λ: nesse caso, $\det(A) = \lambda$, e sabe-se que $\det(A \cdot B)$ corresponde a multiplicar a linha correspondente de B por λ, de modo que $\det(A \cdot B) = \lambda \cdot \det(B) = \det(A) \cdot \det(B)$.

(ii) Troca de duas linhas: nesse caso, $\det(A) = -1$, e $A \cdot B$ corresponde a trocar as duas linhas correspondentes em B, o que troca o sinal do determinante. Assim, $\det(A \cdot B) = -\det(B) = \det(A) \cdot \det(B)$.

(iii) Substituição de uma linha pela soma dela com um múltiplo de outra linha: nesse caso, $\det(A) = 1$, e essa operação não altera o valor do determinante. Logo, $\det(A \cdot B) = \det(B) = \det(A) \cdot \det(B)$.

Em todos os três casos, portanto, vale $\det(A \cdot B) = \det(A) \cdot \det(B)$ quando A é elementar.

Caso 2: A é não singular.

Se A é invertível, então A pode ser escrita como um produto de matrizes elementares:

$$A = E_1 \cdot E_2 \cdots E_k.$$

Aplicando repetidamente o resultado do Caso 1, obtemos

$$\det(A \cdot B) = \det(E_1 \cdots E_k \cdot B) = \det(E_1) \cdot \det(E_2 \cdots E_k \cdot B) = \cdots = \det(E_1) \cdot \det(E_2) \cdots \det(E_k) \cdot \det(B).$$

Por outro lado, aplicando o mesmo raciocínio a A isoladamente, segue que

$$\det(A) = \det(E_1) \cdot \det(E_2) \cdots \det(E_k).$$

Substituindo, concluímos que

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Caso 3: A é singular.

Se A é singular, então $\det(A) = 0$, e é suficiente mostrar que $A \cdot B$ também é singular, de modo que $\det(A \cdot B) = 0$ e a igualdade se verifica trivialmente. De fato, como A é singular, existe um vetor não nulo $\mathbf{v} \in \mathbb{R}^n$ tal que $A\mathbf{v} = \mathbf{0}$. Suponha, por absurdo, que $A \cdot B$ seja não singular. Então existiria um vetor $\mathbf{w}$ tal que $B\mathbf{w} = \mathbf{v}$ (pois B necessariamente seria sobrejetora caso $A \cdot B$ fosse invertível). Mas então

$$(A \cdot B)\mathbf{w} = A(B\mathbf{w}) = A\mathbf{v} = \mathbf{0},$$

com $\mathbf{w} \neq \mathbf{0}$ (pois $\mathbf{v} \neq \mathbf{0}$), o que contradiz a hipótese de que $A \cdot B$ é não singular. Logo, $A \cdot B$ é singular, e portanto

$$\det(A \cdot B) = 0 = \det(A) \cdot \det(B).$$

Combinando os três casos, concluímos que, para quaisquer matrizes quadradas A e B de mesma ordem,

$$\det(A \cdot B) = \det(A) \cdot \det(B),$$

como queríamos demonstrar. □

Definição 6.1.7. Seja $A \in M_{n\times n}(\mathbb{R})$. Definimos o cofator do elemento a_{ij} da matriz A como

$$\Delta_{ij}^A = (-1)^{i+j} \det(A(i|j)).$$

A matriz $B = \left[\Delta_{ij}^A\right]_{n\times n}$ será chamada de matriz dos cofatores de A e sua transposta será chamada de matriz adjunta de A, denotada por $\text{adj}(A)$.

Proposição 6.1.7. Uma matriz $A \in M_{n\times n}(\mathbb{R})$ é invertível se, e somente se, $\det(A) \neq 0$.

Demonstração. ($\Rightarrow$) Seja A invertível. Pela definição, existe uma matriz B tal que

$$A \cdot B = B \cdot A = I_n.$$

Aplicando a propriedade do determinante ao produto de matrizes, temos

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Como $A \cdot B = I_n$, segue que

$$\det(A) \cdot \det(B) = \det(I_n) = 1.$$

Portanto, $\det(A) \neq 0$.

($\Leftarrow$) Suponha que $\det(A) \neq 0$.

Passo 1: As colunas de A são linearmente independentes.

De fato, se as colunas $a_1, a_2, \ldots, a_n$ de A fossem linearmente dependentes, alguma coluna poderia ser escrita como combinação linear das demais, digamos

$$a_n = c_1 a_1 + c_2 a_2 + \cdots + c_{n-1} a_{n-1}.$$

Substituindo a_n por $a_n - c_1 a_1 - \cdots - c_{n-1} a_{n-1}$ (operação que não altera o determinante), obteríamos uma coluna nula, e portanto $\det(A) = 0$, contradizendo a hipótese. Logo, as colunas de A são linearmente independentes.

Passo 2: As colunas formam uma base de $\mathbb{R}^n$.

Como A possui n colunas e elas são linearmente independentes em $\mathbb{R}^n$, e todo conjunto de n vetores linearmente independentes em um espaço de dimensão n é uma base, segue que as colunas de A formam uma base de $\mathbb{R}^n$.

Passo 3: O posto de A é n.

O posto de A é, por definição, a dimensão do espaço gerado por suas colunas. Como essas colunas formam uma base de $\mathbb{R}^n$, esse espaço tem dimensão n. Logo,

$$\text{posto}(A) = n.$$

Conclusão.

Como $\text{posto}(A) = n$, a matriz A tem posto completo, e portanto A é invertível. □

Proposição 6.1.8. Seja $A \in M_{n\times n}(\mathbb{R})$. Então,

$$\text{adj}(A) \cdot A = \det(A) \cdot I_n.$$

Demonstração. O elemento da posição (i, j) do produto $\text{adj}(A) \cdot A$ é dado por

$$(\text{adj}(A) \cdot A)_{ij} = \sum_{k=1}^{n} \Delta_{ki}^{A} \, a_{kj}.$$

Se $i = j$, essa soma corresponde à expansão de Laplace do determinante pela coluna j, logo

$$(\text{adj}(A) \cdot A)_{jj} = \det(A).$$

Se $i \neq j$, a soma $\sum_{k=1}^{n} \Delta_{ki}^{A} \, a_{kj}$ é igual ao determinante da matriz obtida de A substituindo sua coluna i pela coluna j. Essa matriz possui duas colunas iguais (a coluna i e a coluna j originais coincidem), portanto seu determinante é zero. Assim,

$$(\text{adj}(A) \cdot A)_{ij} = 0.$$

Portanto,

$$\text{adj}(A) \cdot A = \det(A) \cdot I_n.$$ □

Proposição 6.1.9. Se $A \in M_{n \times n}(\mathbb{R})$ é invertível, então

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A).$$

Demonstração. Se A é invertível, então $\det(A) \neq 0$. Pela proposição anterior,

$$\text{adj}(A) \cdot A = \det(A) \cdot I_n.$$

Multiplicando ambos os lados por $\dfrac{1}{\det(A)}$, obtemos

$$\left(\frac{1}{\det(A)} \text{adj}(A) \right) \cdot A = I_n.$$

Logo,

$$A^{-1} = \frac{1}{\det(A)} \text{adj}(A).$$

□

Definição 6.1.8. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \setminus \{0\}$. Dizemos que a é congruente a b módulo n se a diferença $a - b$ é divisível por n, isto é, existe um inteiro k tal que $a - b = kn$. Escrevemos:

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

Exemplo 6.1.5. Considere as congruências:

1. $17 \equiv 5 \pmod{12}$, pois $17 - 5 = 12$;
2. $25 \equiv 1 \pmod{4}$, pois $25 - 1 = 24 = 6 \cdot 4$;
3. $-3 \equiv 7 \pmod{10}$, pois $-3 - 7 = -10 = (-1) \cdot 10$.

Definição 6.1.9. Dado $n \in \mathbb{N} \setminus \{0\}$, a classe de congruência de um inteiro a módulo n é o conjunto

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Exemplo 6.1.6. A classe de congruência de 3 módulo 5 é

$$[3]_5 = \{\cdots, -7, -2, 3, 8, 13, 18, \cdots\}.$$

Definição 6.1.10. Se $k \in \mathbb{N} \setminus \{0\}$, então

$$\mathbb{Z}_k = \{[0]_k, [1]_k, [2]_k, \ldots, [k-1]_k\}$$

é o conjunto de todos os restos possíveis quando dividimos um inteiro por k.

Exemplo 6.1.7. Temos $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$.

Definição 6.1.11. Um elemento $[a] \in \mathbb{Z}_k$ será invertível quando existir $[b] \in \mathbb{Z}_k$ tal que $[a] \cdot [b] = [1]$. Nesse caso, $[b]$ é chamado de inverso de $[a]$.

Definição 6.1.12. Dados dois inteiros a e b, não ambos nulos, o *máximo divisor comum* (mdc) de a e b, denotado por $\text{mdc}(a, b)$, é o maior inteiro positivo que divide simultaneamente a e b, isto é:

$$\text{mdc}(a, b) = \max\{d \in \mathbb{Z}; d \mid a \text{ e } d \mid b\}$$

Exemplo 6.1.8. Calcule $\text{mdc}(48, 18)$.

Solução: Listando os divisores de cada número:

- Divisores de 48: $1, 2, 3, 4, 6, 8, 12, 16, 24, 48$
- Divisores de 18: $1, 2, 3, 6, 9, 18$

Os divisores comuns são: $1, 2, 3, 6$. Portanto:

$$\text{mdc}(48, 18) = 6$$

Proposição 6.1.10 (Algoritmo da divisão)**.** Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = b \cdot q + r, \quad 0 \leq r < |b|.$$

Demonstração. **Existência.** Considere o conjunto

$$S = \{a - b \cdot q \mid q \in \mathbb{Z}\} \cap \mathbb{Z}_+.$$

Como S é um subconjunto não vazio de $\mathbb{Z}_+$, pelo Princípio da Boa Ordenação (PBO), S possui um elemento mínimo. Seja $r = a - b \cdot q_0$ esse elemento mínimo, para algum $q_0 \in \mathbb{Z}$. Por construção, $r \geq 0$. Resta mostrar que $r < |b|$.

Suponha, por contradição, que $r \geq |b|$. Então

$$r' = r - |b| = a - b \cdot q_0 - |b| \geq 0,$$

e $r' < r$, o que contradiz a minimalidade de r em S. Portanto, $0 \leq r < |b|$, e existem $q, r \in \mathbb{Z}$ satisfazendo $a = b \cdot q + r$.

Unicidade. Suponha que existam $q, q' \in \mathbb{Z}$ e $r, r' \in \mathbb{Z}$ com $0 \leq r, r' < |b|$ tais que

$$a = b \cdot q + r = b \cdot q' + r'.$$

Subtraindo, obtemos $b \cdot (q - q') = r' - r$, logo $|b|$ divide $|r' - r|$. Como $0 \leq |r' - r| < |b|$, a única possibilidade é $|r' - r| = 0$, isto é, $r = r'$. Consequentemente, $b \cdot (q - q') = 0$ e, como $b \neq 0$, conclui-se que $q = q'$. □

Proposição 6.1.11 (Teorema de Bézout)**.** Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Então existem inteiros $x, y \in \mathbb{Z}$ tais que:

$$ax + by = \text{mdc}(a, b)$$

Em outras palavras, o máximo divisor comum de a e b pode ser expresso como combinação linear inteira de a e b.

Demonstração. Seja $d = \text{mdc}(a, b)$ e considere o conjunto:

$$S = \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$$

O conjunto S é não vazio, pois $a^2 + b^2 > 0$ pertence a S. Pelo PBO, S possui um elemento mínimo; seja $m = ax_0 + by_0$ esse mínimo.

Passo 1: $m \mid a$ **e** $m \mid b$**.**

Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ com $0 \leq r < m$ tais que:

$$a = qm + r \implies r = a(1 - qx_0) + b(-qy_0)$$

Se $r > 0$, então $r \in S$, contradizendo a minimalidade de m. Logo $r = 0$, e portanto $m \mid a$. De forma análoga, $m \mid b$.

Passo 2: $d \mid m$**.**

Como $d \mid a$ e $d \mid b$, temos $d \mid (ax_0 + by_0)$, logo $d \mid m$.

Conclusão: Do Passo 1, $m \leq d$. Do Passo 2, $d \leq m$. Portanto $m = d$, ou seja:

$$\text{mdc}(a, b) = ax_0 + by_0. \qquad \square$$

Exemplo 6.1.9. Expresse $\text{mdc}(48, 18)$ como combinação linear de 48 e 18.

Solução: Aplicando o Algoritmo da divisão:

$$\begin{aligned} 48 &= 2 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Logo $\text{mdc}(48, 18) = 6$. Realizando a substituição retroativa:

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ &= 18 - 1 \cdot (48 - 2 \cdot 18) \\ &= 3 \cdot 18 - 1 \cdot 48 \end{aligned}$$

Portanto:

$$\text{mdc}(48, 18) = 48 \cdot (-1) + 18 \cdot (3)$$

Proposição 6.1.12. Um elemento $[a] \in \mathbb{Z}_k$ é invertível se, e somente se, $\text{mdc}(a, k) = 1$.

Demonstração. ($\Rightarrow$) Suponha que $[a]$ seja invertível. Então existe $[b]$ tal que $[a] \cdot [b] = [1]$, ou seja, $ab \equiv 1 \pmod{k}$. Logo, existe um inteiro t tal que $ab - 1 = kt$. Qualquer divisor comum de a e k divide 1, portanto $\text{mdc}(a, k) = 1$.

($\Leftarrow$) Se $\text{mdc}(a, k) = 1$, pelo Teorema de Bézout existem inteiros u, v tais que $au + kv = 1$. Reduzindo módulo k, obtemos $au \equiv 1 \pmod{k}$, logo $[a] \cdot [u] = [1]$ e $[a]$ é invertível. $\square$

Corolário 6.1.1. Seja $A \in M_{n\times n}(\mathbb{R})$. O determinante da matriz A será invertível em $\mathbb{Z}_k$ se $\text{mdc}(\det(A), k) = 1$.

Definição 6.1.13. O conjunto $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$, munido das operações de adição e multiplicação definidas módulo 26, possui estrutura de *anel comutativo*. Para quaisquer $a, b \in \mathbb{Z}_{26}$:

$$a \oplus b \equiv a + b \pmod{26} \qquad \text{e} \qquad a \otimes b \equiv a \cdot b \pmod{26}$$

Nessa estrutura valem: fechamento, associatividade, comutatividade, elemento neutro aditivo, elemento inverso aditivo, elemento neutro multiplicativo e distributividade.

Observação 6.1.1. O anel $\mathbb{Z}_{26}$ **não** é um corpo, pois nem todo elemento não nulo possui inverso multiplicativo. Um elemento $a \in \mathbb{Z}_{26}$ é invertível se, e somente se, $\text{mdc}(a, 26) = 1$. Os elementos invertíveis são:

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

Esses constituem o *grupo multiplicativo* $\mathbb{Z}_{26}^*$.

Os conceitos apresentados neste capítulo constituem a base teórica necessária para compreender o funcionamento da *Cifra de Hill*. Com apoio nesses fundamentos, o próximo capítulo desenvolverá o processo de codificação e decodificação de mensagens, evidenciando a articulação entre teoria matemática e aplicação prática.

7 CODIFICAÇÃO E DECODIFICAÇÃO UTILIZANDO A CIFRA DE HILL

Neste capítulo apresenta-se o funcionamento da *Cifra de Hill*, descrevendo de forma detalhada o processo de codificação e decodificação de mensagens por meio de operações matriciais e aritmética modular. O objetivo não é apenas expor o algoritmo, mas discutir cada etapa sob a perspectiva de seu potencial e de seus desafios no contexto do ensino de matrizes.

A exposição está organizada em duas grandes seções: a codificação (Seção 7.2) e a decodificação (Seção 7.3). Em cada etapa do algoritmo, além do procedimento matemático, são apresentadas **notas pedagógicas** que discutem como o professor pode conduzir aquele momento em sala de aula, quais erros os estudantes tendem a cometer e em quais situações o uso de tecnologia é recomendado sem comprometer a aprendizagem conceitual.

7.1 Considerações Iniciais sobre o Algoritmo

Antes de apresentar o exemplo completo, é necessário situar o estudante diante da estrutura geral do método. A Cifra de Hill opera com **blocos de letras**, transformando-os simultaneamente por meio de uma multiplicação matricial seguida de redução modular. Essa característica a distingue das cifras de substituição simples, como a Cifra de César, e é exatamente o que a torna resistente à análise de frequência de letras individuais (SINGH, 2001).

O funcionamento do método depende de três elementos fundamentais, que precisam estar claros antes de iniciar qualquer exemplo:

1. **A matriz-chave** A, que deve ser invertível em $\mathbb{Z}_{26}$, ou seja, $\text{mdc}(\det(A),\, 26) = 1$ e $\det(A) \neq 0$.
2. **A tabela de conversão** entre letras e números inteiros de 0 a 25.
3. **A operação de redução módulo 26**, que garante que todos os valores resultantes correspondam a uma letra válida do alfabeto latino.

A necessidade de reduzir módulo 26 decorre diretamente do fato de o alfabeto latino possuir exatamente 26 letras. Ao multiplicar um vetor pela matriz-chave, os valores

resultantes podem ser maiores que 26 e portanto, não corresponderiam a nenhuma letra válida. A operação módulo 26 garante que todos os valores permaneçam no intervalo $\{0, 1, 2, \ldots, 25\}$. Em termos matemáticos, se c é o valor resultante da multiplicação, o valor cifrado c' é dado por:

$$c' \equiv c \pmod{26},$$

o que significa que c' é o resto da divisão de c por 26. Por exemplo, se a multiplicação produz o valor 29, tem-se:

$$29 = 1 \cdot 26 + 3 \implies 29 \equiv 3 \pmod{26},$$

que corresponde à letra D. Dessa forma, a redução módulo 26 atua como um mecanismo de *wraparound*, fazendo com que os valores numéricos "circulem" dentro do intervalo do alfabeto.

Nota pedagógica — A redução modular como ponto de partida. Recomenda-se que o professor não apresente a redução modular apenas como uma etapa técnica do algoritmo, mas como uma necessidade que emerge naturalmente do problema. Uma boa estratégia é começar perguntando aos alunos: *"Se eu obtiver o número 57 após uma multiplicação, a qual letra ele corresponderia?"* Diante da impossibilidade imediata, o estudante percebe a necessidade de um sistema de "reciclagem" dos valores, o que motiva a introdução da aritmética modular de forma orgânica. Essa abordagem está alinhada ao princípio da reinvenção guiada de Freudenthal (1991), segundo o qual os estudantes devem encontrar a necessidade do conceito antes de recebê-lo pronto.

7.2 Codificação de Mensagens

Para ilustrar o processo de codificação, será utilizada a mensagem "ATAQUE HOJE". Os passos a seguir constituem o algoritmo completo, apresentado de forma progressiva.

Passo 1 — Escolha da matriz-chave

O primeiro passo consiste em escolher uma matriz-chave $A \in M_{n\times n}(\mathbb{Z})$ invertível em $\mathbb{Z}_{26}$. De acordo com o Corolário 6.1.1, deve-se escolher A tal que $\text{mdc}(\det(A), 26) = 1$. Para este exemplo, adotamos $n = 2$ e a matriz:

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

Verificação da validade da chave:

$$\det(A) = 3 \cdot 5 - 3 \cdot 2 = 15 - 6 = 9.$$

Como mdc(9, 26) = 1, a matriz A é invertível em $\mathbb{Z}_{26}$ e, portanto, válida como chave.

Nota pedagógica — A escolha da matriz-chave. A verificação da condição mdc(det(A), 26) = 1 é um momento privilegiado para retomar o conceito de máximo divisor comum e sua relação com a invertibilidade modular (Proposição 6.1.12). O professor pode propor que os alunos testem outras matrizes e verifiquem, por conta própria, quais são ou não válidas como chave. Por exemplo, a matriz $B = \begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix}$ é tal que $\det(B) = 2$, e como mdc(2, 26) = $2 \neq 1$, ela não é invertível em $\mathbb{Z}_{26}$ e não pode ser usada. Esse exercício de tentativa e verificação fortalece a compreensão do papel do determinante, que com frequência é ensinado apenas como um número a ser calculado, sem que seu significado estrutural seja explorado.

Erro comum: os estudantes podem confundir a condição $\det(A) \neq 0$ em $\mathbb{R}$ com a condição de invertibilidade em $\mathbb{Z}_{26}$. É importante deixar claro que em $\mathbb{Z}_{26}$ não basta o determinante ser não nulo: ele precisa ser coprimo com 26. Por exemplo, det = 13 não nulo em $\mathbb{R}$, mas $\text{mdc}(13, 26) = 13$, logo a matriz não é invertível em $\mathbb{Z}_{26}$.

Passo 2 — Conversão das letras em números

Cada letra do alfabeto é associada a um número inteiro de 0 a 25, conforme a Tabela 4. Essa correspondência transforma a mensagem em uma sequência de vetores numéricos sobre os quais é possível aplicar operações algébricas.

Tabela 4 – Conversão de letras para números

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: Elaborado pelo autor (2026).

A mensagem “ATAQUE HOJE”, ignorando o espaço, é convertida letra a letra:

$$\underbrace{A}_{0}\ \underbrace{T}_{19}\ \underbrace{A}_{0}\ \underbrace{Q}_{16}\ \underbrace{U}_{20}\ \underbrace{E}_{4}\ \underbrace{H}_{7}\ \underbrace{O}_{14}\ \underbrace{J}_{9}\ \underbrace{E}_{4}$$

Sugestão de atividade prévia: antes do exemplo completo, peça aos alunos que convertam palavras de sua escolha em sequências numéricas e depois reconstruam as palavras a partir de sequências dadas. Esse exercício simples consolida a tabela de conversão e reduz erros de substituição nas etapas seguintes.

Passo 3 — Organização em blocos

Como a matriz-chave é 2×2, a mensagem é organizada em blocos de tamanho 2. Cada bloco formará um vetor coluna sobre o qual a multiplicação matricial será aplicada:

$$\mathbf{v}_1 = \begin{pmatrix} 0 \\ 19 \end{pmatrix} \ (AT), \qquad \mathbf{v}_2 = \begin{pmatrix} 0 \\ 16 \end{pmatrix} \ (AQ), \qquad \mathbf{v}_3 = \begin{pmatrix} 20 \\ 4 \end{pmatrix} \ (UE),$$

$$\mathrm{v}_4 = \begin{pmatrix} 7 \\ 14 \end{pmatrix} \ (HO), \qquad \mathbf{v}_5 = \begin{pmatrix} 9 \\ 4 \end{pmatrix} \ (JE).$$

Nota pedagógica — O papel do espaço e de mensagens com número ímpar de letras. O professor deve antecipar que os estudantes podem perguntar: *"O que fazemos com os espaços?"* e *"E se a mensagem tiver um número ímpar de letras se vamos separar em blocos de duas letras?"* Ambas as situações merecem atenção antes de iniciar os cálculos, e não depois.

Quanto aos espaços, a convenção mais simples é ignorá-los na codificação, embora existam variantes que os incluem como um símbolo adicional. Quanto ao número ímpar de letras, a convenção é acrescentar a letra X ao final da mensagem para completar o último bloco. Por exemplo, a palavra "SOL" tornaria-se "SOLX" antes da conversão. O professor pode explorar com os alunos o problema que surgiria se esse preenchimento não fosse feito: o último bloco teria apenas um elemento e a multiplicação matricial não estaria definida.

A escolha do tamanho do bloco não é arbitrária: ela está diretamente ligada à ordem da matriz-chave. O professor pode aproveitar esse momento para perguntar: *"O que aconteceria se usássemos uma matriz* 3×3 *como chave?"* A resposta, blocos de três letras, abre uma discussão natural sobre como a dimensão da chave afeta tanto a segurança do método quanto a complexidade dos cálculos. Matrizes de ordem maior tornam a cifra mais segura, mas também mais trabalhosa. Para o contexto de sala de aula com cálculo manual, a ordem 2 é a mais indicada; para implementações computacionais, ordens maiores são plenamente viáveis e podem ser exploradas em atividades com planilhas ou linguagens de programação.

Passo 4 — Multiplicação matricial e redução módulo 26

Para cada bloco $\mathbf{v}_i$, calcula-se $A \cdot \mathbf{v}_i$ e reduz-se o resultado módulo 26. O resultado é o bloco cifrado $\mathbf{c}_i$.

Bloco 1: $\mathbf{v}_1 = (0,\, 19)^\top$

$$A \cdot \mathbf{v}_1 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 3{\cdot}0 + 3{\cdot}19 \\ 2{\cdot}0 + 5{\cdot}19 \end{pmatrix} = \begin{pmatrix} 57 \\ 95 \end{pmatrix}.$$

Redução:

$$57 = 2{\cdot}26 + 5 \implies 57 \equiv 5 \pmod{26} \quad (F),$$

$$95 = 3{\cdot}26 + 17 \implies 95 \equiv 17 \pmod{26} \quad (R).$$

$$\therefore \quad \mathbf{c}_1 = (5,\, 17)^\top \longrightarrow \mathbf{FR}.$$

Bloco 2: $\mathbf{v}_2 = (0,\, 16)^\top$

$$A \cdot \mathbf{v}_2 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 0 \\ 16 \end{pmatrix} = \begin{pmatrix} 48 \\ 80 \end{pmatrix}.$$

Redução:

$$48 = 1{\cdot}26 + 22 \implies 48 \equiv 22 \pmod{26} \quad (W),$$

$$80 = 3{\cdot}26 + 2 \implies 80 \equiv 2 \pmod{26} \quad (C).$$

$$\therefore \quad \mathbf{c}_2 = (22,\, 2)^\top \longrightarrow \mathbf{WC}.$$

Bloco 3: $\mathbf{v}_3 = (20,\, 4)^\top$

$$A \cdot \mathbf{v}_3 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 20 \\ 4 \end{pmatrix} = \begin{pmatrix} 72 \\ 60 \end{pmatrix}.$$

Redução:

$$72 = 2{\cdot}26 + 20 \implies 72 \equiv 20 \pmod{26} \quad (U),$$

$$60 = 2{\cdot}26 + 8 \implies 60 \equiv 8 \pmod{26} \quad (I).$$

$$\therefore \quad \mathbf{c}_3 = (20,\, 8)^\top \longrightarrow \mathbf{UI}.$$

Bloco 4: $\mathbf{v}_4 = (7,\, 14)^\top$

$$A \cdot \mathbf{v}_4 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 63 \\ 84 \end{pmatrix}.$$

Redução:

$$63 = 2{\cdot}26 + 11 \implies 63 \equiv 11 \pmod{26} \quad (L),$$

$$84 = 3{\cdot}26 + 6 \implies 84 \equiv 6 \pmod{26} \quad (G).$$

$$\therefore \quad \mathbf{c}_4 = (11,\, 6)^\top \longrightarrow \mathbf{LG}.$$

Bloco 5: $\mathbf{v}_5 = (9,\, 4)^\top$

$$A \cdot \mathbf{v}_5 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 9 \\ 4 \end{pmatrix} = \begin{pmatrix} 39 \\ 38 \end{pmatrix}.$$

Redução:

$$39 = 1{\cdot}26 + 13 \implies 39 \equiv 13 \pmod{26} \quad (N),$$

$$38 = 1{\cdot}26 + 12 \implies 38 \equiv 12 \pmod{26} \quad (M).$$

$$\therefore \quad \mathbf{c}_5 = (13,\, 12)^\top \longrightarrow \mathbf{NM}.$$

A mensagem original "ATAQUE HOJE" foi, portanto, cifrada como:

FRWCUILGNM

Nota pedagógica — O custo computacional e o papel da tecnologia. Cada bloco exige dois produtos internos de vetores, dois quocientes e dois restos de divisão. Com cinco blocos, o exemplo completo envolve 20 multiplicações, 10 adições, 10 divisões e 10 operações de resto, tudo isso sujeito a erros de atenção que, no contexto da *Cifra de Hill*, produzem efeitos imediatamente visíveis: uma letra errada na mensagem cifrada resultará, na decodificação, em uma letra incorreta na mensagem recuperada. Esse mecanismo de verificação imediata é uma das virtudes didáticas do método e deve ser explorado pelo professor: o estudante não precisa esperar a correção para saber se acertou, a incoerência do texto decodificado já indica onde ocorreu o erro.

No entanto, é importante reconhecer que o volume de cálculo pode ser um obstáculo ao engajamento, especialmente em turmas com dificuldades em aritmética básica. Algumas estratégias podem ser adotadas:

- **Divisão de trabalho em grupos:** cada grupo realiza a codificação de um bloco e os resultados são reunidos pela turma. Isso reduz o esforço individual sem eliminar o aprendizado.
- **Uso de planilha eletrônica para verificação:** após o cálculo manual, o professor pode mostrar como os mesmos resultados são obtidos em uma planilha (Excel, LibreOffice Calc ou Google Sheets), utilizando as funções `MMULT` (multiplicação matricial) e `MOD` (resto da divisão). Isso não substitui o cálculo manual, mas reforça o resultado e introduz o estudante ao uso de ferramentas computacionais para Álgebra Linear.

- **Uso de calculadora científica para a aritmética:** é recomendável permitir calculadora a partir do Passo 4. O objetivo da atividade é a compreensão do *processo* matricial e da lógica modular, não a fluência em multiplicação de inteiros grandes. Proibir a calculadora nesse ponto frequentemente desvia a atenção do conceito para o cálculo aritmético.

Erro comum: ao realizar a redução modular, pode acontecer de muitos estudantes simplesmente subtraírem 26 do resultado, o que é suficiente apenas quando o resultado está no intervalo [26, 51]. Para valores como 95 ou 80, é necessário subtrair 26 mais de uma vez (ou calcular o quociente e o resto diretamente). O professor deve alertar explicitamente para esse ponto antes de iniciar os cálculos.

Outro erro que pode ocorrer: confundir a ordem do produto $A \cdot \mathbf{v}$ com $\mathbf{v} \cdot A$. Como a multiplicação de matrizes não é comutativa (Observação 6.1.1), essas duas expressões produzem resultados distintos, e $\mathbf{v} \cdot A$ nem sequer está definida quando $\mathbf{v}$ é vetor coluna e A é 2×2. Reforçar a ordem correta do produto é essencial antes de cada bloco.

7.3 Decodificação de Mensagens

A decodificação é o processo inverso: dada a mensagem cifrada "FRWCUILGNM", deseja-se recuperar o texto original "ATAQUEHOJE". Para isso, é necessário calcular a matriz inversa de A em $\mathbb{Z}_{26}$ e aplicá-la a cada bloco cifrado.

Antes de iniciar, convém retomar a estrutura geral: se $\mathbf{c} = A\mathbf{v} \pmod{26}$, então, multiplicando ambos os lados à esquerda por A^{-1}:

$$A^{-1}\mathbf{c} \equiv A^{-1}(A\mathbf{v}) \equiv \mathbf{v} \pmod{26}.$$

O vetor original $\mathbf{v}$ é recuperado. A existência de A^{-1} em $\mathbb{Z}_{26}$ é garantida pela condição $\text{mdc}(\det(A), 26) = 1$, verificada no Passo 1.

Nota pedagógica — A decodificação como motivação para a matriz inversa. Em muitos livros didáticos, a matriz inversa é introduzida como uma definição formal antes de qualquer motivação. A Cifra de Hill oferece uma situação em que a necessidade da inversa emerge naturalmente: *"Se eu posso cifrar multiplicando por A, como desfaço essa operação?"* Essa pergunta, colocada pelo professor antes de enunciar qualquer definição, cria o contexto cognitivo que Ausubel (2003) denomina de organizador avançado, uma estrutura prévia que prepara o estudante para assimilar o conceito formal de forma mais significativa.

Recomenda-se que o professor apresente a decodificação em uma aula separada da codificação, permitindo que os estudantes primeiro internalizem o processo de cifração antes de enfrentar o desafio adicional da inversão modular.

Passo 1 — Cálculo do inverso de $\det(A)$ em $\mathbb{Z}_{26}$

Sabe-se que $\det(A) = 9$. Precisamos encontrar 9^{-1} em $\mathbb{Z}_{26}$, isto é, um inteiro x tal que:

$$9x \equiv 1 \pmod{26}.$$

Testando valores de x de 1 a 25:

Tabela 5 – Busca do inverso de 9 em $\mathbb{Z}_{26}$

x	$9x$	$9x \pmod{26}$
1	9	9
2	18	18
3	27	**1** ✓

Fonte: Elaborado pelo autor (2026).

Portanto, $9^{-1} \equiv 3 \pmod{26}$, pois $9 \cdot 3 = 27 = 1 \cdot 26 + 1 \equiv 1 \pmod{26}$.

Nota pedagógica — Métodos para encontrar o inverso modular. O método de busca exaustiva apresentado acima é adequado para fins pedagógicos introdutórios, pois é intuitivo e não exige conhecimentos prévios além da definição de congruência. No entanto, o professor deve apresentá-lo como um primeiro recurso, sinalizando que existem métodos mais eficientes para casos práticos:

- **Algoritmo de Euclides estendido:** permite encontrar o inverso modular de qualquer elemento sem a necessidade de teste exaustivo, sendo especialmente útil para módulos maiores. O exemplo apresentado no Exemplo 6.1.9 do Capítulo 6 ilustra esse procedimento.
- **Planilha ou calculadora:** a fórmula `=MOD(9*A1, 26)` em uma planilha, arrastada para as linhas correspondentes a $x = 1, 2, \ldots, 25$, permite identificar o inverso em segundos. Recomenda-se usar essa ferramenta para verificação, não como substituto do raciocínio.

Erro comum: os estudantes podem interpretar 9^{-1} em $\mathbb{Z}_{26}$ como $\frac{1}{9}$ (a fração decimal), o que é conceitualmente incorreto nesse contexto. O professor deve enfatizar

que estamos no anel $\mathbb{Z}_{26}$, onde as operações são definidas módulo 26 e a noção de fração não se aplica. A analogia com o inverso multiplicativo em $\mathbb{R}$ pode ser útil como ponto de partida (*"assim como* $5 \cdot \frac{1}{5} = 1$ *em* $\mathbb{R}$*, queremos encontrar* x *tal que* $9 \cdot x \equiv 1$ *em* $\mathbb{Z}_{26}$*"*), mas deve ser usada com cuidado para não reforçar a confusão com frações.

Passo 2 — Cálculo da matriz adjunta

Pela Definição 6.1.7, a matriz adjunta de $A = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ é:

$$\operatorname{adj}(A) = \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix}.$$

Como precisamos trabalhar em $\mathbb{Z}_{26}$, convertemos os coeficientes negativos:

$$-3 \equiv 23 \pmod{26}, \qquad -2 \equiv 24 \pmod{26}.$$

Logo:

$$\operatorname{adj}(A) \equiv \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \pmod{26}.$$

Nota pedagógica — Números negativos em $\mathbb{Z}_{26}$. A conversão de coeficientes negativos para sua representação positiva em $\mathbb{Z}_{26}$ é um ponto que pode gerar dúvidas. O professor pode utilizar a seguinte explicação intuitiva: assim como um arco de $-90°$ é côngruo a um arco de $270°$ (pois $270° + 90° = 360° \equiv 0°$), em $\mathbb{Z}_{26}$ um deslocamento de -3 é côngruo a um deslocamento de 23, já que $23 + 3 = 26 \equiv 0$. Da mesma forma que arcos côngruos a $360°$ representam a mesma posição final no ciclo trigonométrico, elementos côngruos módulo 26 representam o mesmo resto, basta trocar a "volta completa" de $360°$ pela "volta completa" de 26 unidades. Essa analogia, já familiar aos estudantes do estudo de arcos e ciclos trigonométricos, é matematicamente precisa no contexto da aritmética modular e pode tornar essa etapa mais natural para os estudantes.

Erro comum: ao calcular a adjunta de matrizes 2×2, estudantes podem trocar os sinais dos elementos da diagonal secundária ou esquecerem de trocar as posições dos elementos da diagonal principal. Vale a pena retomar a fórmula explícita: para

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \operatorname{adj}(A) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Passo 3 — Cálculo de A^{-1} em $\mathbb{Z}_{26}$

Pela Proposição 6.1.9, a inversa de A em $\mathbb{Z}_{26}$ é:

$$A^{-1} \equiv (\det A)^{-1} \cdot \operatorname{adj}(A) \pmod{26} = 3 \cdot \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \pmod{26} = \begin{pmatrix} 15 & 69 \\ 72 & 9 \end{pmatrix} \pmod{26}.$$

Reduzindo módulo 26:

$$69 = 2{\cdot}26 + 17 \implies 69 \equiv 17 \pmod{26},$$

$$72 = 2{\cdot}26 + 20 \implies 72 \equiv 20 \pmod{26}.$$

Portanto:

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

Verificação: é altamente recomendável confirmar que $A \cdot A^{-1} \equiv I_2 \pmod{26}$ antes de prosseguir para a decodificação:

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} = \begin{pmatrix} 3{\cdot}15 + 3{\cdot}20 & 3{\cdot}17 + 3{\cdot}9 \\ 2{\cdot}15 + 5{\cdot}20 & 2{\cdot}17 + 5{\cdot}9 \end{pmatrix} = \begin{pmatrix} 105 & 78 \\ 130 & 79 \end{pmatrix}.$$

Reduzindo módulo 26:

$$105 = 4{\cdot}26 + 1 \implies 105 \equiv 1 \pmod{26},$$

$$78 = 3{\cdot}26 + 0 \implies 78 \equiv 0 \pmod{26},$$

$$130 = 5{\cdot}26 + 0 \implies 130 \equiv 0 \pmod{26},$$

$$79 = 3{\cdot}26 + 1 \implies 79 \equiv 1 \pmod{26}.$$

$$\therefore \quad A \cdot A^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \pmod{26}.$$

Nota pedagógica — A verificação como hábito matemático. A etapa de verificação $A \cdot A^{-1} \equiv I_2 \pmod{26}$ não é apenas uma precaução técnica: ela é uma oportunidade pedagógica fundamental. O professor pode apresentá-la como um **hábito matemático**, a prática de verificar o resultado antes de usá-lo em etapas subsequentes. No contexto da Cifra de Hill, o custo de usar uma matriz inversa incorreta é alto: toda a decodificação será errada, e o erro só será percebido no final.

Do ponto de vista da aprendizagem, a verificação reforça a definição de matriz inversa ($A \cdot A^{-1} = I$) de forma ativa. Em vez de o estudante memorizar a definição, ele a

aplica concretamente para checar seu próprio cálculo. Esse movimento de validação é o que Brousseau (1997) denomina situação de validação, o próprio contexto do problema oferece ao estudante meios de verificar a correção de suas respostas, reduzindo a dependência exclusiva da autoridade do professor.

Sugestão: peça aos alunos que calculem também $A^{-1} \cdot A$ e verifiquem que o resultado é o mesmo. Isso reforça a comutatividade da inversa, propriedade que pode parecer óbvia para o professor, mas não é evidente para o estudante que acabou de aprender que a multiplicação de matrizes em geral não é comutativa.

Passo 4 — Decodificação de cada bloco

Aplica-se A^{-1} a cada bloco cifrado $\mathbf{c}_i$ e reduz-se módulo 26 para recuperar o bloco original $\mathbf{v}_i$.

Bloco 1: $\mathbf{c}_1 = (5,\, 17)^\top$

$$A^{-1} \cdot \mathbf{c}_1 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 5 \\ 17 \end{pmatrix} = \begin{pmatrix} 75 + 289 \\ 100 + 153 \end{pmatrix} = \begin{pmatrix} 364 \\ 253 \end{pmatrix}.$$

$$364 = 14{\cdot}26 + 0 \implies 364 \equiv 0 \pmod{26} \quad (A),$$

$$253 = 9{\cdot}26 + 19 \implies 253 \equiv 19 \pmod{26} \quad (T).$$

$$\therefore \quad \mathbf{v}_1 = (0,\, 19)^\top \longrightarrow \mathbf{AT}.$$

Bloco 2: $\mathbf{c}_2 = (22,\, 2)^\top$

$$A^{-1} \cdot \mathbf{c}_2 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 22 \\ 2 \end{pmatrix} = \begin{pmatrix} 330 + 34 \\ 440 + 18 \end{pmatrix} = \begin{pmatrix} 364 \\ 458 \end{pmatrix}.$$

$$364 \equiv 0 \pmod{26} \quad (A),$$

$$458 = 17{\cdot}26 + 16 \implies 458 \equiv 16 \pmod{26} \quad (Q).$$

$$\therefore \quad \mathbf{v}_2 = (0,\, 16)^\top \longrightarrow \mathbf{AQ}.$$

Bloco 3: $\mathbf{c}_3 = (20,\, 8)^\top$

$$A^{-1} \cdot \mathbf{c}_3 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 300 + 136 \\ 400 + 72 \end{pmatrix} = \begin{pmatrix} 436 \\ 472 \end{pmatrix}.$$

$$436 = 16{\cdot}26 + 20 \implies 436 \equiv 20 \pmod{26} \quad (U),$$

$$472 = 18{\cdot}26 + 4 \implies 472 \equiv 4 \pmod{26} \quad (E).$$

$$\therefore \quad \mathbf{v}_3 = (20,\, 4)^\top \longrightarrow \mathbf{UE}.$$

Bloco 4: $\mathbf{c}_4 = (11,\, 6)^\top$

$$A^{-1} \cdot \mathbf{c}_4 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 11 \\ 6 \end{pmatrix} = \begin{pmatrix} 165 + 102 \\ 220 + 54 \end{pmatrix} = \begin{pmatrix} 267 \\ 274 \end{pmatrix}.$$

$$267 = 10{\cdot}26 + 7 \implies 267 \equiv 7 \pmod{26} \quad (H),$$

$$274 = 10{\cdot}26 + 14 \implies 274 \equiv 14 \pmod{26} \quad (O).$$

$$\therefore \quad \mathbf{v}_4 = (7,\, 14)^\top \longrightarrow \mathbf{HO}.$$

Bloco 5: $\mathbf{c}_5 = (13,\, 12)^\top$

$$A^{-1} \cdot \mathbf{c}_5 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 13 \\ 12 \end{pmatrix} = \begin{pmatrix} 195 + 204 \\ 260 + 108 \end{pmatrix} = \begin{pmatrix} 399 \\ 368 \end{pmatrix}.$$

$$399 = 15{\cdot}26 + 9 \implies 399 \equiv 9 \pmod{26} \quad (J),$$

$$368 = 14{\cdot}26 + 4 \implies 368 \equiv 4 \pmod{26} \quad (E).$$

$$\therefore \quad \mathbf{v}_5 = (9,\, 4)^\top \longrightarrow \mathbf{JE}.$$

A mensagem decodificada é:

ATAQUEHOJE

que, reintroduzindo o espaço suprimido antes da cifração, corresponde à mensagem original **"ATAQUE HOJE"**.

7.4 Síntese do Algoritmo e Quadro Comparativo

A tabela 7 resume as etapas do algoritmo de codificação e decodificação, destacando o conceito matemático mobilizado em cada fase e os principais erros a evitar. Esse tabela pode ser utilizado pelo professor como material de apoio para os estudantes durante a execução das atividades práticas.

Tabela 6 – Síntese do algoritmo da Cifra de Hill com observações pedagógicas

Etapa	**Operação**	**Conceito mobilizado**	**Erro possível**
Escolha da chave	Verificar $\text{mdc}(\det A, 26) = 1$	Determinante; invertibilidade modular	Confundir $\det A \neq 0$ em $\mathbb{R}$ com invertibilidade em $\mathbb{Z}_{26}$
Conversão	Letras $\rightarrow$ inteiros em $\{0, \ldots, 25\}$	Tabela de codificação	Erros de substituição; esquecer de tratar espaços
Organização em blocos	Agrupar pares de inteiros em vetores coluna	Vetores; adequação ao tamanho da chave	Ignorar blocos incompletos (número ímpar de letras)
Multiplicação matricial	$\mathbf{c} = A\mathbf{v}$	Produto matriz-vetor	Inverter a ordem: $\mathbf{v} \cdot A$ (não definida)
Redução modular	$c' \equiv c \pmod{26}$	Aritmética modular; resto da divisão	Subtrair 26 apenas uma vez quando o resultado excede 51
Inverso modular	Encontrar $(\det A)^{-1}$ em $\mathbb{Z}_{26}$	Inverso multiplicativo; Teorema de Bézout	Interpretar 9^{-1} como a fração $1/9$
Matriz adjunta	$\text{adj}(A)$ com coeficientes reduzidos mod 26	Cofatores; transposição; representação de negativos	Trocar elementos ou sinais na adjunta 2×2
Decodificação	$\mathbf{v} = A^{-1}\mathbf{c} \pmod{26}$	Aplicação da inversa; verificação	Esquecer de verificar $A \cdot A^{-1} \equiv I$ antes de decodificar

Fonte: Elaborado pelo autor (2026).

7.5 Considerações sobre a Viabilidade Didática

A apresentação detalhada do algoritmo neste capítulo evidencia tanto o potencial quanto as tensões inerentes ao uso da Cifra de Hill como recurso didático. É necessário reconhecer essas tensões com clareza, para que o professor possa preparar-se adequadamente para enfrentá-las.

A primeira tensão diz respeito ao **custo cognitivo do algoritmo**. O processo completo de codificação e decodificação de uma mensagem de dez letras, como o exemplo apresentado, exige um volume considerável de cálculo. Para estudantes com dificuldades em operações aritméticas básicas, esse volume pode desviar a atenção do conceito matemático central para a execução mecânica de contas. A estratégia recomendada é distribuir as

etapas ao longo de mais de uma aula, permitir o uso de calculadora a partir do Passo 4 e adotar a divisão de trabalho em grupos conforme descrito nas notas pedagógicas da Seção 7.2.

A segunda tensão diz respeito à **aritmética modular como pré-requisito**. A Cifra de Hill pressupõe a compreensão de congruência e de inverso modular, conteúdo que não integra explicitamente o currículo do Ensino Médio segundo a BNCC e que, portanto, precisa ser construído ao longo da própria sequência didática (Atividade 3 da sequência proposta no Capítulo 8). O professor deve avaliar, a partir do diagnóstico de sua turma, quanto tempo será necessário para essa construção antes de iniciar a Atividade 4.

A terceira tensão é, paradoxalmente, uma virtude: os **erros são visíveis**. Um equívoco em qualquer etapa, seja na multiplicação, seja na redução modular ou no cálculo da inversa, produz um texto decodificado incoerente, que o próprio estudante pode identificar como incorreto sem depender da correção do professor. Essa característica transforma os erros em oportunidades de revisão e de discussão, alinhando-se ao que Brousseau (1997) denomina situações de validação, nas quais o contexto do problema oferece retroalimentação imediata ao estudante.

Em suma, a Cifra de Hill não é um recurso de aplicação trivial: ela exige planejamento, tempo e sensibilidade pedagógica. Quando bem conduzida, no entanto, oferece ao estudante uma experiência rara no ensino de matrizes: a de usar os conceitos para resolver um problema com finalidade clara, verificar os resultados por conta própria e perceber que a matemática abstrata tem consequências concretas e imediatamente observáveis. Com base nessa articulação entre fundamentos matemáticos e aplicação contextualizada, o capítulo seguinte apresenta o produto educacional elaborado nesta dissertação.

8 PRODUTO EDUCACIONAL: SEQUÊNCIA DIDÁTICA PARA O ENSINO DE MATRIZES COM A CIFRA DE HILL

8.1 Apresentação

Considerando os fundamentos teóricos discutidos nos capítulos anteriores e o potencial pedagógico da *Cifra de Hill* evidenciado no processo de codificação e decodificação, apresenta-se, neste capítulo, como produto educacional uma sequência didática para o ensino de matrizes no Ensino Médio. O produto foi elaborado com o objetivo de favorecer uma aprendizagem significativa dos conceitos de matriz quadrada, multiplicação de matrizes, determinante, matriz inversa e aritmética modular, articulando teoria e aplicação em um contexto motivador.

A sequência é composta por quatro atividades progressivas, pensadas para turmas do Ensino Médio, preferencialmente do 2º ou 3º ano, e distribuídas ao longo de aproximadamente seis aulas de 50 minutos, conforme a Tabela 8. O fio condutor é a *Cifra de Hill*: parte-se de uma forma mais simples de criptografia (Cifra de César) para construir, de modo gradual, os conceitos matemáticos necessários — multiplicação de matrizes, determinante, matriz inversa e aritmética modular — até a aplicação plena da cifra matricial na última atividade.

A organização das atividades segue a lógica de uma sequência didática, compreendida como um conjunto de atividades ordenadas, estruturadas e articuladas em torno de um objetivo de aprendizagem definido (ZABALA, 1998), e organizada em etapas progressivas que conduzem o aluno da mobilização de conhecimentos prévios ao domínio do conteúdo (DOLZ; NOVERRAZ; SCHNEUWLY, 2004). Esse arranjo respeita também os princípios da aprendizagem significativa (AUSUBEL, 2003): cada etapa é introduzida por uma situação motivadora que ativa conhecimentos prévios antes da formalização matemática. A criptografia cumpre aqui a função de organizador avançado ao conferir ao conteúdo um contexto real, reconhecível e socialmente relevante antes mesmo de sua apresentação formal.

Reconhece-se, de antemão, uma limitação importante: a sequência não foi aplicada empiricamente em sala de aula ao longo desta pesquisa. Trata-se, portanto, de uma proposta fundamentada teoricamente, cujos resultados efetivos dependem de validação em

campo. Investigações futuras são necessárias para avaliar o impacto real na aprendizagem, na motivação discente e na consolidação dos conceitos envolvidos.

8.2 Vinculação com a BNCC: habilidades, lacunas e posicionamento curricular

A Base Nacional Comum Curricular (BNCC) não contempla, para o Ensino Médio, habilidades que tratem explicitamente de matrizes, determinantes ou matrizes inversas como objetos matemáticos autônomos. Essa ausência é uma lacuna curricular reconhecida na literatura (cf. Capítulo 3) e tem consequências práticas diretas: muitos materiais didáticos e planejamentos docentes abordam o tema de forma marginal ou excessivamente procedimental, sem articulação com aplicações.

A habilidade mais diretamente relacionada ao conteúdo desta sequência é a EM13MAT301, que orienta os estudantes a:

> Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais (BRASIL, 2018, p. 536).

Contudo, essa habilidade aborda matrizes apenas de modo indireto, no contexto da resolução de sistemas lineares. A codificação e a decodificação matricial exigem conteúdos — como multiplicação de matrizes, cofatores, adjunta e invertibilidade em $\mathbb{Z}_k$ — que não possuem correspondência direta em nenhuma habilidade da BNCC do Ensino Médio, conforme as habilidades mobilizadas na sequência didática da Tabela 7.

O professor que optar por desenvolver esta sequência deve embasar sua escolha no Projeto Político-Pedagógico (PPP) da escola, nos referenciais curriculares estaduais que complementam a BNCC, ou em decisões colegiadas de área.

Esse posicionamento não invalida a proposta: a BNCC estabelece uma base mínima, não um teto curricular. A inclusão de matrizes como conteúdo autônomo é pedagogicamente justificável e aparece com frequência em livros didáticos, planejamentos escolares e propostas curriculares voltadas ao Ensino Médio. O que se exige do docente é clareza sobre o enquadramento curricular de sua decisão.

Tabela 7 – Habilidades da BNCC mobilizadas pela sequência didática

Código	**Enunciado resumido**	**Observação crítica**
EM13MAT301	Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais.	Única habilidade que menciona, ainda que indiretamente, matrizes na BNCC do Ensino Médio. Não contempla operações matriciais, determinantes ou inversas como objetos de estudo autônomos.
EM13MAT103	Interpretar e compreender textos científicos ou divulgados pelas mídias, que empregam unidades de medida de diferentes grandezas e as conversões possíveis entre elas, adotadas ou não pelo Sistema Internacional (SI), como as de armazenamento e velocidade de transferência de dados, ligadas aos avanços tecnológicos.	Pertinente aos padrões de recorrência da aritmética modular.
—	Matrizes, determinante e matriz inversa como objetos autônomos.	Não há habilidade específica na BNCC para esses conteúdos.

Fonte: Elaborado pelo autor (2026).

8.3 Objetivos da sequência didática

A sequência didática tem como objetivo geral proporcionar ao estudante do Ensino Médio uma compreensão contextualizada e conceitualmente fundamentada dos principais tópicos de álgebra matricial, utilizando a *Cifra de Hill* como fio condutor.

Os objetivos específicos são:

1. Desenvolver nos estudantes a capacidade de operar com matrizes — adição, multiplicação e inversão — compreendendo o significado de cada operação.
2. Promover a compreensão do determinante como grandeza que indica a invertibilidade de uma matriz.
3. Introduzir a aritmética modular como sistema numérico com regras próprias.
4. Favorecer a aprendizagem significativa ao apresentar a criptografia como situação real.

5. Estimular o protagonismo discente por meio de atividades investigativas.

8.4 Organização geral da sequência

A sequência está organizada em quatro atividades progressivas, conforme a Tabela 8:

Tabela 8 – Visão geral da sequência didática

Aula(s)	**Atividade**	**Conteúdo Central**	**Habilidades BNCC**	**Objetivo**
1	Atividade 1 – Cifra de César	Substituição simples	EM13MAT301	Introduzir o conceito de código
2–3	Atividade 2 – Matrizes e Determinantes	Multiplicação de matrizes; determinante	EM13MAT301	Compreender invertibilidade
4	Atividade 3 – Congruência Modular	Congruência e inverso modular	EM13MAT103	Compreender aritmética modular
5–6	Atividade 4 – *Cifra de Hill*	Codificação matricial	EM13MAT301 EM13MAT103	Aplicar matrizes na criptografia

Fonte: Elaborado pelo autor (2026).

A progressão é intencional: da *Cifra de César* para a *Cifra de Hill*. Cada atividade prepara o terreno para a seguinte, de modo que o estudante nunca seja confrontado com um conceito novo sem ter antes construído os subsunçores necessários (AUSUBEL, 2003).

A Atividade 2, referente aos conteúdos de matrizes e determinantes, foi elaborada com base nos exercícios e na abordagem teórica apresentados na apostila de Matemática do curso pré-vestibular do Sistema Poliedro de Ensino (Sistema Poliedro de Ensino, 2024), adaptados e reorganizados para atender aos objetivos específicos desta sequência didática.

8.5 Descrição detalhada das atividades

8.5.1 Atividade 1 – Codificação e decodificação com a Cifra de César

- **Duração:** 1 aula (50 minutos)
- **Objetivo:** Sensibilizar os estudantes para o conceito de criptografia.

- **Conteúdos:** Substituição alfabética simples.
- **Habilidades BNCC:** EM13MAT301.
- **Material:** Folha impressa conforme Apêndice 1.
- **Metodologia:**

  1. *Acolhida e problematização (10 min).* O professor inicia a aula com uma pergunta disparadora, como: "Como vocês acham que exércitos e governos trocavam mensagens secretas antes da internet?". Espera-se gerar um breve debate oral, registrando no quadro as hipóteses levantadas pela turma.
  2. **Contextualização histórica (10 min).** Apresentação breve (oral ou com slide) sobre Júlio César e o uso da cifra que leva seu nome, destacando o deslocamento fixo do alfabeto como princípio de funcionamento.
  3. **Atividade prática em duplas (20 min).** Distribuição da folha impressa (Apêndice 1), contendo um alfabeto cifrado com deslocamento fixo. Em duplas, os estudantes codificam uma palavra curta escolhida por eles e trocam com outra dupla para decodificar.
  4. **Socialização e fechamento (10 min).** Algumas duplas compartilham as palavras codificadas/decodificadas com a turma. O professor sistematiza o conceito de *chave de cifra* e antecipa que, nas próximas aulas, a turma vai conhecer uma versão mais robusta desse método, baseada em matrizes.

- **Avaliação sugerida:** Observação informal do engajamento dos estudantes durante a atividade em duplas e da qualidade das hipóteses levantadas na problematização inicial.

8.5.2 Atividade 2 – Matrizes e Determinantes

- **Duração:** 2 aulas (100 minutos)
- **Objetivo:** Consolidar operações com matrizes.
- **Conteúdos:** Produto de matrizes; determinante; matriz inversa.
- **Habilidades BNCC:** EM13MAT301.
- **Material:** Apêndices 2 e 3.
- **Metodologia:**

  1. **Aula 1 – Produto de matrizes e determinante (50 min).**

  - *Retomada (10 min):* revisão rápida de notação matricial e de como identificar a ordem de uma matriz, verificando se há domínio suficiente para prosseguir (ver também as orientações gerais sobre gestão de conhecimentos prévios).
  - *Exposição dialogada (20 min):* o professor apresenta a definição de produto de matrizes e a fórmula recursiva do determinante (expansão de Laplace), resolvendo um exemplo de matriz 2×2 e um de 3×3 no quadro, com participação ativa da turma na resolução.
  - *Exercícios guiados (20 min):* os estudantes resolvem, individualmente ou em duplas, os exercícios do Apêndice 2, com o professor circulando pela sala para esclarecer dúvidas pontuais.

2. **Aula 2 – Matriz inversa (50 min).**
  - *Retomada (5 min):* recuperação do conceito de determinante trabalhado na aula anterior, com pergunta direcionada sobre o que aconteceria se o determinante fosse igual a zero.
  - *Exposição dialogada (20 min):* apresentação do conceito de matriz inversa, da relação com o determinante (matriz invertível $\Leftrightarrow \det \neq 0$) e do método da matriz adjunta para calcular a inversa.
  - *Prática orientada (20 min):* resolução dos exercícios do Apêndice 3, com correção coletiva dos itens mais desafiadores ao final da aula.
  - *Fechamento (5 min):* o professor conecta o conteúdo com a próxima etapa, adiantando que matrizes invertíveis serão essenciais para decodificar mensagens cifradas por matrizes.

- **Avaliação sugerida:** Resolução dos exercícios dos Apêndices 2 e 3, com correção coletiva e feedback individualizado durante a circulação pela sala.

8.5.3 Atividade 3 – Congruência Modular

- **Duração:** 1 aula (50 minutos)
- **Objetivo:** Introduzir a aritmética modular.
- **Conteúdos:** Congruência módulo n; inverso modular.
- **Habilidades BNCC:** EM13MAT103.
- **Material:** Apêndice 4.
- **Metodologia:**

1. *Situação-problema inicial (10 min).* O professor retoma a ideia de arcos côngruos a 360°, já trabalhada em Trigonometria: um arco de 390° corresponde à mesma posição final que um arco de 30°, pois $390° - 360° = 30°$, e ambos são ditos côngruos. A partir dessa ideia, propõe à turma a seguinte questão: se as 26 letras do alfabeto forem organizadas em um ciclo (de 0 a 25), qual letra corresponde à posição 28? Assim como o arco "dá uma volta completa"a cada 360° e recomeça a contagem, o ciclo de letras "dá uma volta completa"a cada 26 posições, de modo que $28 \equiv 2 \pmod{26}$. Essa conexão conduz a turma a perceber intuitivamente a ideia de congruência módulo n, que será formalizada a seguir.

- *Formalização do conceito (15 min).* Apresentação da definição de congruência módulo n e de suas propriedades básicas, retomando a analogia dos arcos côngruos para dar suporte intuitivo à notação $a \equiv b \pmod{n}$.

- *Inverso modular (15 min).* Introdução do conceito de inverso multiplicativo módulo n, com um exemplo resolvido passo a passo mostrando como encontrá-lo, preparando o terreno para o uso desse conceito na decodificação da Cifra de Hill.

- *Exercícios (10 min).* Resolução do Apêndice 4, contendo questões discursivas (justificar se dois números são congruentes) e objetivas (calcular restos e inversos modulares).

Avaliação sugerida: Exercícios discursivos e objetivos do Apêndice 4, avaliando tanto o cálculo quanto a justificativa conceitual das respostas.

8.5.4 Atividade 4 – Codificação e Decodificação com a Cifra de Hill

- **Duração:** 2 aulas (100 minutos)
- **Objetivo:** Integrar todos os conceitos desenvolvidos anteriormente.
- **Conteúdos:** Multiplicação matricial módulo 26; matriz inversa em $\mathbb{Z}_{26}$.
- **Habilidades BNCC:** EM13MAT301 e EM13MAT103.
- **Material:** Apêndices 5 e 6.
- **Metodologia:**

1. **Aula 1 – Codificação com a Cifra de Hill (50 min).**

- *Retomada integradora (10 min):* o professor recupera, de forma dialogada, os três conceitos que serão combinados nesta atividade: produto de matrizes (Atividade 2), congruência módulo n (Atividade 3) e a ideia geral de cifra por substituição (Atividade 1).
- *Apresentação do método (15 min):* explicação de como transformar palavras em vetores numéricos e como multiplicar esses vetores por uma matriz-chave, reduzindo o resultado módulo 26 (incluindo a regra da letra X para palavras de tamanho ímpar, indicada nas orientações gerais).
- *Prática guiada (20 min):* em duplas, os estudantes codificam uma palavra própria usando a matriz-chave fornecida no Apêndice 5, com apoio do professor para os cálculos módulo 26.
- *Fechamento (5 min):* troca das mensagens codificadas entre duplas, que serão decodificadas na aula seguinte.

2. **Aula 2 – Decodificação e síntese (50 min).**

- *Retomada (5 min):* revisão rápida do processo de cálculo da matriz inversa módulo 26, incluindo a busca pelo inverso modular do determinante.
- *Prática guiada (25 min):* os estudantes calculam a matriz inversa da chave em $\mathbb{Z}_{26}$ e a utilizam para decodificar a mensagem recebida da dupla parceira, usando o Apêndice 6 como roteiro.
- *Socialização (10 min):* algumas duplas compartilham as mensagens decodificadas, verificando se o resultado corresponde à mensagem original.
- *Síntese final (10 min):* discussão coletiva retomando todo o percurso da sequência didática – da Cifra de César à Cifra de Hill – destacando como conceitos de diferentes áreas da Matemática (álgebra matricial e aritmética modular) se articulam na resolução de um mesmo problema.

- **Avaliação sugerida:** Avaliação processual, considerando a participação nas atividades em dupla, a correção da codificação e decodificação realizadas e a qualidade da discussão na síntese final.

8.6 Orientações gerais ao professor

Algumas considerações transversais merecem atenção especial:

- **Gestão dos conhecimentos prévios:** verificar domínio de álgebra básica antes da Atividade 2.

- **Uso de tecnologia:** o uso de planilhas ou softwares é opcional.
- **Erros como oportunidade:** incentivar revisão e validação.
- **Adaptação do formalismo:** priorizar compreensão conceitual.
- **Palavras com número ímpar de letras:** acrescentar a letra X ao final.

8.7 Avaliação da aprendizagem

A avaliação proposta é predominantemente processual e formativa.

Sugere-se, ao final da sequência, a aplicação de um questionário reflexivo com perguntas abertas, como:

1. O que você sabia sobre matrizes antes desta sequência?
2. Em que momento teve mais dificuldade?
3. Você identifica outras aplicações para matrizes?
4. A abordagem pela *Cifra de Hill* ajudou na compreensão?

8.8 Considerações sobre o produto educacional

A sequência didática aqui apresentada constitui uma proposta fundamentada, mas não definitiva. Seu valor pedagógico real somente poderá ser avaliado após sua implementação em sala de aula.

Pesquisadores e professores que desejem aplicar e aprimorar esta sequência são encorajados a documentar o processo e compartilhar os resultados com a comunidade de Educação Matemática.

Por fim, ressalta-se que a *Cifra de Hill* é apenas uma das possíveis entradas para o ensino contextualizado de matrizes. A presente sequência não esgota as possibilidades didáticas do tema.

9 CONSIDERAÇÕES FINAIS

Esta dissertação partiu da seguinte questão norteadora: *quais fundamentos teóricos e matemáticos sustentam a viabilidade da Cifra de Hill como estratégia didática para o ensino de matrizes no Ensino Médio?* Com base na investigação desenvolvida ao longo dos capítulos anteriores, é possível responder que a viabilidade da Cifra de Hill como estratégia didática repousa sobre três ordens de fundamentos articulados: matemáticos, pedagógicos e curriculares.

Do ponto de vista **matemático**, a Cifra de Hill mobiliza, de forma integrada e necessária, os principais conceitos da álgebra matricial presentes no currículo do Ensino Médio: multiplicação de matrizes, determinante, matriz inversa e aritmética modular. Diferentemente de abordagens que tratam esses conceitos de forma isolada e procedimental, o método criptográfico exige sua articulação simultânea para que o processo de codificação e decodificação funcione. Essa característica confere ao conteúdo uma coerência interna que dificilmente emerge em exercícios descontextualizados.

Do ponto de vista **pedagógico**, os referenciais da Educação Matemática adotados nesta pesquisa sustentam a pertinência da proposta. A teoria da aprendizagem significativa de Ausubel (2003) fundamenta a organização da sequência didática de Dolz, Noverraz e Schneuwly (2004) e Zabala (1998): cada atividade é introduzida por uma situação motivadora que ativa conhecimentos prévios antes da formalização matemática, seguindo etapas articuladas que conduzem progressivamente o aluno ao domínio do conteúdo. Nesse sentido, a criptografia opera como um contexto de aplicação que confere sentido ao conteúdo, aproximando-se da função de organizador avançado ao apresentar, antes da formalização, uma situação concreta na qual o uso das matrizes é genuinamente necessário. Skovsmose (2000) e Freudenthal (1991) reforçam essa perspectiva ao defenderem que a matemática deve ser aprendida em contextos nos quais sua necessidade emerge do próprio problema, e não como conjunto de regras apresentadas previamente. Além disso, a Cifra de Hill possui uma virtude pedagógica singular: os erros cometidos nas operações matriciais produzem mensagens incoerentes que o próprio estudante pode identificar sem depender da correção do professor, caracterizando o que Brousseau (1997) denomina situação de validação.

Do ponto de vista **curricular**, a análise da BNCC revelou uma lacuna relevante: as matrizes, os determinantes e as matrizes inversas não possuem habilidades específicas no Ensino Médio, sendo abordadas apenas indiretamente no contexto de sistemas lineares.

Essa ausência, longe de inviabilizar a proposta, reforça sua pertinência: a Cifra de Hill oferece ao professor um argumento concreto e socialmente relevante para justificar a inclusão desses conteúdos, ancorando-os em aplicações relacionadas à segurança da informação e às tecnologias digitais presentes no cotidiano dos estudantes.

Em relação aos objetivos específicos estabelecidos na introdução, considera-se que todos foram alcançados no âmbito desta pesquisa teórico-bibliográfica. O primeiro objetivo, analisar as principais dificuldades relacionadas ao ensino e à aprendizagem de matrizes no Ensino Médio, foi desenvolvido no Capítulo 3, que identificou como principais obstáculos o ensino excessivamente procedimental, a fragilidade de conhecimentos prévios e a ausência de contextualizações que confiram sentido às operações matriciais. O segundo objetivo, estudar os fundamentos matemáticos da Cifra de Hill, foi cumprido nos Capítulos 5, 6 e 7, que apresentaram, com rigor formal, os conceitos de matriz invertível, determinante, adjunta, aritmética modular e o algoritmo completo de codificação e decodificação. O terceiro objetivo, identificar o potencial pedagógico da criptografia como recurso de contextualização, foi desenvolvido ao longo dos Capítulos 4, 5 e 7, com ênfase nas notas pedagógicas que discutem cada etapa do algoritmo sob a perspectiva do ensino. O quarto objetivo, elaborar uma sequência didática fundamentada na *Cifra de Hill*, materializou-se no produto educacional apresentado no Capítulo 8, composto por quatro atividades progressivas distribuídas ao longo de seis aulas, com orientações metodológicas, instrumentos de avaliação e apêndices de apoio ao professor.

Reconhece-se, contudo, que esta pesquisa apresenta limitações que precisam ser explicitadas com clareza. Por tratar-se de investigação exclusivamente teórico-bibliográfica, o potencial pedagógico da Cifra de Hill permanece como hipótese fundamentada, e não como resultado empiricamente verificado. A sequência didática elaborada não foi aplicada em sala de aula, de modo que seus efeitos reais sobre a aprendizagem, a motivação discente e a consolidação dos conceitos envolvidos são ainda desconhecidos. Ademais, reconhece-se que o volume de cálculo exigido pelo algoritmo pode representar um obstáculo ao engajamento em turmas com dificuldades em aritmética básica, e que a aritmética modular, pré-requisito indispensável para a Atividade 4, não integra explicitamente o currículo do Ensino Médio segundo a BNCC, exigindo do professor planejamento adicional para sua introdução.

Investigações futuras são necessárias e urgentes para superar essas limitações. Propõe-se, em especial: (1) a aplicação empírica da sequência em turmas do 2º ou 3º ano do Ensino Médio, com coleta sistemática de dados sobre aprendizagem e motivação; (2) a validação do produto educacional por especialistas em Educação Matemática e professores da Educação Básica, antes ou em paralelo à aplicação em sala de aula; e (3) estudos comparativos que confrontem a Cifra de Hill com outros contextos de aplicação de matrizes,

como transformações geométricas no plano ou modelagem de situações econômicas a fim de identificar em quais contextos e para quais perfis de turma cada abordagem se mostra mais eficaz.

Do ponto de vista formativo, a realização desta pesquisa no âmbito do PROFMAT reforça a relevância da articulação entre teoria e prática na formação continuada de professores. O mestrado profissional cumpre papel fundamental ao incentivar a reflexão crítica sobre a prática pedagógica e ao promover a elaboração de materiais que dialoguem diretamente com as demandas da sala de aula.

Por fim, espera-se que esta dissertação possa contribuir para o debate sobre o ensino contextualizado de matrizes e inspirar outros docentes e pesquisadores a explorar a interface entre criptografia e Educação Matemática. A Cifra de Hill não esgota as possibilidades dessa interface, mas evidencia, com clareza, que conceitos matemáticos frequentemente percebidos como abstratos e sem aplicação podem ganhar vida e significado quando situados em contextos reais, reconhecíveis e socialmente relevantes.

Apêndices

Apêndice 1 – Codificação e decodificação de mensagens utilizando a Cifra de César

Aluno (a): _____ Turma: _____

Atividade 1 - Codificação e decodificação de mensagens utilizando a Cifra de César

Preencha a tabela do alfabeto modificado abaixo, deslocando a letra A algumas unidades adiante (por exemplo, A = F, B = G ,C = H, ...):

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

Letra original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Letra modificada													

Após preencher a tabela, escreva uma frase curta com 3 ou 4 palavras utilizando o alfabeto modificado e envie a algum colega para ver se ele consegue descobrir o que está escrito (não pode xingar ou Júlio César pode enviar as legiões romanas atrás de você !)

Frase original:

_____

_____

Frase codificada:

_____

_____

Destaque a folha aqui e envie a mensagem codificada para algum colega:

_____

_____

Apêndice 2 – Exercícios de multiplicação entre matrizes, cálculo de determinantes e cálculo de matrizes inversíveis e não inversíveis – 1ª parte

Aluno(a): Turma:

Atividade 2 - Matrizes e Determinantes

Considere o texto para as questões 1 e 2:

André, Beto e Carlos trabalham em uma mesma empresa e resolveram almoçar juntos em uma lanchonete do tipo *fast-food*. Todos os três costumam comer hambúrgueres, batatas fritas, tomar refrigerantes e comer tortas de frutas como sobremesa. A tabela a seguir apresenta as intenções dos pedidos de cada um:

	Hambúrguer	Fritas	Refrigerante	Torta
André	2	2	2	1
Beto	1	3	1	2
Carlos	2	1	1	3

Perto da empresa em que trabalham há três opções de lanchonetes do agrado de todos e a próxima tabela fornece o preço unitário de cada produto nas lanchonetes consideradas:

	Mc' Ronalds	Burguer-Ring	Rob's
Hambúrguer	R$5,00	R$7,00	R$4,00
Fritas	R$3,00	R$2,50	R$2,50
Refrigerante	R$2,00	R$1,50	R$2,00
Torta	R$4,00	R$4,00	R$5,00

1. Cada um dos três considerou quanto gastaria em cada lanchonete para comer exatamente o que desejava e um deles afirmou que gastaria, no máximo, R$ 30,00. Quem poderia ter feito tal afirmação?

a) Somente Carlos.

b) Somente Beto.

c) Somente André.

d) André ou Beto.

e) Beto ou Carlos.

2. Depois de muita discussão, os três resolveram ir a uma dessas três lanchonetes em que apenas um deles gastou a quantia de R$ 24,00. Assim, se todos fizeram o pedido que desejavam, pode-se concluir que:

a) eles comeram no Mc' Ronalds.

b) eles comeram no Burguer-Ring.

c) eles comeram no Rob's.

d) eles não comeram no Mc' Ronalds.

e) eles não comeram no Burguer-Ring.

Apêndice 3 – Exercícios de multiplicação entre matrizes, cálculo de determinantes e cálculo de matrizes inversíveis e não inversíveis – 2ª parte

3. Calcule o valor dos determinantes das matrizes:

a) $A = \begin{bmatrix} 2 & 4 \\ -6 & 3 \end{bmatrix}$

b) $B = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$

c) C= $\begin{bmatrix} 4 & 1 & 2 \\ -1 & 0 & 2 \\ 3 & 2 & 4 \end{bmatrix}$

d) $D = \begin{bmatrix} 3 & 2 & 1 \\ 0 & -5 & 6 \\ 4 & 1 & 1 \end{bmatrix}$

4. Determine a matriz inversa das matrizes, caso existir:

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

b) $B = \begin{bmatrix} 2 & 6 \\ 1 & 3 \end{bmatrix}$

c) C= $\begin{bmatrix} 2 & -3 & 3 \\ 2 & 2 & 3 \\ 3 & -2 & 2 \end{bmatrix}$

5. Uma das técnicas de se criptografar consiste em identificar cada letra do alfabeto com um determinado número e escrever a mensagem na forma de uma matriz. O remetente codifica essa matriz de mensagem usando uma matriz de codificação, enquanto o destinatário consegue ler a mensagem usando uma matriz de decodificação.

Esse processo é válidado em razão de que as matrizes de codificação e decodificação são inversas uma da outra. Seja C a matriz de codificação e D a matriz de decodificação, tem - se que D . C = C . D = I, onde I é a matriz identidade. Suponha que o remetente codifica uma mensagem com a seguinte matriz de codificação

$$C = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$$

A matriz de decodificação D que o destinatário deverá usar para ler a mensagem será:

a) $\begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix}$

b) $\begin{bmatrix} -3 & -1 \\ -5 & -2 \end{bmatrix}$

c) $\begin{bmatrix} -3 & -1 \\ 5 & 2 \end{bmatrix}$

d) $\begin{bmatrix} 3 & -1 \\ 5 & -2 \end{bmatrix}$

e) $\begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$

Aluno(a): Turma:

Atividade 3 - Congruência Modular

1. Determine o resto da divisão de 7^{202} por 6 utilizando propriedades de congruência modular. Explique cada passo do seu raciocínio.

2. Resolva a congruência

$$3x \equiv 4 \pmod 7$$

e encontre todos os valores de x no conjunto dos inteiros módulo 7 e justifique o método utilizado.

3. Qual é o valor de 5^{103} mod 4?

a) 0

b) 1

c) 2

d) 3

e) 4

4. Qual dos números abaixo é congruente a 17 módulo 6?

a) 10

b) 11

c) 12

d) 13

e) 14

5. Se a ≡ 2 mod 5 e b ≡ 3 mod 5 , então a+b é congruente a:

a) 0 mod 5

b) 1 mod 5

c) 2 mod 5

d) 3 mod 5

e) 4 mod 5

Apêndice 5 – Codificação e Decodificação de mensagens utilizando a Cifra de Hill - 1ª parte

Aluno(a): Turma:

Atividade 4 - Codificação e Decodificação de mensagens utilizando a Cifra de Hill

1. *Vamos codificar uma palavra?*

Para codificação ou decodificação, utilize a tabela a seguir:

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

Passo 1 : Escolha a matriz-chave A $_{2x2}$ para a codificação. Lembre-se que o determinante *d* da matriz A deve satisfazer *mdc* (d, 26) =1 e d ≠ 0.

$$A = \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} \qquad d = \det(A) = \begin{vmatrix} \square & \square \\ \square & \square \end{vmatrix}$$

Passo 2 : Escolha uma palavra que queira codificar e converter cada letra para número conforme a tabela 1. Caso a palavra tenha um número ímpar de letras, acrescentar a letra X ao final. Por exemplo, SOL → SOLX.

_____

Passo 3 : Construir em blocos de tamanho 2 a palavra escolhida.

(,)

(,)

(,)

Passo 4 : Multiplicar a matriz-chave A pelos blocos do passo anterior dispostos em matriz coluna.

$$\begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} \cdot \begin{bmatrix} \square \\ \square \end{bmatrix} =$$

$$\begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} \cdot \begin{bmatrix} \square \\ \square \end{bmatrix} =$$

Passo 5: Reduzir os resultados das multiplicações de matrizes passo anterior a módulo 26.

Passo 6: Converter os números obtidos da etapa anterior de acordo com a tabela. Assim a palavra codificada fica

_____

Apêndice 6 – Codificação e Decodificação de mensagens utilizando a Cifra de Hill - 2ª parte

2. *Agora vamos decodificar a palavra anterior?*

Passo 1: Calcular a matriz inversa A^{-1} de A. Primeiro, calcule a matriz dos cofatores *cof (A)*, e depois a matriz adjunta adj (A) = $(cof\ (A))^T$ e substitua na expressão

$$A^{-1} = \frac{1}{\det(A)} . adj(A)$$

a)

$A =$ [☐ ☐ ; ☐ ☐]

b)

$cof(A) =$ [☐ ☐ ; ☐ ☐]

c)

$adj(A) =$ [☐ ☐ ; ☐ ☐]

d)

$A^{-1} = \frac{1}{☐} \cdot$ [☐ ☐ ; ☐ ☐]

Passo 2: Transcreva a palavra codificada de acordo com a tabela da página anterior em números e construa em blocos de tamanho 2;

(,)

(,)

(,)

Passo 3 : Multiplicar a matriz-chave A^{-1} pelos blocos do passo anterior dispostos em matriz coluna.

[☐ ☐ ; ☐ ☐] · [☐ ; ☐] =

[☐ ☐ ; ☐ ☐] · [☐ ; ☐] =

Passo 5: Reduzir os resultados das multiplicações de matrizes passo anterior a módulo 26.

Passo 6: Converter os números obtidos da etapa anterior de acordo com a tabela. Assim a palavra decodificada fica

_____

Gabaritos das Atividades 2 e 3

Atividade 2

1. A
2. B
3. a) 30 b) 1 c) -10 d) 35
4. a)

$$A^{-1} = \begin{bmatrix} 3/5 & 1/5 \\ -2/5 & 1/5 \end{bmatrix}$$

b) Não admite inversa.

c)

$$C^{-1} = \begin{bmatrix} -2/5 & 0 & 3/5 \\ -1/5 & 1/5 & 0 \\ 2/5 & -1/5 & -2/5 \end{bmatrix}$$

5. E

Atividade 3

1. Como $7 \equiv 1 \pmod 6$ porque $7 = 6 \cdot 1 + 1$, ou seja, 7 deixa resto 1 quando dividido por 6. Aplicando a propriedade da congruência, Se $a \equiv b \pmod n$, então $\mathbf{a^k \equiv b^k \pmod n}$ para qualquer expoente k.

Portanto:

1. $7^{202} \equiv 1^{202} \pmod 6$
2. $7^{202} \equiv 1 \pmod 6$

Assim 7^{202} / 6 tem resto 1.

2. Para resolver $3x \equiv 4 \pmod 7$, precisamos encontrar o *inverso de 3 módulo 7*, ou seja, um número 3^{-1} tal que:

$$3 \cdot 3^{-1} \equiv 1 \pmod 7$$

Testando os valores de 1 a 6:

k	3·k	3·k (mod 7)
1	3	3
2	6	6
3	**9**	**2**
4	12	5
5	**15**	**1** ✓
6	18	4

$3^{-1} \equiv 5 \pmod 7$, pois $3 \cdot 5 = 15 = 2 \cdot 7 + 1$.

Multiplicando ambos lados da equação $3x \equiv 4 \pmod 7$ por 5, temos

$$5 \cdot 3x \equiv 5 \cdot 4 \pmod 7$$

Reduzindo:

$$15x \equiv 1 \pmod 7 \text{ e } 20 \equiv 6 \pmod 7$$

Assim:

$$x \equiv 6 \pmod 7$$

3. B
4. A
5. B

REFERÊNCIAS

Alchetron. *Lester S. Hill*. Alchetron — The Free Social Encyclopedia. Acesso em: 21 fev. 2026. Disponível em: <https://alchetron.com/Lester-S-Hill>.

ANTON, H.; RORRES, C. *Álgebra linear com aplicações*. 8. ed. Porto Alegre: Bookman, 2001.

AUSUBEL, D. P. *Aquisição e retenção de conhecimentos: uma perspectiva cognitiva*. Lisboa: Plátano, 2003.

BARBOSA, L.; CORNELISSEN, M. G. Cifra de Hill: Uma aplicação ao estudo de matrizes. *Revista Ciências Exatas e Naturais*, v. 19, n. 2, p. 152–167, 2017.

BOLDRINI, J. L. et al. *Álgebra linear*. 3. ed. São Paulo: Harbra, 1986.

BRANDÃO, M. M. D. Uma adaptação da cifra de Hill para estudo de matrizes. *Revista de Matemática da UFOP*, v. 5, n. 1, p. 78–94, 2018.

BRASIL. *Base Nacional Comum Curricular*. Brasília, 2018. Disponível em: <http://basenacionalcomum.mec.gov.br/>. Acesso em: 21 fev. 2026.

BROEMELING, L. D. An account of early statistical inference in arab cryptology. *The American Statistician*, v. 65, n. 4, p. 255–257, 2011.

BROUSSEAU, G. *Theory of Didactical Situations in Mathematics*. 1. ed. Dordrecht: Kluwer Academic Publishers, 1997.

CAYLEY, A. A memoir on the theory of matrices. *Philosophical Transactions of the Royal Society of London*, v. 148, p. 17–37, 1858.

CHARLOT, B. *Da relação com o saber às práticas educativas*. São Paulo: Cortez, 2013.

D'AMBROSIO, U. *Educação matemática: da teoria à prática*. Campinas: Papirus, 1996.

DOLZ, J.; NOVERRAZ, M.; SCHNEUWLY, B. Sequcias didicas para o oral e a escrita: apresentao de um procedimento. In: SCHNEUWLY, B.; DOLZ, J. (Ed.). *Gêneros orais e escritos na escola*. Campinas, SP: Mercado de Letras, 2004.

DORIER, J.-L. et al. The obstacle of formalism in linear algebra. In: DORIER, J.-L. (Ed.). *On the Teaching of Linear Algebra*. Dordrecht: Kluwer Academic Publishers, 2000. p. 85–124.

DUVAL, R. *Registros de representação semiótica e funcionamento cognitivo da compreensão em matemática*. Campinas: Papirus, 2003. 11–33 p.

EVARISTO, J.; PERDIGÃO, E. *Introdução à álgebra abstrata*. Maceió: EDUFAL, 2002.

EVES, H. *Introdução à história da matemática*. Campinas: Editora da Unicamp, 2004.

FALEIROS, A. C. *Criptografia*. São Carlos: SBMAC, 2011.

FREUDENTHAL, H. *Revisiting Mathematics Education: China Lectures*. 1. ed. Dordrecht: Kluwer Academic Publishers, 1991.

GIOVANNI, J. R.; BONJORNO, J. R.; JúNIOR, J. R. G. *Matemática completa: ensino médio*. São Paulo: FTD, 2005.

HILL, L. S. Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, v. 36, n. 6, p. 306–312, 1929.

Johns Hopkins University. *Photograph of James Joseph Sylvester*. Digital Library, Sheridan Libraries. Acesso em: 21 fev. 2026. Disponível em: <https://digital.library.jhu.edu/islandora/photograph-james-joseph-sylvester-1>.

KAHN, D. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner, 1996.

KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography*. 3. ed. Boca Raton: CRC Press, 2021.

KLINE, M. *Mathematical Thought from Ancient to Modern Times*. New York: Oxford University Press, 1972.

KUHN, M. C. Dificuldades de aprendizagem em matemática: um estudo de caso em turmas de 1º ano do Ensino Médio. *Educação Matemática em Revista*, Brasília, v. 27, n. 76, p. 1–18, 2022.

LIMA, E. L. *A matemática do ensino médio*. 9. ed. Rio de Janeiro: SBM, 2012. v. 2.

MAIOLI, M. *A contextualização na matemática do ensino médio*. 211 p. Tese (Doutorado) — Pontifícia Universidade Católica de São Paulo, São Paulo, 2012.

MEYER, C. D. *Matrix Analysis and Applied Linear Algebra*. Philadelphia: SIAM, 2000.

MJ2 Artesanos. *Réplicas*. MJ2 Artesanos — Blog. Acesso em: 21 fev. 2026. Disponível em: <https://www.mj2artesanos.es/blog/category/replicas/>.

O'CONNOR, J. J.; ROBERTSON, E. F. *Arthur Cayley — Pictures*. MacTutor History of Mathematics Archive, University of St Andrews. Acesso em: 21 fev. 2026. Disponível em: <https://mathshistory.st-andrews.ac.uk/Biographies/Cayley/pictdisplay/>.

O'CONNOR, J. J.; ROBERTSON, E. F. *Leonard Adleman — Pictures*. MacTutor History of Mathematics Archive, University of St Andrews. Acesso em: 15 mar. 2026. Disponível em: <https://mathshistory.st-andrews.ac.uk/Biographies/Adleman/pictdisplay/>.

PERKINS, A. *#MathArtChallenge 95: Magic Squares*. 2020. Arbitrarilyclose. Acesso em: 21 fev. 2026. Disponível em: <https://arbitrarilyclosecom.wordpress.com/2020/08/01/mathartchallenge-95-magic-squares/>.

QUARESMA, P.; PINHO, A. *Análise de Frequências da Língua Portuguesa*. Coimbra, 2007. Disponível em: <https://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/interTIC07pqap.pdf>. Acesso em: 22 maio 2025.

SAID, T. *O desafio de Alan Turing à inteligência humana*. 2024. Outras Palavras (republicado do Jornal da USP). Acesso em: 21 fev. 2026. Disponível em: <https://outraspalavras.net/outrasmidias/o-desafio-de-alan-turing-a-inteligencia-humana/>.

SANTOS, J. P. de O. *Introdução à teoria dos números*. 3. ed. Rio de Janeiro: IMPA, 2020.

SIERPINSKA, A. On some aspects of students' thinking in linear algebra. In: DORIER, J.-L. (Ed.). *On the Teaching of Linear Algebra*. Dordrecht: Kluwer Academic Publishers, 2000. p. 209–246.

SINGH, S. *O livro dos códigos: a ciência do sigilo — da Antiguidade à era quântica*. Rio de Janeiro: Record, 2001.

Sistema Poliedro de Ensino. *Ensino Médio e Pré-Vestibular: Matemática*. 2. ed. São Paulo: Poliedro, 2024. Apostila de curso pré-vestibular.

SKOVSMOSE, O. *Educação matemática crítica: a questão da democracia*. Campinas: Papirus, 2000.

STEINBRUCH, A.; WINTERLE, P. *Álgebra linear*. São Paulo: Pearson Prentice Hall, 1987.

STINSON, D. R.; PATERSON, M. *Cryptography: Theory and Practice*. 4. ed. Boca Raton: CRC Press, 2019.

ZABALA, A. *A prática educativa: como ensinar*. Porto Alegre: Artmed, 1998.