INSTITUTO FEDERAL DA PARAÍBA
CAMPUS CAJAZEIRAS
CURSO DE LICENCIATURA EM MATEMÁTICA

IVANILDO LEITE BATISTA

ENSINO DE MATRIZES: FUNDAMENTOS TEÓRICOS E APLICAÇÕES

CAJAZEIRAS
2025

IVANILDO LEITE BATISTA

ENSINO DE MATRIZES: FUNDAMENTOS TEÓRICOS E APLICAÇÕES

Monografia apresentada junto ao **Curso de Licenciatura em Matemática** do **Instituto Federal da Paraíba**, como requisito parcial à obtenção do título de **Licenciado em Matemática**.

Orientador:

Prof. Me. Leonardo Ferreira Soares.

Coorientador:

Prof. Dr. Vinicius Martins Teodósio Rocha.

CAJAZEIRAS

2025

IFPB / Campus Cajazeiras
Coordenação de Biblioteca
Biblioteca Prof. Ribamar da Silva
Catalogação na fonte: Cícero Luciano Félix CRB-15/750

B333e Batista, Ivanildo Leite.

Ensino de matrizes: fundamentos teóricos e aplicações / Ivanildo Leite Batista. – Cajazeiras, 2025.
60f. : il.

Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Cajazeiras, 2025.

Orientador: Prof. Me. Leonardo Ferreira Soares.
Coorientador: Prof. Dr. Vinicius Martins Teodósio Rocha.

1. Ensino de matemática. 2. Matriz. 3. Teoria dos números. 4. Criptografia. 5. Computação gráfica. I. Instituto Federal da Paraíba. II. Título.

IFPB/CZ CDU: 51:37(043.2)

IVANILDO LEITE BATISTA

ENSINO DE MATRIZES: FUNDAMENTOS TEÓRICOS E APLICAÇÕES

Monografia apresentada ao programa de **Curso de Licenciatura em Matemática** do **Instituto Federal da Paraíba**, como requisito parcial à obtenção do título de **Licenciado em Matemática**.

Data de aprovação: 07/03/2025

Banca Examinadora:

gov.br Documento assinado digitalmente
LEONARDO FERREIRA SOARES
Data: 17/03/2025 16:31:13-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Leonardo Ferreira Soares
Instituto Federal da Paraíba - IFPB

gov.br Documento assinado digitalmente
VINICIUS MARTINS TEODOSIO ROCHA
Data: 17/03/2025 14:39:34-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Vinicius Martins Teodósio Rocha
Instituto Federal da Paraíba - IFPB

gov.br Documento assinado digitalmente
WILLIAM DE SOUZA SANTOS
Data: 17/03/2025 15:29:37-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. William de Souza Santos
Instituto Federal da Paraíba - IFPB

gov.br Documento assinado digitalmente
STANLEY BORGES DE OLIVEIRA
Data: 17/03/2025 15:17:50-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Stanley Borges de Oliveira
Instituto Federal da Paraíba - IFPB

Dedico este trabalho aos meus avós paternos (in memoriam) Maria Porcina das Chagas Santos e João Batista Sobrinho.

AGRADECIMENTOS

Primeiramente agradeço a Deus por todas as conquistas pessoais e profissionais obtidas durante a graduação, principalmente nos momentos difíceis que ressignificaram minhas dúvidas e necessidades de aprendizagem enquanto ser humano e professor em formação inicial.

À minha família (pais, irmãos, tios(as), primos(as), etc) que sempre me deu o suporte necessário para conseguir alcançar meus objetivos e continuar estudando, buscando a construção de diálogos e entendimentos em torno das novas formas de socialização do conhecimento.

Ao meus amigos Natanael Pessoa Lustoza, Laís Saraiva Oliveira, Dlaânio da Silva Correia, Victor Emanoel da Silva Souza, Virlene Duarte Menezes, Eric da Silva Santos, Francisco Vandernilso de Oliveira, Joyce Pereira de Souza, Francisco Bruno Gonçalves Euzébio e Artur Henrique de Sousa Sucupira que nos encontros e desencontros de opiniões e situações-problema respeitaram as minhas limitações/dificuldades, possibilitando de forma colaborativa a realização de pesquisas, projetos e sobretudo novos vínculos de convivência.

A todos os(as) meus(inhas) ex-professores(as) da escola Antônio Fernandes, EEIF Antônio Landim de Macêdo e EEEP Leopoldina Gonçalves Quezado que compartilharam seus conhecimentos e trajetórias acadêmicas com o propósito de impulsinar positivamente minhas perspectivas de futuro a curto, médio e longo prazo.

Aos professores orientadores Leonardo Ferreira Soares e Vinicius Martins Teodósio Rocha por toda dedicação, disponibilidade de tempo, educação e acompanhamento das atividades de pesquisa, produção e revisão textual do trabalho.

Aos professores William de Souza Santos e Stanley Borges de Oliveira pelas correções, sugestões e pela aceitação da participação na banca examinadora.

Por fim, destaco minha gratidão ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - Campus Cajazeiras e ao corpo docente do Curso Superior de Licenciatura em Matemática por todos os aprendizados consolidados entre 2021 e 2025.

“É melhor você tentar algo, vê-lo não funcionar e aprender com isso, do que não fazer nada.”

Mark Zuckerberg

RESUMO

O processo de ensino e aprendizagem da Matemática associado ao estudo de matrizes é, não de forma generalizada, considerado difícil e muitas vezes desvinculado da realidade humana por uma parte considerável do alunado, pelo fato do engessamento de metodologias tradicionais de capacitação curricular que estão limitadas ao desenvolvimento de abordagens didático-pedagógicas unicamente numéricas. Com base nisso, o presente trabalho busca apresentar múltiplas aplicações de matrizes, havendo um direcionamento específico para três campos de estudos: Teoria dos Números, Criptografia e a Computação Gráfica. O estudo é uma pesquisa de natureza básica, exploratória, de abordagem qualitativa e procedimento bibliográfico que contempla quatro aplicações de matrizes: Criptografia - Cifras de Hill, imagens binárias, algoritmo de Euclides estendido e transformações geométricas bidimensionais. Ademais, os resultados permitem a formação de um ensino de Matemática significativo ao mostrar como as matrizes podem estar incorporadas em diversos objetos matemáticos, principalmente aqueles mencionados nesta monografia.

Palavras-chave: Algoritmo de Euclides Estendido; Aplicações de Matrizes; Criptografia; Ensino de Matemática; Imagens Binárias; Transformações Geométricas.

ABSTRACT

The process of teaching and learning Mathematics associated with the study of matrices is, not generally, considered difficult and often disconnected from human reality by a considerable part of the student body, due to the rigidity of traditional methodologies of curricular training that are limited to the development of solely numerical didactic-pedagogical approaches. Based on this, this work seeks to present multiple applications of matrices, with a specific focus on three fields of study: Number Theory, Cryptography and Computer Graphics. The study is a basic, exploratory research, with a qualitative approach and bibliographic procedure that includes four applications of matrices: Cryptography - Hill ciphers, binary images, extended Euclid algorithm and two-dimensional geometric transformations. Furthermore, the results allow for the development of meaningful Mathematics teaching by showing how matrices can be incorporated into various mathematical objects, especially those mentioned in this monograph.

Keywords: Extended Euclid's Algorithm; Applications of Matrices; Encryption; Mathematics Teaching; Binary Images; Geometric Transformations.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SÍMBOLOS

$\mathbb{R}$	Conjunto dos números reais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{R}^2$	Conjunto dos pares ordenados $(x, y) \in \mathbb{R}$
$\mathbb{Z}_+^*$	Conjunto dos números inteiros positivos
$\forall$	Para todo
$\in$	Pertence
$\pm$	Mais ou menos
$\sum$	Somatório
$\exists$	Existe
$\nexists$	Não existe
$\prod$	Produtório
$\neq$	Diferente de
$<$	Menor que
$>$	Maior que
$\leq$	Menor ou igual
$\geq$	Maior ou igual
α	Letra grega alfa
β	Letra grega beta
$\longleftrightarrow$	Se e somente se
sen	Seno
$\cos$	Cosseno
$\equiv$	Congruente
$\Rightarrow$	Implicação
$\mid$	Divide

SUMÁRIO

1 INTRODUÇÃO

Com as crescentes mudanças no cenário social, econômico e sobretudo educacional das escolas em pleno século XXI, que integra tecnologias e recursos humanos variados, é de fundamental importância que a construção do conhecimento seja sistematizada por ideias, fatos e investigações científicas que permitam atribuir significados para as múltiplas formas de pensar, interagir e organizar saberes, desvinculando-se de técnicas de memorização do ensino tradicional que outrora era considerado adequado.

O ensino de Matemática frequentemente deixa lacunas quando conceitos são apresentados como verdades absolutas, limitando questionamentos e possíveis descobertas científicas por parte de alunos e professores. Isso ocorre porque, por razões diversas, muitas vezes não há o interesse em explorar a origem das bases teóricas dos conteúdos abordados em sala de aula. No entanto, é justamente essa investigação sobre as raízes dos conceitos que pode despertar a curiosidade e o pensamento crítico dos alunos, incentivando uma compreensão mais profunda e significativa da Matemática.

Polya (1995) argumenta que o docente que almeja desenvolver nos discentes a habilidade de solucionar problemas deve, antes de tudo, despertar neles a curiosidade para enfrentar desafios. Além disso, é essencial oferecer oportunidades para que os alunos pratiquem e exercitem essa habilidade de forma autônoma, construindo assim um aprendizado mais produtivo. Em uma perspectiva semelhante, Santos (2008, p. 28) reforça essa ideia ao destacar que “[...] as atitudes e falas do professor contribuem significativamente para a formação de opiniões na escola básica, repercutindo e moldando os significados atribuídos pelos alunos”.

Outra situação recorrente nas aulas de Matemática é a mecanização de cálculos sem finalidades específicas. O aluno que faz o uso do livro didático ou de qualquer outro material pedagógico sem conhecer a gênese de cada componente curricular acaba ficando bloqueado ao desenvolvimento de habilidades básicas, apresenta dificuldades de interpretação contextual, desmotivado devido a repetição exacerbada de exercícios e com raciocínio lógico limitado (Jacobik, 2010).

As matrizes inicialmente, na Educação Básica, são estudadas no segundo ano do Ensino Médio, geralmente através da apresentação de sua forma genérica, principais tipos e algumas aplicações a depender do material disponibilizado pela escola, grade curricular e prioridades estipuladas pelo professor regente no início do ano letivo para atender outras carências estudantis. Além disso, no Ensino Superior, elas são usadas como ferramentas de ensino, pesquisa e modelagem de situações-problema em disciplinas como Álgebra Linear, Cálculo Numérico e Cálculo Diferencial e Integral.

A motivação central da construção desta monografia foi a participação na monitoria de Matemática Básica II, disciplina do terceiro período do Curso Superior de Licenciatura em Matemática do Instituto Federal da Paraíba - Campus Cajazeiras, que abrange em sua ementa técnicas de resolução de sistemas lineares, determinantes e matrizes, mas sem incluir diretamente as aplicações dos conteúdos selecionados. A monitoria é uma prática acadêmica destinada para apoiar os estudantes em fase inicial de aprendizagem com atividades complementares (tira-dúvidas em horários extraclasse, organização de materiais, promoção de discussões, trocas de ideias, etc) intermediadas por um tutor que atua em parceria com o professor titular (Frison, 2016).

Ainda sobre a monitoria de Matemática Básica II, os encontros eram realizados no formato híbrido (presencial e/ou online) com o predomínio de resoluções de questões de vestibulares, olímpiadas de Matemática e concursos. No entanto, como a maioria dos exercícios não eram contextualizados, exigindo uma interpretação mais objetiva, surgiu a pergunta norteadora que possibilitou a investigação deste trabalho: Como as matrizes podem ser aplicadas em diferentes áreas do saber que utilizam a Matemática como fundamento teórico ou ferramenta de ensino?.

Quanto à organização, no segundo capítulo (2), após a introdução, são apresentados os principais tipos de matrizes, suas configurações, propriedades, tópicos de Teoria dos Números e um recorte histórico do conceito de matrizes, começando pelo desenvolvimento de sistemas lineares para resolver problemas do dia a dia em diferentes civilizações, passando em seguida para a formação do cálculo do determinante por vários matemáticos ao longo do tempo.

Posteriormente, no terceiro capítulo (3), quatro aplicações de matrizes são apresentadas com o propósito de mostrar como elas podem ser empregadas em vários objetos de conhecimento, de início temos as Cifra de Hill que possibilitam a codificação e decodificação de mensagens secretas, a relação entre matrizes e imagens binárias/booleanas, a combinação da Identidade de Bézout e o cálculo do Máximo Divisor Comum com o Algoritmo de Euclides estendido, encerrando com transformações geométricas bidimensionais. Por fim, no quarto capítulo (4) estão as considerações finais, reforçando os objetivos da pesquisa, algumas críticas e apontamentos de novas aplicações que podem ser temáticas de outros trabalhos acadêmicos.

1.1 Objetivo geral

- Apresentar as múltiplas aplicações de matrizes em diferentes áreas do conhecimento, desde a Teoria dos Números, Computação Gráfica e a Criptografia, demonstrando a versatilidade delas enquanto ferramentas matemáticas.

1.2 Objetivos específicos

- Compreender a aplicabilidade do uso de matrizes em algoritmos criptográficos, em especial as Cifras de Hill;
- Abordar como as matrizes são usadas para representar e manipular imagens binárias/booleanas;
- Determinar o máximo divisor comum entre dois números inteiros x e y e a Identidade de Bézout $x \cdot m + y \cdot m = mdc(x,y)$, $(m,n) \in \mathbb{Z}$, usando o Algoritmo de Euclides Estendido;
- Explorar o papel das matrizes na realização de transformações geométricas bidimensionais, como a rotação, expansão, contração e translação, fundamentais em áreas como a Computação Gráfica e a Robótica.

1.3 Metodologia

Este trabalho é caracterizado como uma pesquisa de natureza básica porque visa construir novos conhecimentos a partir de verdades e interesses universais já desenvolvidos ou em desenvolvimento pela ciência, exploratória em relação aos seus objetivos pelo fato de vale-se de uma investigação que possibilita uma maior familiarização com um determinado assunto e de abordagem qualitativa com generalizações e entendimentos que não exigem métodos estatísticos ou probabilísticos (Prodanov, 2013). Ademais, é adotado um procedimento bibliográfico, para Gill (2002, p. 44):

> A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho dessa natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas.

As referências bibliográficas são, em maior parte, obras cujos conteúdos são ministrados em cursos de Álgebra Linear, Teoria dos Números, História da Matemática e em programas de aperfeiçoamento de professores como o Mestrado Profissional em Matemática em Rede Nacional (PROFMAT).

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são abordadas as bases teóricas que sustentam os resultados apresentados no capítulo (3). As definições, propriedades, teoremas e outros objetos matemáticos associados ao estudo de matrizes e de alguns assuntos de Teoria dos Números são provenientes de pesquisas em Iezzi e Hazzan (2013), Lipschutz e Lipson (2011), Hefez (2016) e Domingues e Iezzi (2003). Ademais, no final do capítulo são apresentadas algumas informações históricas.

2.1 Definição de matriz e sua representação genérica

Definição 1. Uma matriz é um agrupamento retangular de números reais (ou não), que estão dispostos em m linhas e n colunas conforme a representação da equação (1), cuja ordem, ou dimensão, é expressada por $m \times n$.

$$M_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{1}$$

Exemplos de matrizes:

$$A_{3\times 3} = \begin{pmatrix} 1 & 4 & 1 \\ 2 & 10 & 0 \\ 3 & 8 & 7 \end{pmatrix} \qquad B_{3\times 2} = \begin{bmatrix} 10 & 8 \\ 12 & 7 \\ 9 & 6 \end{bmatrix} \qquad C_{2\times 3} = \begin{Vmatrix} 1 & 8 & 5 \\ 9 & 6 & 4 \end{Vmatrix}$$

Observações:

$i)$ Quando a quantidade de linhas e colunas é igual, ou seja, $m = n$, a matriz é classificada como quadrada e para este caso a sua ordem corresponde a tal igualdade.

$ii)$ Podem ser formadas por parênteses ( ), colchetes [ ] ou barras verticais duplas ‖ ‖.

$iii)$ Cada elemento genérico de uma matriz é denotado por a_{ij}, i é a indicação da linha, j a coluna em que o elemento está localizado e a corresponde a letra minúscula designada para a matriz.

$iv)$ As linhas são enumeradas de cima para baixo (1 a m), enquanto que as colunas são enumeradas da esquerda para direita (1 a n).

v) As matrizes também podem ser formadas por determinadas leis de formação em função de i e de j. Na equação (2) temos uma matriz $C = (c_{ij})_{3\times 3}$ tal que $c_{ij} = i^2 + j^2$.

$$C = \begin{pmatrix} 2 & 5 & 10 \\ 5 & 8 & 13 \\ 10 & 13 & 18 \end{pmatrix} \tag{2}$$

2.2 Operações aritméticas com matrizes

Os elementos de uma matriz ou são alterados ou reposicionados para atender o desenvolvimento de situações-problema com diferentes níveis de complexidade e necessidade. Estas mudanças ocorrem com a subtração, adição e multiplicação de matrizes conforme exposto a seguir:

2.2.1 Adição/Subtração de matrizes

Definição 2. Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$ duas matrizes de ordem $m \times n$. A soma ou a diferença dos elementos de A e B irá resultar em uma terceira matriz $C = [c_{ij}]_{m\times n}$:

$$\begin{aligned}
A \pm B &= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \pm \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} \\
A \pm B &= \begin{pmatrix} a_{11} \pm b_{11} & a_{12} \pm b_{12} & \dots & a_{1n} \pm b_{1n} \\ a_{21} \pm b_{21} & a_{22} \pm b_{22} & \dots & a_{2n} \pm b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} \pm b_{m1} & a_{m2} \pm b_{m2} & \dots & a_{mn} \pm b_{mn} \end{pmatrix} \\
A \pm B &= \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \dots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{pmatrix}
\end{aligned}$$

Duas ou mais matrizes só podem ser adicionadas ou subtraídas se possuirem a mesma ordem, caso contrário, elas não são consideradas *conformes*, inviabilizando a realização das operações mencionadas. A mesma condição é utilizada para afirmar que duas ou mais matrizes são iguais, acrescentando a exigência de possuirem os mesmos elementos em posições correspondentes.

Questão 1: Dadas as matrizes $A = \begin{pmatrix} 1 & 7 \\ 1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 7 \\ 3 & 7 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 7 \\ 3 & 4 \\ 4 & 4 \end{pmatrix}$ e $D = \begin{pmatrix} 8 & 7 \\ 4 & 3 \\ 0 & 6 \end{pmatrix}$. Determine $A+B$, $B-A$, $C+D$ e $A-C$.

Resoluções:

$$
\begin{aligned}
i)\ A+B &= \begin{pmatrix} 1 & 7 \\ 1 & 2 \end{pmatrix} + \begin{pmatrix} 4 & 7 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 14 \\ 4 & 9 \end{pmatrix} \\
ii)\ B-A &= \begin{pmatrix} 4 & 7 \\ 3 & 7 \end{pmatrix} - \begin{pmatrix} 1 & 7 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 2 & 5 \end{pmatrix} \\
iii)\ C+D &= \begin{pmatrix} 1 & 7 \\ 3 & 4 \\ 4 & 4 \end{pmatrix} + \begin{pmatrix} 8 & 7 \\ 4 & 3 \\ 0 & 6 \end{pmatrix} = \begin{pmatrix} 9 & 14 \\ 7 & 7 \\ 4 & 10 \end{pmatrix} \\
iv)\ A-C &= \begin{pmatrix} 1 & 7 \\ 1 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 7 \\ 3 & 4 \\ 4 & 4 \end{pmatrix} = \nexists
\end{aligned}
$$

Propriedades:

1. $A_{m\times n} \pm B_{m\times n} = B_{m\times n} \pm A_{m\times n}$;

2. $A_{m\times n} \pm (B_{m\times n} \pm C_{m\times n}) = (A_{m\times n} \pm B_{m\times n}) \pm C_{m\times n}$;

3. Existe um elemento neutro $N_{m\times n}$ (matriz nula) tal que $A_{m\times n} \pm N_{m\times n} = N_{m\times n} \pm A_{m\times n} = A_{m\times n}$;

4. Existe um elemento oposto $-A_{m\times n}$ de modo que $A_{m\times n} + (-A_{m\times n}) = (-A_{m\times n}) + (A_{m\times n}) = N_{m\times n}$ (matriz nula);

5. Existe um elemento de cancelamento $L_{m\times n}$ tal que $A_{m\times n} \pm L_{m\times n} = B_{m\times n} \pm L_{m\times n}$ se, e somente se, $A_{m\times n} = B_{m\times n}$.

2.2.2 Multiplicação de matrizes

Definição 3. O produto de duas matrizes $A = [a_{ij}]_{m\times n}$ e $B = [b_{ij}]_{n\times z}$ so é possível se a quantidade de colunas de A for igual a quantidade de linhas de B, resultando em uma matriz $C = [c_{ij}]_{m\times z}$, multipicando os elementos das linhas de A pelos elementos das colunas de B. É importante destacar que a ordem de resolução tomada no produto AB é relevante, uma vez que as matrizes A e B podem ser comutáveis ou não. As operações abaixo são a generalização do produto AB.

$$A\cdot B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1j} & \dots & b_{1z} \\ b_{21} & b_{22} & \dots & b_{2j} & \dots & b_{2z} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nj} & \dots & b_{nz} \end{pmatrix}$$

$$A\cdot B = \begin{pmatrix} \sum_{k=1}^{n} a_{1k}\cdot b_{k1} & \sum_{k=1}^{n} a_{1k}\cdot b_{k2} & \dots & \sum_{k=1}^{n} a_{1k}\cdot b_{kj} & \dots & \sum_{k=1}^{n} a_{1k}\cdot b_{kz} \\ \sum_{k=1}^{n} a_{2k}\cdot b_{k1} & \sum_{k=1}^{n} a_{2k}\cdot b_{k2} & \dots & \sum_{k=1}^{n} a_{2k}\cdot b_{kj} & \dots & \sum_{k=1}^{n} a_{2k}\cdot b_{kz} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{ik}\cdot b_{k1} & \sum_{k=1}^{n} a_{ik}\cdot b_{k2} & \dots & \sum_{k=1}^{n} a_{ik}\cdot b_{kj} & \dots & \sum_{k=1}^{n} a_{ik}\cdot b_{kz} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{mk}\cdot b_{k1} & \sum_{k=1}^{n} a_{mk}\cdot b_{k2} & \dots & \sum_{k=1}^{n} a_{mk}\cdot b_{kj} & \dots & \sum_{k=1}^{n} a_{mk}\cdot b_{kz} \end{pmatrix}$$

$$A\cdot B = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1j} & \dots & c_{1z} \\ c_{21} & c_{22} & \dots & c_{2j} & \dots & c_{2z} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{i1} & c_{i2} & \dots & c_{ij} & \dots & c_{iz} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mj} & \dots & c_{mz} \end{pmatrix}$$

As multiplicações também podem ser realizadas através de subdivisões dos elementos das matrizes A e B em submatrizes. Contudo, as colunas da matriz A e as linhas de B devem ser divididas da mesma maneira.

Questão 2: Calcule o produto AB, sabendo que $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ e $B = \begin{pmatrix} 4 & 5 \\ 6 & 7 \\ 8 & 9 \end{pmatrix}$, subdivindido-as em matrizes menores.

Resolução:

$$A \cdot B = \begin{pmatrix} \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} & \begin{vmatrix} 3 \\ 6 \end{vmatrix} \\ \begin{vmatrix} 7 & 8 \end{vmatrix} & \begin{vmatrix} 9 \end{vmatrix} \end{pmatrix} \cdot \begin{pmatrix} \begin{vmatrix} 4 \\ 6 \end{vmatrix} & \begin{vmatrix} 5 \\ 7 \end{vmatrix} \\ \begin{vmatrix} 8 \end{vmatrix} & \begin{vmatrix} 9 \end{vmatrix} \end{pmatrix} \tag{3}$$

$$A \cdot B = \begin{pmatrix} (A_1)_{2\times 2} & (A_2)_{2\times 1} \\ (A_3)_{1\times 2} & (A_4)_{1\times 1} \end{pmatrix} \cdot \begin{pmatrix} (B_1)_{2\times 1} & (B_2)_{2\times 1} \\ (B_3)_{1\times 1} & (B_4)_{1\times 1} \end{pmatrix} \tag{4}$$

$$A \cdot B = \begin{pmatrix} A_1 \cdot B_1 + A_2 \cdot B_3 & A_1 \cdot B_2 + A_2 \cdot B_4 \\ A_3 \cdot B_1 + A_4 \cdot B_3 & A_3 \cdot B_2 + A_4 + B_4 \end{pmatrix} \tag{5}$$

$$A \cdot B = \begin{pmatrix} \begin{vmatrix} 40 \\ 94 \end{vmatrix} & \begin{vmatrix} 46 \\ 109 \end{vmatrix} \\ \begin{vmatrix} 148 \end{vmatrix} & \begin{vmatrix} 172 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} 40 & 46 \\ 94 & 109 \\ 148 & 172 \end{pmatrix} \tag{6}$$

Propriedades:

1. $(A_{m\times p} + B_{m\times p}) \cdot C_{p\times z} = A_{m\times p} \cdot C_{p\times z} + B_{m\times p} \cdot C_{p\times z}$;
2. $A_{m\times m} \cdot B_{m\times m} \neq B_{m\times m} \cdot A_{m\times m}$ (Há casos em que A e B são comutáveis);
3. $A_{m\times n} \cdot (B_{n\times p} \cdot C_{p\times z}) = (A_{m\times n} \cdot B_{n\times p}) \cdot C_{p\times z}$;
4. $k \cdot (A_{m\times n} \cdot B_{n\times p}) = A_{m\times n} \cdot (k \cdot B_{n\times p}) = (k \cdot A_{m\times n}) \cdot B_{n\times p},\ k \in \mathbb{R}$;
5. Existe um elementos neutro $I_{m\times m}$ tal que $A_{m\times m} \cdot I_{m\times m} = I_{m\times m} \cdot A_{m\times m} = A_{m\times m}$.
6. A existência do produto $A_{m\times n} \cdot B_{n\times p} = O_{m\times p}$ (matriz nula) não significa que A e B são ambas matrizes nulas.

Quando a multiplicação é realizada por um número real h a partir de uma matriz $A_{m\times n}$, a matriz resultante será encontrada multiplicando-se h por todos os elementos de $A_{m\times n}$ segundo a generalização abaixo:

$$\begin{aligned} h \cdot A &= h \cdot \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \\ h \cdot A &= \begin{pmatrix} h \cdot a_{11} & h \cdot a_{12} & \dots & h \cdot a_{1n} \\ h \cdot a_{21} & h \cdot a_{22} & \dots & h \cdot a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h \cdot a_{m1} & h \cdot a_{m2} & \dots & h \cdot a_{mn} \end{pmatrix} \end{aligned}$$

Propriedades da multiplicação de uma matriz por um valor real:

1. $d\cdot(A_{m\times n}+B_{m\times n}) = d\cdot A_{m\times n}+d\cdot B_{m\times n},\ d\in\mathbb{R};$
2. $(d+e)\cdot A_{m\times n} = d\cdot A_{m\times n}+e\cdot A_{m\times n},\ \ (e,d)\in\mathbb{R};$
3. $d\cdot(e\cdot A_{m\times n}) = (d\cdot e)\cdot A_{m\times n},\ (e,d)\in\mathbb{R};$
4. Existe um número real p tal que $p\cdot A_{m\times n} = A_{m\times n}$.

Questão 3: Determine se as matrizes $A = \begin{pmatrix} 1 & 2 \\ 4 & 8 \end{pmatrix}$ e $B = \begin{pmatrix} 8 & 7 \\ 17 & -6 \end{pmatrix}$ são comutáveis e em seguida calcule $2\cdot A\cdot B$.

Resolução: As matrizes A e B não são comutativas, pois

$$
\begin{aligned}
A\cdot B &= \begin{pmatrix} 1 & 2 \\ 4 & 8 \end{pmatrix}\cdot\begin{pmatrix} 8 & 7 \\ 17 & -6 \end{pmatrix} = \begin{pmatrix} 42 & -5 \\ 168 & -20 \end{pmatrix}\\
B\cdot A &= \begin{pmatrix} 8 & 7 \\ 17 & -6 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 \\ 4 & 8 \end{pmatrix} = \begin{pmatrix} 36 & 72 \\ -7 & -14 \end{pmatrix}
\end{aligned}
$$

Ademais,

$$
\begin{aligned}
2\cdot A\cdot B &= 2\cdot\begin{pmatrix} 1 & 2 \\ 4 & 8 \end{pmatrix}\cdot\begin{pmatrix} 8 & 7 \\ 17 & -6 \end{pmatrix}\\
2\cdot A\cdot B &= \begin{pmatrix} 2 & 4 \\ 8 & 16 \end{pmatrix}\cdot\begin{pmatrix} 8 & 7 \\ 17 & -6 \end{pmatrix}\\
2\cdot A\cdot B &= \begin{pmatrix} 84 & -10 \\ 336 & -40 \end{pmatrix}
\end{aligned}
$$

2.3 Classificação de matrizes

Na literatura existem diversos tipos de matrizes, cada uma com sua configuração e características. Algumas que aparecem recorrentemente em problemas da Matemática são a transposta, inversa, identidade, nula, coluna e linha.

2.3.1 Matriz transposta

Definição 4. $(S_1)^T = [s_{ij}]_{m\times n}$ é uma matriz transposta em relação a uma matriz $(S_1) = [s_{ji}]_{n\times m}$ quando as linhas e as colunas de S_1 são permutadas para originar $(S_1)^T$. No tocante aos elementos de (S_1) e $(S_1)^T$ temos que $[s_{ij}]_{m\times n} = [s_{ji}]_{n\times m}$ para quaisquer i e j. Notação matricial:

$$S = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m1} & s_{m2} & \dots & s_{mn} \end{pmatrix} \text{ e } S^T = \begin{pmatrix} s_{11} & s_{21} & \dots & s_{m1} \\ s_{12} & s_{22} & \dots & s_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1n} & s_{2n} & \dots & s_{mn} \end{pmatrix}$$

Propriedades:

1. $(A^T_{n\times m})^T = A_{m\times n}$;
2. $(A_{m\times n} \pm B_{m\times n})^T = A^T_{n\times m} \pm B^T_{n\times m}$;
3. $(y \cdot A^T_{n\times m}) = y \cdot A^T_{n\times m}, y \in \mathbb{R}$;
4. $(A_{m\times n} \cdot B_{n\times v})^T = B^T_{v\times n} \cdot A^T_{n\times m}$;
5. $I^T_{n\times n} = I_{n\times n}$;

Questão 4: Sejam $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ e $B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 3 & 4 & 1 \end{pmatrix}$. Forneça $G = (A^T)^T + B^2 \cdot (A \cdot B)^T$.

Resolução:

$$\begin{aligned} G &= (A^T)^T + B^2 \cdot (A \cdot B)^T \\ G &= \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 3 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 3 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 3 \\ 1 & 1 & 4 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} \\ G &= \begin{pmatrix} 139 & 308 & 477 \\ 19 & 38 & 57 \\ 248 & 543 & 838 \end{pmatrix} \end{aligned}$$

2.3.2 Matriz inversa

Definição 5. $A_{n\times n}$ é denominada inversível se existir uma segunda matriz $S_{n\times n}$ que satisfaça a equação (7).

$$S_{n\times n}\cdot A_{n\times n} = A_{n\times n}\cdot S_{n\times n} = I_{n\times n} \tag{7}$$

Se a existência de $S_{n\times n}$ for viável, então $S_{n\times n}$ é a inversa de $A_{n\times n}$ e é única. É comum que os elementos de $S_{n\times n}$ geralmente sejam determinados por 3 métodos: Sistemas lineares, operações elementares ou inversibilidade por matriz adjunta[1] (ver equação 8)

$$A^{-1} = \frac{adj(A)}{det(A)} \tag{8}$$

Propriedades:

1. $(A_{n\times n}\cdot B_{n\times n})^{-1} = B^{-1}_{n\times n}\cdot A^{-1}_{n\times n}$;

   Demonstração. Se a inversa de $(A_{n\times n}\cdot B_{n\times n})$ existir ela será única de modo que $(A^{-1}_{n\times n}\cdot B^{-1}_{n\times n})\cdot(A_{n\times n}\cdot B_{n\times n}) = (A_{n\times n}\cdot B_{n\times n})\cdot(A^{-1}_{n\times n}\cdot B^{-1}_{n\times n})$. Note que:

$$\begin{aligned}(B^{-1}_{n\times n}\cdot A^{-1}_{n\times n})\cdot(A_{n\times n}\cdot B_{n\times n}) &= B^{-1}_{n\times n}\cdot(A^{-1}_{n\times n}\cdot A_{n\times n})\cdot B_{n\times n} = B^{-1}_{n\times n}\cdot B_{n\times n} = I_{n\times n}\\ (A_{n\times n}\cdot B_{n\times n})\cdot(B^{-1}_{n\times n}\cdot A^{-1}_{n\times n}) &= A_{n\times n}\cdot(B_{n\times n}\cdot B^{-1}_{n\times n})\cdot A^{-1}_{n\times n} = A_{n\times n}\cdot A^{-1}_{n\times n} = I_{n\times n}\end{aligned}$$

   Portanto, $(A_{n\times n}\cdot B_{n\times n})^{-1} = B^{-1}_{n\times n}\cdot A^{-1}_{n\times n}$.

   ■

2. $(A_{n\times n}\pm B_{n\times n})^{-1} \neq A^{-1}_{n\times n}\pm B^{-1}_{n\times n}$;

3. $(A^{-1}_{n\times n})^{-1} = A_{n\times n}$;

   Demonstração. Trivialmente $I^{-1}_{n\times n} = I_{n\times n}$ e $A^{-1}_{n\times n}\cdot A_{n\times n} = I_{n\times n}$ (caso a inversa exista). Logo,

$$\begin{aligned}A^{-1}_{n\times n}\cdot A_{n\times n} &= I_{n\times n}\\ (A^{-1}_{n\times n}\cdot A_{n\times n})^{-1} &= (I_{n\times n})^{-1}\\ A^{-1}_{n\times n}\cdot(A^{-1}_{n\times n})^{-1} &= I_{n\times n}\\ A_{n\times n}\cdot A^{-1}_{n\times n}\cdot(A^{-1}_{n\times n})^{-1} &= A_{n\times n}\\ (A^{-1}_{n\times n})^{-1} &= A_{n\times n}\end{aligned}$$

   ■

[1] É sugerida a leitura de Howard e Rorres (2012, p. 111).

4. $(u \cdot A^{-1}_{n\times n}) = \dfrac{1}{u} \cdot A^{-1}_{n\times n}, u \in \mathbb{R}$ e $u \neq 0$;

5. $(A^{-1}_{n\times n})^T = (A^T_{n\times n})^{-1}$;

   Demonstração. Admitindo que $A^{-1}_{n\times n} \cdot A_{n\times n} = I_{n\times n}$ e sabendo que $I^T_{n\times n} = I_{n\times n}$, então:

$$\begin{array}{rcl} A^{-1}_{n\times n} \cdot A_{n\times n} & = & I_{n\times n} \\ (A^{-1}_{n\times n} \cdot A_{n\times n})^T & = & I^T_{n\times n} \\ A^T_{n\times n} \cdot (A^{-1}_{n\times n})^T & = & I_{n\times n} \\ (A^T_{n\times n})^{-1} \cdot A^T_{n\times n} \cdot (A^{-1}_{n\times n})^T & = & (A^T_{n\times n})^{-1} \cdot I_{n\times n} \\ (A^{-1}_{n\times n})^T & = & (A^T_{n\times n})^{-1} \end{array}$$

   ■

6. A inversa de $A_{n\times n}$ existe se o determinante[2] de A for diferentes de zero;

7. Se A^{-1} existir, então $A_{n\times n} \cdot B_{n\times p} = A_{n\times n} \cdot C_{n\times p}$ se, e somente se, $B_{n\times p} = C_{n\times p}$.

Questão 5: Encontre a inversa de $D = \begin{pmatrix} 3 & 5 \\ 7 & 9 \end{pmatrix}$.

Resolução: Como $det(D) \neq 0$, então D é inversível. Admitindo que $E = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ seja a inversa de $D_{2\times 2}$, então:

$$\begin{array}{rcl} D_{2\times 2} \cdot E_{2\times 2} & = & \begin{pmatrix} 3 & 5 \\ 7 & 9 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 3a+5c & 3b+5d \\ 7a+9c & 7b+9d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ E_{2\times 2} \cdot D_{2\times 2} & = & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 3 & 5 \\ 7 & 9 \end{pmatrix} = \begin{pmatrix} 3a+7b & 5a+9b \\ 3c+7d & 5c+9d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array}$$

Logo,

$$\begin{pmatrix} 3a+5c & 3b+5d \\ 7a+9c & 7b+9d \end{pmatrix} = \begin{pmatrix} 3a+7b & 5a+9b \\ 3c+7d & 5c+9d \end{pmatrix} \Rightarrow E_{2\times 2} = \begin{pmatrix} -\frac{9}{8} & \frac{5}{8} \\ \frac{7}{8} & -\frac{3}{8} \end{pmatrix}$$

[2] Em Iezzi e Hazzan (2013, p. 82-120) estão os meios de resolução quanto ao cálculo do determinante de uma matriz de ordem 2 ou superior.

2.3.3 Matriz identidade

Definição 6. Uma matriz identidade (também chamada matriz unidade) $U = [u_{ij}]_{n \times n}$ apresenta todos os elementos da diagonal principal iguais a 1, enquanto que os demais são todos iguais a zero.

$$U_{n\times n} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ ou } U_{n\times n} = [u_{ij}]_{n\times n} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

2.3.4 Matriz nula

Definição 7. $O = [o_{ij}]_{m \times n}$ é uma matriz nula se todos os seus elementos o_{ij} são iguais a zero.

$$O_{m\times n} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

2.3.5 Matriz coluna

Definição 8. É toda matriz $C = [c_{ij}]_{m \times 1}$ que apresenta apenas uma coluna.

$$C = \begin{pmatrix} c_{11} \\ c_{21} \\ c_{31} \\ c_{41} \\ \vdots \\ c_{m1} \end{pmatrix}$$

2.3.6 Matriz linha

Definição 9. $L = [l_{ij}]_{1\times n}$ é uma matriz linha porque contém somente uma linha e n colunas.

$$L = \begin{pmatrix} l_{11} & l_{12} & \dots & l_{1n} \end{pmatrix}$$

2.4 Tópicos de Teoria dos Números

2.4.1 MDC: Máximo Divisor Comum

Definição 10. De acordo com Hefez (2016, p. 74), "[...] um número inteiro d será dito um *divisor comum* de a e b se $d \mid a$ e $d \mid b$", assumindo que a e b sejam números inteiros iguais ou não. A partir desta definição, um número inteiro $f \geq 0$ será chamado ***máximo divisor comum*** (mdc) de outros dois, ou mais, inteiros a e b caso atenda dois critérios:

- 1º Critério: $f \mid a$ e $f \mid b$;
- 2º Critério: Se $p \mid a$ e $p \mid b$, então $p \mid f$, $p \in \mathbb{Z}$.

O *mdc* é utilizado em contextos problemáticos que necessitam da divisão em partes iguais e com a maior quantidade possível de elementos envolvidos. O recorte de peças metálicas em indústrias, a distribuição de funcionários de uma empresa em turnos de trabalhos e a cobertura de pisos com ladrilhos são alguns exemplos em que o máximo divisor comum torna-se importante para o cumprimento de exigências formais ou informais relacionadas a economidade de recursos. A seguir estão as principais proposições, lemas, propriedades e exemplos para o cálculo do *mdc* (Domingues; Iezzi, 2003).

PROPOSIÇÕES:

Proposição 1. [*Identidade de Bézout*] Para todo par ordenado $(x,y) \in \mathbb{Z}$ existe um segundo par ordenado $(c,d) \in \mathbb{Z}$, não únicos, tal que $mdc(x,y) = x\cdot(c) + y\cdot(d)$.

Proposição 2. Se x e y forem números inteiros coprimos entre si, então a Identidade de Bézout correspondene é $x\cdot(c)+y\cdot(d) = 1$, $(c,d) \in \mathbb{Z}$.

Proposição 3. Caso $s = mdc(x,y), (x,y) \in \mathbb{Z}$, então $mdc\left(\dfrac{x}{s}, \dfrac{y}{s}\right) = \dfrac{mdc(x,y)}{s} = 1$.

LEMAS:

Lema 1. Sejam x e y números inteiros, com x restritamente positivo. Se por hipótese x divide y, então $mdc(x,y) = x$.

Demonstração. De fato, é trivial que $x \mid x$, $x > 0$, e por suposição é conhecido que $x \mid y$ (Critério 1). Se x e y apresentarem um divisor inteiro z em comum, ou seja, $z \mid x$ e $z \mid y$ (Critério 2), é notório que $z \mid x$.

■

Lema 2. Pela divisão euclidiana (ver Definição 12), dados x e y inteiros quaisquer existem outros dois inteiros únicos q (quociente) e r (resto) de modo que $r = x - y \cdot q$, resultando na equivalência de que o máximo divisor comum $g = mdc(x,y)$ apenas se, e só se, $g = mdc(y,r)$.

PROPRIEDADES: Para todo $(x,y) \in \mathbb{Z}$, não ambos iguais a zero, são válidas as igualdades abaixo:

1. $mdc(x,y) = mdc(y,x)$;
2. $mdc(0,x) = mdc(x,x) = |x|$;
3. $mdc(x,y) = mdc(-x,y) = mdc(x,-y) = mdc(-x,-y)$;
4. $mdc(x^n,y^n) = mdc(x,y)^n$, $n \in \mathbb{N}$;
5. $mdc(x,y) = mdc(x+y,y)$;
6. $mdc(x,y) = mdc(x+k\cdot y,y)$, $k \in \mathbb{Z}$;

   Demonstração. Seja $d = mdc(x,y)$. Por linearidade, como $d \mid x$ e $d \mid y$, temos que $d \mid (x+k\cdot y)$, $k \in \mathbb{Z}$. Sendo assim, d é um divisor comum entre y e $(x+k\cdot y)$. Para provar que $d = mdc(x+k\cdot y,y)$, basta verificar que d é o maior dos divisores comuns entre tais números. De fato, se c é um outro divsor comum entre x e $(x+k\cdot y)$, então $c \mid y$ e $c \mid (x+k\cdot y)$, novamente, por linearidade, segue-se que $c \mid [(x+k\cdot y)-(k\cdot y)]$, portanto $c \mid x$, como já sabíamos que $c \mid y$, concluímos que c é um divisor comum entre x e y, mas tendo em vista que d é o máximo divisor comum entre x e y, então $c \leq d$. Por fim, $d = mdc(x+k\cdot y,y)$. ■

7. $mdc(n\cdot x,n\cdot y) = n\cdot mdc(x,y)$, $n \in \mathbb{N}$.

Questão 6: Calcule o $mdc(924, 7980)$.

Resolução: Com a decomposição em fatores primos verifica-se que $924 = 2^2 \cdot 3 \cdot 7 \cdot 11$ e $7980 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 19$. Os únicos fatores em comum em ambos os números são 2^2, 3 e 7, logo $mdc(924, 7980) = 2^2 \cdot 3 \cdot 7 = 84$.

2.4.2 Congruência modular

A congruência modular, ou aritmética modular, é uma das subáreas de estudos da Teoria dos Números que analisa as relações envolvidas entre os restos da divisão de números inteiros. Ela é aplicável em problemas da Matemática que trabalham com calendários, padrões geométricos, sistemas criptográficos, notas musicais e outros fenônemos periódicos.

Definição 11. Dados $a, b \in \mathbb{Z}$ é dito que a é congruente, ou côngruo, em relação a b módulo m, $m \in Z_+^*$, se, e somente se, m dividir a diferença entre a e b. Notação:

$$a \equiv b \pmod{m} \longleftrightarrow m \mid a - b \tag{9}$$

Propriedades: Para quaisquer a, b, c e $d \in \mathbb{Z}$ são verdadeiras as congruências abaixo:

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

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

   Demonstração. As hipóteses apresentadas são de que $m \mid a - b$ e $m \mid b - c$. Diante disso,

$$a - b = m \cdot k, k \in \mathbb{Z} \tag{10}$$

$$b - c = m \cdot g \longleftrightarrow b = m \cdot g + c, g \in \mathbb{Z} \tag{11}$$

   Percebe-se que é possível substituir a equação (11) na equação (10). Assim,

$$a - (m \cdot g + c) = m \cdot k$$
$$a - m \cdot g - c = m \cdot k$$
$$a - c = m \cdot k + m \cdot g$$
$$a - c = m \cdot (k + g)$$
$$a - c = m \cdot s, s \in \mathbb{Z}$$

   Portanto, por transitividade, $a \equiv c \pmod{m}$. ■

3. $a \equiv b \pmod{m} \longleftrightarrow a \pm c \equiv b \pm c \pmod{m}$;

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

5. $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow a+c \equiv b+d \pmod{m}$;

6. $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$;

7. $a \equiv b \pmod{m}$ e $d \mid m \Rightarrow a \equiv b \pmod{d}$, d é um inteiro maior do que 1;

Demonstração. A partir das duas hipóteses temos que

$$a - b = m \cdot w, w \in \mathbb{Z} \tag{12}$$
$$m = d \cdot f, f \in \mathbb{Z} \tag{13}$$

A equação (13) é substituível na equação (12), então

$$\begin{aligned} a-b &= (d \cdot f) \cdot w \\ a-b &= d \cdot (f \cdot w) \\ a-b &= d \cdot r, r \in \mathbb{Z} \end{aligned}$$

Em conclusão, $a \equiv b \pmod{d}$ ■

8. $a \equiv b \pmod{m} \Rightarrow a^h \equiv b^h \pmod{m}$, $h \in \mathbb{N}$.

Questão 7: Determine o resto de $102 \cdot 64 + 81$ na divisão por 5.

Resolução: Os números 102, 64 e 81 deixam, respectivamente, restos iguais a 2, 4 e 1 na divisão por 5. Com efeito disso, o resto desejado é 2, pois:

$$\begin{aligned} 102 \cdot 64 + 81 &\equiv 2 \cdot 4 + 1 \pmod{5} \\ 102 \cdot 64 + 81 &\equiv 8 + 1 \pmod{5} \\ 102 \cdot 64 + 81 &\equiv 9 \pmod{5} \\ 102 \cdot 64 + 81 &\equiv 4 \pmod{5} \end{aligned}$$

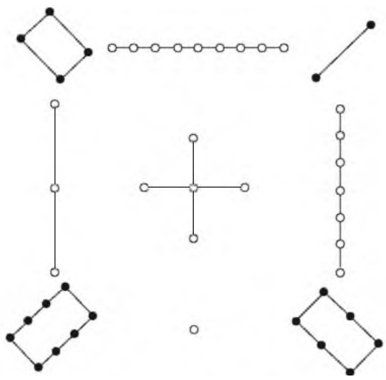
2.5 Contexto histórico de matrizes

Os livros didáticos geralmente estruturam o ensino de matrizes em uma sequência de conteúdos específicos: Matrizes, determinantes e sistemas lineares. Porém, ao contrário do que é explorado nos livros didáticos, as matrizes foram originadas a partir dos estudos de sistemas lineares e dos determinantes. Alguns dos primeiros registros históricos de matrizes remotam aos séculos XVIII e XVI a.C. com os babilônios desenvolvendo e resolvendo problemas algébricos sobre sistemas de equações lineares, impiricamente, utilizando duas varíaveis e considerando situações cotidianas em torno da agricultura e de relações comerciais, expressando as incógnitas envolvidas por meio de palavras, tais como "comprimento", "largura" e "área" (Boyer; Merzbach, 2012). Para fins de exemplificação:

> [...] em um texto da Babilônia antiga, achamos duas equações lineares simultâneas em duas incógnitas, chamadas respectivamente "primeiro anel de prata" e "segundo anel de prata". Se as denotarmos por x e y, em nossa notação as equações são $x/7 + y/11 = 1$ e $6x/7 = 10y/11$ [...] (Boyer; Merzbach, 2012, p. 44).

Dentre os principais padrões matemáticos mais antigos encontrados por pesquisadores que remetem a formação de uma matriz, o Quadrado mágico de Luo Shu (ver Figura 2.1) representa o que hoje em dia é uma matriz de ordem 3, cuja soma de seus valores em qualquer direção resulta em 15. Ele está veiculado a lenda de que uma tartarura o criou a partir de marcas em seu casco duante o reinado do imperador Yu em 2800 a.C. (Machado, 2013).

Figura 2.1 – Quadrado mágico de Luo Shu



Fonte: Extraído de Eves (2011, p. 269)

Os chineses no período de 200 a.C. a 100 a.C demonstraram uma maior proximidade com o atual conceito de matrizes em comparação aos babilônios devido a publicação da obra "*Nove Capítulos sobre a Arte Matemática*" durante a Dinastia Han, exibindo problemas comumente resolvidos na atualidade com um sistema de equações (O'Connor; Robertson, 1996). Exemplo extraído de Eves (2011, p. 268):

> Três feixes de uma colheita de boa qualidade, dois feixes de uma de qualidade regular e um feixe de uma de má qualidade são vendidos por 39 dou. Dois feixes de boa, três de regular e um de má são vendidos por 34 dou. Um feixe de boa, dois de regular e três de má são vendidos por 26 dou. Qual o preço do feixe para cada uma das qualidades?

Outra questão proposta:

> Havia três tipos de milho: três pacotes do primeiro tipo, dois do segundo e um do terceiro, totalizando 39 unidades de milho. Dois pacotes do primeiro, três pacotes do segundo e um do terceiro somando 34 unidades e, um pacote do primeiro, dois do segundo e três do terceiro que totalizam 26 unidades. Sabendo que os pacotes de milho do mesmo tipo levam a mesma quantidade de unidades, quantas unidades do milho contém um pacote de cada tipo? (Silva, 2014, p. 11).

Segundo Silva (2014), o autor ao resolver a questão fez a disposição dos números envolvidos, isto é, os coeficientes, em uma tabela retangular realizando-se algumas operações elementares de modo a obter a quantidade de cada tipo de milho nos pacotes, sendo esse procedimento hodiernamente conhecido como Eliminação Gaussiana ou Escalonamento. Vejamos a seguir as transformações realizadas com $c_x \in x = \{1,2,3\}$ os valores correspondentes das colunas:

Figura 2.2 – Resolução do problema dos três tipos de milho

1	2	3
2	3	2
3	1	1
26	34	39

1	0	3
2	5	2
3	1	1
26	24	39

0	0	3
4	5	2
8	1	1
39	24	39

0	0	3
0	5	2
36	1	1
99	24	39

$c_2 = 3c_2 - 2c_3$ $\qquad$ $c_1 = 3c_1 - c_3$ $\qquad$ $c_1 = 5c_1 - 4c_2$

Fonte: Adaptado de Silva (2014).

Foi somente em 1683 que a ideia do determinante como polinômio que se associa a um quadrado de números surgiu em razão da publicação de um trabalho do matemático japonês Seki Kowa, em que "[...] considerado o maior matemático japonês do século XVII, chegou a essa noção por meio do estudo de sistemas lineares, sistematizando o velho procedimento chinês (para o caso de duas equações apenas)"(Iezzi; Hazzan, 2013, p. 133). Posteriormente, Leibiniz criou uma representação para os coeficientes de um sistema linear de 3 equações analogamente ao utilizado em matrizes para linhas e colunas de modo que 2_1 indicasse a segunda linha e a primeira coluna do elemento a_{12} de uma matriz, a fim de identicar a posição dos elementos para o cálculo do determinante.

Em sequência, de acordo com O'Connor e Robertson (1996), o matemático escocês Colin Maclaurin apresentou alguns resultados para o cálculo do determinante em sistemas de equações lineares que resultassem em matrizes de ordem 2, 3 e 4 por meio da Regra de Cramer, com a publicação de sua obra "*Tratado de álgebra*" em 1748, cabendo apenas a Gabriel Cramer a generalização de tal regra para sistemas lineares de ordem $n \times n$ a partir do artigo "*Introdução à Análise de Curvas Algébricas*" (1750).

As demais contribuições foram dadas por Étienne Bézout, Alexandre Théophile Vandermonde e Pierre Simon de Laplace, que criaram métodos para o cálculo do determinante em 1764, 1771 e 1772, respectivamente. Laplace sem usar o termo determinante, fazendo a colocação da palavra resultante no lugar, forneceu a expansão do determinante para sistemas $n \times n$ por meio de um teorema que leva o seu nome (O'Connor; Robertson, 1996).

Ademais, os matemáticos alemães Carl Gustav Jacobi, em torno de 1830, e posteriormente Leopold Kronecker, em 1850, e Karl Weierstrass, em 1860, dedicaram-se ao estudo dos resultados associados as matrizes, mas com um enfoque específico na ideia de transformações lineares, cabendo a Jacobi, conhecido na época como "O grande algorista", o desenvolvimento de um teorema que permite a manipulação de uma fila de uma matriz quadrada qualquer a partir da combinação dos elementos de outras filas paralelas (Iezzi; Hazzan, 2013; O'Connor; Robertson, 1996).

Além disso, em consonância com essa conjuntura histórica, é importante destacar que:

> O termo Determinante foi utilizado pela primeira vez pelo matemático alemão Carl Friedrich Gauss em *Disquisitiones Arithmeticae* (1801) ao discutir formas quadráticas. Ele usou o termo porque o determinante determina as propriedades da forma quadrática. No entando, o conceito não é o mesmo de hoje. No mesmo trabalho, Gauss estabelece os coeficientes de suas formas quadráticas em matrizes retangulares. Ele descreve a multiplicação de matrizes (como composição, pois ele ainda não atingiu o conceito de álgebra matricial) e da inversa de uma matriz no contexto particular das matrizes de coeficientes de formas quadráticas (Aquino, 2021, p. 18).

Arthur Cayley (1821-1895) e James Joseph Sylvester (1814-1897) foram os principais responsáveis pela definição de matriz, Sylvester criuo a nomenclatura ao publicar um artigo na *Philosophical Magazine* e Cayley explorou o lado algébrico ao estudar sistemas de equações lineares e transformações do tipo $x' = a \cdot x + b \cdot y$ e $y' = c \cdot x + d \cdot y$ que são mudanças entre os pontos (x,y) e (x',y') com $(a,b,c,d) \in \mathbb{R}$ (Bernardes; Roque, 2016; Eves, 2011).

3 APLICAÇÕES

Este capítulo apresenta quatro aplicações de matrizes abrangendo os conceitos, propriedades e tópicos de Teoria dos Números da fundamentação teórica (Capítulo 2). Vale ressaltar que outras definições são apresentadas, por meio de um viés não axiomático, como forma de subsidiar determinadas características de cada aplicação.

3.1 Criptografia: Cifras de Hill

A Criptografia é uma das ramificações da Teoria da Informação, área do conhecimento proveniente da evolução dos *hardwares*, *softwares* e das redes globais de transmissão de dados, envolvendo códigos denominados **cifras**, além de **textos comuns** que são mensagens não codificadas e mensagens codificadas, sendo estas últimas chamadas de **criptogramas** (Hefez, 2016; Howard; Rorres, 2012). Em razão das crescentes formas de comunicações e da contínua troca de informações entre dispostivos eletrônicos (computadores, celulares, *tablets*, etc) surgiu a necessidade de codificar e decodificar mensagens, sobretudo aquelas consideradas confidenciais para um determinado grupo de pessoas, popularmente associadas ao emprego de serviços militares, ações diplomáticas e programas de Estados.

O ato de transformar um texto comum em um criptograma é denominado de cifrar ou criptografar, enquanto que o processo oposto é chama-se decifrar. Segundo Hefez (2016), a Criptografia não objetiva "esconder" fisicamente as informações que são transmitidas entre remetentes e destinários, mas encontrar métodos para ocultar o real significado que tais informações apresentam, permitindo com que apenas os indivíduos interessadoss nelas consigam entender as cifras. As Cifras de César, em homenagem ao general romano Júlio César, talvez seja um dos sistemas criptográficos mais famosos da história. Este mecanismo substitui cada letra do alfabeto convencional por outra letra a partir de um padrão lógico.

Quadro 3.1 – Cifras de César: Substituições de letras

Letras do Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M
Cifra de César	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*
Letras do Alfabeto	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifra de César	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

Fonte: Autor

Para elucidar a utilização do Quadro 3.1, caso o remetente decida enviar uma informação, hipoteticamente, com a frase "A matemática e a natureza" o destinário receberia como retorno "D PDWHPDWLFD H D QDWXUHCD", sendo necessário o gabarito do Quadro 3.1 para decifrar a mensagem.

Outro sistema que usa operações matriciais foi o criado pelo matemático americano Lester Sanders Hill (1891–1961) em 1929. As **Cifras de Hill** atribuem para cada letra do alfabeto um número natural que conforme apresentado no Quadro 3.2 estão entre 0 e 25, incluindo os extremos, fixando para Z o número 0.

Quadro 3.2 – Cifras de Hill: Correspondência entre letras e números.

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

Fonte: Autor

Para explicar o passo a passo da codificação e decodificação de uma mensagem com este sistema, Howard e Rorres (2012) utilizam uma de matriz de ordem 2, mas neste trabalho iremos fazer o uso de uma matriz de ordem 3×3, levando em consideração o conceito de congruência modular, visto na seção (2.4.2), da Aritmética.

CODIFICAÇÃO

1) Tome uma matriz $M_{3\times3}$ com entradas inteiras e determinante diferente de zero.

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \tag{14}$$

2) Separe as letras que formam a mensagem que será enviada pelo remetente em ternos sequenciais, caso seja necessário complementar algum terno uma letra qualquer deve ser adicionada, trocando em seguida pelos valores numéricos correspondentes fornecidos no Quadro 3.2. Exemplo:

$$ME\ CHAMO\ IVANILDO$$

$$MEC\ HAM\ OIV\ ANI\ LDO$$

$$13\ 5\ 3 \quad 8\ 1\ 13 \quad 15\ 9\ 22 \quad 1\ 14\ 9 \quad 12\ 4\ 15$$

$$x_1\ x_2\ x_3 \quad x_4\ x_5\ x_6 \quad x_7\ x_8\ x_9 \quad x_{10}\ x_{11}\ x_{12} \quad x_{13}\ x_{14}\ x_{15}$$

3) Com cada terno formado anteriormente, construa uma matriz $A_{3\times 1}$ e multiplique ela pela matriz M a sua esquerda. Com as multiplicações realizadas, os elementos das matrizes encontradas serão as cifras correspondentes para cada conjunto de ternos de modo que seja possível obter um texto cifrado. Vejamos:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \pmod{26} \tag{15}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x_4 \\ x_5 \\ x_6 \end{pmatrix} \equiv \begin{pmatrix} b_4 \\ b_5 \\ b_6 \end{pmatrix} \pmod{26} \tag{16}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x_7 \\ x_8 \\ x_9 \end{pmatrix} \equiv \begin{pmatrix} b_7 \\ b_8 \\ b_9 \end{pmatrix} \pmod{26} \tag{17}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x_{10} \\ x_{11} \\ x_{12} \end{pmatrix} \equiv \begin{pmatrix} b_{10} \\ b_{11} \\ b_{12} \end{pmatrix} \pmod{26} \tag{18}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x_{13} \\ x_{14} \\ x_{15} \end{pmatrix} \equiv \begin{pmatrix} b_{13} \\ b_{14} \\ b_{15} \end{pmatrix} \pmod{26} \tag{19}$$

O destinatário terá como resultado a mensagem $b_1\ b_2\ b_3\ \ b_4\ b_5\ b_6\ \ b_7\ b_8\ b_9\ \ b_{10}\ b_{11}\ b_{12}$ $b_{13}\ b_{14}\ b_{15}$ (letras ou números). Para os valores que excederem 25 considera-se os restos dos mesmos na divisão por 26.

DECODIFICAÇÃO

A decodificação é o processo contrário da codificação, ou seja, é a tradução das cifras recebidas pelo destinatário. Os ternos obtidos anteriormente são advindos da matriz C referente a equação (20).

$$C \equiv M \cdot A \equiv \underbrace{\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}}_{Matriz\ codificadora(M)} \cdot \underbrace{\begin{pmatrix} x_i \\ x_{i+1} \\ x_{i+2} \end{pmatrix}}_{Terno(A)} \equiv \underbrace{\begin{pmatrix} b_i \\ b_{i+1} \\ b_{i+2} \end{pmatrix}}_{Cifras(C)} \pmod{26}\ com\ 1 \leq i \leq 13 \tag{20}$$

Para que a mensagem seja lida pelo destinatário é obrigatório o uso da matriz inversa da matriz codificadora módulo 26, cuja formação é dada pela equação (21), em que $R = det(M)^{-1}$ é o inverso multiplicativo modular do determinante de M tal que $det(M) \cdot R \equiv R \cdot det(M) \equiv 1 \pmod{26}$.

$$M^{-1} \equiv R \cdot adj(M) \quad (\text{mod } 26)^1 \tag{21}$$

Por fim, para decodificar cada terno de cifras utiliza-se a equação (22).

$$K \equiv M^{-1} \cdot C \pmod{26} \tag{22}$$

Observações:

- Tanto o remetente quanto o destinário necessitam conhecer M e M^{-1} para realizar trocas de mensagens instantâneas;
- No passo a passo apresentado foi utilizada uma matriz de Hill de ordem 3, mas para matrizes de Hill de ordem $n \times n$ o processo é de forma análoga, cabendo o agrupamento do texto comum em conjuntos de n letras com as devidas correspondências numéricas;
- As correspondências entre letras e numéros do Quadro 3.2 pode possuir variações para a inserção de novas simbologias, mas a mudança implica na alteração do módulo 26;
- $M^{-1} \pmod{26}$ só existe se o $mdc(det(M), 26) = 1$.

Questão 08: Decodifique a mensagem $QRDTKAGF$, sabendo que ela foi formada pela matriz codificadora $C = \begin{pmatrix} 7 & 4 \\ 3 & 5 \end{pmatrix}$.

Resolução: Do Quadro 3.2 verifica-se que a mensagem em números é 17 18 4 20 11 1 7 e 6, possibilitando formar os pares $(17, 18)$, $(4, 20)$, $(11, 1)$ e $(7, 6)$. Além disso, temos que

$$C^{-1} \equiv J \cdot adj(C) \equiv 17 \cdot \begin{pmatrix} 5 & -4 \\ -3 & 7 \end{pmatrix} \equiv \begin{pmatrix} 85 & -68 \\ -51 & 119 \end{pmatrix} \equiv \underbrace{\begin{pmatrix} 7 & 10 \\ 1 & 15 \end{pmatrix}}_{\substack{\text{Matriz} \\ \text{Decodificadora}}} \pmod{26} \tag{23}$$

[1] Nas congruências modulares envolvendo operações matriciais considera-se a aplicação da Definição 11 nos elementos das matrizes resultantes das operações.

O inverso multiplicativo modular $J = det(C)^{-1}$ do determinante de C, $det(C) = 23$, é 17, pois $17 \cdot 23 \equiv 23 \cdot 17 \equiv 1 \pmod{26}$. A decodificação é baseada nas operações abaixo:

$$\begin{pmatrix} 7 & 10 \\ 1 & 15 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 299 \\ 287 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 1 \end{pmatrix} \pmod{26} \tag{24}$$

$$\begin{pmatrix} 7 & 10 \\ 1 & 15 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 228 \\ 304 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 18 \end{pmatrix} \pmod{26} \tag{25}$$

$$\begin{pmatrix} 7 & 10 \\ 1 & 15 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 87 \\ 26 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 0 \end{pmatrix} \pmod{26} \tag{26}$$

$$\begin{pmatrix} 7 & 10 \\ 1 & 15 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} 109 \\ 97 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 19 \end{pmatrix} \pmod{26} \tag{27}$$

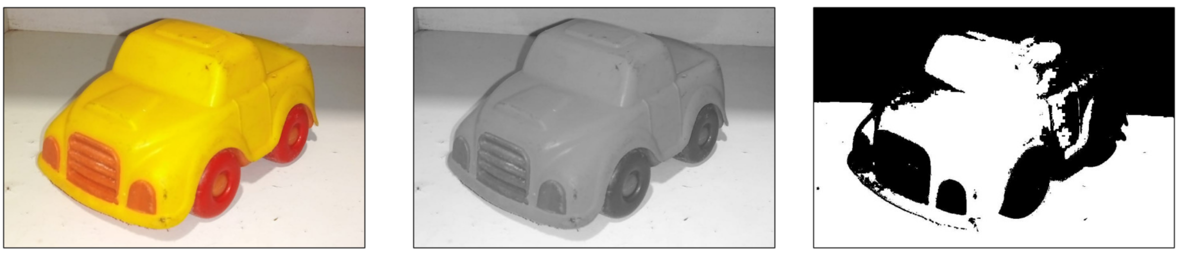
Resposta: Conforme os valores encontrados e o Quadro 3.2 o texto comum é $MATRIZES$.

Sugestão de exercício complementar: Decodifique a mensagem secreta SGDRUN formada pela matriz codificadora $\begin{pmatrix} 7 & 2 & 9 \\ 11 & 1 & 6 \\ 7 & 1 & 1 \end{pmatrix}$.

3.2 Imagens Binárias

Segundo Andrade (2020, p. 19), "a imagem digital é a representação numérica de uma imagem bidimensional, constituída por uma matriz binária (composta por zero e um) de modo a permitir seu processamento, sua transferência, sua impressão ou sua reproducão". Quanto à tipologia, existem diversos formatos de arquivos de imagens digitais, tais como o RGB (sistema de cores em tons de vermelho, verde e azul), o PGM (*Portable Gray Map*) que está associado a variação dos tons de cinzas e o PBM (*Portable Bitmap*) que lida com *bitmaps* monocromáticos (ver Figura 3.1).

Figura 3.1 – Carrinho de brinquedo em RGB, PGM e PBM, respectivamente.

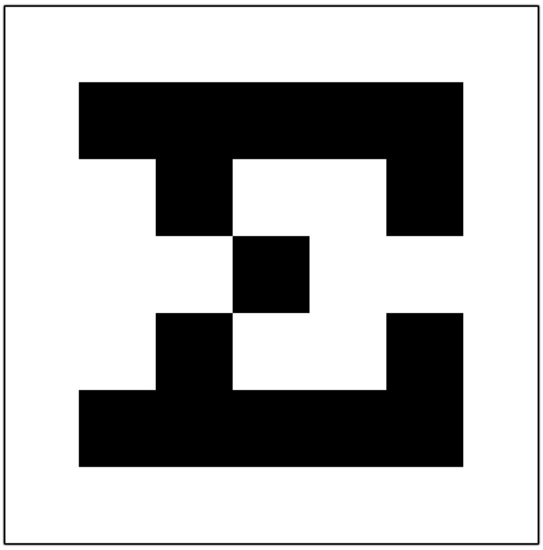


Fonte: Autor

Toda imagem presente em dispositivos eletrônicos é compreendida computacionalmente como um conjunto de pequenas partes constituintes denominadas de *pixels*, sendo estes por sua vez formados por *bits*, as menores unidades de informações em um arquivo tecnológico. A quantidade de *bits* por *pixel* varia conforme o número de canais de cores existentes em uma imagem, podendo ser 32 ou 64 *bits* por *pixel* para os casos em que as imagens são complexas, isto é, com muitas variações de cores ou apenas 1 *bit* para as figuras em preto e branco. Adicionalmente, o número de tonalidades de cores que uma imagem pode conter é dado por 2^n, em que n é o quantitativo de *bits* por *pixel* (*bpp*) (Gonzalez; Woods, 2010)

Os *bitmaps* (mapa de *bits*, em português) são os elementos formadores das cores que uma imagem apresenta por meio de uma tabela de códigos. Uma imagem em que cada *pixel* admite somente um único valor numérico (*bit*) 0 ou 1 tem 2 cores possíveis: preto (1) o branco (0). A Figura 3.2 ilustra o operador somatório com 49 *pixels*.

Figura 3.2 – Operador somatório



Fonte: Autor

A Figura 3.2 está atrelada a uma matriz $A = [a_{ij}]_{7\times7}$, que respeita as operações lógicas booleanas e mudanças de seus elementos para formar outros tipos de matrizes. No sistema de numeração decimal a soma, subtração e multiplicação de elementos de matrizes sempre irão implicar em números formados pelo conjunto $F = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, contendo 10 algarismos, com e sem repetições. Contudo, considerando a lógica booleana, quando duas ou mais imagens binárias são combinadas ou decompostas as suas respectivas matrizes são modificadas conforme os operadores do Quadro 3.3 (Gonzalez; Woods, 2010).

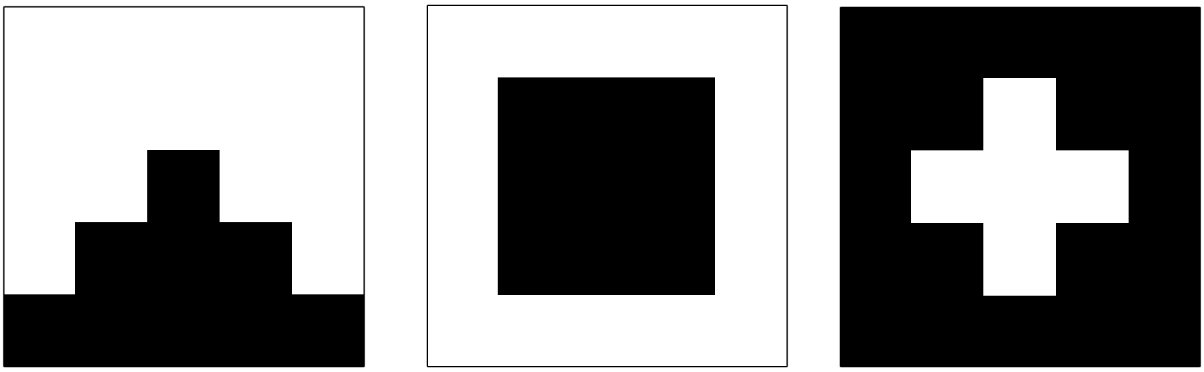
Quadro 3.3 – Operadores Booleanos

Entradas		Saídas				
A	B	$A+B$ (OR)	$A\cdot B$ (AND)	$\overline{A\cdot B}$ (NAND)	$\overline{A+B}$ (NOR)	Negação (NOT)
0	0	0	0	1	1	$\overline{A}$=1
0	1	1	0	1	0	
1	0	1	0	1	0	$\overline{A}$=0
1	1	1	1	0	0	

Fonte: Autor

Para explicitar como tais operadores podem estar relacionados ao estudo de matrizes e as imagens binárias, sejam A, B e C matrizes quadradas de ordem 5 cujas representações booleanas estão na Figura 3.3.

Figura 3.3 – Imagens booleanas: Matrizes A (esquerda), B (centro) e C (direita)



Fonte: Autor

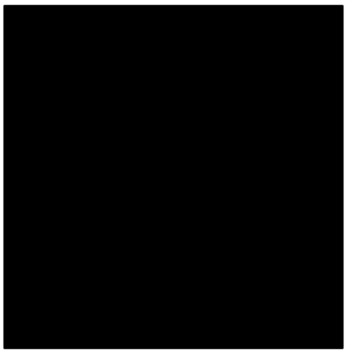
1 - União de imagens binárias

A adição das matrizes A, B e C terá como resultado a matriz D conforme a igualdade (28).

$$D = \underbrace{\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}}_{A} + \underbrace{\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}}_{B} + \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}}_{C} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{28}$$

Note que as operações booleanas utilizadas formam uma imagem binária somente com a cor preta (Figura 3.4).

Figura 3.4 – Imagem booleana da matriz D



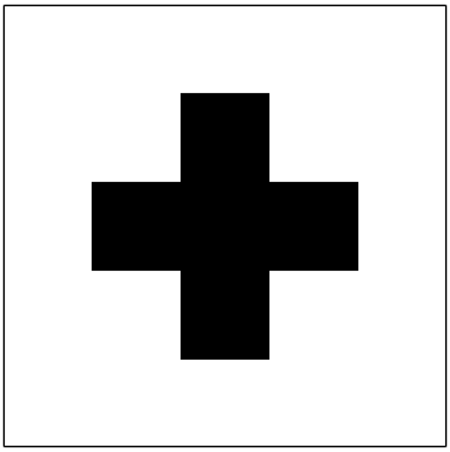
Fonte: Autor

O operador lógico OR permite a correção de defeitos visuais em contornos, regiões com lacunas e segmentos estreitos por meio de um elemento estruturante (outra matriz).

2 - Imagem binária complementar

O NOT (negação) possibilita a inversão dos valores lógicos 1 para 0, ou vice-versa, trocando o preto pelo branco, realizando uma polarização das imagens binárias. Na Computação Gráfica esse processo de inversão permite uma melhor visualização de imagens ao dilatar ou deletar regiões pixelizadas. Tomando como referência a matriz C e sua condificação binária é possível obter a Figura 3.5.

Figura 3.5 – Imagem binária complementar da matriz C.



Fonte: Autor

3 - Intersecção de imagens binárias

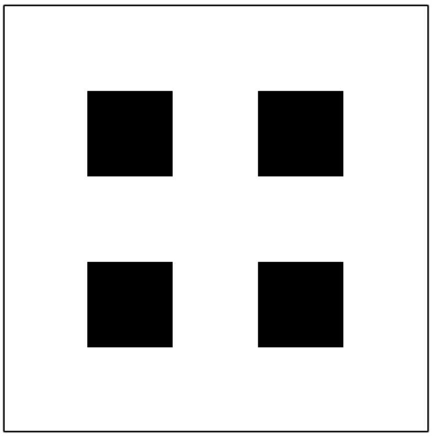
Ao contrário da aritmética tradicional, a multiplicação de matrizes na lógica booleana é *pixel* a *pixel*, geralmente com imagens de mesmo tamanho, com o operador

AND atuando como um filtro de erosão, alterando o valor lógico 1 para O, removendo dessa maneira elementos indesejados. Observe a multiplicação das matrizes B e C na equação (29).

$$Z = \underbrace{\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}}_{B} \cdot \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}}_{C} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{29}$$

A matriz booleana Z origina a imagem binária da Figura 3.6.

Figura 3.6 – Imagem binária da matriz Z.



Fonte: Autor

Considerando uma imagem booleana como uma relação binária entre dois conjuntos (matrizes) A e B, implicando em outro conjunto C (matriz resultante) são válidas as seguintes propriedades da Algébra Booleana (Daghlian, 2008):

1. $A+B = B+A$ e $A \cdot B = B \cdot A$ (Comutatividade)
2. $A+(B+C) = (A+B)+C$ e $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ (Associatividade)
3. $A+A = A$ e $A \cdot A = A$ (Idempotência)
4. $A+(A \cdot B) = A$ e $A \cdot (A+B) = A$ (Absorção)
5. $A+(B \cdot C) = (A+B) \cdot (A+C)$ e $A \cdot (B+C) = (A \cdot B)+(A \cdot C)$ (Distributividade)
6. $A+0 = A$ e $A \cdot 1 = A$ (Identidades)

7. $\overline{A \cdot B} = \overline{A} + \overline{B}$ e $\overline{A+B} = \overline{A} \cdot \overline{B}$ (Leis de Morgan)

8. $\overline{\overline{A}} = A$ (Involução)

9. $A + \overline{A} = 1$ e $A \cdot \overline{A} = 0$ (Complemento)

3.3 Algoritmo de Euclides Estendido

Definição 12. O Algoritmo de Euclides é um metodo de divisões sucessivas que permite determinar o máximo divisor comum (mdc) de dois números inteiros a e b. Na divisão euclidiana, dados $a, b \in \mathbb{Z}$, $a \geq b > 0$, pode-se encontrar dois inteiros únicos q_1 e r_1 tal que (Hefez, 2016):

$$a = b \cdot q_1 + r_1,\ 0 \leq r_1 < b \tag{30}$$

O método visa fornecer o $mdc(a,b)$ aplicando-se consecutivamente a divisão com resto. Inicialmente é realizada a divisão de a por b, em seguida a divisão de b pelo resto parcial da divisão anterior (r_1), posteriormente a divisão de r_1 por r_2 (resto da divisão de b por r_1) e assim por diante até chegar em uma divisão com resto igual a zero 0, aparecendo porque $b > r_1 > r_2 > r_3 > \cdots \geq 0$ não pode conter mais do que b inteiros. Em uma notação algébrica, o algoritmo é resumido pela progressão de igualdades abaixo:

$$\begin{array}{rcl}
a & = & b \cdot q_1 + r_1,\ 0 \leq r_1 < b \\
b & = & r_1 \cdot q_2 + r_2,\ r_2 < r_1 \\
r_1 & = & r_2 \cdot q_3 + r_3,\ r_3 < r_2 \\
r_2 & = & r_3 \cdot q_4 + r_4,\ r_4 < r_3 \\
\vdots & = & \qquad \vdots \\
r_{n-2} & = & r_{n-1} \cdot q_n + r_n,\ r_n < r_{n-1} \\
r_{n-1} & = & r_n \cdot q_{n+1} + 0
\end{array}$$

Pelos lemas (1) e (2) e seus resultados:

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \cdots = mdc(r_{n-1},r_n) = mdc(r_n,0) = r_n \tag{31}$$

Em um processo contrário, o mesmo algoritmo também é utilizado para determinar os inteiros x_0 e y_0 para formar a equação diafontina $a \cdot x_0 + b \cdot y_0 = mdc(a,b) = r_n$ (ver Proposição 1).

Questão 09: Determine o $mdc(64,123)$ e encontre um par de inteiros (m,n) de modo que $64m + 123n = mdc(64,123)$.

Solução: Pelo o Algoritmo Euclidiano,

$$\begin{aligned}
123 &= 64\cdot 1+59\\
64 &= 59\cdot 1+5\\
59 &= 5\cdot 11+4\\
5 &= 4\cdot 1+1\\
4 &= 1\cdot 4+0
\end{aligned}$$

O $mdc(64,123)=1$. Ademais,

$$\begin{aligned}
1 &= 5-4\cdot 1\\
1 &= (-59)+5\cdot 12\\
1 &= (-59)\cdot 13+64\cdot 12\\
1 &= 64\cdot(25)+123\cdot(-13)
\end{aligned}$$

Os inteiros m e n são, respectivamente, 25 e -13.

Através do exemplo anterior percebe-se que tanto o $mdc(64,123)$ quanto os inteiros m,n foram calculados separadamente. A versão estendida do Algoritmo de Euclides se difere do antecedente pelo fato de indicar simultaneamente o mdc desejado e a Identidade de Bézout vinculada a ele.

Conforme Hefez (2016) aponta, a extensão do algoritmo com a utilização de operações matriciais elementares ocorre com base nas seguintes etapas:

1ª Etapa: Considere a matriz $(E1)_{2\times 3}$, de modo que $a\geq b$.

$$(E1)=\begin{pmatrix} b & 1 & 0\\ a & 0 & 1\end{pmatrix},\ a=b\cdot q_1+r_1 \tag{32}$$

2ª Etapa: Subtraia da segunda linha (l_2) a multiplicação da primeira linha (l_1) por q_1, isto é, $l_2=l_2-q_1\cdot l_1$.

$$(E2)=\begin{pmatrix} b & 1 & 0\\ a-b\cdot q_1 & -q_1 & 1\end{pmatrix}=\begin{pmatrix} b & 1 & 0\\ r_1 & -q_1 & 1\end{pmatrix},\ b=r_1\cdot q_2+r_2 \tag{33}$$

3ª Etapa: Da primeira linha (l_1) subtraia cada elemento pela multiplicação de q_2 pela linha l_2.

$$(E3)=\begin{pmatrix} b-q_2\cdot r_1 & 1+q_1\cdot q_2 & -q_2\\ r_1 & -q_1 & 1\end{pmatrix}=\begin{pmatrix} r_2 & 1+q_1\cdot q_2 & -q_2\\ r_1 & -q_1 & 1\end{pmatrix},\ r_1=r_2\cdot q_3+r_3 \tag{34}$$

4ª Etapa: Realize a combinação linar $l_2=l_2-q_3\cdot l_1$.

$$(E4)=\begin{pmatrix} r_2 & 1+q_1\cdot q_2 & -q_2\\ r_3 & -q_1-q_3-q_1\cdot q_2\cdot q_3 & 1+q_2\cdot q_3\end{pmatrix},\ r_2=r_3\cdot q_4+r_4 \tag{35}$$

5ª Etapa: Execute $l_1=l_1-q_4\cdot l_2$.

$$(E5)=\begin{pmatrix} r_4 & 1+q_1\cdot(q_2+q_4+q_2\cdot q_3\cdot q_4)+q_3\cdot q_4 & -q_2-q_4\cdot(1+q_2\cdot q_3)\\ r_3 & q_1\cdot(-1-q_2\cdot q_3)-q_3 & 1+q_2\cdot q_3\end{pmatrix} \tag{36}$$

$$(E5)=\begin{pmatrix} r_4 & c & f\\ r_3 & g & v\end{pmatrix},\ r_3=r_4\cdot q_5+r_5 \tag{37}$$

O algoritmo continua alternando as combinação lineares entre l_1 e l_2 até chegar em uma matriz EW que satisfaz duas situações:

$$(EW)=\begin{cases}\begin{pmatrix} 0 & t & j\\ r_n & y_0 & x_0\end{pmatrix},\ W=2p+1,\ p\in\mathbb{Z},\ (j,t)\in\mathbb{Z};\\ \begin{pmatrix} r_n & y_0 & x_0\\ 0 & l & h\end{pmatrix},\ W=2z, z\in\mathbb{Z},\ (h,l)\in\mathbb{Z}.\end{cases}$$

Questão 10: Através do Algoritmo de Euclides Estendido, determine o $mdc(311,235)$ e o $mdc(24,20)$, encontrando para cada mdc uma Identidade de Bézout.

Resolução: Tomando $a=311$, $b=235$, $a_1=24$, $b_1=20$ e tendo em vista que $a\geq b$ e $a_1\geq b_1$, então:

1)

$$(E1)=\begin{pmatrix} 235 & 1 & 0\\ 311 & 0 & 1\end{pmatrix}\xrightarrow[311=235\cdot 1+76]{l_2=l_2-1\cdot l_1}(E2)=\begin{pmatrix} 235 & 1 & 0\\ 76 & -1 & 1\end{pmatrix}\xrightarrow[235=76\cdot 3+7]{l_1=l_1-3\cdot l_2}(E3)=\begin{pmatrix} 7 & 4 & -3\\ 76 & -1 & 1\end{pmatrix}$$

$$(E3)=\begin{pmatrix} 7 & 4 & -3\\ 76 & -1 & 1\end{pmatrix}\xrightarrow[76=7\cdot 10+6]{l_2=l_2-10\cdot l_1}(E4)=\begin{pmatrix} 7 & 4 & -3\\ 6 & -41 & 31\end{pmatrix}\xrightarrow[7=6\cdot 1+1]{l_1=l_1-1\cdot l_2}(E5)=\begin{pmatrix} 1 & 45 & -34\\ 6 & -41 & 31\end{pmatrix}$$

$$(E5)=\begin{pmatrix} 1 & 45 & -34\\ 6 & -41 & 31\end{pmatrix}\xrightarrow[6=1\cdot 6]{l_2=l_2-6\cdot l_1}(E6)=\begin{pmatrix} 1 & 45 & -34\\ 0 & -311 & 235\end{pmatrix}$$

2)

$$(E1)=\begin{pmatrix} 20 & 1 & 0\\ 24 & 0 & 1\end{pmatrix}\xrightarrow[24=20\cdot 1+4]{l_2=l_2-1\cdot l_1}(E2)=\begin{pmatrix} 20 & 1 & 0\\ 4 & -1 & 1\end{pmatrix}\xrightarrow[20=4\cdot 5]{l_1=l_1-5\cdot l_2}(E3)=\begin{pmatrix} 0 & 6 & -5\\ 4 & -1 & 1\end{pmatrix}$$

Portanto, $mdc(311,235) = 311 \cdot (-34) + 235 \cdot (45) = 1$ e $mdc(24,20) = 24 \cdot (1) + 20 \cdot (-1) = 4$.

Questão 11: Dado que $Q_n = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$ e $r_0 = b$, prove que $\begin{pmatrix} a \\ b \end{pmatrix} = \prod_{i=1}^{n} Q_i \cdot \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$ com $n \in \mathbb{N}$.

Demonstração. De fato, pelo Algoritmo de Euclides temos que

$$\begin{aligned}
\begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} b \cdot q_1 + r_1 \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} b \\ r_1 \end{pmatrix} \\
\begin{pmatrix} b \\ r_1 \end{pmatrix} &= \begin{pmatrix} r_1 \cdot q_2 + r_2 \\ r_1 \end{pmatrix} = \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \\
\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} &= \begin{pmatrix} r_2 \cdot q_3 + r_3 \\ r_2 \end{pmatrix} = \begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} \\
\begin{pmatrix} r_2 \\ r_3 \end{pmatrix} &= \begin{pmatrix} r_3 \cdot q_4 + r_4 \\ r_3 \end{pmatrix} = \begin{pmatrix} q_4 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_3 \\ r_4 \end{pmatrix} \\
\vdots \qquad & \qquad \vdots \qquad\qquad \vdots \\
\begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} &= \begin{pmatrix} r_{n-1} \cdot q_n + r_n \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}
\end{aligned}$$

Definindo $T_n = \begin{pmatrix} a \\ b \end{pmatrix} = Q_1 \cdot Q_2 \cdot \ldots \cdot Q_n \cdot \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$ e $Q_n = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$, T_n é válida para todo n natural. Justificativa:

1) Passo base: $\forall n \in \mathbb{N}$ T_1 é verdadeira:

$$T_1 = \begin{pmatrix} a \\ b \end{pmatrix} = Q_1 \cdot \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} b \cdot q_1 + r_1 \\ b \end{pmatrix}$$

2) Passo indutivo: Partindo da suposição que T_n é verdadeira para todo $n = k$, $k \in \mathbb{N}$, T_{k+1} também é verdadeira:

$$T_k = \begin{pmatrix} a \\ b \end{pmatrix} = \prod_{i=1}^{k} Q_i \cdot \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} \quad [\textit{Hipótese de indução}]$$

Note que

$$\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} = \begin{pmatrix} q_{k+1} \cdot r_k + r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} q_{k+1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = Q_{k+1} \cdot \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}$$

Logo,

$$T_{k+1} = \left(\prod_{i=1}^{k} Q_i\right) \cdot Q_{k+1} \cdot \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \underbrace{Q_1 \cdot Q_2 \cdot \ldots \cdot Q_k \cdot \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}}_{Hipótese} = \begin{pmatrix} a \\ b \end{pmatrix}$$

Portanto, pelo Princípio de Indução Finita (PIF), a igualdade $\begin{pmatrix} a \\ b \end{pmatrix} = \prod_{i=1}^{n} Q_i \cdot \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$ sempre é verdadeira para qualquer n natural.

$\blacksquare$

3.4 Transformações Geométricas 2D

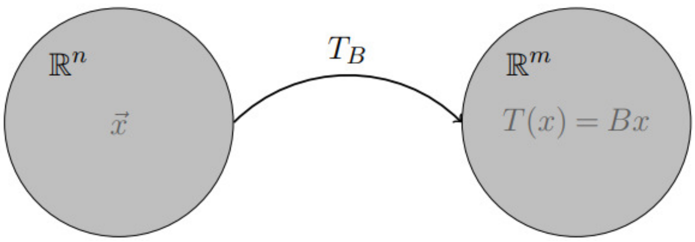
No cotidiano, principalmente em ambientes digitais, é comum a visualização de imagens bidimensionais que são submetidas a diversas mudanças em suas composições originais, podendo ser aumentadas, diminuídas, refletidas, distorcidas, entre outras alterações. Tais transformações, matematicamente, são explicadas com a utilização de operações matriciais e de transformações lineares.

Definição 13. Se $B_{m\times n}$ é uma matriz, então a transformação linear matricial $T : \mathbb{R}^n \to \mathbb{R}^m$ será válida se, e somente se, forem verificadas duas condições (Boldrini, 1980):

1. $T(\overrightarrow{x} + \overrightarrow{y}) = T(\overrightarrow{x}) + T(\overrightarrow{y}), \forall(\overrightarrow{x}, \overrightarrow{y}) \in \mathbb{R}^n$ [Aditividade]
2. $T(a\overrightarrow{x}) = aT(\overrightarrow{x})$, com $a \in \mathbb{R}$ e $\overrightarrow{x} \in \mathbb{R}^n$ [Homogeneidade]

Em suma, a transformação linear $T : \mathbb{R}^n \to \mathbb{R}^m$ trata-se de uma associação de cada vetor x de $\mathbb{R}^n$ [domínio de T] a um vetor de $\mathbb{R}^m$ [contradomínio de $T(x)$] com o uso de uma matriz B com m linhas e n colunas. Os vetores de ambos os espaços vetoriais apresentam três características em comum: Comprimento (ou norma), direção e sentido.

Figura 3.7 – Transformação linear entre $\mathbb{R}^n$ e $\mathbb{R}^m$.



Fonte: Autor

Questão 12: Seja $T:\mathbb{R}^2 \to \mathbb{R}^2$ definida por $T\left(\begin{bmatrix}1\\6\end{bmatrix}\right)=\begin{bmatrix}7\\4\end{bmatrix}$ e $T\left(\begin{bmatrix}2\\3\end{bmatrix}\right)=\begin{bmatrix}5\\9\end{bmatrix}$. Determine a matriz da transformação linear T.

Resolução: Os vetores $\overrightarrow{v_1}=(1,6)$ e $\overrightarrow{v_2}=(2,3)$ formam uma base[2] em $\mathbb{R}^2$, permitindo encontrar a partir de um vetor $\overrightarrow{v_3}=(x,y)$ uma combinação linear:

$$\begin{aligned}(x,y) &= h\cdot(1,6)+k\cdot(2,3),\forall(k,h)\in\mathbb{R}\\(x,y) &= (h,6h)+(2k,3k)\\(x,y) &= (h+2k,6h+3k)\end{aligned}$$

Com isso,

$$\begin{cases}x=1h+2k\\y=6h+3k\end{cases}\Rightarrow (h,k)=\left(\frac{-3x+2y}{9},\frac{6x-y}{9}\right)$$

Assim,

$$\begin{aligned}T(x,y) &= T\left[\left(\frac{-3x+2y}{9}\right)\cdot(1,6)+\left(\frac{6x-y}{9}\right)\cdot(2,3)\right]\\T(x,y) &= \left(\frac{-3x+2y}{9}\right)\cdot T(1,6)+\left(\frac{6x-y}{9}\right)\cdot T(2,3)\\T(x,y) &= \left(\frac{-3x+2y}{9}\right)\cdot(7,4)+\left(\frac{6x-y}{9}\right)\cdot(5,9)\\T(x,y) &= \left(\frac{9x+9y}{9},\frac{-12x+54x+8y-9y}{9}\right)\\T(x,y) &= \left(x+y,\frac{42x-y}{9}\right)\\T(x,y) &= \begin{bmatrix}1 & 1\\\frac{42}{9} & -\frac{1}{9}\end{bmatrix}\cdot\begin{bmatrix}x\\y\end{bmatrix}\end{aligned}$$

Resposta: A matriz da transformação linear é $\begin{bmatrix}1 & 1\\\frac{42}{9} & -\frac{1}{9}\end{bmatrix}$.

Considerando os objetos do mundo físico e digital como espaços vetoriais, ou seja, um conjunto de vetores, são válidos os axiomas abaixo, em que $\overrightarrow{a}=(a_1,a_2,a_3,\dots,a_n)$ e $\overrightarrow{b}=(b_1,b_2,b_3,\dots,b_n)$ são vetores de $\mathbb{R}^n$ e g,j escalares (Cunha; Castro, 2010).

1. $\overrightarrow{a}+\overrightarrow{b}=\overrightarrow{b}+\overrightarrow{a}$ (Comutatividade da adição)

2. $\overrightarrow{c}+(\overrightarrow{a}+\overrightarrow{b})=(\overrightarrow{c}+\overrightarrow{a})+\overrightarrow{b}$, com $\overrightarrow{c}=(c_1,c_2,c_3,\dots,c_n)\in\mathbb{R}^n$ (Associatividade da adição)

[2] Na Àlgebra Linear, uma base é um conjunto de vetores (X) que fazem parte de um espaço vetorial (Y) que são linearmente independentes (LI) tal que X forme Y (Howard; Rorres, 2012).

3. $\exists\ \overrightarrow{0} \in \mathbb{R}^n$ tal que $\overrightarrow{0} + \overrightarrow{a} = \overrightarrow{a}$ (Existência do vetor nulo $\overrightarrow{0}$)

4. $\forall\ \overrightarrow{a} \in \mathbb{R}^n, \exists - \overrightarrow{a} \in \mathbb{R}^n$ tal que $\overrightarrow{a} + (-\overrightarrow{a}) = \overrightarrow{0}$ (Existência do vetor oposto $-\overrightarrow{a}$)

5. $1 \cdot \overrightarrow{a} = \overrightarrow{a}$ (Elemento neutro da multiplicação)

6. $g \cdot (j \cdot \overrightarrow{a}) = (g \cdot j) \cdot \overrightarrow{a}$

7. $(g + j) \cdot \overrightarrow{a} = g \cdot \overrightarrow{a} + j \cdot \overrightarrow{a}$

8. $g \cdot (\overrightarrow{a} + \overrightarrow{b}) = g \cdot \overrightarrow{a} + g \cdot \overrightarrow{b}$

Algumas das principais transformações geométricas lineares são a rotação, reflexão e a expansão/contração uniforme. As explicações a seguir são originadas de Boldrini (1980), mas com algumas releituras para possibilitar um entendimento mais objetivo e simples das referidas mudanças geométricas no $\mathbb{R}^2$.

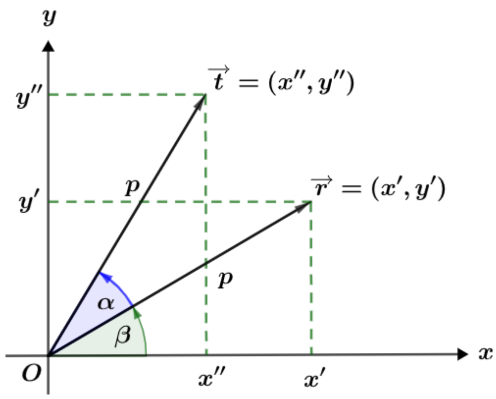
Rotação:

Definição 14. É uma transformação linear na qual os vetores são rotacionados por um determinado ângulo α ao redor da origem do plano cartesiano. Para esta transformação, a matriz que permite a rotação dos vetores, no sentido anti-horário, é dada por M_α (ver equação 38).

$$M_\alpha = \begin{pmatrix} \cos(\alpha) & -\operatorname{sen}(\alpha) \\ \operatorname{sen}(\alpha) & \cos(\alpha) \end{pmatrix} \tag{38}$$

Demonstração. Considere $\overrightarrow{r}$ um vetor de comprimento p e extremidade em (x', y'). Admita que $\overrightarrow{r}$ foi rotacionado no sentido anti-horário, alcançando a extremidade (x'', y'') do vetor $\overrightarrow{t}$ com o mesmo comprimento de $\overrightarrow{r}$ (ver Figura 3.8).

Figura 3.8 – Rotação do vetor $\overrightarrow{r}$



Fonte: Autor

Em coordenadas polares :

$$x' = p \cdot \cos(\beta) \tag{39}$$

$$y' = p \cdot \operatorname{sen}(\beta) \tag{40}$$

Além disso,

$$x'' = p \cdot \cos(\beta+\alpha) = p \cdot [\cos(\beta) \cdot \cos(\alpha) - \operatorname{sen}(\beta) \cdot \operatorname{sen}(\alpha)] \tag{41}$$

$$y'' = p \cdot \operatorname{sen}(\beta+\alpha) = p \cdot [\operatorname{sen}(\beta) \cdot \cos(\alpha) + \cos(\beta) \cdot \operatorname{sen}(\alpha)] \tag{42}$$

Substituindo as equações (39) e (40) nas equações (41) e (42), respectivamente, conclui-se que

$$x'' = x' \cdot \cos(\alpha) - y' \cdot \operatorname{sen}(\alpha) \tag{43}$$

$$y'' = y' \cdot \cos(\alpha) + x' \cdot \operatorname{sen}(\alpha) \tag{44}$$

Na forma matricial:

$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} \cos(\alpha) & -\operatorname{sen}(\alpha) \\ \operatorname{sen}(\alpha) & \cos(\alpha) \end{bmatrix} \cdot \begin{bmatrix} x' \\ y' \end{bmatrix} \tag{45}$$

■

Questão 13: Um retângulo tem vértices localizados nos pontos $A = (0,0)$, $B = (5,0)$, $C = (5,3)$ e $D = (0,3)$, sendo as extremidades dos vetores $\overrightarrow{u} = (x_1, y_1)$, $\overrightarrow{v} = (x_2, y_2)$, $\overrightarrow{w} = (x_3, y_3)$ e $\overrightarrow{c} = (x_4, y_4)$, respectivamente. Forneça a localização dos referidos pontos após uma rotação de 120° no sentido anti-horário.

Resolução: Denominando de $\overrightarrow{u'} = (x'_1, y'_1)$, $\overrightarrow{v'} = (x'_2, y'_2)$, $\overrightarrow{w'} = (x'_3, y'_3)$ e $\overrightarrow{c'} = (x'_4, y'_4)$ os vetores rotacionados em torno da origem, as suas extremidades serão dadas por:

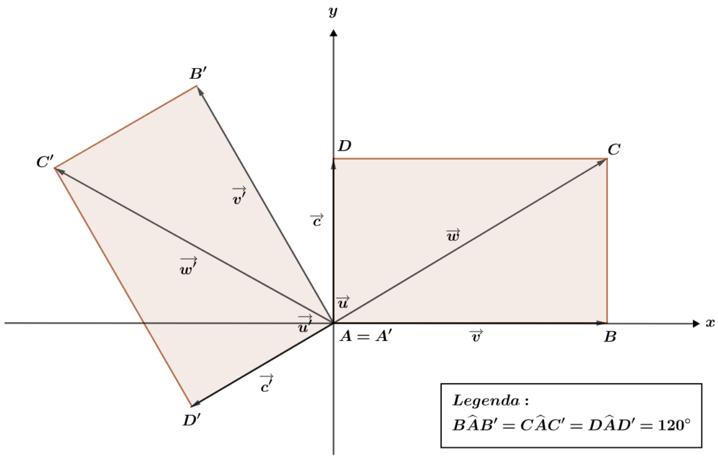
$$\begin{bmatrix} x'_1 & x'_2 & x'_3 & x'_4 \\ y'_1 & y'_2 & y'_3 & y'_4 \end{bmatrix} = \begin{bmatrix} \cos(120^\circ) & -\operatorname{sen}(120^\circ) \\ \operatorname{sen}(120^\circ) & \cos(120^\circ) \end{bmatrix} \cdot \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{bmatrix}$$

$$\begin{bmatrix} x'_1 & x'_2 & x'_3 & x'_4 \\ y'_1 & y'_2 & y'_3 & y'_4 \end{bmatrix} = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 0 & 5 & 5 & 0 \\ 0 & 0 & 3 & 3 \end{bmatrix}$$

$$\begin{bmatrix} x'_1 & x'_2 & x'_3 & x'_4 \\ y'_1 & y'_2 & y'_3 & y'_4 \end{bmatrix} = \begin{bmatrix} 0 & -\frac{5}{2} & \frac{-5-3\sqrt{3}}{2} & -\frac{3\sqrt{3}}{2} \\ 0 & \frac{5\sqrt{3}}{2} & \frac{5\sqrt{3}-3}{2} & -\frac{3}{2} \end{bmatrix}$$

Resposta: Os novos vértices do retângulo, conforme a Figura 3.9 e os cálculos anteriores, após a rotação de 120° são $A' = (0,0)$, $B' = \left(-\frac{5}{2}, \frac{5\sqrt{3}}{2}\right)$, $C' = \left(\frac{-5-3\sqrt{3}}{2}, \frac{5\sqrt{3}-3}{2}\right)$ e $D' = \left(-\frac{3\sqrt{3}}{2}, -\frac{3}{2}\right)$

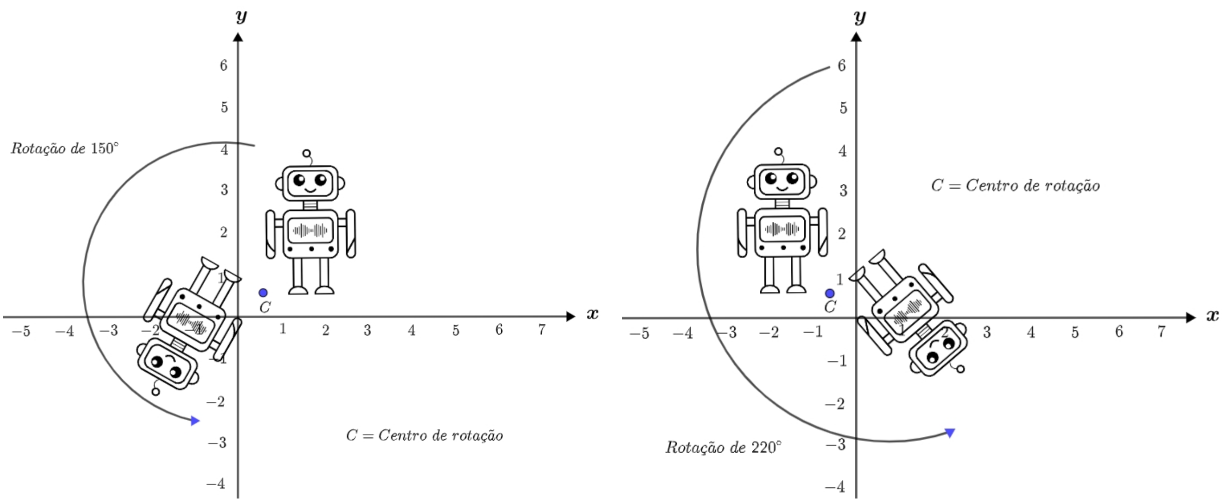
Figura 3.9 – Rotação do retângulo $ABCD$ em 120° no sentido anti-horário



Fonte: Autor

A Figura 3.10 mostra que a mesma matriz de rotação também se aplica para imagens/ilustrações no $\mathbb{R}^2$ com n-vetores, independentemente do formato ou posição de origem.

Figura 3.10 – Rotações no $\mathbb{R}^2$



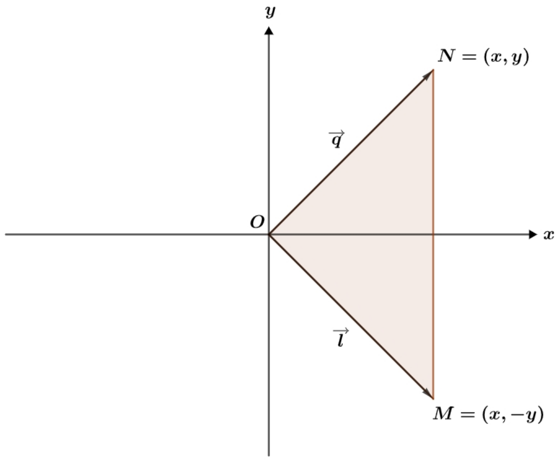
Fonte: Autor

Reflexão:

Definição 15. Consiste em uma transformação linear que muda a localização de um ou mais pontos que estão em um determinado quadrante ou eixo do plano cartesiano, movendo-os para os seus respectivos pontos simétricos no quadrante ou eixo oposto.

Seja N (extremidade do vetor $\overrightarrow{q}$) um ponto de coordenadas (x,y), refletido em relação ao eixo das abcissas até atingir as coordenadas de $M = (x,-y)$, extremidade do vetor $\overrightarrow{l}$ com a mesma norma de $\overrightarrow{q}$, porém com direção e sentido diferentes (ver Figura 3.11). A transformação linear mencionada de $\mathbb{R}^2$ em $\mathbb{R}^2$ é definida por $T(x,y) = (x,-y)$ ou $T\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$.

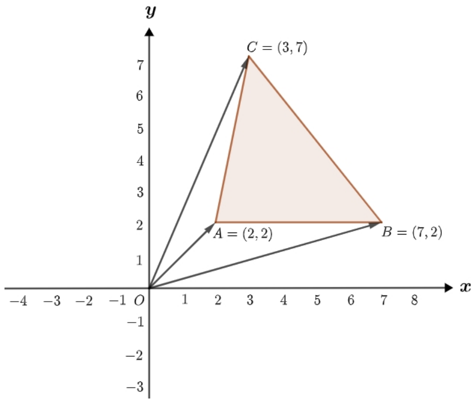
Figura 3.11 – Transformação linear $T(x,y) = (x,-y)$ aplicada no ponto N



Fonte: Autor

Questão 14: O triângulo escaleno da Figura 3.12 é formado pelas extremidades dos vetores $\overrightarrow{OA} = (2,2)$, $\overrightarrow{OB} = (7,2)$ e $\overrightarrow{OC} = (3,7)$. Encontre, através da matriz de reflexão em torno do eixo x, as coordenadas de A', B' e C', pontos simétricos dos vértices originais do triângulo ABC.

Figura 3.12 – Triângulo escaleno ABC



Fonte: Autor

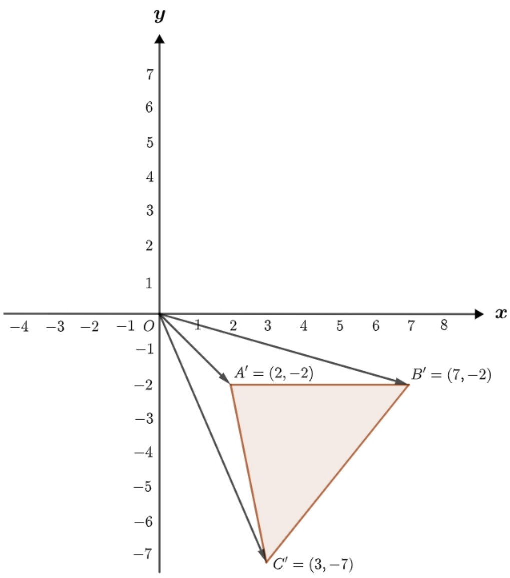
Resolução: Nomeando de $A' = (x_1, y_1)$, $B' = (x_2, y_2)$ e $C' = (x_3, y_3)$ as coordenadas solicitadas, então:

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 7 & 3 \\ 2 & 2 & 7 \end{bmatrix}$$

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix} = \begin{bmatrix} 2 & 7 & 3 \\ -2 & -2 & -7 \end{bmatrix}$$

Resposta: $A' = (2, -2)$, $B' = (7, -2)$ e $C' = (3, -7)$.

Figura 3.13 – Triângulo escaleno $A'B'C'$



Fonte: Autor

Para reflexões em relação ao eixo y, $y = x$ e $y = -x$, tornam-se necessárias, de modo respectivo, as matrizes $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ e $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$.

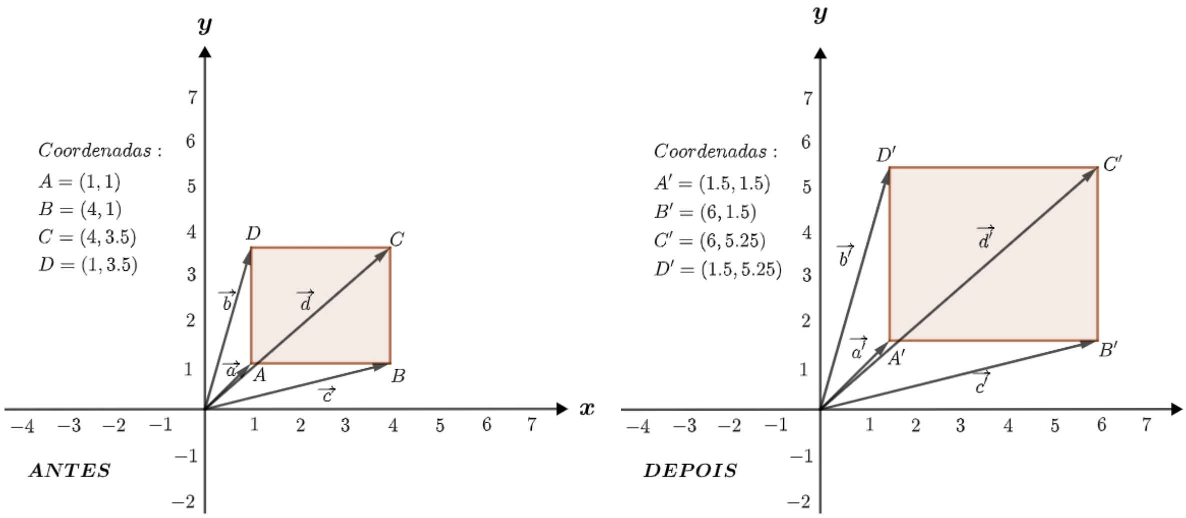
Expansão/contração uniforme:

Definição 16. É uma transformação linear que multiplica ou divide as coordenadas de um ou mais pontos do plano cartesiano por um valor real k positivo. Ao considerar os espaços vetoriais submetidos pela expansão/contração, Boldrini (1980, p. 147) menciona que ela "[...] leva cada vetor do plano num vetor de mesma direção e sentido [...]". A expansão se dá quando $k > 1$ e a contração para $0 < k < 1$. Notação:

$$T = \begin{cases} (x,y) \in \mathbb{R}^2 \\ \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \end{cases}$$

A Figura 3.14 é um exemplo da expansão do retângulo $ABCD$ com coordenadas originais $A = (1,1)$, $B = (4,1)$, $C = (4,3.5)$ e $D = (1,3.5)$ para $k = 1,5$.

Figura 3.14 – Expansão do retângulo $ABCD$**.**



Fonte: Autor

Questão 15: Determine a matriz da transformação linear de expansão uniforme $T(x,y) = h \cdot (x,y)$, $h \in \mathbb{R}$, tendo em vista que $T(1,2) = (3,6)$ e $T(3,4) = (9,12)$.

Resolução: Denominando $\overrightarrow{e} = (1,2)$ e $\overrightarrow{s} = (3,4) \in \mathbb{R}^2$, então é possível encontrar uma combinação linear para um terceiro vetor $\overrightarrow{j} = (x,y)$ de modo que:

$$\begin{aligned} (x,y) &= a \cdot (1,2) + b \cdot (3,4), \forall a,b \in \mathbb{R} \\ (x,y) &= (a,2a) + (3b,4b) \\ (x,y) &= (a+3b, 2a+4b) \end{aligned}$$

Reescrevendo a e b em função de x e y obtem-se que

$$\begin{cases} 1a + 3b = x \\ 2a + 4b = y \end{cases} \Rightarrow (a,b) = \left(\frac{-4x+3y}{2}, \frac{2x-y}{2} \right)$$

Com efeito,

$$(x,y) = \left(\frac{-4x+3y}{2} \right) \cdot (1,2) + \left(\frac{2x-y}{2} \right) \cdot (3,4)$$

Assim

$$\begin{array}{rcl} T(x,y) & = & T\left[\left(\frac{-4x+3y}{2}\right)\cdot(1,2)+\left(\frac{2x-y}{2}\right)\cdot(3,4)\right] \\ T(x,y) & = & \left(\frac{-4x+3y}{2}\right)\cdot T(1,2)+\left(\frac{2x-y}{2}\right)\cdot T(3,4) \\ T(x,y) & = & \left(\frac{-4x+3y}{2}\right)\cdot(3,6)+\left(\frac{2x-y}{2}\right)\cdot(9,12) \\ T(x,y) & = & (3x,3y) \\ T(x,y) & = & \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}\cdot\begin{bmatrix} x \\ y \end{bmatrix} \end{array}$$

Resposta: $\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$.

Translação (Adicional):

Definição 17. A translação é uma tranformação geométrica bidimensional, não linear, que faz o uso da adição de matrizes. Ela possibilita a movimentação de vetores no $\mathbb{R}^2$ para uma determinada direção e sentido, conservando a norma.

Notação:

$$T\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} x \\ y \end{bmatrix}+\begin{bmatrix} m \\ n \end{bmatrix}, \overrightarrow{v}=\begin{bmatrix} m \\ n \end{bmatrix}\in\mathbb{R}^2 \tag{46}$$

A ausência da linearidade é por causa das propriedades de aditividade e homogeneidade (ver Definição 13). Dados dois vetores $\overrightarrow{b}=\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$ e $\overrightarrow{c}=\begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$ observa-se que $T(\overrightarrow{b}+\overrightarrow{c})\neq T(\overrightarrow{b})+T(\overrightarrow{c})$ e $T(\alpha\cdot\overrightarrow{v})\neq\alpha\cdot T(\overrightarrow{v})$, com $\alpha\in\mathbb{R}$:

1)

$$T\left(\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}+\begin{bmatrix} x_2 \\ y_2 \end{bmatrix}\right)=T\left(\begin{bmatrix} x_1+x_2 \\ y_1+y_2 \end{bmatrix}\right)=\left(\begin{bmatrix} x_1+x_2+m \\ y_1+y_2+n \end{bmatrix}\right) \tag{47}$$

Todavia,

$$T\left(\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}\right)+T\left(\begin{bmatrix} x_2 \\ y_2 \end{bmatrix}\right)=\begin{bmatrix} x_1+m \\ y_1+n \end{bmatrix}+\begin{bmatrix} x_2+m \\ y_2+n \end{bmatrix}=\begin{bmatrix} x_1+x_2+2m \\ y_1+y_2+2n \end{bmatrix} \tag{48}$$

2)

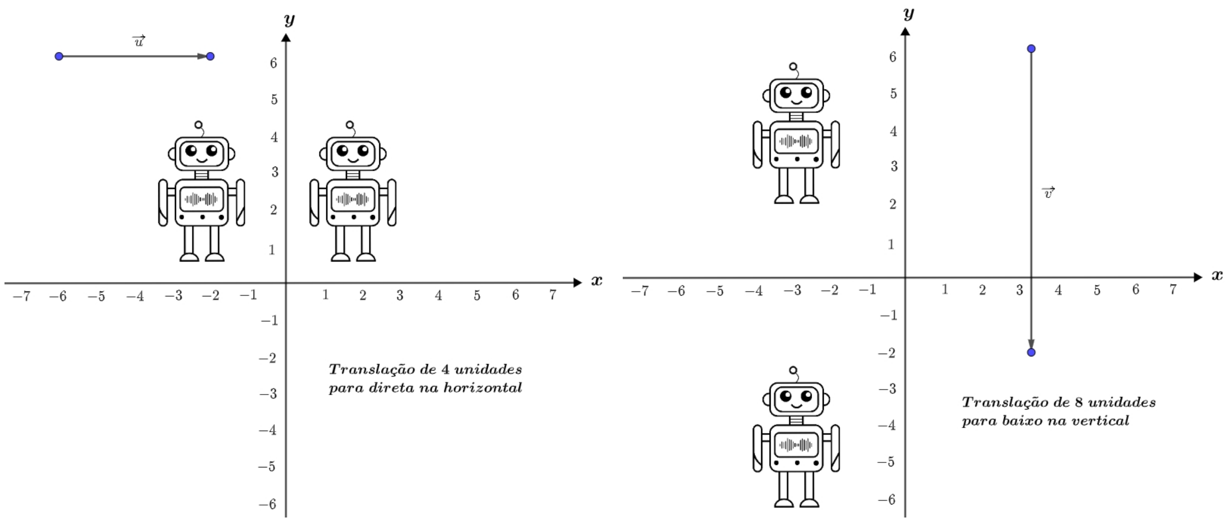
$$T\left(\alpha\cdot\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right)=T\left(\begin{bmatrix} \alpha\cdot x_1 \\ \alpha\cdot x_2 \end{bmatrix}\right)=\begin{bmatrix} \alpha\cdot x_1+m \\ \alpha\cdot x_2+n \end{bmatrix} \tag{49}$$

Contudo,

$$\alpha \cdot T\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \alpha \cdot \left(\begin{bmatrix} x_1 + m \\ x_2 + n \end{bmatrix}\right) = \begin{bmatrix} \alpha \cdot x_1 + \alpha \cdot m \\ \alpha \cdot x_2 + \alpha \cdot n \end{bmatrix} \quad (50)$$

Na Figura 3.15 estão dois exemplos de translações com normas, sentidos e direções especificadas.

Figura 3.15 – Tranlações no $\mathbb{R}^2$



Fonte: Autor

Sugestão de pesquisa ao leitor: Boldrini (1980) ainda apresenta duas transformações geométricas: O cisalhamento horizontal e a reflexão na origem.

4 CONSIDERAÇÕES FINAIS

Neste trabalho foram apresentadas quatro aplicações de matrizes, mostrando como elas estão integradas em problemas matemáticos de características teóricas e contextualizadas, enfatizando também as definições, propriedades e observações que fundamentam tais aplicações. No início da pesquisa, as primeiras impressões eram de que as matrizes representavam apenas mecanismos aritméticos para realizar operações elementares, vistas no cotidiano em tabelas para organizar informações simples e agregadas. No entanto, com os resultados encontrados na literatura, novas perspectivas de aprendizagem foram formadas, conectando as matrizes a outras áreas do conhecimento, como a Teoria dos Números, a Computação Gráfica e a Criptografia, conforme o objetivo geral proposto.

Vale destacar que não foram demonstradas todas as propriedades e definições, uma vez que a delimitação do objetivo geral e dos objetivos específicos foi feita com base na decisão de mostrar como as matrizes estão inseridas nos resultados selecionados. Sobre os objetivos específicos, foi possível entender o funcionamento de sistemas criptográficos dentro da Matemática e como as Cifras de Hill podem ser utilizadas em atividades que necessitam da codificação e decodificação de mensagens, estando também as matrizes presentes no dia a dia em *QR Codes* e códigos de barras, exemplos de imagens binárias. Em relação ao Algoritmo de Euclides Estendido é importante enfatizar que a sua aplicabilidade é mais voltada para o Ensino Superior, enquanto que as transformações geométricas bidimensionais podem ser contempladas na Educação Básica e no Ensino Superior, havendo apenas a necessidade de adaptar o ensino a partir do nível de aprendizagem de cada turma.

Por mais que seja uma pesquisa de natureza básica, espera-se dos leitores desta monografia uma ressignificação do conceito de matriz, desassociando-a da ideia de ser meramente um conteúdo visto no Ensino Médio, com operações aritméticas que permitem a resolução de exercícios que não refletem a realidade da Matemática no dia a dia. Em particular, no âmbito da Educação Básica, o ensino de matrizes geralmente perpassa pela análise de situações-problema no início ou no final dos capítulos dos livros didáticos, trazendo questionamentos que necessitam de uma interpretação ou diálogo coletivo entre professor-alunos e alunos-alunos. Em uma breve pesquisa nos materiais do Plano Nacional do Livro Didático do Ensino Médio (PNLD) observou-se que as aplicações de matrizes são abordadas por meio de uma abordagem informativa, com a apresentação de exercícios propostos que envolvem telas *touchscreen*, resoluções de imagens, transformações geométricas e planilhas eletrônicas.

Por fim, como sugestões de novas pesquisas acadêmicas, indica-se o uso de matrizes na análise de circuitos elétricos, nos modelos econômicos de Leontief que ganhou o Prêmio Nobel de Economia em 1973, na organização de grandes volumes de informações com o suporte de Inteligências Artificiais e na Teoria dos Grafos.

REFERÊNCIAS

ANDRADE, Fabíolla dos Santos. **Imagens digitais e matrizes: Uma aplicação no ensino médio**. 92 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) — Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista (BA), 2020.

AQUINO, Marco Aurélio Silva de. **Métodos de resolução de sistemas lineares**. 98 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) — Universidade Federal do Maranhão, São Luis, 2021.

BERNARDES, Aline; ROQUE, Tatiana. História da noção de matriz: Uma releitura sob a luz de novas abordagens historiográficas. **Revista Brasileira de História da Matemática**, v. 16, n. 31, p. 1–19, 2016.

BOLDRINI, José Luiz. **Álgebra Linear**. 3. ed. São Paulo: Harbra, 1980.

BOYER, Carl; MERZBACH, Uta C. **História da matemática**. 3. ed. São Paulo: Blucher, 2012.

CUNHA, Francisco Gêvane Muniz; CASTRO, Jânio Kléo Sousa. **Álgebra Linear**. Fortaleza-CE: UAB/IFCE, 2010.

DAGHLIAN, Jacob. **Lógica e álgebra de Boole**. 4. ed. São Paulo: Atlas, 2008.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra Moderna**. 4. ed. São Paulo: Atual, 2003.

EVES, Howard. **Introdução à historia da matematica**. 5. ed. Campinas: Editora da Unicamp, 2011.

FRISON, Lourdes Maria Bragagnolo. Monitoria: uma modalidade de ensino que potencializa a aprendizagem colaborativa e autorregulada. **Pro-Posições**, UNICAMP - Faculdade de Educação, v. 27, n. 1, p. 133–153, Jan 2016. ISSN 0103-7307. Disponível em: <https://doi.org/10.1590/0103-7307201607908>.

GILL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GONZALEZ, Rafael C.; WOODS, Richard C. **Processamento digital de imagens**. 3. ed. São Paulo: Pearson Prentice Hall, 2010.

HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2016. Coleção PROFMAT.

HOWARD, Anton; RORRES, Chris. **Álgebra linear com aplicações**. 10. ed. Porto Alegre: Bookman, 2012.

IEZZI, Gelson; HAZZAN, Samuel. **Fundamentos de matemática elementar: sequências, matrizes, determinantes e sistemas**. 8. ed. São Paulo: Atual, 2013.

JACOBIK, Guilherme Santinho. Problemas matemáticos e modelos mentais de resolução: Possibilidade de reflexão e aprendizagem. **Ciências & Cognição**, v. 15, p. 173–183, 2010.

LIPSCHUTZ, Seymour; LIPSON, Marc. **Álgebra linear**. 4. ed. Porto Alegre: Bookman, 2011. Coleção Schaum.

MACHADO, José Samuel. **Quadrados mágicos com aplicações**. 35 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) — Universidade Federal do Ceará, Fortaleza, 2013.

O'CONNOR, John Joseph; ROBERTSON, Edmund Frederick. **Matrices and determinants**. 1996. Disponível em: <https://mathshistory.st-andrews.ac.uk/HistTopics/Matrices_and_determinants/>. Acessado em: 06 fev. 2025.

POLYA, George. **A arte de resolver problemas: Um novo aspecto do método matemático**. Rio de Janeiro: Interciência, 1995.

PRODANOV, Cleber Cristiano. **Metodologia do trabalho científico: Métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

SANTOS, Vinícius de Macêdo. A matemática escolar, o aluno e o professor: Paradoxos aparentes e polarizações em discussão. **Cadernos CEDES**, v. 28, n. 74, p. 25–38, 2008.

SILVA, Carlos Danísio Macedo. **A essência dos determinantes na sua origem**. 42 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) — Universidade Federal do Ceará, Juazeiro do Norte, 2014.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Cajazeiras - Código INEP: 25008978
Rua José Antônio da Silva, 300, Jardim Oásis, CEP 58.900-000, Cajazeiras (PB)
CNPJ: 10.783.898/0005-07 - Telefone: (83) 3532-4100

Documento Digitalizado Restrito

Entrega de Trabalho de Conclusão de Curso

Assunto:	Entrega de Trabalho de Conclusão de Curso
Assinado por:	Ivanildo Leite
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Informação Pessoal (Art. 31 da Lei no 12.527/2011)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Ivanildo Leite Batista**, **DISCENTE (202112020024) DE LICENCIATURA EM MATEMÁTICA - CAJAZEIRAS**, em 17/03/2025 20:06:02.

Este documento foi armazenado no SUAP em 17/03/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1422372
Código de Autenticação: 09f5456875