UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIAS EXATAS
CURSO DE LICENCIATURA EM MATEMÁTICA

Almir Estevam dos Santos Junior

Um estudo sobre aplicações matriciais

Rio Tinto – PB
2021

Almir Estevam dos Santos Junior

Um estudo sobre aplicações matriciais

Trabalho Monográfico apresentado à Coordenação do Curso de Licenciatura em Matemática como requisito parcial para obtenção do título de Licenciado em Matemática.

Orientador: Prof. Me. Marcos André J. Valcacio

Rio Tinto – PB

2021

Catalogação na publicação
Seção de Catalogação e Classificação

J95e Santos Junior, Almir Estevam dos.
Um estudo sobre aplicações matriciais / Almir Estevam dos Santos Junior. - Rio Tinto, 2021.
61 f. : il.

Orientação: Marcos André José Valcacio.
Monografia (Graduação) - UFPB/CCAE.

1. Matrizes. 2. Aplicações matriciais. 3. Algoritmo de Euclides. 4. Criptografia. 5. Cadeia de Markov. I. Valcacio, Marcos André José. II. Título.

UFPB/CCAE CDU 51

Elaborado por Michelle de Kássia Fonseca Barbosa - CRB-738

Almir Estevam dos Santos Junior

Um estudo sobre aplicações matriciais

Trabalho Monográfico apresentado à Coordenação do Curso de Licenciatura em Matemática como requisito parcial para obtenção do título de Licenciado em Matemática.

Orientador: Prof. Me. Marcos André José Valcacio

Aprovado em: 8 de julho de 2021

BANCA EXAMINADORA:

Prof. Me. Marcos André José Valcácio (Orientador)
UFPB / DCX

Prof. Dr. Carlos Alberto Gomes de Almeida
UFPB / DCX

Prof. Dr. Ary Vasconcelos Medino
UnB / MAT

AGRADECIMENTOS

Agradeço primeiramente a Deus por me conceder sabedoria e forças para redigir este trabalho. A minha família por me apoiar, não só durante minha trajetória acadêmica, mas ao longo de minha vida. A minha namorada, pois esteve sempre ao meu lado nos momentos difíceis e de angústia, me incentivando e me ajudando a supera-los.

A todos os meus professores do cursos de Licenciatura em matemática da Universidade Federal da Paraíba / Campus IV pelos valiosos ensinamentos durante minha formação, em especial ao meu orientador Marcos André José Valcacio por aceitar e me auxiliar na condução deste trabalho, pelo incentivo e colaboração ao longo dessa jornada.

Finalizando, agradeço também a todos meus amigos e colegas de curso por compartilhar bons momentos de aprendizagem e experiências comigo.

"Não há um ramo da matemática, por mais
abstrata que seja, que não possa ser aplicada
algum dia aos fenômenos do mundo real."
(Nikolai Lobachevski)

RESUMO

A Teoria da Álgebra Linear é aplicada em diversas áreas e por diversos profissionais em diversos domínios, como científicos e tecnológicos. Como acadêmico do curso de Licenciatura em Matemática, monitor do componente curricular "Introdução à Álgebra Linear", em três períodos letivos (2018.1 e 2; 2019.1) percebi o quanto precisamos estudar sobre a aplicabilidades da álgebra linear em outras áreas de conhecimento. Diante do exposto, o objetivo desse estudo consiste em demonstrar, através de algumas aplicações e representações matriciais, a importância da utilização das ferramentas trazidas pela Álgebra Linear em outras áreas mostrando a sua aplicabilidade. Além disso, apresentamos algumas demonstrações sobre os principais conceitos da teoria dos números, criptografia, probabilidades e Cadeias de Markov. Para tanto, recorremos a revisão da literatura sobre a teoria das matrizes. Utilizando referencial pertinente, como Anton e Horres (2012), Boldrini (1980), Carvalho (2009), Kolman e Hill (2013) dentre outros. Os resultados revelaram que as aplicações matriciais podem ser utilizadas em diferentes áreas do conhecimento por meio de aplicações práticas.

Palavras-chave: Matrizes; Aplicações matriciais; Algoritmo de Euclides; Criptografia; Cadeia de Markov.

ABSTRACT

The Theory of Linear Algebra is applied in several areas and by different professionals in different domains, such as scientific and technological. As an academic in the Mathematics Degree course, monitor of the curricular component "Introduction to Linear Algebra", in three academic periods (2018.1 and 2; 2019.1) I realized the necessary study on the applicability of linear algebra in other areas of knowledge. Given the above, the objective of this study is to demonstrate, through some applications and matrix representations, the importance of using the tools brought by Linear Algebra in other areas showing its applicability. In addition, we present some accounts on the main concepts of number theory, cryptography, probabilities and Markov Chains. For that, we resorted to a review of the literature on matrix theory. Using relevant references, such as Anton and Horres (2012), Boldrini (1980), Carvalho (2009), Kolman and Hill (2013) among others. The results revealed that matrix applications can be used in different areas of knowledge through practical applications.

Keywords: Matrices; Matrix applications; Euclid's algorithm; Cryptography; Markov chain.

LISTA DE ILUSTRAÇÕES

Figura 1 – Euclides de Alexandria (323 – 283 a.C.) 28
Figura 2 – Lester S. Hill (1891 – 1956) 36
Figura 3 – Andrei Andreevich Markov (1856 – 1922) 45

SUMÁRIO

1	**INTRODUÇÃO**	**10**
2	**MATRIZES**	**12**
2.1	UMA BREVE ABORDAGEM HISTÓRICA	**12**
2.2	CONCEITOS E DEFINIÇÕES INICIAIS	**14**
2.2.1	**Tipos especiais de matrizes**	**14**
2.3	OPERAÇÕES COM MATRIZES E SUAS PROPRIEDADES	**18**
2.3.1	**Adição**	**18**
2.3.2	**Multiplicação por Escalar**	**18**
2.3.3	**Transposição**	**19**
2.3.4	**Multiplicação de Matrizes**	**19**
2.4	OPERAÇÕES ELEMENTARES SOBRE LINHAS	**20**
2.4.1	**Forma Escada (Forma escalonada reduzida por linhas)**	**21**
2.5	SISTEMAS DE EQUAÇÕES LINEARES E MATRIZES	**22**
2.6	DETERMINANTES DE UMA MATRIZ QUADRADA	**23**
2.7	MATRIZ INVERSA	**25**
3	**O ALGORITMO DE EUCLIDES REPRESENTADO POR MATRIZES**	**28**
3.1	EUCLIDES DE ALEXANDRIA	**28**
3.2	O ALGORITMO DE EUCLIDES	**28**
3.3	REPRESENTANDO MATRICIALMENTE O ALGORÍTIMO DE EUCLIDES	**31**
4	**CRIPTOGRAFIA: CIFRAS DE HILL**	**36**
4.1	LESTER S. HILL	**36**
4.2	ARITMÉTICA MODULAR E MATRIZES	**36**
4.2.1	**Congruência módulo m**	**37**
4.2.2	**Congruência e matrizes**	**39**
4.3	CRIPTOGRAFANDO UMA MENSAGEM ATRAVÉS DAS CIFRAS DE HILL	**40**
4.4	DESCRIPTOGRAFANDO UMA CIFRA DE HILL DE ORDEM 2	**42**
5	**CADEIAS DE MARKOV**	**45**
5.1	ANDREI ANDREYEVICH MARKOV	**45**
5.2	CONCEITOS BÁSICOS DE PROBABILIDADE	**45**
5.3	PROCESSOS ESTOCÁSTICOS E CADEIAS DE MARKOV	**47**
5.3.1	**Cadeia de Markov a longo prazo**	**52**
5.4	CADEIAS DE MARKOV NA GENÉTICA	**55**
6	**CONSIDERAÇÕES FINAIS**	**59**
	REFERÊNCIAS	**60**

1 INTRODUÇÃO

A Teoria da Álgebra Linear pode ser aplicada em diversas áreas e por diversos profissionais, dentre eles destacamos os cientistas da computação, economistas, estatísticos, físicos, engenheiros entre outros. Além disso, pode-se dizer que a importância da Álgebra Linear está diretamente ligada à sua presença e aplicabilidade em diversos domínios, como científicos, tecnológicos e da própria matemática.

Dessa forma, esse estudo teve como objetivo demonstrar através de algumas aplicações e representações matriciais a importância de utilizar as ferramentas trazidas pela Álgebra Linear em outras áreas do conhecimento, ponto este, muitas vezes esquecido ou não abordado de maneira aprofundada no curso de Introdução à Álgebra Linear, como também, dar outro sentido ao que é ensinado em sala de aula mostrando a sua aplicabilidade.

A minha experiência como aluno da disciplina de “Introdução à Álgebra Linear” e posteriormente, como monitor no "Projeto de monitoria integrada: proposta interdisciplinar para o ensino de Matemática"da Universidade Federal da Paraíba / Campus IV, durante três períodos letivos (2018 e 2019), foram aspectos que suscitaram o interesse de pesquisa por esta temática.

Para tanto, realizamos uma pesquisa bibliográfica na área da Matemática Pura, especificamente em Álgebra Linear, onde discutimos sobre um estudo com relação as matrizes aplicadas na representação do Algoritmo de Euclides, na Criptografia e nas Cadeias de Markov. Suscitando assim, a discussão sobre os conceitos e fundamentos da teoria matricial inseridos nestas aplicações, proporcionando também, a observação de alguns conceitos abstratos presentes nesta teoria sobre uma perspectiva diferente. Para tanto, este estudo, propriamente dito, está dividido em cinco capítulos.

No segundo, abordamos uma breve discussão histórica sobre como se deu o aparecimento e o desenvolvimento dos estudos relacionados as matrizes e, uma revisão das definições e conceitos básicos referentes ao estudo das mesmas, os quais são abordados em cursos introdutórios de Álgebra Linear e que são a base teórica para o nosso estudo.

No terceiro capítulo dissertamos como o algoritmo de Euclides pode ser representado através de matrizes. Inicialmente é apresentada uma revisão biográfica do matemático grego Euclides de Alexandria, e em seguida são apresentados definições e exemplos sobre o algoritmo criado por ele. Ao final do capítulo trazemos duas aplicações práticas do algoritmo de Euclides, mostrando como representa-las matricialmente.

No quarto capítulo, discutimos como as matrizes podem ser aplicadas a criptografia, nas chamadas Cifras de Hill. A princípio, apresentamos o criador deste método criptográfico, o matemático Lester S. Hill. Em seguida discorremos sobre os tópicos da aritmética modular, e também da analogia existente entre eles e a aritmética matricial, tópicos estes, que são inerentes ao estudo das cifras de Hill. Ainda neste capítulo, apresentamos como podemos criptografar uma mensagem através das cifras de Hill, e por conseguinte, como podemos descriptografa-la utilizando a congruência módulo m em matrizes.

No quinto, abordamos como as matrizes são utilizadas e aplicadas nas Cadeias de Markov. Fazemos menção à biografia do matemático Andrei Andreyevich Markov, o responsável pela criação das cadeias por nós estudadas e que levam o seu nome. Tratamos posteriormente sobre conceitos básicos de probabilidade, os quais se fazem minimamente necessários para o nosso estudo em Cadeias de Markov. Em seguida definimos o que vem a ser uma Cadeia de Markov e as demais definições relacionadas a mesma. E por fim, apresentamos como as cadeias de Markov podem ser utilizadas, ou modeladas, em problemas envolvendo a genética.

No sexto e último capítulo são apresentadas as considerações finais, na qual verificamos a aplicabilidade da Álgebra Linear em situações de outras áreas do conhecimento, como foco especial no estudo das matrizes.

2 MATRIZES

2.1 UMA BREVE ABORDAGEM HISTÓRICA

As origens das matrizes são imprecisas, mas é possível encontrar vestígios de seu uso entre os séculos II e IV a.C. Entretanto seu desenvolvimento se deu apenas no final do século XVII. Historiadores afirmam que por volta de 300 a.C. os babilônicos já davam indícios do surgimento de matrizes por meio do estudo de sistemas de equações lineares, especificamente em problemas envolvendo equações lineares simultâneas, as quais eram utilizadas para simular situações de seu cotidiano.

Contudo, o primeiro problema conhecido de método de matriz foi escrito na China, entre 200 a.C. e 100 a.C. durante a Dinastia Han. O Chiu-Chang Suan-Shu ou "Os Nove capítulos sobre a arte matemática", foi uma obra de destaque na época, pois trazia problemas matemáticos diversos sobre agricultura, solução de equações, mensuração de terrenos, propriedades dos triângulos retângulos, etc. Em seu oitavo capítulo "A Maneira de Calcular Usando Flechas", a obra traz problemas que remetem à sistemas lineares de três a seis incógnitas, os quais trazem soluções para estas equações utilizando os números organizados em linhas e colunas, assemelhando-se a matrizes. O processo utilizado para estas soluções é bastante semelhante à técnica criada por Carl Friedrich Gauss (1777-1855) no século XIX, a chamada "eliminação gaussiana"(com uma única diferença: as equações eram agrupadas em colunas ao invés de linhas). Vejamos com se dava a solução do primeiro problema trazido neste oitavo capítulo da obra chinesa.

Problema 2.1.1 *Há três classes de milho, sendo que três sacos da primeira classe, dois da segunda classe e um da terceira totalizam 39 medidas. Dois da primeira, três da segunda e um da terceira totalizam 34 medidas. E um da primeira, dois da segunda e três da terceira totalizam 26 medidas. Quantas medidas do grão tem cada saco de cada classe? (Anton e Rorres (2012), p. 538)*

Equacionando o problema, teríamos:

$$\begin{cases} 3x+2y+z=39 \\ 2x+3y+z=34 \\ x+2y+3z=26 \end{cases}$$

onde diríamos que x, y e z seriam, respectivamente, as medidas das 1ª, 2ª e 3ª classes de milho. Mas, nas condições da obra chinesa, este problema era resolvido da seguinte maneira: Os coeficientes do sistema de três equações eram configurados em colunas como uma tabela, em uma espécie de tabuleiro, onde a 1ª equação era posicionada da última coluna da direita seguida das demais equações para a esquerda. Tais coeficientes eram representados por varas vermelhas (para coeficientes negativos) e pretas (para coeficientes positivos). Se em alguma célula da tabela surgisse um coeficiente nulo, esta célula era deixada em branco.

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

Agora, efetuando sucessivas operações a partir da 1ª coluna (à direita), é possível reduzir a tabela acima para a seguinte tabela.

		3
	5	2
36	1	1
99	24	39

Esta segunda tabela nos fornecerá um novo sistema de equações

$$\begin{cases} 3x+2y+z=39 \\ 5y+z=24 \\ 36z=99 \end{cases}$$

que tem como solução: x = 37/4, y = 17/4 e z = 11/4.

De agora em diante, o uso e estudo de matrizes se via ainda engatinhando. Matemáticos renomados como Leibniz (1646 - 1716), Cramer (1704 - 1752), Laplace (1749 - 1827), Lagrange (1736 - 1813) e muitos outros, permeavam seus estudos entre sistemas de equações lineares, matrizes e determinantes, mas até então, as operações e o conceito de matrizes ainda não estavam bem definidos.

De acordo com Anton e Rorres (2012), foi apenas em 1850 que James Joseph Sylvester (1814 - 1897) utilizou o termo "matriz" pela primeira vez, onde definiu-a como um "arranjo oblongo de termos", e que posteriormente compartilhou de suas ideias sobre matrizes com Arthur Cayley (1821 - 1895). Em 1858, Cayley tornou-se o principal percursor do estudo matricial ao publicar sua obra "Memoir on the Theory of Matrices"ou "Ensaio sobre a Teoria de Matrizes", que trazia operações e definições básicas e inovadoras ao estudo de matrizes, dando um sentido diferente as operações com matrizes ao aplica-las no estudo de transformações lineares no plano, onde Cayley mostra que a partir da matriz:

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

é possível expressar a transformação:

$$\begin{cases} x' = ax+by \\ y' = cx+dy \end{cases}$$

A partir daí, teoria das matrizes continuou em constante desenvolvimento, tornando-se hoje, uma importante ferramenta nas diversas áreas científicas e tecnológicas.

2.2 CONCEITOS E DEFINIÇÕES INICIAIS

Nesta seção, temos como objetivo apresentar alguns conceitos e definições sobre matrizes. Assim, faremos uma breve revisão do que é estudado sobre matrizes em um curso introdutório de Álgebra linear. A presente seção está baseada nas obras de Boldrini (1980), Hoffman e Kunze (1970) e Lay, Camelier e Iório (1999), de modo que o leitor poderá consulta-las caso haja necessidade de aprofundamento.

Uma matriz A de ordem *m* por *n* é uma tabela quadrangular $m \times n$ de elementos sobre um corpo K, que podem ser números (reais ou complexos), funções, polinômios, etc, os quais ficam dispostos em *m* linhas e *n* colunas. Representamos tal matriz da seguinte maneira:

$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

ou simplesmente A, que pode ser representada também por $[a_{ij}]_{m\times n}$, onde $i \in \{1,2,3,...,m\}$ e $j \in \{1,2,3,...,n\}$.

Definição 2.2.1 *Dizemos que as matrizes $A = [a_{ij}]_{m\times n}$ e $B = [b_{ij}]_{x\times y}$ são iguais, se elas tem o mesmo número de linhas ($m = x$) e colunas ($n = y$) e todos os seus elementos correspondentes são iguais ($a_{ij} = b_{ij}$).*

Exemplo 2.2.2 *As matrizes de ordem 2 por 3 abaixo são iguais:*

$$\begin{bmatrix} cos\ 60^\circ & 2^3 \\ 2 & 1 \\ 4^2 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & 8 \\ 2 & log\ 10 \\ 16 & 12^0 \end{bmatrix}$$

2.2.1 Tipos especiais de matrizes

Recebem nomes especias as matrizes que tem uma utilidade relativamente maior ao estudo dessa teoria, e também aquelas que possuem propriedades que as diferenciam de uma matriz qualquer.

Dada uma matriz $A_{m\times n}$, dizemos que A é uma matriz:

- Matriz Retangular

Definição 2.2.3 *Uma matriz é dita retangular quando $m \neq n$, ou seja, quando o número de linhas é diferente ao número de colunas.*

Exemplo 2.2.4

$$A_{3\times 2} = \begin{bmatrix} 1 & 2 \\ 29 & 13 \\ 4 & 1 \end{bmatrix} e\ B_{2\times 4} = \begin{bmatrix} 1 & 2 & 0 & 5 \\ 9 & 3 & 8 & 6 \end{bmatrix}$$

- Matriz Quadrada

Definição 2.2.5 *Dizemos que uma matriz é quadrada quando $m = n$. E dizemos que a ordem de A é m por m, ou simplesmente A tem ordem m. Podemos expressar a matriz A genericamente por*

$$A_{m\times m} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1m} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2m} \\ a_{31} & a_{32} & a_{33} & \dots & a_{1m} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & a_{m2} & \dots & a_{mm} \end{bmatrix}$$

Exemplo 2.2.6

$$B = \begin{bmatrix} 11 & 2 & 13 & 4 \\ 0 & 2 & 3 & 10 \\ 1 & 2 & 4 & 5 \\ 7 & 8 & 7 & 1 \end{bmatrix} e\ C = \begin{bmatrix} 7 & 1 \\ 1 & 8 \end{bmatrix}$$

- Matriz Nula ou Matriz Zero

Definição 2.2.7 *Uma matriz é considerada nula quando para todo i e j os elementos $a_{ij} = 0$.*

Exemplo 2.2.8

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} e\ F = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

- Matriz Linha

Definição 2.2.9 *Matriz linha é uma matriz A cujo o número de linhas é igual a 1 ($m = 1$). E dizemos que ela tem ordem 1 por n. Podendo A, ser genericamente expressa por*

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \end{bmatrix}$$

Exemplo 2.2.10

$$A = \begin{bmatrix} 0 & -1 & 2 & 3 & 4 \end{bmatrix} e\ B = \begin{bmatrix} 1 & 9 & 0 \end{bmatrix}$$

- Matriz Coluna

Definição 2.2.11 *Matriz coluna é uma matriz A cujo o número de colunas é igual a 1 ($n = 1$). E dizemos que ela tem ordem m por 1. Podendo A, ser genericamente expressa por*

$$A = \begin{bmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \vdots \\ a_{m1} \end{bmatrix}$$

Exemplo 2.2.12

$$G = \begin{bmatrix} 5 \\ 4 \\ -3 \\ 2 \\ 1 \end{bmatrix} e\ H = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$$

- Matriz Diagonal

Definição 2.2.13 *Chama-se uma matriz A de diagonal quando ela é quadrada ($m = n$) e os elementos $a_{ij} = 0$ para todo $i \neq j$. Onde A é genericamente expressa por*

$$A = \begin{bmatrix} a_{11} & 0 & ... & 0 \\ 0 & a_{22} & ... & 0 \\ \vdots & \vdots & ... & \vdots \\ 0 & 0 & ... & a_{nn} \end{bmatrix}$$

Exemplo 2.2.14

$$J = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} e\ K = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$$

- Matriz Identidade ou Matriz Unidade

Definição 2.2.15 *Uma matriz é dita identidade quando $m = n$ e tem os elementos*

$$a_{ij} = \begin{cases} 1, \forall i = j \\ 0, \forall i \neq j \end{cases}$$

Denotamos tal matriz por I_n, ou simplesmente por I.

Exemplo 2.2.16

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} e\ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- Matriz Triangular Superior

Definição 2.2.17 *Dizemos que uma matriz é triangular superior quando $m = n$ e tem os elementos $a_{ij} = 0$ para todo $i > j$, isto é, significa dizer que todos os elementos que ficam abaixo da diagonal principal são iguais a zero.*

Exemplo 2.2.18

$$L = \begin{bmatrix} 2 & -1 & 1 \\ 0 & -4 & 2 \\ 0 & 0 & 3 \end{bmatrix} e\ M = \begin{bmatrix} 7 & 6 & 1 & 9 \\ 0 & -5 & -2 & 1 \\ 0 & 0 & 5 & 4 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

- Matriz Triangular Inferior

Definição 2.2.19 *Dizemos que uma matriz é triangular Inferior quando $m = n$ e tem os elementos $a_{ij} = 0$ para todo $i < j$, isto é, significa dizer que todos os elementos que ficam acima da diagonal principal são iguais a zero.*

Exemplo 2.2.20

$$N = \begin{bmatrix} 2 & 0 & 0 \\ 9 & -4 & 0 \\ 4 & -1 & 3 \end{bmatrix} e\ O = \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix}$$

- Matriz Simétrica

Definição 2.2.21 *Uma matriz é dita simétrica quando $m = n$ e tem os elementos $a_{ij} = a_{ji}$ para todo i e j, onde, em relação a diagonal principal, a parte inferior é um reflexo da parte superior.*

Exemplo 2.2.22

$$P = \begin{bmatrix} 1 & 4 \\ 4 & 2 \end{bmatrix} e\ Q = \begin{bmatrix} 1 & 3 & 5 \\ 3 & -2 & 1 \\ 5 & 1 & 3 \end{bmatrix}$$

- Matriz Anti-Simétrica

Definição 2.2.23 *Uma matriz é dita anti-simétrica quando $m = n$ e tem os elementos $a_{ij} = -a_{ji}$ para todo i e j.*

Exemplo 2.2.24

$$R = \begin{bmatrix} 1 & 2 & -1 & 7 \\ -2 & 1 & -3 & 1 \\ 1 & 3 & 1 & 6 \\ -7 & -1 & -6 & 1 \end{bmatrix} e\ S = \begin{bmatrix} 2 & 8 \\ -8 & 4 \end{bmatrix}$$

2.3 OPERAÇÕES COM MATRIZES E SUAS PROPRIEDADES

2.3.1 Adição

Definição 2.3.1 *Dadas as matrizes A e B de mesma ordem $m \times n$, dizemos que a soma de A com B é uma matriz de mesma ordem, denotada por A+B, cujos elementos são somas dos correspondentes de A e B, isto é,*

$$A + B = [a_{ij} + b_{ij}]_{m \times n}$$

Exemplo 2.3.2

$$A + B = \begin{bmatrix} 1 & 3 & 0 \\ 6 & 1 & -8 \\ 5 & 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & -2 & 5 \\ 7 & 9 & 7 \\ 1 & -3 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 5 \\ 13 & 10 & -1 \\ 6 & -3 & 0 \end{bmatrix}$$

Propriedades 2.3.3 *Sejam A, B e C matrizes de mesma ordem, então:*

i) A+B = B+A (Comutatividade)
ii) (A+B)+C = A+(B+C) (Associatividade)
iii) A+0 = A, onde 0 = $0_{m \times n}$ (Existência do elemento neutro)
iv) A+(-A) = 0

2.3.2 Multiplicação por Escalar

Definição 2.3.4 *Seja $A = [a_{ij}]_{m \times n}$ e α um escalar qualquer (número real ou complexo), o produto de $A = [a_{ij}]_{m \times n}$ por esse escalar é igual a $B = [b_{ij}]_{m \times n}$, onde $b_{ij} = \alpha \cdot a_{ij}$.*

Exemplo 2.3.5 *Dado $\alpha = -3$, temos:*

$$\alpha \cdot A = (-3) \cdot \begin{bmatrix} 1 & 0 & 5 \\ -4 & 2 & -1 \\ 10 & -3 & 0 \end{bmatrix} = \begin{bmatrix} -3 & 0 & -15 \\ 12 & -6 & 3 \\ -30 & 9 & 0 \end{bmatrix}$$

Propriedades 2.3.6 *Dados os escalares α e λ e as matrizes A e B de mesma ordem, temos as seguintes propriedades:*

i) $(\alpha+\lambda)\cdot A = \alpha\cdot A+\lambda\cdot A$
ii) $\alpha\cdot(A+B) = \alpha\cdot A+\alpha\cdot B$
iii) $\alpha\cdot(\lambda\cdot A) = (\alpha\cdot\lambda)\cdot A$
iv) $1\cdot A = A$
v) $0\cdot A = 0_{m\times n}$

2.3.3 Transposição

Definição 2.3.7 *Dada* $A = [a_{ij}]_{m\times n}$*, podemos obter a sua transposta* $A^t = [t_{ij}]_{n\times m}$*, onde as linhas de* A^t *são as colunas de A (*$t_{ij} = a_{ji}$*).*

Exemplo 2.3.8

$$A = \begin{bmatrix} 1 & 3 & 5 \\ 3 & -2 & 1 \end{bmatrix}_{2\times 3} \qquad A^t = \begin{bmatrix} 1 & 3 \\ 3 & -2 \\ 5 & 1 \end{bmatrix}_{3\times 2}$$

Propriedades 2.3.9

i) Se $A = A^t$*, então a matriz A é dita Simétrica.*
ii) $(A^t)^t = A$ *(A transposta da transposta de A é a própria matriz A)*
iii) $(A+B)^t = A^t+B^t$
iv) $(\alpha\cdot A)^t = \alpha\cdot A^t$*, onde* α *é um escalar qualquer.*

2.3.4 Multiplicação de Matrizes

Definição 2.3.10 *Sejam* $A = [a_{ij}]_{m\times n}$ *e* $B = [b_{xy}]_{n\times p}$*. Definimos a multiplicação de A por B como A·B = R, onde* $R = [r_{uv}]_{m\times p}$ *e*

$$r_{uv} = \sum_{\alpha=1}^{n} a_{u\alpha}b_{\alpha v} = a_{u1}b_{1v}+\ldots+a_{un}b_{nv}$$

Só é possível a multiplicação entre duas matrizes $A_{m\times n}$ e $B_{s\times p}$ se $n = s$, ou seja, se o mesmo número de colunas da primeira matriz for igual ao número de linhas da segunda matriz. Além disso, a matriz R (matriz-resultado) terá o mesmo número de linhas de A e o mesmo número de colunas de B, isto é, será de ordem $m\times p$.

Ademais, o elemento r_{ij} é obtido somando-se os produtos resultantes da multiplicação dos elementos da i-ésima linha da primeira matriz pelos elementos correspondentes da j-ésima coluna da segunda matriz, como podemos ver no exemplo abaixo.

Exemplo 2.3.11

$$A\cdot B = \begin{bmatrix} 1 & 2 \\ -2 & 1 \\ 1 & 3 \\ -7 & -1 \end{bmatrix}_{4\times 2} \cdot \begin{bmatrix} 1 & 3 & 0 \\ 6 & 1 & -8 \end{bmatrix}_{2\times 3}$$

$$= \begin{bmatrix} 1\cdot 1+2\cdot 6 & 1\cdot 3+2\cdot 1 & 1\cdot 0+2\cdot(-8) \\ (-2)\cdot 1+1\cdot 6 & (-2)\cdot 3+1\cdot 1 & (-2)\cdot 0+1\cdot(-8) \\ 1\cdot 1+3\cdot 6 & 1\cdot 3+3\cdot 1 & 1\cdot 0+3\cdot(-8) \\ (-7)\cdot 1+(-1)\cdot 6 & (-7)\cdot 3+(-1)\cdot 1 & (-7)\cdot 0+(-1)\cdot(-8) \end{bmatrix}_{4\times 3}$$

$$= \begin{bmatrix} 13 & 5 & -16 \\ 4 & -5 & -8 \\ 19 & 6 & -24 \\ -13 & -22 & 8 \end{bmatrix}_{4\times 3}$$

A seguir, um exemplo em que não é possível a multiplicação entre duas matrizes, pois número de colunas da primeira matriz não é igual ao número de linhas da segunda matriz.

Exemplo 2.3.12

$$A\cdot B = \begin{bmatrix} 1 & 3 \\ -1 & 0 \\ 1 & -1 \\ -6 & 1 \end{bmatrix}_{4\times 2} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & -4 \\ 0 & 1 & -1 \end{bmatrix}_{3\times 3} = \nexists$$

Propriedades 2.3.13 *Sejam A, B e C matrizes de ordem quaisquer, se $n = s$ na multiplicação de duas matrizes quaisquer $(M_1)_{m\times n}$ por $(M_2)_{s\times p}$, então valem as seguintes propriedades:*

i) $A\cdot B \neq B\cdot A$ *(Não vale em geral a comutatividade)*
ii) $(AB)\cdot C = A\cdot(BC)$ *(Associatividade)*
iii) $A\cdot(B+C) = A\cdot B + A\cdot C$ *(Distributividade à esquerda em relação à soma)*
iv) $(A+B)\cdot C = A\cdot C + B\cdot C$ *(Distributividade à direita em relação à soma)*
v) $A\cdot 0 = 0$ *e* $0\cdot A = 0$*, onde* $0 = 0_{m\times n}$
vi) $(AB)^t = B^t\cdot A^t$

2.4 OPERAÇÕES ELEMENTARES SOBRE LINHAS

Existem três operações elementares possíveis sobre as linhas de uma matriz, que são:

i) Permuta das i-ésimas e j-ésimas linhas. $(L_i \leftrightarrow L_j)$
ii) Multiplicação da i-ésimas linha por um escalar λ não nulo. $(L_i \to \lambda L_i)$
iii) Substituição da i-ésima linha pela i-ésima linha mais λ vezes a j-ésima linha. $(L_i \to L_i + \lambda L_j)$

Definição 2.4.1 *Sejam A e B matrizes de ordem $m\times n$. Dizemos que B é* ***linha equivalente*** *a A, se B for obtida de A por meio de sucessivas operações elementares sobre as linhas de A. Denotamos este processo por $A \to B$ ou $A \sim B$.*

Exemplo 2.4.2 *A matriz* $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & -4 \\ 3 & 2 & 4 \end{bmatrix}$ *é linha equivalente a* $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, *pois:*

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & -4 \\ 3 & 2 & 4 \end{bmatrix} L_3 \to L_3 - 3 \cdot L_1 \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & -4 \\ 0 & 2 & 4 \end{bmatrix} L_2 \to \frac{1}{2} \cdot L_2 \Rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 2 & 4 \end{bmatrix} L_3 \to L_3 - 2 \cdot L_2 \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 8 \end{bmatrix} L_3 \to \frac{1}{8} \cdot L_3 \Rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} L_2 \to L_2 + 2 \cdot L_3 \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = B$$

2.4.1 Forma Escada (Forma escalonada reduzida por linhas)

Definição 2.4.3 *Dadas as matrizes A e B de ordem* $m \times n$, *dizemos que B é a* ***forma escada*** *de A se* $B \sim A$ *e :*

i) O 1º elemento não nulo de cada linha não nula é igual a 1, o qual chamamos de "Pivô"ou "Líder".
ii) Toda linha nula, se existir, ocorre abaixo das linhas não nulas.
iii) Cada coluna que contém o pivô, tem todos os elementos restantes iguais a zero.
iv) Se as linhas $1, \ldots, r$ *são as linhas não nulas, e se o pivô da linha i ocorre na coluna* C_i, *então* $C_1 < C_2 < \ldots < C_r$, *isto é, em quaisquer duas linhas sucessivas não nulas, o pivô da linha inferior ocorre mais à direita que o pivô da linha inferior, o que impõe a forma escada à matriz.*

Observação: O número de zeros que precede cada pivô aumenta linha após linha, até que sobrem apenas linhas nulas, caso haja.

Além do Exemplo 2.4.2, vejamos outros exemplos com relação a redução de matrizes à forma escada.

Exemplo 2.4.4

$$A = \begin{bmatrix} 0 & -1 & 0 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 1 \end{bmatrix}; B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} e\, C = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ -5 & 1 & 0 \end{bmatrix}$$

Podemos observar que:
- A matriz A não é a forma escada, pois não satisfaz as condições (i) e (ii).

- A matriz B é a forma escada pois satisfaz todas as condições.
- A matriz C não é a forma escada, pois não satisfaz as condições (iii) e (iv).

2.5 SISTEMAS DE EQUAÇÕES LINEARES E MATRIZES

Um sistema de equações lineares com m equações e n incógnitas é um conjunto de equações do seguinte tipo:

$$\begin{cases} a_{11} \cdot x_1 + a_{12} \cdot x_2 + ... + a_{1n} \cdot x_n = b_1 \\ a_{21} \cdot x_1 + a_{22} \cdot x_2 + ... + a_{2n} \cdot x_n = b_2 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad \vdots \\ a_{m1} \cdot x_1 + a_{m2} \cdot x_2 + ... + a_{mn} \cdot x_n = b_m \end{cases} \tag{1}$$

com $a_{ij}, 1 \leq i \leq m, 1 \leq j \leq n$, números reais (ou complexos).

Uma solução para o sistema acima é dada por uma n-upla de números $(x_1, x_2, x_3, ..., x_n)$ que satisfaça de modo simultâneo estas m equações. Além disso, podemos representar o sistema 1 da seguinte forma matricial:

$$\begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \vdots & ... & \vdots \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

ou simplesmente $A \cdot X = B$, onde A, X e B são respectivamente as matrizes dos coeficientes, das incógnitas e dos termos independentes.

Exemplo 2.5.1 *O sistema*

$$\begin{cases} x_1 + 3x_2 - x_3 = -2 \\ -x_1 - 2x_2 + 3x_3 = 1 \\ 2x_1 - x_2 + 5x_3 = 3 \end{cases} \tag{2}$$

pode ser representado da seguinte forma matricial:

$$\begin{bmatrix} 1 & 3 & -1 \\ -1 & -2 & 3 \\ 2 & -1 & 5 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -2 \\ 1 \\ 3 \end{bmatrix}$$

Podemos ainda, expressar o sistema por meio da chamada *matriz ampliada do sistema*, onde cada linha é uma representação de forma abreviada da equação correspondente do sistema.

Denotaremos a matriz ampliada do sistema por A^*.

$$A^* = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_2 \end{bmatrix}$$

Tal matriz nos possibilita encontrar a solução do sistema linear, de modo eficiente e prático, utilizando das operações lineares sobre linhas de uma matriz. Como veremos no exemplo abaixo.

Exemplo 2.5.2 *Utilizando o sistema 2 do Exemplo 2.5.1, podemos resolve-lo a partir de sua matriz ampliada*

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

Utilizando sucessivas operações sobre linhas, obtemos a seguinte matriz como resultado

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

que é a matriz ampliada do sistema abaixo, onde x_1, x_2 e x_3 são soluções do sistema (1).

$$\begin{cases} x_1 = 1 \\ x_2 = -1 \\ x_3 = 0 \end{cases}$$

Definição 2.5.3 *Dois sistemas lineares são ditos equivalentes se suas matrizes ampliadas A^* e B^* forem equivalentes.*

2.6 DETERMINANTES DE UMA MATRIZ QUADRADA

Dada uma matriz A de ordem $m \times m$, podemos associar um número real, chamado de determinante, a esta matriz, cujo valor nos permite dizer se esta matriz é ou não singular, ou seja, se a matriz admite ou não uma inversa, assunto este, que veremos mais a frente. Denotamos o determinante de uma matriz A por $det(A)$, $|A|$ ou $det\ [a_{ij}]$.

De modo geral, um determinante de uma matriz $m \times m$ é definido através de determinantes de submatrizes de ordem $(m-1) \times (m-1)$, isto é, se uma matriz A tem ordem 3 (m=3), o $det(A)$ é definido através dos determinantes das submatrizes A_{ij}, 2×2, que são obtidas da matriz A eliminando-se as linhas i e as colunas j.

Definição 2.6.1 *Dada $A = [a_{ij}]_{m\times m}$, chamamos de determinante de A, o número real dado por:*

$$\textit{(I)}\ det(A) = \sum_{i=1}^{m} a_{ij}\cdot(-1)^{i+j}\cdot|A_{ij}|,\ \textit{para j fixo.}$$

ou

$$\textit{(II)}\ det(A) = \sum_{j=1}^{m} a_{ij}\cdot(-1)^{i+j}\cdot|A_{ij}|,\ \textit{para i fixo.}$$

onde $m \geq 2$ e A_{ij} é a matriz obtida de A por meio da eliminação da i-ésima linha e da j-ésima coluna.

Exemplo 2.6.2 *Calcule o determinante da matriz* $A = \begin{bmatrix} 1 & 3 & 0 \\ 1 & 2 & -4 \\ 3 & 2 & 4 \end{bmatrix}$

$$det(A) = a_{11}\cdot(-1)^{1+1}\cdot|A_{11}| + a_{12}\cdot(-1)^{1+2}\cdot|A_{12}| + a_{13}\cdot(-1)^{1+3}\cdot|A_{13}|$$

$$det(A) = 1\cdot(-1)^2\cdot\begin{vmatrix} 2 & -4 \\ 2 & 4 \end{vmatrix} + 3\cdot(-1)^3\cdot\begin{vmatrix} 1 & -4 \\ 3 & 4 \end{vmatrix} + 0\cdot(-1)^4\cdot\begin{vmatrix} 1 & 2 \\ 3 & 2 \end{vmatrix}$$

Logo,

$$det(A) = 1\cdot 16 + (-3)\cdot 16 + 0\cdot(-4) = -32$$

Além disso, chamamos de *cofator*, ou *complemento algébrico* do elemento a_{ij}, o número $\Delta_{ij} = (-1)^{i+j}\cdot|A_{ij}|$, que é o determinante da submatriz A_{ij} afetado pelo sinal de $(-1)^{i+j}$. E a partir destes cofatores podemos formar a matriz $\bar{A}$, que é a *matriz dos cofatores* de A, onde $\bar{A} = [\Delta_{ij}]_{m\times m}$.

Exemplo 2.6.3 *Seja* $A = \begin{bmatrix} 2 & 3 & -3 \\ 3 & 3 & 2 \\ 4 & 2 & -1 \end{bmatrix}$,

$$\Delta_{11} = (-1)^{1+1}\cdot\begin{vmatrix} 3 & 2 \\ 2 & -1 \end{vmatrix} = -7$$

$$\Delta_{12} = (-1)^{1+2}\cdot\begin{vmatrix} 3 & 2 \\ 4 & -1 \end{vmatrix} = 11$$

$$\vdots$$

Então, $\bar{A} = \begin{bmatrix} -7 & 11 & -6 \\ -3 & 10 & 8 \\ 15 & -13 & -3 \end{bmatrix}$

Propriedades 2.6.4

i) Se uma matriz A possuir uma linha ou coluna nula, então $det(A) = 0$.
ii) $det(A^t) = det(A)$
iii) Se permutarmos duas linhas de uma matriz A, $det(A)$ *troca de sinal.*
iv) Se uma matriz A possuir duas linhas ou colunas iguais, então $det(A) = 0$.
v) Se multiplicarmos a linha de uma matriz A por um escalar, λ*, então* $det(A)$ *também fica multiplicado por* λ.
vi) $det(A+B) \neq det(A) + det(B)$. *(Em geral)*
vii) $det(A \cdot B) = det(A) \cdot det(B)$.

2.7 MATRIZ INVERSA

Definição 2.7.1 *Sejam A e B matrizes quadradas de mesma ordem, dizemos que A é inversível e B é uma inversa de A se, e somente se,* $AB = BA = I$. *Denotamos a inversa de A por* A^{-1}.

Em outras palavras, podemos, igualmente, definir a inversão de matrizes da seguinte maneira:

Definição 2.7.2 *Seja A uma matriz quadrada, dizemos que A é inversível e* A^{-1} *é uma inversa de A se pudermos encontrar uma matriz quadrada de mesma ordem tal que* $AA^{-1} = A^{-1}A = I$.

Exemplo 2.7.3 *Se* $A = \begin{bmatrix} 1 & 3 \\ -2 & -5 \end{bmatrix}$ *e* $B = \begin{bmatrix} -5 & -3 \\ 2 & 1 \end{bmatrix}$, *então:*

$$AB = \begin{bmatrix} 1 & 3 \\ -2 & -5 \end{bmatrix} \cdot \begin{bmatrix} -5 & -3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ e}$$

$$BA = \begin{bmatrix} -5 & -3 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 \\ -2 & -5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Assim, $B = A^{-1}$.

O teorema a seguir nos mostra que se a matriz quadrada A possui uma inversa, então esta inversa é única.

Teorema 2.7.4 *Se B e C são ambas inversas da matriz A, então B = C.*
Demonstração. *Como B e C são inversas de A, então AB = BA = I e AC = CA = I. Com isto, tem-se: B = BI = B(AC) = (BA)C = IC = C, e portanto, B = C.* ■

Há mais de uma forma de se obter a inversa de uma matriz A, uma delas é através de operações elementares sobre linhas, a qual não nos convém mostra-la no momento, outra é por meio da *matriz adjunta*, que é obtida a partir da transposta da matriz dos cofatores, $adj(A) = \bar{A}^t$.

Teorema 2.7.5 *Dizemos que uma matriz quadrada A é inversível se, e somente se, $det(A) \neq 0$. E sua inversa e dada por:*

$$A^{-1} = \frac{1}{det(A)} \cdot [adj(A)]$$

Demonstração. *Ver em Boldrini (1980), pág. 76* ■

O teorema acima nos garante encontrar a inversa de matrizes de ordem n, entretanto, como em nossas aplicações focamos necessariamente em matrizes de ordem 2, para fins práticos, podemos utilizar do teorema a seguir para encontrar rapidamente a inversa de uma matriz de ordem 2.

Teorema 2.7.6 *A matriz quadrada*

$$A = \begin{bmatrix} x & y \\ w & z \end{bmatrix}$$

é inversível se, e somente se, $xz - yw \neq 0$, onde a inversa é dada pela seguinte fórmula

$$A^{-1} = \frac{1}{xz-yw} \cdot \begin{bmatrix} z & -y \\ -w & x \end{bmatrix} \text{ ou } A^{-1} = \begin{bmatrix} \frac{z}{xz-yw} & -\frac{y}{xz-yw} \\ -\frac{w}{xz-yw} & \frac{x}{xz-yw} \end{bmatrix}$$

Demonstração. *Se A é invertível, então $AA^{-1} = I_2$ e $A^{-1}A = I_2$. Daí temos que*

$$AA^{-1} = \begin{bmatrix} x & y \\ w & z \end{bmatrix} \cdot \begin{bmatrix} \frac{z}{xz-yw} & -\frac{y}{xz-yw} \\ -\frac{w}{xz-yw} & \frac{x}{xz-yw} \end{bmatrix} = \begin{bmatrix} \frac{xz-yw}{xz-yw} & \frac{-xy+yx}{xz-yw} \\ \frac{wz-zw}{xz-yw} & \frac{xy-yw}{xz-yw} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

Analogamente, $A^{-1}A = I_2$. ■

A expressão $xz - yw$ apresentada no Teorema 2.7.6 acima nada mais é do que o determinante de A, e portanto podemos reescrever o teorema citado da seguinte forma:

Teorema 2.7.7 *Dizemos que a matriz quadrada A é inversível se, e somente se, $det(A) \neq 0$, onde a inversa é dada pela seguinte fórmula*

$$A^{-1} = \frac{1}{det(A)} \cdot \begin{bmatrix} z & -y \\ -w & x \end{bmatrix} \tag{3}$$

Exemplo 2.7.8 *Seja* $A = \begin{bmatrix} 3 & -1 \\ -4 & -2 \end{bmatrix}$, *determine a inversa de A.*

Temos que $det(A) = 3 \cdot (-2) - (-4) \cdot (-1) = -10$. Portanto, A é inversível e

$$A^{-1} = \frac{1}{-10} \cdot \begin{bmatrix} -2 & 1 \\ 4 & 3 \end{bmatrix} = \begin{bmatrix} \frac{-2}{-10} & \frac{1}{-10} \\ \frac{4}{-10} & \frac{3}{-10} \end{bmatrix} = \begin{bmatrix} \frac{1}{5} & -\frac{1}{10} \\ -\frac{2}{5} & -\frac{3}{10} \end{bmatrix}$$

Observações:

I) Se $det(A) = 1$, então temos que:

$$A^{-1} = \begin{bmatrix} z & -y \\ -w & x \end{bmatrix} \tag{4}$$

II) Se $det(A) = -1$, então temos que:

$$A^{-1} = \begin{bmatrix} -z & y \\ w & -x \end{bmatrix} \tag{5}$$

III) Se A é uma matriz inversível, ou seja, existe A^{-1}, então o sistema $A \cdot X = B$ tem única solução, e esta solução é da forma:

$$X = A^{-1} \cdot B \tag{6}$$

E assim, concluímos a nossa base teórica referente aos conteúdos trazidos pela teoria da Álgebra matricial.

3 O ALGORITMO DE EUCLIDES REPRESENTADO POR MATRIZES

3.1 EUCLIDES DE ALEXANDRIA

Figura 1 – Euclides de Alexandria (323 – 283 a.C.)

Fonte: http://acervocientificoprofmaciel.blogspot.com/2013/12/euclides-de-alexandria-o-fenomeno-da.html. Acesso em: 27 nov. 2020

Euclides de Alexandria foi um matemático grego que viveu aproximadamente entre 323-283 a.C. De acordo com Boyer (1974) e Eves (2011), sabe-se muito pouco sobre a vida de Euclides, apenas que ele atuou como professor na renomada escola de matemática de Alexandria, na Grécia, e que provavelmente tenha se formado em matemática pela escola platônica de Atenas. Euclides era um estudioso de diversas áreas, dentre elas a astronomia, óptica, cônicas e mecânica. Entretanto, uma parte das obras que ele escreveu se perderam, restando apenas cinco delas atualmente. Ele tornou-se bastante conhecido pela sua obra na área da geometria, *Os Elementos*, que foi rapidamente difundida, estudada e amplamente traduzida para diversos idiomas ao longo da história. Tal obra era dividida em treze capítulos, os quais eram subdivididos entre geometria plana elementar, teoria dos números e geometria no espaço.

3.2 O ALGORITMO DE EUCLIDES

Nesta seção iremos apresentar alguns teoremas e definições que nos auxiliarão posteriormente em nossas aplicações no que diz respeito a representação matricial do Algoritmo de Euclides. Os teoremas e definições aqui apresentadas foram retiradas das obras de Carvalho (2009), Santos (2006) e Milies e Coelho (2001), que podem ser consultadas caso o leitor necessite de um aprofundamento maior com relação as teorias aqui apresentadas.

A grande maioria dos estudantes das ciências exatas indubitavelmente conhece o método que possibilita encontrar-mos o mdc entre dois números por meio da decomposição deles em

fatores primos. No entanto, quando tais números vão ganhando proporções maiores, a tarefa de decompor estes números por meio deste método se torna um tanto dificultosa. Para facilitar nesta tarefa, existe um método baseado em divisões sucessivas conhecido como *O algoritmo de Euclides*, que foi trazido em sua obra *Os Elementos*. Tal ferramenta nos permite encontrar o mdc entre dois números grandes sem muitas dificuldades. Para entendermos melhor como funciona este algoritmo, vejamos alguns resultados importantes a seguir.

Lema 3.2.1 *Se a = b.q + r, com 0<r<b, onde q é o quociente e r é o resto da divisão de a por b, então mdc(a,b) = mdc(b,r).*
Demonstração. *Seja $d = mdc(a,b)$. Então temos que $d|a$ e $d|b \Longrightarrow d|a - b.q \Longrightarrow d|r$ e $d|b$. Por outro lado, se $d'|r$ e $d'|b \Longrightarrow d'|b.q + r \Longrightarrow d'|a$ e $d'|b \Longrightarrow d'|d$. Portanto, $mdc(b,r) = d$.* ■

Como podemos ver pelo lema acima, para encontrar o $mdc(a,b)$ basta encontrarmos o $mdc(b,r)$. Mas além disso, ao aplicar-mos o lema acima *n* vezes, fazendo divisões sucessivas, teremos o teorema a seguir.

Teorema 3.2.2 *(Algoritmo de Euclides) Dados $a,b \in \mathbb{Z}_+$, $b \neq 0$ tais que:*

$$\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b \\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2 \\
&\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n \cdot q_{n+1}
\end{aligned}$$

Dessa forma, mdc(a,b) = r_n

Com isto, o teorema acima nos diz que ao realizarmos estas sucessivas divisões o $mdc(a,b)$ é o último resto diferente de zero. Para divisões sucessivas utilizaremos o seguinte esquema abaixo, o qual é dado o nome de "*O Algoritmo de Euclides*":

	q_1	q_2	q_3	....	....	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	...	...	r_n	0	

Podemos observar também que este processo realizado nos remete ao Teorema de Bézout, o qual afirma que podemos encontrar inteiros r e s tais que $mdc(a,b) = ar + bs$. Isto se dá pois, na 1ª divisão

$$r_1 = a - q_1 \cdot b$$

ou seja, r_1 está escrito como combinação linear de a e b. Já na 2ª divisão feita, temos que

$$b = r_1 \cdot q_2 + r_2 \Longrightarrow b = (a - q_1 \cdot b) \cdot q_2 + r_2$$
$$\Longrightarrow r_2 = -q_2 \cdot a + (1 + q_1 \cdot q_2) \cdot b$$

O que nos permite também, escrever r_2 como combinação linear de a e b. Repetindo estas divisões sucessivamente, podemos encontrar uma expressão para r_n que também poderá ser escrita como combinação linear de a e b, onde $r_n = d$ representado no Teorema de Bézout abaixo.

Teorema 3.2.3 *(Teorema de Bézout) Dados $a, b \in \mathbb{Z}$, tal que $mdc(a,b) = d$, então existem $r, s \in \mathbb{Z}$ tais que $d = ar + bs$.*

Exemplo 3.2.4 *Vamos calcular o mdc(896,664). Temos:*

	1	*2*	*1*	*6*	*4*
896	*664*	*232*	*200*	*32*	*8*
232	*200*	*32*	*8*	*0*	

Logo, mdc(896,664) = 8.

Agora encontraremos a combinação linear para 8, ou seja, r e s tais que $8 = 896.r + 664.s$. *Pelo Algoritmo de Euclides temos:*

896 = 664(1) + 232 $\Longrightarrow$ 232 = 896 - 664(1)
664 = 232(2) + 200 $\Longrightarrow$ 200 = 664 - 232(2)
232 = 200(1) + 32 $\Longrightarrow$ 32 = 232 - 200(1)
200 = 32(6) + 8 $\Longrightarrow$ 8 = 200 - 32(6)
32 = 8(4)

Assim, temos que:

8 = 200 - 32(6) = 200 - [232 - 200(1)](6)
8 = 200(7) - 232(6) = [664 - 232(2)](7) - 232(6)
8 = 232(20) - 664(7) = [896 - 664(1)](20) - 664(7)
8 = 664(27) - 896(20)
8 = 896(-20) + 664(27)

Portanto, nas condições do Teorema de Bézout, os inteiros r e s são respectivamente -20 e 27.

Exemplo 3.2.5 *Vamos calcular o mdc(2226,988). Temos:*

	2	3	1	19	1	5
2226	988	250	238	12	10	2
250	238	12	10	2	0	

Logo, mdc(2226,988) = 2

Agora encontraremos a combinação linear para 2. Pelo Algoritmo de Euclides temos:

2226 = 988(2) + 250 $\Longrightarrow$ 250 = 2226 - 988(2)
988 = 250(3) + 238 $\Longrightarrow$ 238 = 988 - 250(3)
250 = 238(1) + 12 $\Longrightarrow$ 12 = 250 - 238(1)
238 = 12(19) + 10 $\Longrightarrow$ 10 = 238 - 12(19)
12 = 10(1) + 2 $\Longrightarrow$ 2 = 12 - 10(1)
10 = 2(5)

Assim, temos que:

2 = 12 - 10(1) = 12 - [238 - 12(19)](1)
2 = 12(20) - 238(1) = [250 - 238(1)](20) - 238(1)
2 = 250(20) - 238(21) = 250(20) - [988 - 250(3)](21)
2 = 250(83) - 988(21) = [2226 - 988(2)](83) - 988(21)
2 = 2226(83) - 988(187)
2 = 2226(83) + 988(-187)

Portanto, nas condições do Teorema de Bézout, os inteiros r e s são respectivamente 83 e –187.

3.3 REPRESENTANDO MATRICIALMENTE O ALGORÍTIMO DE EUCLIDES

O algoritmo de Euclides é um dos mais antigos algoritmos matemáticos em uso atualmente. Ele caracteriza-se por permitir encontrar, de modo eficaz, o máximo divisor comum entre dois números inteiros diferentes de zero. Ademais, dados os inteiros a e b positivos, o algoritmo de Euclides permite encontrar inteiros *r* e *s* tais que $mdc(a,b) = ar + bs$, resultados este, fundamental para a resolução de equações diofantinas.

Mostremos aqui que essa expressão pode ser obtida através do uso de uma matriz quadrada de ordem 2, o que nos permite escrever de forma elegante o algotitmo de Euclides, e consequentemente, encontrar a solução r e s da equação $mdc(a,b) = ar + bs$. A seguir mostraremos alguns exemplos de como isso funciona utilizando os exemplos da seção anterior.

Exemplo 3.3.1 *Sendo* $a = 896$ *e* $b = 664$*, pelo Exemplo 3.2.4, o número* 8*, o último resto não nulo, é o máximo divisor comum de* 896 *e* 664*, ou seja,* $mdc(896,664) = 8$*. Agora substituímos*

a primeira igualdade:

$$896 = 664(1) + 232$$

pela seguinte igualdade de matrizes:

$$\begin{cases} 896 = 664(1) + 232(1) \\ 664 = 664(1) + 232(0) \end{cases} \Longrightarrow \begin{bmatrix} 896 \\ 664 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 664 \\ 232 \end{bmatrix}$$

Analogamente, escrevendo todas as igualdades do Exemplo 3.2.4 na forma matricial temos:

$$\begin{bmatrix} 896 \\ 664 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 664 \\ 232 \end{bmatrix}$$

$$\begin{bmatrix} 664 \\ 232 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 232 \\ 200 \end{bmatrix}$$

$$\begin{bmatrix} 232 \\ 200 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 200 \\ 32 \end{bmatrix}$$

$$\begin{bmatrix} 200 \\ 32 \end{bmatrix} = \begin{bmatrix} 6 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 32 \\ 8 \end{bmatrix}$$

Assim,

$$\begin{bmatrix} 896 \\ 664 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 664 \\ 232 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 6 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} 32 \\ 8 \end{bmatrix}$$

$$\begin{bmatrix} 896 \\ 664 \end{bmatrix} = \begin{bmatrix} 27 & 4 \\ 20 & 3 \end{bmatrix} . \begin{bmatrix} 32 \\ 8 \end{bmatrix}$$

Ora, a matriz $\begin{bmatrix} 27 & 4 \\ 20 & 3 \end{bmatrix}$ *é inversível, e por 4, a sua inversa é* $\begin{bmatrix} 3 & -4 \\ -20 & 27 \end{bmatrix}$*. Então, por 6, obtemos a seguinte igualdade matricial:*

$$\begin{bmatrix} 32 \\ 8 \end{bmatrix} = \begin{bmatrix} 3 & -4 \\ -20 & 27 \end{bmatrix} . \begin{bmatrix} 896 \\ 664 \end{bmatrix}$$

Assim, a partir desta igualdade matricial obtemos $8 = (-20) \cdot 896 + 27 \cdot 664$*, e portanto, uma solução é* $(r,s) = (-20, 27)$.

Exemplo 3.3.2 *Sendo $a = 2226$ e $b = 988$, pelo Exemplo 3.2.5, número 2, o último resto não nulo, é o máximo divisor comum de 2226 e 988, ou seja, $mdc(2226, 988) = 2$. Escrevendo todas as igualdades do Exemplo 3.2.5 na forma matricial temos:*

$$\begin{bmatrix} 2226 \\ 988 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 988 \\ 250 \end{bmatrix}$$

$$\begin{bmatrix} 988 \\ 250 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 250 \\ 238 \end{bmatrix}$$

$$\begin{bmatrix} 250 \\ 238 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 238 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 238 \\ 12 \end{bmatrix} = \begin{bmatrix} 19 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 10 \end{bmatrix}$$

$$\begin{bmatrix} 12 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 2 \end{bmatrix}$$

Assim,

$$\begin{bmatrix} 2226 \\ 988 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 988 \\ 250 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot$$

$$\begin{bmatrix} 19 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 2 \end{bmatrix} = \begin{bmatrix} 187 & 178 \\ 83 & 79 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 2 \end{bmatrix}$$

Ora, a matriz $\begin{bmatrix} 187 & 178 \\ 83 & 79 \end{bmatrix}$ é inversível, e por 5, sua inversa é $\begin{bmatrix} -79 & 178 \\ 83 & -187 \end{bmatrix}$. E assim, por 6, obtemos a seguinte igualdade matricial:

$$\begin{bmatrix} 10 \\ 2 \end{bmatrix} = \begin{bmatrix} -79 & 178 \\ 83 & -187 \end{bmatrix} \cdot \begin{bmatrix} 2226 \\ 988 \end{bmatrix}$$

Assim, a partir desta igualdade matricial obtemos $2 = 83 \cdot 2226 + (-187) \cdot 988$, e portanto, uma solução é $(r, s) = (83, -187)$.

Generalizando, ao aplicarmos o algoritmo de Euclides a a e b, obtemos os quocientes não-nulos $q_1, q_2, ..., q_n$, e em seguida calcula-se o produto matricial das matrizes

$$A = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} q_2 & 1 \\ 1 & 0 \end{bmatrix} ... \begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix}$$

e a inversa de A, A^{-1}. A solução procurada é fornecida pela segunda linha da matriz A^{-1}. Assim, pela propriedade *vii* de 2.6.4 e pelo fato de que todas as matrizes do tipo

$$\begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix}$$

possuem determinante igual a $a-1$, temos que, no caso em que n seja par ou n seja ímpar, a matriz A pode ter, respectivamente, determinante igual a 1 ou -1.

Esta generalização pode ser verificada fazendo uma analogia ao algoritmo de Euclides (Teorema 3.2.2), onde

$$a = b \cdot q_1 + r_1$$

$$b = b + r_1 \cdot 0$$

daí, temos que

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} b \\ r_1 \end{bmatrix}$$

e de forma análoga,

$$\begin{bmatrix} b \\ r_1 \end{bmatrix} = \begin{bmatrix} q_2 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\begin{bmatrix} r_{n-2} \\ r_{n-1} \end{bmatrix} = \begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix}$$

$$\implies \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} q_2 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_n & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix}$$

$$= A \cdot \begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix}$$

ademais, como $det \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix} = -1, \forall i \in \{1, ..., n\}$ e pela propriedade *vii* de 2.6.4, segue que

$$detA = (-1)^n$$

logo, A é inversível, pois para todo n o $detA \neq 0$, e portanto, por 6, temos:

$$\begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix} = A^{-1} \cdot \begin{bmatrix} a \\ b \end{bmatrix}$$

Por outro lado, sendo $A = \begin{bmatrix} x & y \\ w & z \end{bmatrix}$, destacamos as seguintes possibilidades:

- Se n é par, então $detA = 1$, e daí por 4, tem-se que $A^{-1} = \begin{bmatrix} z & -y \\ -w & x \end{bmatrix}$

$$\Longrightarrow \begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix} = \begin{bmatrix} z & -y \\ -w & x \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix}$$

  e portanto,

$$r_n = (-w)a + xb$$

  ou $r_n = (-r)a + sb$, onde $w = r$ e $x = s$, que seriam as soluções que são obtidas a partir da segunda linha da matriz A^{-1}, estas encontradas nos exemplos vistos anteriormente.

- Se n é ímpar, então $detA = -1$, e daí por 5, tem-se que $A^{-1} = \begin{bmatrix} -z & y \\ w & -x \end{bmatrix}$

$$\Longrightarrow \begin{bmatrix} r_{n-1} \\ r_n \end{bmatrix} = \begin{bmatrix} -z & y \\ w & -x \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix}$$

  e portanto,

$$r_n = wa + (-x)b \quad \text{ou} \quad r_n = ra + (-s)b$$

E com isto, concluímos nosso capítulo, o qual pudemos observar, por meio do método exposto acima e dos exemplos apresentados, que é possível representar matricialmente e de forma prática o algoritmo de Euclides.

4 CRIPTOGRAFIA: CIFRAS DE HILL

4.1 LESTER S. HILL

Lester S. Hill foi um matemático e educador importante na evolução da criptografia, como também um dos maiores contribuidores da criptologia, a ciência que estuda a criação e a quebra de códigos e cifras. Nascido nos Estados Unidos na cidade de Nova York em 18 de janeiro de 1891, formou-se na Universidade da Colômbia, localizada na cidade onde nasceu, e posteriormente na Universidade de Yale onde obteve o seu doutorado. Ele lecionava matemática e astronomia em cinco diferentes escolas dos Estado Unidos. Além disto, Hill também contribuiu com o Exército Americano antes e durante a Segunda Guerra Mundial, compartilhando seus conhecimentos sobre Cifras - uma maneira de representar, por exemplo, códigos na forma escrita, por meio de letras, números e símbolos gráficos - e códigos algébricos modulares com o governo dos EUA.

Figura 2 – Lester S. Hill (1891 – 1956)

Fonte: https://en.wikipedia.org/wiki/Lester_S._Hill. Acesso em: 23 jul. 2020

O interesse de Hill estava voltado para a aplicabilidade da matemática avançada às comunicações, que o levou a desenvolver vários métodos para quebrar erros nas comunicações telegráficas. No ano de 1929 ele criou as cifras de Hill, consideradas cifras de substituição poligráficas, as quais baseavam-se na Álgebra Linear e operações modulares, utilizando de matrizes e multiplicação de matrizes para criptografar e descriptografar mensagens. Após utilizar de seus conhecimentos matemáticos e dedicar grande parte de sua vida para criar e decodificar sistemas de criptografia, Hill morre no dia 16 de maio de 1956 em sua cidade natal aos 70 anos de uma doença desconhecida.

4.2 ARITMÉTICA MODULAR E MATRIZES

Nesta seção apresentaremos algumas definições que nos serão úteis para o estudo das Cifras de Hill, as quais utilizam de operações matriciais e da aritmética modular para a codificação

e decodificação de mensagens. Vale ressaltar que para questões de aprofundamento ver Anton e Rorres (2012), Bezerra (2018), Lemos (2010) e Santos (2006).

4.2.1 Congruência módulo m

Definição 4.2.1 *Seja m um inteiro, com $m > 1$, dizemos que $a, b \in \mathbb{Z}$ são congruentes módulo m se, e somente se, m divide $a - b$. Neste caso $a \equiv b(mod\ m)$. Se m não divide $a - b$, dizemos que a é incongruente a b e escrevemos $a \not\equiv b(mod\ m)$.*

Exemplo 4.2.2 *Temos $7 \equiv 3(mod\ 2)$, pois 2 divide $(7-3)$; $25 \equiv 9(mod\ 4)$, pois 4 divide $(25-9)$; $22 \not\equiv 4(mod\ 8)$, pois $22-4 = 18$ e 8 não divide 18.*

Proposição 4.2.3 *Se $a, b, c \in \mathbb{Z}$, então valem as seguintes propriedades da congruência módulo m:*

*i) $a \equiv a(mod\ m)$. (**Reflexiva**)*

*ii) Se $a \equiv b(mod\ m)$, então $b \equiv a(mod\ m)$. (**Simétrica**)*

*iii) Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $a \equiv c(mod\ m)$. (**Transitiva**)*

Demonstração. *Ver em Santos (2006), pág. 33* ■

Por possuir tais propriedades acima, dizemos que $\equiv$ é uma relação de equivalência no conjunto $\mathbb{Z}$. Portanto vale a seguinte definição:

Definição 4.2.4 *Seja m um número inteiro positivo e $a, b \in \mathbb{Z}$, dizemos que a é equivalente a b módulo m se $a - b$ for um múltiplo de m.*

Daí, dado um inteiro $m > 1$ arbitrário, pelo algoritmo da divisão, temos que $a \in \mathbb{Z}$ é equivalente módulo m a um e somente um dos inteiros $0, 1, 2, ..., m-1$.

Definimos como resíduo de a módulo m o resto da divisão de a por m, onde a é um inteiro não negativo e denotaremos $\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}$ como sendo o conjunto dos resíduos módulo m.

Em nossas aplicações utilizaremos um alfabeto comum de 26 letras, logo trabalharemos com o conjunto $\mathbb{Z}_{26}$, de resíduos módulo 26. Portanto, a seguir mostraremos como encontrar alguns dos recíprocos módulo 26 da Tabela que nos auxiliará em cálculos futuros que nos permitirá descriptografar as nossas mensagens. E para isto, precisamos apresentar algumas definições importantes sobre Congruência Linear.

Denominamos de Congruência Linear em uma varável a uma congruência da forma $ax \equiv b(modm)$, onde x é uma variável.

Teorema 4.2.5 *Sejam $a, b \in \mathbb{Z}_+^*$ e $mdc(a,b) = d$. Se d não divide c, então a equação Diofantina $ax + by = c$ não possui solução inteira. Se d divide c, a equação $ax + by = c$ possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (b/d)n \ \ e \ \ y = y_0 - (a/d)n, \tag{7}$$

onde n é um inteiro qualquer.
Demonstração. *Ver em Santos (2006), pág. 36* ■

O Teorema 4.2.5 acima nos possibilita agora, determinar com o Teorema a seguir quantas são as possíveis soluções incongruentes que a congruência linear $ax \equiv b(mod\ m)$ possui.

Teorema 4.2.6 *Sejam $a, b, m \in \mathbb{Z}$ tais que $m > 1$ e $mdc(a,m) = d$. No caso em que d não divide b a congruência $ax \equiv b(mod\ m)$ não possui nenhuma solução. E no caso em que d divide b a congruência linear possui exatamente d soluções incongruêntes módulo m.*
Demonstração. *Ver em Santos (2006), pág. 37* ■

Definição 4.2.7 *Dizemos que uma solução x_0 de $ax \equiv b(mod\ m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.*

Definição 4.2.8 *Uma solução $\bar{a}$ de $ax \equiv 1(mod\ m)$ é chamada de um inverso de a módulo m.*

Em outras palavras, podemos escrever a definição acima da seguinte maneira:

Definição 4.2.9 *Dado um número $a \in \mathbb{Z}_m$, dizemos que um número $a^{-1} \in \mathbb{Z}_m$ é um recíproco ou inverso multiplicativo de a módulo m se $aa^{-1} \equiv a^{-1}a \equiv 1\ (mod\ m)$.*

Além disso, podemos concluir pelo Teorema 4.2.6 que se $mdc\,(a,m) = 1$ então a possui um único inverso módulo m, o que nos dá a seguinte proposição:

Proposição 4.2.10 *Dizemos que $a \in \mathbb{Z}_m$ é inversível se, e somente se, $mdc(a,m) = 1$.*

Assim, temos que se a e m são primos entre si, então a tem um único recíproco módulo m, caso contrário, a não possui recíproco módulo m.

A proposição a seguir nos mostra quando um inteiro a é o próprio inverso módulo p, onde p é primo.

Proposição 4.2.11 *Seja p um número primo. Então, $a \in \mathbb{Z}_+^*$ é o próprio inverso módulo p se, e somente se, $a \equiv 1\ (mod\ p)$ ou $a \equiv -1(mod\ p)$.*
Demonstração. *Se a é o seu próprio inverso, então temos que $a^2 \equiv 1(mod\ p) \implies p \mid a^2 - 1$ $\implies p \mid (a-1)(a+1)$. Como p é primo, então $p \mid (a-1)$ ou $p|(a+1) \implies a \equiv 1(mod\ p)$ ou $a \equiv -1(mod\ p)$.*
Analogamente, se $a \equiv 1(mod\ p)$ ou $a \equiv -1(mod\ p)$, então $p \mid (a-1)$ ou $p \mid (a+1) \implies$ $p \mid (a-1)(a+1) \implies p \mid a^2 - 1 \implies a^2 \equiv 1(mod\ p)$, ou seja, a é o seu próprio inverso. ■

A partir destas definições e estes resultados, agora podemos encontrar os recíprocos módulo 26, os quais nos serão muito úteis para descriptografar as mensagens utilizadas em nossas aplicações.

Seja $p = 26$. Dentre os números 1, 2, 3, 4, ..., 25, de acordo com a Proposição 4.2.11, apenas os números 1 e 25 são seus próprios inversos módulo 26, pois $1 \equiv 1(mod\ p)$ e $25 \equiv -1(mod\ p)$. Temos também que os números 3, 5, 7, 9, 11, 15, 17, 19, 21 e 23 tem um recíproco módulo 26, pois são todos primos com o 26 e, portanto, pelo Teorema 4.2.6 e pela Proposição 4.2.10 possuem cada um deles, um único recíproco módulo 26. Assim, eles podem ser agrupados nos seguintes pares:

$$3 \times 9 \equiv 1(mod\ 26) \implies 3^{-1} \equiv 9(mod\ 26)$$
$$5 \times 21 \equiv 1(mod\ 26) \implies 5^{-1} \equiv 21(mod\ 26)$$
$$7 \times 15 \equiv 1(mod\ 26) \implies 7^{-1} \equiv 15(mod\ 26)$$
$$9 \times 3 \equiv 1(mod\ 26) \implies 9^{-1} \equiv 3(mod\ 26)$$
$$11 \times 19 \equiv 1(mod\ 26) \implies 11^{-1} \equiv 19(mod\ 26)$$
$$15 \times 7 \equiv 1(mod\ 26) \implies 15^{-1} \equiv 7(mod\ 26)$$
$$17 \times 23 \equiv 1(mod\ 26) \implies 17^{-1} \equiv 23(mod\ 26)$$
$$19 \times 11 \equiv 1(mod\ 26) \implies 19^{-1} \equiv 11(mod\ 26)$$
$$21 \times 5 \equiv 1(mod\ 26) \implies 21^{-1} \equiv 5(mod\ 26)$$
$$23 \times 17 \equiv 1(mod\ 26) \implies 23^{-1} \equiv 17(mod\ 26)$$

O que nos dará a seguinte tabela abaixo:

Tabela 1 – Recíprocos módulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

4.2.2 Congruência e matrizes

A Aritmética Matricial também terá um papel fundamental para decodificar as mensagens por nós utilizadas. A seguir veremos alguns resultados que nos ajudarão a perceber uma analogia existente entre a Aritmética Matricial e a Aritmética Modular.

A partir das definições vistas anteriormente, pode-se concluir que se a matriz A é inversível, e a sua inversa é denotada por A^{-1}. O que nos mostra a relação de equivalência da inversa A^{-1} com o recíproco a^{-1}, e consequentemente, $AA^{-1} = A^{-1}A = I$ com $aa^{-1} \equiv a^{-1}a \equiv 1(mod\ m)$. Relação esta, que nos permite enunciar a seguinte definição abaixo.

Definição 4.2.12 *Seja m um inteiro positivo, dizemos que uma matriz A com elementos em $\mathbb{Z}_m$ é inversível módulo m se existir uma matriz B com elementos em $\mathbb{Z}_m$ tal que $AB = BA = I(mod\ m)$.*

Como vimos, o Teorema 2.7.7 nos possibilita encontrar de maneira simples a inversa de uma matriz inversível de ordem 2. Ao se fazer uma analogia deste resultado com a definição acima, é possível saber quais matrizes são inversíveis módulo 26 e, consequentemente, obter suas inversas. Em outros termos, dizer que uma matriz quadrada A é inversível se, e somente se, $det(A) \neq 0$, significa dizer que $det(A)$ tem um recíproco. Assim, temos o seguinte teorema.

Teorema 4.2.13 *Uma matriz quadrada A com elementos em $\mathbb{Z}_m$ é inversível módulo m se, e só se, o resíduo de $det(A)$ módulo m tem um recíproco módulo m.*

Pela proposição 4.2.10 temos que o resíduo de det(A) módulo m tem um recíproco módulo m se, e só se, esse resíduo e m são primos entre si, e com isso, obtemos o corolário abaixo.

Corolário 4.2.14 *Uma matriz quadrada A com elementos em $\mathbb{Z}_m$ é inversível módulo m se, e somente se, m e o resíduo de $det(A)$ módulo m são primos entre si.*

Como estamos trabalhando em $\mathbb{Z}_{26}$ (o conjunto de resíduos módulo 26) e como 2 e 13 são os únicos fatores primos de $m = 26$, teremos a seguinte definição abaixo, que nos será bastante útil para o nosso estudo em criptografia.

Definição 4.2.15 *Uma matriz quadrada A com entradas em $\mathbb{Z}_{26}$ é inversível módulo 26 se, e somente se, o resíduo de $det(A)$ módulo 26 não é divisível por 2 ou 13, onde a inversa de A $(mod\ 26)$ é dada pela seguinte fórmula*

$$A^{-1}\ (mod\ 26) = det(A)^{-1}\ .\ \begin{bmatrix} z & -y \\ -w & x \end{bmatrix}\ (mod\ 26) \tag{8}$$

onde, $det(A)^{-1}$ é o recíproco do resíduo de det(A) $(mod\ 26)$.

4.3 CRIPTOGRAFANDO UMA MENSAGEM ATRAVÉS DAS CIFRAS DE HILL

Neste tópico trabalharemos especificamente com uma Cifra de Hill de ordem 2. Assim, consideremos uma matriz qualquer de ordem 2, como por exemplo a matriz M abaixo

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

e a seguinte mensagem de texto comum a ser codificada: "Devagar se vai longe". Na aplicação da Cifra de Hill é necessário que a mensagem esteja em letras maiúsculas e que sejam ignorados acentos e espaços. Por exemplo, a nossa frase ficará da seguinte forma: DEVAGARSEVAI-LONGE. Para codificar a mensagem será inicialmente utilizada a correspondência entre números e letras indicada na tabela abaixo:

Tabela 2 – Alfabeto

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

T	U	V	W	X	Y	Z
20	21	22	23	24	25	0

Agora, agrupando o texto comum em pares de letras obtemos:

DE VA GA RS EV AI LO NG EE

Observação: Quando não é possível agrupar todas as letras do texto em pares, podemos repetir a última letra para formar o último par, por isto adicionamos a letra fictícia "E"ao último par.

Utilizando a Tabela 2, tal agrupamento possui os seguintes respectivos equivalentes numéricos:

4 5 22 1 7 1 18 19 5 22 1 9 12 15 14 7 5 5

- Para codificar o par DE, utilizaremos o produto matricial da nossa matriz M com o primeiro par numérico:

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 13 \\ 19 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 19 \end{bmatrix} \ (mod\ 26)$$

Que fornecerá o texto cifrado MS pela Tabela 2

- Para codificar o par VA, utilizaremos o produto matricial da nossa matriz M com o segundo par numérico:

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 22 \\ 1 \end{bmatrix} = \begin{bmatrix} 45 \\ 25 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 25 \end{bmatrix} \ (mod\ 26)$$

Que fornecerá o texto cifrado SY.

Note que o número 45 não possui equivalente alfabético na Tabela 2, solucionamos este pequeno problema substituindo 45 por 19, pois $45 \equiv 19\ (mod\ 26)$. Assim, codificando os demais pares obteremos os seus respectivos pares de textos cifrados:

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 7 \\ 1 \end{bmatrix} = \begin{bmatrix} 15 \\ 10 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 10 \end{bmatrix} \ (mod\ 26) \implies \text{OJ}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 18 \\ 19 \end{bmatrix} = \begin{bmatrix} 55 \\ 75 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 23 \end{bmatrix} \ (mod\ 26) \implies \text{CW}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 5 \\ 22 \end{bmatrix} = \begin{bmatrix} 32 \\ 71 \end{bmatrix} \equiv \begin{bmatrix} 6 \\ 19 \end{bmatrix} \ (mod\ 26) \implies \text{FS}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 1 \\ 9 \end{bmatrix} = \begin{bmatrix} 11 \\ 28 \end{bmatrix} \equiv \begin{bmatrix} 11 \\ 2 \end{bmatrix} \ (mod\ 26) \implies \text{KB}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 12 \\ 15 \end{bmatrix} = \begin{bmatrix} 39 \\ 57 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 5 \end{bmatrix} \ (mod\ 26) \implies \text{ME}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 35 \\ 35 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 9 \end{bmatrix} \ (mod\ 26) \implies \text{II}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 15 \\ 20 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 20 \end{bmatrix} \ (mod\ 26) \implies \text{OT}$$

Coletando todos os pares cifrados obtemos os seguintes pares de letras:

MS SY OJ CW FS KB ME II OT

que seriam normalmente transmitidas como uma única cadeia (sem espaços):

MSSYOJCWFSKBMEIIOT

4.4 DESCRIPTOGRAFANDO UMA CIFRA DE HILL DE ORDEM 2

Ao enviar uma mensagem codificada o destinatário deve enviar uma chave de criptografia para o destinatário para que ele possa decifrar a mensagem. No nosso caso a chave utilizada para criptografar o nosso texto comum foi a matriz

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

Para decifrar a mensagem, primeiro encontraremos a inversa da M(mod 26) :

$$det(M) = xz - yw = (2).(3) - (1).(1) = 5$$

Desta forma, pela Tabela 1 temos:

$$det(M)^{-1} = 5^{-1} = 21\ (mod\ 26)$$

Assim, pela equação 8 da definição 4.2.15 temos:

$$M^{-1} = 21.\begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 63 & -21 \\ -21 & 42 \end{bmatrix} \equiv \begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} (mod\ 26)$$

Conferindo:

$$M.M^{-1} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}.\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} = \begin{bmatrix} 27 & 26 \\ 26 & 53 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod\ 26)$$

Analogamente para $M^{-1}M = I(mod\ 26)$. Portanto $M^{-1} = \begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}\ (mod\ 26)$

Após encontrarmos a matriz inversa M^{-1}, podemos descriptografar a mensagem criptografada MSSYOJCWFSKBMEIIOT obtida anteriormente. Assim, pela Tabela 2, o equivalente numérico do texto cifrado é:

13 19 19 25 15 10 3 23 6 19 11 2 13 5 9 9 15 20

Agora, para encontrarmos os pares do texto comum multiplicamos cada par (vetor) cifrado pela inversa de M $(mod\ 26)$.

- Para decodificar o par MS, utilizaremos o produto matricial:

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}.\begin{bmatrix} 13 \\ 19 \end{bmatrix} = \begin{bmatrix} 238 \\ 369 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 5 \end{bmatrix}\ (mod\ 26)$$

Que fornecerá, pela Tabela 2, o par de texto DE.

Analogamente, para os demais pares temos:

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}.\begin{bmatrix} 19 \\ 25 \end{bmatrix} = \begin{bmatrix} 334 \\ 495 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 1 \end{bmatrix}\ (mod\ 26)$$

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}.\begin{bmatrix} 15 \\ 10 \end{bmatrix} = \begin{bmatrix} 215 \\ 235 \end{bmatrix} \equiv \begin{bmatrix} 7 \\ 1 \end{bmatrix}\ (mod\ 26)$$

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}.\begin{bmatrix} 3 \\ 23 \end{bmatrix} = \begin{bmatrix} 148 \\ 383 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 19 \end{bmatrix}\ (mod 26)$$

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}.\begin{bmatrix} 6 \\ 19 \end{bmatrix} = \begin{bmatrix} 161 \\ 334 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 22 \end{bmatrix}\ (mod 26)$$

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}.\begin{bmatrix} 11 \\ 2 \end{bmatrix} = \begin{bmatrix} 131 \\ 87 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 9 \end{bmatrix}\ (mod 26)$$

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix}.\begin{bmatrix} 13 \\ 5 \end{bmatrix} = \begin{bmatrix} 168 \\ 145 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 15 \end{bmatrix}\ (mod 26)$$

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 9 \\ 9 \end{bmatrix} = \begin{bmatrix} 144 \\ 189 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 7 \end{bmatrix} \ (mod 26)$$

$$\begin{bmatrix} 11 & 5 \\ 5 & 16 \end{bmatrix} . \begin{bmatrix} 15 \\ 20 \end{bmatrix} = \begin{bmatrix} 265 \\ 395 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 5 \end{bmatrix} \ (mod 26)$$

Feito isto, Tabela 2 encontramos, respectivamente, os seguintes equivalentes alfabéticos desses vetores:

DE VA GA RS EV AI LO NG EE

Que fornece, novamente, a mensagem inicial "Devagar se vai longe". E com isto, percebemos que através das Cifras de Hill podemos codificar e decodificar mensagens de maneira relativamente simples ao utilizarmos matrizes.

5 CADEIAS DE MARKOV

5.1 ANDREI ANDREYEVICH MARKOV

Nascido em 14 de Julho de 1856, na cidade de Ryazan, Rússia, Andrei Andreyevich Markov foi o criador das chamadas Cadeias de Markov. Sua criação se deve pelo fato de Markov ser um assíduo leitor de poesias, o qual, através do poema *Eugene Onegin*, de Pushkin, utlizou de suas cadeias afim de analisar as alterações ocorridas nas vogais e consoantes do poema. Entretanto, as Cadeias de Markov que conhecemos atualmente foram vistas pela primeira vez em seu trabalho publicado no jornal russo Izvestiia de 1906.

Figura 3 – Andrei Andreevich Markov (1856 – 1922)

Fonte: https://mathshistory.st-andrews.ac.uk/Biographies/Markov/. Acesso em: 30 mar. 2021

Estudou e posteriormente foi professor na Universidade de São Petersburgo, onde foi um estimado matemático e estudioso das áreas da Análise matemática, Teoria dos números e Probabilidade. Seus trabalhos mais conhecidos são sobre Cadeias de Markov, os quais surgem a partir de seu interesse na teoria da probabilidade, que tinham por foco principal o estudo aprofundado sobre a natureza das matrizes estocásticas. Além disso, Markov teve seu primeiro livro *Ischislenie Veroiatnostei* ou "O Cálculo de Probabilidades", publicado após o ano de 1900, que ficou bastante conhecido em grande parte do ocidente, e recebeu em anos seguintes novas atualizações, sendo a quarta e última edição publicada em Moscou dois anos após sua morte, que foi em 20 de julho de 1922, em São Petersburgo. Atualmente as Cadeias de Markov são utilizadas principalmente para a resolução de problemas dentro da teoria das probabilidades, em áreas como genética, psicologia, biologia, química, teoria quântica, engenharia, entre outras.

5.2 CONCEITOS BÁSICOS DE PROBABILIDADE

O termo probabilidade é derivado da palavra *probare*, que do latim, significa provar ou testar. De modo geral, a teoria da probabilidade envolve o estudo de experimentos aleatórios, seja das ciências humanas, sociais, exatas, ou das mais diversas áreas. Nesta seção apresentaremos, de modo sucinto, alguns conceitos e definições sobre probabilidade, os quais serão relevantes ao

nosso estudo das Cadeias de Markov. Para este breve referencial tórico, utilizamos por base as obras de Hazzan (2004) e Oliveira (1999), as quais sugerimos ao leitor busca-las, vista alguma necessidade de aprofundar o que venha a ser tratado aqui, onde para nós não nos convém fazer no momento.

Definição 5.2.1 *Damos o nome de espaço amostral, ao conjunto formado por todos os resultados possíveis de um experimento aleatório, o qual denotamos por* Ω.

Exemplo 5.2.2 *No lançamento de uma moeda, existe a possibilidade de o resultado ser cara (Ca) ou coroa (Co). Logo, o espaço amostral deste experimento aleatório é dado por* $\Omega = \{Ca, Co\}$.

Definição 5.2.3 *Seja* Ω *o espaço amostral de um determinado experimento aleatório, chamamos de evento todo subconjunto* $A \subset \Omega$.

Exemplo 5.2.4 *Ao lançar-se um dado de 6 faces, obtêm-se o seguinte espaço amostral:* $\Omega = \{1,2,3,4,5,6\}$. *Vejamos alguns eventos:*

A: ocorrência de números pares. $A = \{2,4,6\}$
B: ocorrência de números maiores que 3. $B = \{4,5,6\}$
C: ocorrência de números negativos. $C = \emptyset$ ***(evento impossível)***
D: ocorrência de números positivos. $D = \{1,2,3,4,5,6\}$ *ou* $D = \Omega$ ***(evento certo)***

Dado um experimento aleatório num espaço amostral Ω, a probabilidade de um evento A ocorrer em Ω, é dada pelo quociente entre o número de elementos do evento A e o número de elementos de Ω, ou seja,

$$P(A) = \frac{\text{número de ocorrências de A}}{\text{número total de ocorrências}}$$

Em outros termos, podemos definir a probabilidade de um evento A ocorrer em Ω da seguinte maneira:

Definição 5.2.5 *Seja* Ω *o espaço amostral de um experimento aleatório , a probabilidade de ocorrer o evento* $A \subset \Omega$ *é dado por*

$$P(A) = \frac{n(A)}{n(\Omega)},$$

onde $n(A)$ *é o número de ocorrências(elementos) de A e* $n(\Omega)$ *é o número de ocorrências(elementos) do espaço amostral* Ω.

Axiomas da Probabilidade

i) Para todo evento $A \subset \Omega$ temos $0 \leq P(A) \leq 1$.
ii) Para todo evento certo Ω temos $P(\Omega) = 1$

iii) Para um número qualquer de eventos mutuamente excludentes $A_1, A_2, A_3, ..., A_n \subset \Omega$, temos:

$$P(A_1 \cup A_2 \cup A_3 \cup ... \cup A_n) = P(A_1) + P(A_2) + P(A_3) + ... + P(A_n)$$

Definição 5.2.6 *(**Probabilidade Condicional**) Seja Ω um espaço amostral e consideremos os eventos A e B associados a este espaço amostral. Chamamos de Probabilidade condicional aquela cuja probabilidade de A ocorrer dado que B ocorreu, e é definida da seguinte maneira*

$$P(A|B) = \frac{P(A \cap B)}{P(B)}, \text{ onde } P(B) > 0.$$

Caso $P(B) = 0$, dizemos que a probabilidade de A dado B é indefinido. Desta forma, ao calcularmos $P(A|B)$, o evento B é visto como um novo espaço amostral reduzido dentro do qual, desejamos obter a probabilidade do evento A.

5.3 PROCESSOS ESTOCÁSTICOS E CADEIAS DE MARKOV

Nesta seção apresentaremos definições inerentes ao estudo das Cadeias de Markov. Tais definições serão aprofundadas posteriormente em nossas aplicações, e foram baseadas nas obras de Anton e Rorres (2012), Boldrini (1980), Haggstrom (2002) , Kolman e Hill (2013) e Pellegrini (2015).

Considere um determinado modelo ou sistema que se encontre em um dentre n estados distintos, e que a evolução deste sistema, isto é, a transição de um estado para o próximo estado se dá mediante certa probabilidade, onde tal probabilidade de transição depende apenas do estado atual que este sistema se encontra, quando isto acontece dizemos que é válida a *propriedade de Markov*. A este processo, descrito anteriormente, denominamos *Processo de Markov*, e uma sequência de estados seguindo este processo damos o nome de *Cadeias de Markov*. Por exemplo, podemos modelar o uso das Cadeias de Markov em situações como: as probabilidades de o clima de determinada cidade estar seco, nublado ou chuvoso; uma pessoa pode ser alérgica ou não-alérgica; pode assistir a um determinado canal de televisão A, B ou C; pode comprar um carro da marca Fiat, Ford ou outra. Podemos definir informalmente que uma Cadeia de Markov é um processo cuja probabilidade de um sistema é descrita por diversos estados, os quais possuem certas probabilidades de transição entre eles, para o qual vale a propriedade de Markov.

Propriedade 5.3.1 *(**Propriedade de Markov**) A probabilidade de que o estado seguinte seja i depende apenas do estado atual j, e da probabilidade de transição de j para i.*

Uma Cadeia de Markov também pode ser caracterizada como um *processo estocástico*, o qual definiremos abaixo.

Definição 5.3.2 *Um Processo Estocástico é a maneira pela qual podemos descrever a evolução de diferentes variáveis aleatórias ao longo de um certo instante s.*

Podemos representar o estado de determinado sistema, em um processo estocástico, a partir de um vetor, a este damos o nome de *vetor de estado*. A sequência destes vetores de estado é utilizada para descrever a evolução deste sistema, que dependem cada um, probabilisticamente, do vetor imediatamente anterior.

Definição 5.3.3 ***(Vetor de Estado)*** *Dado um processo estocástico com n estados possíveis, podemos representar a probabilidade de um sistema qualquer, em cada instante s, por meio do vetor de estado $x(s)$, definido da seguinte maneira*

$$x(s) = \begin{bmatrix} x_1(s) \\ x_2(s) \\ x_3(s) \\ \vdots \\ x_n(s) \end{bmatrix},$$

onde $x_1(s)$ é a probabilidade de o sistema estar no estado 1, $x_2(s)$ é a probabilidade de o sistema estar no estado 2, e assim sucessivamente.

Observações:

I) Os vetores de estados podem ser representados em vetores-linha ou vetores-coluna, como pode-se ver na definição anterior, optamos representa-los por vetores-coluna.

II) Um vetor de estado nada mais é do que um vetor de probabilidades, também chamado de *Vetor Estocástico*, pois é aquele que contém todas as probabilidades.

Definição 5.3.4 ***(Vetor Estocástico)*** *Dizemos que $x \in \mathbb{R}^n$ é estocástico se*

i) $\sum_j x_j = 1$

ii) Todos os x_j são não-negativos.

Definição 5.3.5 ***(Matriz Estocástica)*** *Se todas as linhas ou todas as colunas de uma matriz A forem vetores estocásticos, dizemos A é estocástica.*

Caso todas as linhas ou todas as colunas de A forem simultaneamente vetores estocásticos, dizemos que a matriz A é *duplamente estocástica*.

Agora, suponha que para cada $i, j \in \{1,2,3,..., n\}$, seja t_{ij} a probabilidade de que se um sistema, com n estados, está no estado j num instante qualquer, então ele estará no estado i no instante seguinte, isto é, t_{ij} é a chamada *probabilidade de transição* deste sistema. O que nos convêm escrever matricialmente tais probabilidades de transição como $T = [t_{ij}]_{m\times m}$, que é denominada a *Matriz de Transição* do sistema.

Definição 5.3.6 ***(Matriz de Transição)*** *Se para cada par de estados $i, j \in$ {1,2,3,..., n} a probabilidade de transição do estado j para o estado i é t_{ij}, então a matriz de transição T é dada por $T = [t_{ij}]_{m\times m}$.*

Assim, definidos o que são vetores de estado e o que seria uma matriz de transição, podemos então definir de uma maneira mais formal do que vem a ser uma Cadeia de Markov.

Definição 5.3.7 *Uma Cadeia de Markov é um sistema que pode ser descrito por uma sequência de vetores de estado, os quais em uma sucessão de intervalos de tempo, estão relacionados por uma equação da forma*

$$x(\lambda+1) = Tx(\lambda),$$

onde $T = [t_{ij}]_{m\times m}$ *é uma matriz de transição e* t_{ij} *é a probabilidade de transição do estado j no instante* $s = \lambda$ *para o estado estado i no instante* $s = \lambda + 1$.

Exemplo 5.3.8 *A matriz abaixo é estocástica, e portanto, representa as probabilidades de transição de uma Cadeia de Markov de quatro estados.*

$$T = \begin{array}{c} \text{Estados do sistema no instante } s=\lambda \\ \textbf{(Estado anterior)} \\ \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 0,1 & 0,2 & 0,5 & 0,4 \\ 0,2 & 0,6 & 0,2 & 0,1 \\ 0,5 & 0,1 & 0,1 & 0,1 \\ 0,2 & 0,1 & 0,2 & 0,4 \end{bmatrix} \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} \end{array} \quad \begin{array}{l} \text{Estados do sistema no instante } s=\lambda+1 \\ \textbf{(Novo estado)} \end{array}$$

onde, o elemento t_{11} *= 0,1, é a probabilidade de que o sistema permaneça estado 1 quando está no estado 1; o elemento* t_{12} *= 0,2, é a probabilidade de transição do estado 2 para o estado 1; o elemento* t_{21} *= 0,2, é a probabilidade de transição do estado 1 para o estado 2; E assim por diante.*

Para entendermos melhor, vejamos a seguir um exemplo simples de como podemos utilizar as Cadeias de Markov para modelar situações cotidianas e de áreas diversas.

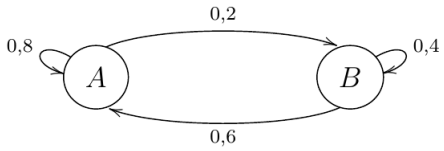
Exemplo 5.3.9 *Suponhamos que uma editora brasileira tem o controle de 30% do mercado de livros. Em certo momento, esta editora resolve contratar uma empresa de publicidade para prever os efeitos que uma campanha de propaganda traria com relação a venda seus produtos. Terminada a campanha a editora concluiu que:*

- Alguém comprando livros da editora A, continuará comprando na editora A com a probabilidade de 80%.

- Alguém não comprando livros da editora A irá migrar para a editora A com probabilidade de 60%. Digamos que o consumo médio de um consumidor é de um livro por mês.

- Chamaremos de A todos aqueles que compram livros da editora A.

- Chamaremos de B aqueles que compram livros de outra editora O Diagrama de transição a seguir, nos permite observar melhor o que está ocorrendo com as probabilidades deste sistema:



E a transição de estados desta Cadeias de Markov serão representadas pela seguinte matriz de transição:

$$T = \begin{array}{c} \begin{array}{cc} A & B \end{array} \\ \left[\begin{array}{cc} 0,8 & 0,6 \\ 0,2 & 0,4 \end{array}\right] \begin{array}{c} A \\ B \end{array} \end{array}$$

Sabendo disto, qual a probabilidade de alguém utilizando a marca A continuar utilizando a marca A após 3 meses da campanha publicitária ($M(3)$)?
Solução: *A Matriz de distribuição de estado inicial abaixo representa a divisão do mercado de livros antes da campanha.*

$$M(0) = \left[\begin{array}{c} 0,3 \\ 0,7 \end{array}\right]$$

Agora note que, multiplicando T por $M(0)$ obtemos $M(1)$:

$$T \cdot M(0) = \left[\begin{array}{cc} 0,8 & 0,6 \\ 0,2 & 0,4 \end{array}\right] \cdot \left[\begin{array}{c} 0,3 \\ 0,7 \end{array}\right] = \left[\begin{array}{c} 0,66 \\ 0,34 \end{array}\right] = M(1)$$

Com isto, podemos observar que a editora A que possuía 30% do mercado de livros, após um mês de uso da campanha publicitária obterá 66% do mercado de livros. Através da Cadeia de Markov, isto pode ser feito sucessivamente para se obter o domínio de mercado da editora A após 3 meses da campanha publicitária. Vejamos

$$M(2) = \left[\begin{array}{cc} 0,8 & 0,6 \\ 0,2 & 0,4 \end{array}\right] \cdot \left[\begin{array}{c} 0,66 \\ 0,34 \end{array}\right] = \left[\begin{array}{c} 0,732 \\ 0,268 \end{array}\right]$$

$$M(3) = \left[\begin{array}{cc} 0,8 & 0,6 \\ 0,2 & 0,4 \end{array}\right] \cdot \left[\begin{array}{c} 0,732 \\ 0,268 \end{array}\right] = \left[\begin{array}{c} 0,7464 \\ 0,2536 \end{array}\right]$$

E assim, concluímos que a editora A terá o domínio de 74,64% do mercado de livros após 3 meses de campanha.

Se quisermos obter o domínio de mercado da editora A após n meses da campanha publicitária, basta continuarmos o processo de Markov, o que nos daria

$$M(4) = \begin{bmatrix} 0,8 & 0,6 \\ 0,2 & 0,4 \end{bmatrix} \cdot \begin{bmatrix} 0,7464 \\ 0,2536 \end{bmatrix} = \begin{bmatrix} 0,7492 \\ 0,2507 \end{bmatrix}$$

$$M(5) = \begin{bmatrix} 0,8 & 0,6 \\ 0,2 & 0,4 \end{bmatrix} \cdot \begin{bmatrix} 0,74928 \\ 0,25072 \end{bmatrix} = \begin{bmatrix} 0,749856 \\ 0,250144 \end{bmatrix}$$

$$\begin{bmatrix} \vdots \end{bmatrix}$$

$$M(\lambda) = \begin{bmatrix} 0,8 & 0,6 \\ 0,2 & 0,4 \end{bmatrix} \cdot \begin{bmatrix} 0,75 \\ 0,25 \end{bmatrix} = \begin{bmatrix} 0,75 \\ 0,25 \end{bmatrix}$$

Observa-se que a cada novo estado, o consumo de livros da editora A aumenta e se aproxima cada vez mais do vetor de estado

$$M(\lambda) = \begin{bmatrix} 0,75 \\ 0,25 \end{bmatrix},$$

onde os valores não mais se alteram, ou seja, a partir deste mês n, a editora A não ultrapassará os 75% do domínio mercado de livros, quanto as demais editoras não ultrapassarão os 25% do domínio mercado de livros.

De forma prática, é possível encontrar os demais vetores de estado de uma Cadeia de Markov a partir de um estado inicial utilizando potências, especificamente, potências da matriz de transição.

Seja $x(0)$ o vetor de estado inicial de uma cadeia de Markov, os vetores de estados subsequentes deste sistema serão

$$x(1) = Tx(0), \quad x(2) = Tx(1), \quad x(3) = Tx(2), \quad x(4) = Tx(3), ...$$

Em termos de $x(0)$, vetor de estado inicial, como $x(1) = Tx(0)$, podemos expressar os vetores de estados acima de seguinte forma

$$x(2) = T[Tx(0)] = T^2x(0), \quad x(3) = T[T^2x(0)] = T^3x(0), \quad x(4) = T[T^3x(0)] = T^4x(0), ...$$

o que nos dá a seguinte equação

$$x(\lambda) = T^{\lambda}x(0) \tag{9}$$

A qual, nos garante calcular o vetor de estado $x(\lambda)$ sem que haja necessidade de calcular os vetores de estados precedentes.

Exemplo 5.3.10 *Encontre o vetor de estado $x(5)$ de uma cadeia de Markov cujo seguinte vetor de estado inicial e a matriz de transição são:*

$$x(0) = \begin{bmatrix} 0,3 \\ 0,5 \\ 0,2 \end{bmatrix} \quad e \quad T = \begin{bmatrix} 0,2 & 0,1 & 0,5 \\ 0,2 & 0,5 & 0,2 \\ 0,6 & 0,4 & 0,3 \end{bmatrix}$$

Solução: *Utilizando a equação 9, temos que*

$$x(5) = T^5 x(0) = \begin{bmatrix} 0,29592 & 0,29511 & 0,29835 \\ 0,28502 & 0,28745 & 0,28502 \\ 0,41906 & 0,41744 & 0,41663 \end{bmatrix} \cdot \begin{bmatrix} 0,3 \\ 0,5 \\ 0,2 \end{bmatrix} = \begin{bmatrix} 0,296001 \\ 0,286235 \\ 0,417764 \end{bmatrix}$$

Exemplo 5.3.11 *Utilize a equação 9 para encontrar o vetor de estado M(9) do Exemplo 5.3.9, ou seja, qual será o domínio de mercado da editora A após 9 meses da campanha publicitária.*
Solução: *Sabemos que o vetor de estado inicial e a matriz de transição são*

$$M(0) = \begin{bmatrix} 0,3 \\ 0,7 \end{bmatrix} \quad e \quad T = \begin{bmatrix} 0,8 & 0,6 \\ 0,2 & 0,4 \end{bmatrix}$$

Assim, temos que:

$$M(9) = T^9 \cdot M(0) = \begin{bmatrix} 0,75 & 0,75 \\ 0,25 & 0,25 \end{bmatrix} \cdot \begin{bmatrix} 0,3 \\ 0,7 \end{bmatrix} = \begin{bmatrix} 0,75 \\ 0,25 \end{bmatrix} \tag{10}$$

e portanto,

$$M(9) = \begin{bmatrix} 0,75 \\ 0,25 \end{bmatrix}, \tag{11}$$

que coincide com o vetor de estado no qual a Cadeia de Markov começa a se estabilizar, isto é, a partir do décimo mês, os valores não mais se alteram.

Ao vetor encontrado no Exemplo 5.3.11 acima, damos o nome de *Vetor Estacionário*, o qual dada uma Cadeia de Markov $(x(1), x(2), x(3), ...)$, o valor de $x(\lambda)$ converge para um determinado vetor estacionário u quando todos os elementos de $x(\lambda)$ tiverem valores próximos ou iguis dos elementos correspondentes de u tomando n suficientemente grande.

5.3.1 Cadeia de Markov a longo prazo

Até agora vimos mecanismos e conceitos que nos possibilitam compreender como é possível realizar previsões a curto e médio prazo utilizando as Cadeias de Markov. Entretanto, para realizarmos previsões a longo prazo, a matriz de transição T deve satisfazer algumas condições, as quais veremos nas definições a seguir.

Definição 5.3.12 *Chamamos de regular a matriz de transição T, de uma Cadeia de Markov, cujo todos seus elementos de alguma potência de T são não nulos.*

Além disso, podemos considerar uma *Cadeia de Markov regular* aquela na qual sua matriz de transição seja regular.

Exemplo 5.3.13 *Considere as seguintes matrizes estocásticas*

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

- A matriz A é regular,pois $A^2 = \begin{bmatrix} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & \frac{3}{4} \end{bmatrix}$ *tem todos os elementos não nulos.*
- A matriz B não é regular, pois

$$B^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B^3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad B^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

isto é, toda as potência B^λ *terá elementos nulos.*

O teorema abaixo nos mostrará que se a matriz T é regular, então é possível realizar previsões a longo prazo independente de conhecermos o vetor de estado inicial $x(0)$.

Teorema 5.3.14 *Seja* $(x(1),x(2),x(3),...,x(\lambda))$ *uma Cadeia de Markov regular e T a matriz de transição desta, então: i) Quando* $\lambda \to \infty$, T^λ *tende a matriz*

$$M = \begin{bmatrix} u_1 & u_1 & ... & u_1 \\ u_2 & u_2 & ... & u_2 \\ \vdots & \vdots & ... & \vdots \\ u_\lambda & u_\lambda & ... & u_\lambda \end{bmatrix}$$

ii) Todas as colunas de M são iguais, sendo dadas pelo seguinte vetor de probabilidades

$$u = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_\lambda \end{bmatrix},$$

onde $u_1 > 0, u_2 > 0, ..., u_\lambda > 0$ *e* $u_1 + u_2 + ... + u_\lambda = 1$.
iii) $\forall$ *x(0),* $T^\lambda x(0) \to u$ *quando* $\lambda \to \infty$, *tal que u seja um vetor estacionário.*
iv) O vetor estacionário u é único vetor que satisfaz a equação

$$Tu = u \tag{12}$$

Demonstração. *Ver Kolman e Hill (2013), pág. 142 - 143.* ■

No Exemplo 5.3.11 encontramos o vetor estacionário do Exemplo 5.3.9 utilizando potências de $T^\lambda x(0)$ (Ver 9). Entretanto, como vimos a pouco, é possível encontrarmos em

previsões a longo prazo, o vetor estacionário de uma matriz de transição regular de outra maneira, e a parte (iv) do Teorema 5.3.14 acima nos garante isto. Podendo assim, escrever a equação 12 como

$$(I_n - T)u = 0, \tag{13}$$

onde u é um vetor de probabilidades e I uma matriz identidade. E portanto, através desta, podemos encontrar o vetor estacionário.

Exemplo 5.3.15 *Seja a nossa matriz, a matriz de transição do Exemplo 5.3.9, que é*

$$T = \begin{bmatrix} 0,8 & 0,6 \\ 0,2 & 0,4 \end{bmatrix}$$

A Cadeia de Markov é regular pois todos seus elementos são não nulos, e possui também, um único vetor estacionário $u = (u_1, u_2)$. Tal vetor pode ser encontrado resolvendo a equação 12, que pode ser escrita da seguinte maneira

$$\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0,8 & 0,6 \\ 0,2 & 0,4 \end{bmatrix} \right) \cdot \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 0,2 & -0,6 \\ -0,2 & 0,6 \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Esse sistema admite infinitas soluções, e a solução geral é dada por $u_1 = 3a$ e $u_2 = a$, onde a é um numero real arbitrário. Logo o vetor u pode ser escrito como

$$u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} 3a \\ a \end{bmatrix} \tag{14}$$

Entretanto, para que u seja um vetor de probabilidade é preciso que

$$1 = u_1 + u_2 = 4a \Longrightarrow a = \frac{1}{4}$$

Agora, substituindo em 14, obtemos o vetor estacionário

$$u = \begin{bmatrix} \frac{3}{4} \\ \frac{1}{4} \end{bmatrix} = \begin{bmatrix} 0,75 \\ 0,25 \end{bmatrix},$$

o qual coincide com os valores encontrados em 11.

5.4 CADEIAS DE MARKOV NA GENÉTICA

Ao modelarmos os conceitos utilizados nas Cadeias de Markov, torna-se possível estudar diversos problemas ligados a genética. Vejamos como isto pode ocorrer na aplicação a seguir.

Suponha que um gene[1] possua dois alelos[2], A e a. Em uma transmissão genética, um individuo pode possuir um dos seguintes genótipos: dominante, híbrido e recessivo, os quais são dados pelas respectivas combinações de alelos AA, Aa e aa. Ao nascer, um individuo recebe por herança um genótipo, o qual depende do cruzamento do genótipo de seu pai com o genótipo da sua mãe, ou seja, o individuo herda alelos de forma aleatória, um de seu pai e o outro de sua mãe, o que nos dará probabilidades distintas de transmissão genética a cada tipo de cruzamento.

Assim, podemos montar a seguinte matriz T com as probabilidades de cruzamento de cada genótipo representadas por suas colunas:

$$T = \begin{array}{c} \\ AA \\ Aa \\ aa \end{array} \begin{array}{c} \begin{array}{cccccc} \{AA,AA\} & \{aa,aa\} & \{AA,aa\} & \{AA,Aa\} & \{aa,Aa\} & \{Aa,Aa\} \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0,5 & 0 & 0,25 \\ 0 & 0 & 1 & 0,5 & 0,5 & 0,5 \\ 0 & 1 & 0 & 0 & 0,5 & 0,25 \end{bmatrix} \end{array}$$

onde, por exemplo, o elemento $t_{11} = 1$, é a probabilidade do cruzamento de AA com AA resultar em AA, isto é, no cruzamento de indivíduos dominantes resultará somente em proles de genótipos dominantes; o elemento $p_{35} = 0,5$, é a probabilidade do cruzamento de aa com Aa resultar em aa, isto é, no cruzamento de indivíduos de genótipo recessivo com genótipo híbrido tem 50% de chances de resultar em proles de genótipo recessivo; e assim sucessivamente.

Ademais, denominamos como $p_{AA}^{(1)}$, $p_{Aa}^{(1)}$ e $p_{aa}^{(1)}$ as porcentagens de em uma população de indivíduos possuir características dominantes, híbridas e recessivas, respectivamente, na primeira geração. E a probabilidade de cruzamento de alelos de um indivíduo dominante com outro dominante é dada por $p_{AA}^{(1)} \cdot p_{AA}^{(1)}$, que é o mesmo que $(p_{AA}^{(1)})^2$. Por exemplo, se quisermos obter as probabilidades de um cruzamento entre indivíduos de genótipos dominantes e híbridos, basta somarmos $p_{AA}^{(1)} \cdot p_{Aa}^{(1)}$ com $p_{Aa}^{(1)} \cdot p_{AA}^{(1)}$, que analogamente pode ser escrita como $2(p_{AA}^{(1)} \cdot p_{Aa}^{(1)})$. Seguindo o mesmo raciocínio para os demais casos, teremos:

[1] **Gene:** São fragmentos de DNA que carregam informações para a produção de uma determinada proteína ou polipeptídio.

[2] **Alelos:** São genes que se juntam para produzir determinada característica.

Tabela 3 – Probabilidades do Cruzamento entre genótipos

Cruzamentos	**Probabilidades**
$\{AA, AA\}$	$(p_{AA}^{(1)})^2$
$\{aa, aa\}$	$(p_{aa}^{(1)})^2$
$\{AA, aa\}$	$2(p_{AA}^{(1)} \cdot p_{aa}^{(1)})$
$\{AA, Aa\}$	$2(p_{AA}^{(1)} \cdot p_{Aa}^{(1)})$
$\{aa, Aa\}$	$2(p_{aa}^{(1)} \cdot p_{Aa}^{(1)})$
$\{Aa, Aa\}$	$(p_{Aa}^{(1)})^2$

Assim, ao transformarmos as probabilidades apresentadas na tabela acima em uma matriz-coluna, nos permitirá encontrar as porcentagens $p_{AA}^{(2)}$, $p_{Aa}^{(2)}$ e $p_{aa}^{(2)}$, que são as porcentagens dos genótipos que podem ser adquiridos por indivíduos da próxima geração, neste caso a segunda, fazendo uma analogia as Cadeias de Markov ao multiplicar as seguintes matrizes:

$$\begin{bmatrix} p_{AA}^{(2)} \\ p_{Aa}^{(2)} \\ p_{aa}^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0,5 & 0 & 0,25 \\ 0 & 0 & 1 & 0,5 & 0,5 & 0,5 \\ 0 & 1 & 0 & 0 & 0,5 & 0,25 \end{bmatrix} \cdot \begin{bmatrix} (p_{AA}^{(1)})^2 \\ (p_{aa}^{(1)})^2 \\ 2(p_{AA}^{(1)} \cdot p_{aa}^{(1)}) \\ 2(p_{AA}^{(1)} \cdot p_{Aa}^{(1)}) \\ 2(p_{aa}^{(1)} \cdot p_{Aa}^{(1)}) \\ (p_{Aa}^{(1)})^2 \end{bmatrix}$$

Ou seja, multiplicando a matriz T com a matriz obtida da Tabela 3 podemos encontrar as porcentagens da segunda geração, e uma vez encontradas, estas nos possibilitam encontrar também as porcentagens da terceira geração e das gerações subsequentes, basta multiplicar novamente a matriz T pelas porcentagens obtidas da geração anterior. A partir deste método, é possível encontrarmos o perfil genético de qualquer geração. Visto isto, supomos a seguinte situação abaixo.

Problema 5.4.1 *(Adaptado de Boldrini (1980)) Em estudo de campo realizado por biólogos em uma plantação de milho, aplicou-se um tipo específico de inseticida afim de se combater uma determinada espécie de percevejo e que, ao mesmo tempo, não fosse nocivo a plantação. Após a aplicação do produto, notou-se que, dos poucos percevejos que sobreviveram, 90% se mostraram resistentes ao inseticida e 10% deles eram não-resistentes (e haviam sobrevivido por razões casuais). No estudo, sabia-se que esta espécie de percevejo tinha um ciclo de vida de um ano e que ele se reproduzem apenas uma vez em cada geração. Além disso, comprovou-se que a resistência ao inseticida é uma característica dominante. Com estes dados em mãos, os biólogos levantaram a seguinte questão: Qual será a porcentagem de percevejos resistentes ao inseticida*

após dois anos, sabendo que o produto não foi aplicado novamente.

Solução: *Como a resistência ao inseticida é uma característica dominante, os percevejos resistentes podem ter genótipos AA ou Aa na proporção 1:2, ou seja, a cada três percevejos, um pode apresentar a característica dominante e dois a característica híbrida. Assim, 30% dos percevejos são dominantes e 60% são híbridos. Temos, portanto, as porcentagens* $p_{AA}^{(1)} = 0,3$, $p_{Aa}^{(1)} = 0,6$ *e* $p_{aa}^{(1)} = 0,1$, *e assim, a distribuição das porcentagens dos percevejos após um ano é dada por*

$$\begin{bmatrix} p_{AA}^{(2)} \\ p_{Aa}^{(2)} \\ p_{aa}^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0,5 & 0 & 0,25 \\ 0 & 0 & 1 & 0,5 & 0,5 & 0,5 \\ 0 & 1 & 0 & 0 & 0,5 & 0,25 \end{bmatrix} \cdot \begin{bmatrix} (0,3)^2 \\ (0,1)^2 \\ 2[(0,3)\cdot(0,1)] \\ 2[(0,3)\cdot(0,6)] \\ 2[(0,1)\cdot(0,6)] \\ (0,6)^2 \end{bmatrix}$$

$$\begin{bmatrix} p_{AA}^{(2)} \\ p_{Aa}^{(2)} \\ p_{aa}^{(2)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0,5 & 0 & 0,25 \\ 0 & 0 & 1 & 0,5 & 0,5 & 0,5 \\ 0 & 1 & 0 & 0 & 0,5 & 0,25 \end{bmatrix} \cdot \begin{bmatrix} 0,09 \\ 0,01 \\ 0,06 \\ 0,36 \\ 0,12 \\ 0,36 \end{bmatrix}$$

$$\begin{bmatrix} p_{AA}^{(2)} \\ p_{Aa}^{(2)} \\ p_{aa}^{(2)} \end{bmatrix} = \begin{bmatrix} 0,36 \\ 0,48 \\ 0,16 \end{bmatrix}$$

ou seja, as porcentagens da segunda geração de percevejos são $p_{AA}^{(2)} = 0,36$, $p_{Aa}^{(2)} = 0,48$ *e* $p_{aa}^{(2)} = 0,16$. *Obtidas estas, podemos encontrar a distribuição das porcentagens dos percevejos após mais um ano, que é dada por*

$$\begin{bmatrix} p_{AA}^{(3)} \\ p_{Aa}^{(3)} \\ p_{aa}^{(3)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0,5 & 0 & 0,25 \\ 0 & 0 & 1 & 0,5 & 0,5 & 0,5 \\ 0 & 1 & 0 & 0 & 0,5 & 0,25 \end{bmatrix} \cdot \begin{bmatrix} (0,36)^2 \\ (0,16)^2 \\ 2[(0,36)\cdot(0,16)] \\ 2[(0,36)\cdot(0,48)] \\ 2[(0,16)\cdot(0,48)] \\ (0,48)^2 \end{bmatrix}$$

$$\begin{bmatrix} p_{AA}^{(3)} \\ p_{Aa}^{(3)} \\ p_{aa}^{(3)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0,5 & 0 & 0,25 \\ 0 & 0 & 1 & 0,5 & 0,5 & 0,5 \\ 0 & 1 & 0 & 0 & 0,5 & 0,25 \end{bmatrix} \cdot \begin{bmatrix} 0,1296 \\ 0,0256 \\ 0,1152 \\ 0,3456 \\ 0,1536 \\ 0,2304 \end{bmatrix}$$

$$\begin{bmatrix} p_{AA}^{(3)} \\ p_{Aa}^{(3)} \\ p_{aa}^{(3)} \end{bmatrix} = \begin{bmatrix} 0,36 \\ 0,48 \\ 0,16 \end{bmatrix}$$

ou seja, após mais um ano, as porcentagens da terceira geração de percevejos são $p_{AA}^{(3)} = 0,36$*,* $p_{Aa}^{(3)} = 0,48$ *e* $p_{aa}^{(3)} = 0,16$*. Com isto, após dois anos, constatou-se que a porcentagem dos percevejos resistentes ao inseticida será* $p_{AA}^{(3)} + p_{Aa}^{(3)} = 0,36 + 0,48 = 0,84$*, ou seja, 84% da população de percevejos é resistente. Assim, se os biólogos quiserem obter melhores resultados no controle da infestação, será mais eficaz aplicar outro tipo de inseticida, pois este matará no máximo 16% dos percevejos.*

Além disso, com o problema acima podemos observar que após a segunda geração a distribuição de porcentagens entre os genótipos não mais se alteram, isto é, se continuarmos iterando o processo para obter as porcentagens das gerações seguintes encontraremos sempre o mesmo resultado, que será o vetor estacionário desta cadeia de Markov.

6 CONSIDERAÇÕES FINAIS

O Algoritmo de Euclides e o Teorema de Bezout foram representados de forma relativamente simples e prática, e demonstramos que a combinação linear entre dois números inteiros dando o Máximo Divisor Comum entre eles pode ser obtida com a utilização de matrizes e as propriedades importantes da multiplicação e inversão matricial.

As propriedades e operações matriciais e da congruência modular possibilita a codificação e decodificação de mensagens de texto. Observamos que nas Cifras de Hill a matriz tem um papel fundamental, pois é por meio dela que se inicia o processo criptográfico ao utilizarmos uma matriz qualquer como uma chave criptográfica, tornando impossível a interceptação e decodificação da mensagem sem que haja conhecimento da "matriz chave".

Em Cadeias de Markov, as matrizes são utilizadas na representação das chamadas "matrizes de transição", as quais trazem as probabilidades de transição de um estado para o outro de um determinado sistema. O processo Markoviano, é um processo probabilístico que depende apenas do estado em que esse sistema se encontra e o seu estado imediatamente anterior, fato este que nos permite utilizar das Cadeias de Markov para modelar situações diversas. Como exemplo, utilizamos das propriedades básicas da representação e multiplicação matricial que se fazem presentes nas Cadeias de Markov para modelar um problema simples na genética, o que nos permitiu prever a eficácia de um determinado tipo de inseticida sobre as futuras gerações de gafanhotos.

O estudo da Álgebra linear está em constante evolução, assim como aqueles relacionados a aplicabilidade das matrizes, por este fato, torna-se inviável abordar os diversos estudos sobre tal aplicabilidade. Portanto, elencamos nesse estudo, algumas aplicações que remetem relativamente a prática dos conceitos fundamentais da teoria de matrizes.

REFERÊNCIAS

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

BEZERRA, Maria de Nazaré Carvalho. **Teoria dos Numeros**: um curso introdutório. Belém: AEDI/UFPA, 2018.

BOLDRINI, José Luis. **Álgebra linear**. São Paulo: Harper & Row do Brasil, 1980.

BOYER, Carl Benjamim. **História da matemática**. São Paulo: Editora da Universidade de São Paulo, 1974.

CARVALHO, João Bosco Pitombeira de. Uma representação matricial para o algoritmo de euclides. **Revista do Professor de Matemática**, IME-USP-SBM, São Paulo, n. 70, p. 34–36, 2009.

EVES, Howard. **Introdução a história da matemática**. Campinas-SP: Editora UNICAMP, 2011.

HAGGSTROM, Olle. **Finite Markov Chains and Algorithmic Applications**. Cambridge - Inglaterra: Cambridge University Press, 2002.

HAZZAN, Samuel. **Fundamentos de matemática elementar. 5**: combinatória, probabilidade. 7. ed. São Paulo: Atual, 2004.

HOFFMAN, Kenneth; KUNZE, Ray. **Álgebra linear**. São Paulo: USP e Polígono, 1970.

KOLMAN, Bernard; HILL, David R. **Introdução à álgebra linear**: com aplicações. 8. ed. Rio de Janeiro: LTC, 2013.

LAY, David C; CAMELIER, Ricardo; IÓRIO, Valéria de Magalhães. **Álgebra linear e suas aplicações**. 2. ed. Rio de Janeiro: LTC, 1999.

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

MILIES, César Polcino; COELHO, Sônia Pitta. **Números**: uma introdução à matemática. 3. ed. São Paulo: Edusp, 2001.

OLIVEIRA, Francisco Estevam Martins de. **Estatística e probabilidade**: Exercícios resolvidos e propostos. 2. ed. São Paulo: Atlas, 1999.

PELLEGRINI, Jerônimo C. **Álgebra linear**. [s.n.], 2015. v. 130. Disponível em: <https://www.ime.unicamp.br/~deleo/MA327/ld4.pdf>. Acesso em: 12 fev. 2021.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. 3. ed. Rio de Janeiro: IMPA, 2006.