UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT/UNIVASF

Dissertação de Mestrado

CRIPTOGRAFIA NA EDUCAÇÃO BÁSICA: UTILIZAÇÃO DA CRIPTOGRAFIA COMO ELEMENTO MOTIVADOR PARA O ENSINO APRENDIZAGEM DE MATRIZES

por

ANDRÉ LUÍS NERIS DE JESUS

Juazeiro - Bahia - Brasil

Julho - 2013

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT/UNIVASF

ANDRÉ LUÍS NERIS DE JESUS

CRIPTOGRAFIA NA EDUCAÇÃO BÁSICA: UTILIZAÇÃO DA CRIPTOGRAFIA COMO ELEMENTO MOTIVADOR PARA O ENSINO APRENDIZAGEM DE MATRIZES

Dissertação apresentada à Coordenação local do Mestrado Profissional em Rede em Matemática - PROFMAT/UNIVASF, como parte dos requisitos para a obtenção do título de Mestre em Matemática.

Orientador: PROF. DOUTOR SEVERINO CIRINO DE LIMA NETO

Juazeiro - Bahia - Brasil

Julho - 2013

Jesus , André Luís Neris de
J58c Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes/ André Luís Neris de Jesus. - -
Juazeiro, 2013
xii, 70 f. : il ; 29cm

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Vale do São Francisco, Campus Juazeiro, Juazeiro-BA, 2013.

Orientador: Profº. Dr. Severino Cirino de Lima Neto

Banca examinadora: Aníbal Livramento da Silva Netto, Carlos Alberto Raposo da Cunha e Lucília Batista Dantas

Referências.

1. Matemática - Criptografia. 2. Matriz. 3. Educação Básica. I. Título. II. Universidade Federal do Vale do São Francisco.

CDD 511

d

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO

Universidade Federal do Vale do São Francisco

Mestrado profissional em Matemática em Rede Nacional

PROFMAT/UNIVASF

PROFMAT

A criptografia como Elemento Motivador no Ensino de Matrizes

Por

André Luis Néris de Jesus

Dissertação aprovada em dezesete

Prof. Dr. Carlos Alberto Raposo da Cunha
Examinador Externo- UFSJ

Profa. Dra. Lucília Batista Dantas Pereira
Examinadora Externa- UPE

Prof. Dr. Aníbal Livramento da Silva Netto
Examinador Interno- UNIVASF

Prof. Dr. Severino Cirino de Lima Neto
Orientador- UNIVASF

Juazeiro

2013

Agradecimento

A Deus, pela essência da vida.

Aos meus pais Manuel e Antonieta, pelo estímulo ao longo da minha vida.

À minha esposa Lucineide, pelo apoio, incentivo e carinho.

Aos meus filhos João Gabriel e Janaina, pela compreensão nos momentos de ausência.

Aos outros familiares, pelo amor e dedicação para comigo.

Ao meu orientador, pela amizade e orientação, sem as quais esta dissertação não teria sido possível.

Aos professores doutores da banca de qualificação, Aníbal Livramento da Silva Netto, Carlos Alberto Raposo da Cunha e Lucília Batista Dantas Pereira pela leitura carinhosa e cuidadosa e, principalmente, pelas sugestões apresentadas.

A SBM, por viabilizar um mestrado acadêmico em Matemática, com intuito de qualificar os professores de Matemática das escolas públicas de todo o país.

Aos colegas e professores do Mestrado, pela excelente relação pessoal que criamos. Em especial, ao meu grande amigo Levi, pelo apoio durante a confecção desta dissertação.

Agradeço à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES pelo auxílio financeiro.

Enfim, a todos que contribuíram para o sucesso desta dissertação, meu muito obrigado.

RESUMO

Este trabalho teve como objetivo geral investigar a possibilidade de implementar uma sequência didática para o desenvolvimento do tema criptografia, aliado aos conteúdos de matrizes. Para alcançar o objetivo geral da pesquisa foram traçados os seguintes objetivos específicos, como: investigar a relação entre a criptografia e os conteúdos de matrizes da Educação Básica; pesquisar e selecionar sequência didática com o tema criptografia para matrizes; desenvolver atividades aliando o tema criptografia aos conteúdos de matrizes na Educação Básica; implementar a Sequência Fedathi com o conteúdo de matrizes associado a temática da criptografia. Ao longo deste trabalho conceituamos criptografia e todas as terminologias associadas a essa temática, em especial cifras mono e polialfabéticas, esteganografia e etc. Depois foi abordado a parte histórica e sua evolução ao longo dos tempos, dando destaque especial a utilização da criptografia durantes as guerras e sua relação com a informática. Sendo a matemática a principal ferramenta da criptografia, assim foi abordo alguns resultados da matemática, que são de extrema importância para o funcionamento da criptografia, dando ênfase ao estudo das matrizes e aritmética modular. É dado um destaque especial as cifras de Hill, fundamentada matematicamente com a aritmética modular, com um enfoque maior a utilização dos conceitos de matrizes e determinantes para criptografar e decifrar as mensagens. Por fim, descreve-se uma Sequência Fedathi para alunos do Ensino Médio, abordando os conteúdos de matrizes e utilizando a criptografia para facilitar o ensino aprendizagem da matemática. A metodologia pedagógica tem como base a aprendizagem por resolução de problemas explorados, na qual são categorizados os níveis de desenvolvimento do pensamento lógico, que uma pessoa utiliza quando é solicitada a resolver um problema.

Palavras-Chave: Criptografia; Aritmética modular; Matriz; Educação Básica; Sequência Fedathi.

ABSTRACT

This study investigated the possibility to implementing a teaching sequence method for development of the encryption theme, associated to the matrices contents. The general objective had alcanced following specific objectives such as: to investigate the relationship between encryption and the Basic Education matrices content; to research and select instructional sequence with the theme encryption for matrices; to develop activities associated the encryption contents to the Basic Education matrices; to implement the Fedathi Sequence with the matrices content associated with the encryption theme. In this paper we conceptualize cryptography and all terminologies connect with this subject, in particular mono ciphers and polyalphabetic, steganography, etc. Then was went aboarded the historic part and its evolution over time, giving special emphasis to the use of encryption during the wars and their reaction with the informatics. The mathematics is the main tool of the cryptography. Therefore, it was approached some mathematics results, which are extremely important for the encryption operation, emphasizing the study of matrices and modular arithmetic. It is given a special focus to the Hill ciphers, based on the modular arithmetic mathematically, with a greater focus to the use of the matrices and determinants to encrypt concepts and decrypt messages. So, we describe a Fedathi Sequence for high school students, addressing the matrices contents , sing the encryption to facilitate the mathematics teaching and learning process. The teaching methodology has based on the resolution learning problems explored, which are categorized on the development levels of the logical thinking, that a person uses when asked to resolute a problem.

Keywords: Encryption; Modular Arithmetic; Matrix; Basic Education; Sequence Fedathi.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Motivação

Com o advento da Matemática Moderna (nas décadas de 1960 e 1970) os livros didáticos, sob influência desse paradigma, privilegiavam a conceituação em detrimentos das aplicações, desse modo a formação dos alunos em matemática ficava pautada em uma concepção extremamente voltada para a matemática pura. No entanto, a Matemática Moderna fracassou por dar muita ênfase a parte conceitual e formal da matemática. A fim de familiarizar gradativamente os alunos com o método matemático, deve dotá-los de habilidades para lidar desembaraçadamente com os mecanismos do cálculo e dar-lhes condições para mais tarde saber utilizar seus conhecimentos em situações da vida real, o ensino da matemática deve abranger três componentes fundamentais, que chamaremos de conceituação, manipulação e aplicações.

A manipulação é, dos três, o componente mais difundido nos livros-texto adotados nas escolas. Consequentemente, predominam - nas salas de aula, nas listas de exercícios e nos exames as operações com elaboradas frações numéricas ou algébricas, - os cálculos de radicais, as equações com uma ou mais incógnitas, as identidades

trigonométricas e vários outros tipos de questões que, embora necessárias para o adestramento dos alunos, não são motivadas, não provêm de problemas reais, não estão relacionadas com a vida atual, nem com as demais ciências e nem mesmo com outras áreas da matemática (LIMA, 1999).

Diante de um panorama em que os livros didáticos de matemática dão muita ênfase a parte manipulativa da matemática. Como fica evidenciado no livro Exame de Textos - Análise de Livros de Matemática para o Ensino Médio os autores consideram que a falta de aplicações é considerada como o grande problema dos livros didáticos brasileiros (LIMA, 2001).

E como a criptografia possibilita interligar os conteúdos matemáticos à situações do mundo real, e ajuda a desenvolver habilidades e competências na resolução de problemas, a criar estratégias de resolução, a ter autonomia durante o processo de aprendizagem (GROENWALD e FRANKE, 2008).

A carência de aplicações nos livros de matemática e tendo a criptografia como um tema relacionado ao dia a dia foram as motivações para pensar em como aplicar metodologia que envolva os conteúdos matemáticos no Ensino Médio com o tema criptografia.

1.2 Objetivos

Este trabalho teve como objetivo geral investigar a possibilidade de implementar uma Sequência Didática para o desenvolvimento do tema criptografia aliado aos conteúdos de matrizes.

Para alcançar o objetivo geral da pesquisa foram traçados os seguintes objetivos

específicos: investigar a relação entre a criptografia e os conteúdos de matrizes da Educação Básica; pesquisar e selecionar sequência didática com o tema criptografia para matrizes; desenvolver atividades aliando o tema criptografia aos conteúdos de matrizes na Educação Básica; implementar a Sequência Fedathi com o conteúdo de matrizes associado a temática da criptografia.

1.3 Metodologia

A metodologia de pesquisa adotada foi a Sequência Fedathi (SF), a qual é uma proposta metodológica desenvolvida por professores, pesquisadores e alunos de pós-graduação da Faculdade de Educação da Universidade Federal do Ceará - UFC, integrantes do Grupo de Pesquisa Fedathi que, em meados dos anos 90, se reuniram com o intuito de discutir sobre questões relativas à didática da matemática (BORGES NETO e SANTANA, 2003).

Ela se baseia no ensino por resolução de problemas explorado por George Polya, nos anos 70, e, inicialmente, foi desenvolvida para o ensino de matemática, mas atualmente é utilizada de forma mais abrangente, em outras áreas, como o ensino de ciências e o ensino assistido por computador. A maior diferença entre a proposta metodológica de Fedathi e a de Polya (1978) está no fato que esta é centrada no indivíduo, enquanto a Sequência Fedathi é centrada na mediação que deve ocorrer entre o professor e alunos.

Esta metodologia pedagógica tem como base a aprendizagem por resolução de problemas explorados, na qual são categorizados os níveis de desenvolvimento do pensamento lógico, que uma pessoa utiliza quando é solicitada a resolver um problema. Sua aplicação divide-se nas seguintes fases: tomada de posição,

maturação , solução e prova.

Esta metodologia se apresenta esquematizada em quatro níveis assim especificados:

- nível 1: tomada de posição - apresentação do problema neste nível, o professor apresenta o problema para o aluno, que deve ter como um dos meios para sua resolução a aplicação do conhecimento a ser ensinado. Para apresentar o problema, o docente deve realizar um diagnóstico inicial, a fim de identificar o nível de conhecimento do grupo, principalmente no que diz respeito aos pré-requisitos necessários para o que pretende trabalhar;
- Nível 2: Maturação - compreensão e identificação das variáveis envolvidas no problema destinado à discussão entre o professor e os alunos, a respeito do problema em foco; os alunos devem buscar compreender o problema e tentar identificar os possíveis caminhos que possam levar a uma solução;
- Nível 3: Solução - apresentação e organização de esquemas/modelos que visem à solução do problema aqui, os alunos deverão organizar e apresentar soluções, que possam conduzi-los a encontrar o que está sendo solicitado no problema; esses modelos podem ser escritos em linguagem matemática, ou, simplesmente, através de desenhos, esquemas ou mesmo por meio de verbalizações;
- Nível 4: Prova - apresentação e formalização do modelo matemático a ser ensinado Neste último nível, a didática do professor é determinante para a aquisição do conhecimento por parte dos

> alunos, pois além de ter que manter a atenção e a motivação do grupo, ele deverá fazer uma conexão entre as respostas apresentadas pelos alunos e o modelo científico; deverá introduzir o novo saber através de sua notação simbólica em linguagem matemática.

Borges Neto (2001) indicam que a Sequência Fedathi é uma proposta de trabalho com olhos na formação do professor, e ressaltam a necessidade das seguintes habilidades: hábito de estudo da matemática; costume de estudo em grupo com outros professores de matemática; praxe de observar, ouvir e motivar os alunos para que eles possam desenvolver as atividades propostas na Sequência Fedathi; e disposição constante de anotar novas soluções apresentadas pelos alunos, para que possam permitir reformular o planejamento do professor, bem como a aplicação da Sequência Fedathi.

1.4 Apresentação do Trabalho

Este trabalho apresenta a criptografia como uma aplicação que pode ser usada nas aulas de matemática da Educação Básica, por apresentar aplicações de tópicos da disciplina, que permitem que ela seja explorada e adaptada a atividades na sala de aula.

No capítulo dois faz-se um breve resumo do uso da criptografia ao longo do tempo, desde sua utilização militar até as aplicações na era da computação. Mostraremos a história da codificação de mensagens e descreveremos a evolução das técnicas utilizadas, o processo evolutivo das diversas formas de criptografia, desde a antiguidade até os dias atuais.

No capítulo três, da revisão bibliográfica, definimos e explicamos conceitos da

criptografia básica, dando destaque ao funcionamento dos métodos de cifragem por substituição e transposição, criptografia de chave simétrica e assimétrica. Também é evidenciado como podemos utilizar a criptografia na Educação Básica.

O capítulo quatro destina-se a introduzir os conteúdos matrizes e determinantes destacando suas definições, propriedades e principais teoremas. Em seguida, é dada a noção de congruência, através de exemplos de aplicações e mostrar suas propriedades. Congruência é a relação entre dois números, que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto. Este assunto possui muitas aplicações no cotidiano das pessoas, como: criptografia, códigos de barras, CPF, CNPJ, ISBN, ISSN, calendários e diversos fenômenos periódicos. É um tema bastante atual e que pode ser trabalhado já na Educação Básica, possibilitando excelente oportunidade de contextualização no processo de ensino/aprendizagem de matemática.

O capítulo cinco estudamos a criptografia utilizando matrizes e uma classe de sistemas poligráficos, chamados cifras de Hill como motivador de situações problema para alunos no Ensino Médio. Apresentamos, também, exemplos sobre como criptografar e decifrar uma mensagem, através da cifra de Hill, relacionando com os conteúdos de matrizes e congruência.

O capítulo seis trata da aplicação da Sequência Fedathi de uma aula de matrizes, tendo a criptografia como elemento motivador para a aula.

Por fim, a conclusão, é feita uma análise geral do trabalho, sobretudo com relação aos objetivos propostos na dissertação.

Capítulo 2

História

2.1 Aspectos Gerais

Para indicar a importância da criptografia ao longo do tempo Singh (2003) diz: "A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de código e os decifradores, uma corrida armamentista intelectual que teve um forte impacto na história humana". A partir desta citação, descreveremos uma série de episódios nos quais estavam presente o uso da criptografia.

Os primórdios da criptografia remonta aos egípcios que, por volta de 4000 a.C., utilizavam hieróglifos para cifrar alguns de seus documentos. De acordo com Du Sautoy (2007), o exército espartano já utilizava criptografia no século V a.C. Nesse processo, o emissor e o receptor da mensagem possuíam cilindros com as mesmas dimensões, chamados de cítalas. Para codificar uma mensagem, o emissor inicialmente enrolava uma faixa de pergaminho ao redor da cítala, de modo que espiralasse o cilindro. Depois, escrevia a mensagem sobre o pergaminho, ao longo do comprimento da cítala. Desenrolando-se o pergaminho a mensagem fica codificada. Para decifrar a mensagem era necessário, que o receptor tivesse, uma cítala de mesmo

diâmetro para enrolar a tira de couro e ler a mensagem.

Outro evento, relacionado à guerra remonta à época das Guerras da Gália de Júlio César e de acordo com Singh (2003) César, descreve como enviou uma mensagem para Cícero, que estava cercado e prestes a se render. Ele substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem incompreensível para o inimigo. Outro exemplo de cifra utilizada por Júlio César consistia em substituir cada letra da mensagem original por outra que estivesse três posições à frente no mesmo alfabeto, como pode ser visto na tabela 2.1. Dessa forma, César utilizava o alfabeto normal para escrever a mensagem, e o alfabeto cifrado era utilizado para codificar a mensagem que posteriormente seria enviada. Esse método de criptografia ficou conhecido como Cifra de César.

Alfabeto Nornal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabela 2.1: **Método de substituição utilizado por Júlio César. Fonte: Singh (2003).**

Nesse panorama, as cifras de César se enquadram como as cifras de substituição monoalfabéticas e, não são seguras, pois possui 25 chaves em potencial. Logo, ao ser interceptada, se desconfiarem que o método utilizado foi a Cifra de César era necessário verificar 25 possibilidades para decifrar a mensagem, o que a torna uma cifra simples de decodificar. Outro elemento que torna as cifras de substituição inseguras é a possibilidade de utilizar o método de decifração, baseado no estudo da frequência das letras de um determinado alfabeto.

Por conta destas facilidades em conseguir decifrar a mensagem interceptada foi que surgiu a necessidade de criar novas cifras, mais elaboradas e mais difíceis de

serem descobertas. A solução encontrada, no século XVI, pelo diplomata francês Blaise Vigenère, foi uma cifra de substituição polialfabética (SINGH, 2003). Essa cifra foi denominada Cifra de Vigenère, e utiliza 26 alfabetos cifrados diferentes, para cifrar uma mensagem, como pode ser visto na tabela 2.2.

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

Tabela 2.2: **Quadro de Vigenère. Fonte: Singh (2003).**

Para decifrar a mensagem, o destinatário precisa saber que alfabeto usar para cada letra da mensagem, e isso é previamente informado por uma palavra-chave. A enorme vantagem da cifra de Vigenère é que ela é imune à análise de frequências; por esse fato, ficou conhecida, por quase dois séculos, como a "cifra indecifrável". Mesmo sendo tão mais complexa, a cifra de Vigenère foi quebrada pelo matemático inglês Charles Babbage, por volta de 1850, que fez um estudo do padrão que a palavra-chave criava ao ser repetidamente utilizada, ao longo do texto.

Com a utilização de métodos estatísticos fica fácil quebrar os códigos da cifras de substituição. Uma maneira de superar esse problema foi dividir o texto em grupos

de letras, e criptografar o texto comum por grupos, em vez de uma letra de cada vez. Um dos métodos de criptografar, que utiliza essa ideia, é a chamada Cifra de Hill, que se utiliza de transformações matriciais e de um sistema poligráfico, o qual é um sistema de criptografia, em que o texto comum é dividido em conjuntos de n letras. Essa cifra recebeu esse nome, pois faz referência a Lester S. Hill, que introduziu esse sistema em dois artigos escritos em 1929 e 1931: "Cryptography in the Algebraic Alphabet", e "Concerning Certain Linear Transformation Apparatus of Cryptography" (HOWARD e RORRES, 2001).

2.1.1 Criptografia e a 2ª Guerra Mundial

Já no século passado, durante a Segunda Guerra Mundial, a comunicação entre os alemãs no fronte de batalha utiliza-se de criptografia, no entanto, as mensagens eram criptografadas utilizando a máquina enigma, que fora desenvolvida especialmente para cifrar mensagens sendo usada pelos alemãs, para proteger as comunicações entre os comandos e as embarcações navais.

Malagutti et al(2012, p.72) descreve de forma sucinta como como funciona a Máquina Enigma:

> Uma letra do texto é pressionada no teclado, uma corrente elétrica passa pelos diversos componentes de cifragem da máquina, acendendo uma luz no "painel de lâmpadas", a letra acendida é a codificação da letra digitada. E cada vez que uma letra é pressionada, as peças móveis da máquina mudam de posição e, se numa próxima vez que a mesma letra for teclada, provavelmente será cifrada como algo diferente.

Dessa forma, o uso dos métodos tradicionais de análise da frequência de letras não eram suficientes para conseguir decifrar a mensagem. Ela tinha como diferencial ser elétrico-mecânica e, funcionando com três a oito rotores. Quando o usuário pressionava uma tecla, o rotor da esquerda avançava uma posição, provocando a

rotação dos demais rotores à direita, sendo que esse movimento dos rotores gerava diferentes combinações de encriptação. Dessa forma, a codificação da mensagem pela Máquina Enigma era muito difícil decodificação, pois era necessário ter outra máquina dessas e saber qual a chave utilizada para realizar a codificação.

E seu processo para decifrar mensagem é descrito por Malagutti et al(2012, p.81) da seguinte forma:

> O processo de decifração da máquina enigma é extremamente simples, desde que o receptor da mensagem saiba como o equipamento foi configurado quando a mensagem foi criptografada. O soldado ao receber uma mensagem cifrada tinha apenas que digitar as letras cifradas em sua própria máquina. Se sua máquina tivesse configurada exatamente da mesma forma como a do remetente da mensagem, as letras que apareceriam no painel de lâmpadas formariam o texto original.

Este tipo de criptografia é conhecido como criptografia simétrica, porque a operação de decifrar é inversa à operação de cifrar. A chave de decodificação é também a mesma chave de codificação.

A segurança da máquina enigma estava no fato de que era impossível calcular rapidamente a chave dentre bilhões de possibilidades. No entanto, nesse período, um matemático, Alan Turing e sua equipe, tiveram um papel relevante, pois desenvolveram o primeiro computador operacional para o serviço de inteligência britânico, chamado de Colossus. Era um gigantesco computador, projetado especialmente para decifrar mensagens cifradas pela máquina enigma, que utilizava tecnologia de relés, e que podia ler 5.000 letras por segundo, através de um sistema fotoelétrico, e todas as possíveis combinações de mensagens codificadas eram comparadas com as mensagens geradas pelas chaves criptográficas do Colossus, para revelar a configuração da máquina usada pelos alemães.

Figura 2.1: **Ilustração da Máquina Enigma. Fonte: Malagutti et al. (2012)**

2.1.2 Criptografia e Informática

Em 1976, Bailey Whitfield Diffie e Martin Edward Hellman publicaram um artigo denominado "New Directions in Cryptography", no volume 22 da revista IEEE Transactions on Information Theory. Neste artigo descreveram o primeiro método para trocar uma chave secreta entre dois agentes, usando um canal público. O trabalho de Diffie e Hellman foi um marco na criptografia, e abriu as portas para a criptografia de Chave Pública (FALEIROS, 2011).

Até meados da década de 1970, a transmissão de mensagem fazia uso exclusivamente de chaves privadas para criptografar e decifrar mensagens. Em 1976, uma mudança de paradigma ocorreu quando Diffie e Hellman propuseram o uso de chaves públicas. Em 1978, foi inventado o mais conhecido dos métodos de criptografia de chave pública, o RSA sendo Rivest, Shamir e Adleman os seus criadores. As letras RSA correspondem as iniciais dos inventores do código. Existem outros códigos de chave pública, mas o RSA é o mais utilizado em aplicações comerciais (COUTINHO, 2011).

Atualmente, a criptografia é largamante utilizada na internet, em segurança a fim de autenticar os usuários para lhes fornecer acesso aos sites e possibilitar proteção de transações financeiras e em comunicação.

Neste breve resumo histórico, percebemos o quanto a criptografia evoluiu e as formas de enviar mensagem mudaram durante séculos, desde a antiguidade. Foram usadas tatuagens nos corpos dos escravos, invenção de sinais, linguagens secretas, pinturas, conversas em particular, troca de sinais, etc. Mas o desenvolvimento da ciência e da tecnologia causaram grandes mudanças nas formas de transmitir as mensagens, e assim apareceram formas modernas de enviar mensagens e transmitir informações. Tanto que, atualmente, as chamadas telefônicas transitam entre satélites, nossos e-mail passam por diversos computadores e o comércio eletrônico se populariza com o advento da internet. E com a criptografia podemos garantir que há privacidade nas comunicações. Nesse panorama histórico a matemática tem muita importância e de acordo com Singh (2003, p.13):

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação.

Capítulo 3

Revisão Bibliográfica

Este capítulo apresenta a referência bibliográfica da pesquisa, as terminologias, história e aplicações da criptografia, a importância do tema criptografia para o desenvolvimento da atividade didática para o ensino de matemática no Ensino Médio, procurando associar a criptografia com os conteúdos de matriz e determinante.

3.1 Definições

De acordo com Tkotz (2005), Cripto vem do grego kryptos e significa esconder, ocultar. Grafia também vem do grego graphein, e significa escrever. Criptografia, portanto, significa escrita oculta ou escrita secreta. Para Coutinho (2011), a criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. Já a comunicação secreta, quando é obtida através da ocultação da mensagem, é conhecida como esteganografia, nome derivado das palavras gregas steganos, que significa coberto, e graphein, que significa escrever.

Enquanto que para Shokranian (2012), a criptografia e a teoria dos códigos são ramos distintos e servem para propósitos diferentes. Enquanto na criptografia a principal questão é como transmitir uma mensagem da fonte A para uma fonte B, de modo que as fontes não autorizadas não tenham acesso ao conteúdo da mensagem; a teoria dos códigos a preocupação está em transmitir informações da fonte A para a fonte B, com segurança, para que a fonte B possa recebê-la corretamente. Portanto, na transmissão de uma informação existem dois tipos de segurança: a segurança contra fontes não autorizadas, que pertencem à criptografia, e a segurança contra danificação da informação, que pertence a teoria dos códigos.

Para Howard e Rorres (2001), as mensagens não codificadas são os textos comuns, e as mensagens codificadas são textos cifrados ou criptogramas. Já o processo de converter um texto comum, em cifrado, é denominado cifrar ou criptografar, e o processo inverso de converter um texto cifrado em comum é chamado decifrar.

A técnica de manter mensagens seguras é chamada de criptografia. A técnica de tentar descobrir o conteúdo de mensagens cifradas é chamada de criptoanálise, e seus praticantes são chamados de criptoanalistas. E o conjunto destas duas técnicas é chamado de criptologia. A cifra é o nome dado a qualquer forma de substituição criptográfica, no qual cada letra é substituída por outra letra ou símbolo. Cada cifra pode ser considerada em termos de um método geral de codificação conhecido como algoritmo e uma chave, que especifica os detalhes exatos de uma codificação em particular. Neste caso, o algoritmo consiste em substituir cada letra do alfabeto original por uma letra do alfabeto cifrado, e o alfabeto cifrado pode consistir em qualquer rearranjo do alfabeto original. A chave define o alfabeto cifrado exato que será usado em uma codificação em particular (SINGH, 2003).

3.1.1 Cifras de Substituição e Transposição

No estudo das cifras, o fundamental é o ocultamento da informação, há uma unidade básica de substituição formada por letras ou símbolos, isolados ou agrupados, e os métodos de cifrar são divididos segundo sua natureza: métodos de cifragem por substituição e método de cifragem por transposição. No primeiro método, troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição. Já o segundo método, os conteúdos das mensagens não codificada e criptografada são os mesmos, porém as letras são postas em ordem diferente (permutadas). No método da transposição, ocorre apenas um embaralhamento das letras, dispostas em uma ordem predeterminada para cifrar e decifrar. A transposição faz com que cada letra mantenha sua identidade, mas muda sua posição (MALAGUTTI et al.,2010).

Já a cifra de substituição monoalfabética é o nome dado a qualquer cifra de substituição, na qual o alfabeto cifrado pode consistir em símbolos, assim como letras ou símbolos. E a cifra substituição polialfabética é uma técnica que permite que diferentes símbolos cifrados possam representar o mesmo símbolo do texto claro.

3.1.2 Classificação da Criptografia quanto às Chaves

A criptografia, de chave simétrica, possui este nome porque os processos de criptografar e decifrar são realizados com uma única chave, ou seja, tanto o emissor quanto o receptor detêm a mesma chave, e esta deve ser mantida em segredo para que se possa garantir a confidencialidade das mensagens ou da comunicação.

A criptografia assimétrica, mais conhecida como criptografia de chave pública, utiliza uma par de chaves denominadas chave privada e chave pública. Qualquer uma das chaves podem ser usada para criptografar os dados, porém a mesma não pode ser usada para, decifrá-lo, ou seja, se a criptografia for realizada com chave púbica, somente a respectiva chave privada poderá decifrar, ou vice-versa. Para que este tipo de criptografia obtenha sucesso é fundamental que a chave privada seja mantida em segredo, enquanto a chave púbica pode, e deve ser divulgada a outros usuários, que desejam se comunicar (STALLINGS, 2008).

3.1.2.1 Criptografia de Chave Simétrica

Na figura 3.1 podemos visualizar o funcionamento da criptografia simétrica. O texto puro é criptografado em texto cifrado pelo emissor, utilizando uma chave secreta. Após ser transmitida, a mensagem cifrada é então decifrada pelo receptor utilizando a mesma chave secreta.

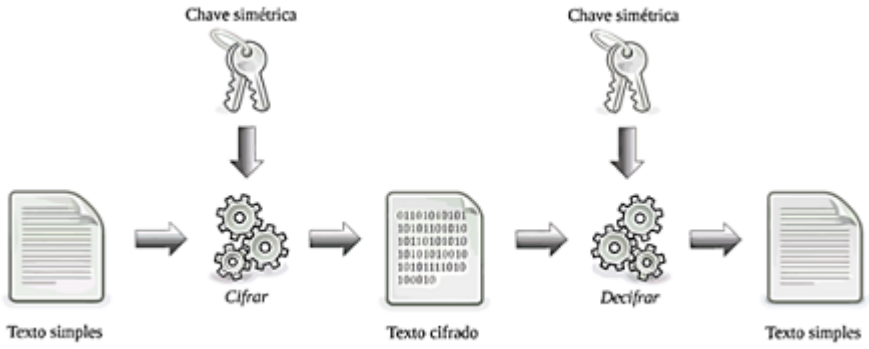


Figura 3.1: **Criptografia Simétrica. Fonte: Pigatto (2012).**

A criptografia de chave simétrica tem como vantagem o fato que os algoritmos, deste tipo, são rápidos e podem operar em tamanhos arbitrários de mensagens. E tendo como desvantagem a dificuldade de gerenciar a chave compartilhada entre o emissor e o receptor, a qual deve ser enviada de modo seguro a todos os usuários autorizados, antes que as mensagens possam ser trocadas e ainda deve ser mantida em segredo (MORENO et al., 2005).

3.1.2.2 Criptografia de Chave Assimétrica

De acordo com Pigatto (2012), a grande vantagem dos sistemas assimétricos é permitir que qualquer um possa enviar a mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chave como é feito no modelo simétrico. A confiabilidade da mensagem é garantida enquanto a chave privada estiver segura. Na figura 3.2 podemos visualizar o funcionamento da criptografia assimétrica. O emissor da mensagem utiliza a chave pública do receptor para criptografar o texto comum em texto cifrado, e após o recebimento do texto criptografado, o receptor utiliza-se da chave privada para decifrar o texto cifrado, dessa forma obtém-se o texto legível.

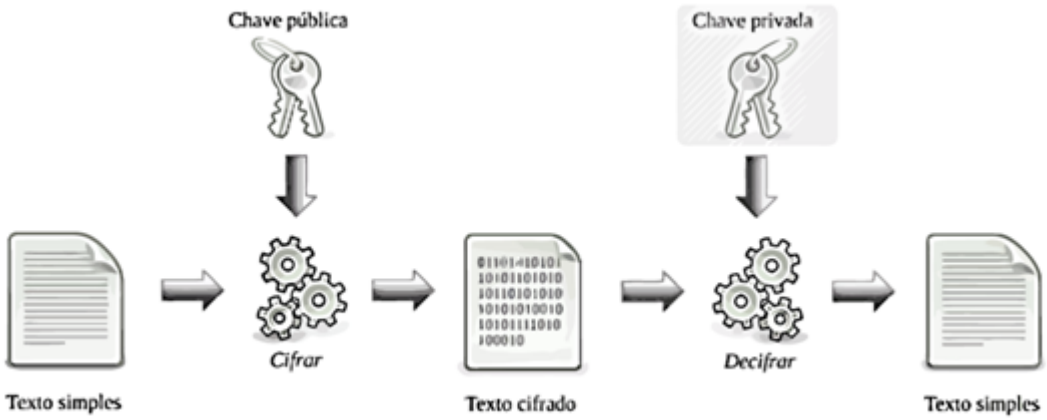


Figura 3.2: **Criptografia Assimétrica. Fonte: Pigatto (2012).**

Devido ao fato de uma chave ser pública e a outra ser mantida em segredo, um criptossistema de chave pública deve atender as seguintes condições:

1. Deve ser possível criptografar ou descriptografar(decifrar) uma mensagem dada a chave apropriada;

2. Deve ser computacionalmente inviável derivar a chave privada a partir da chave pública.

3.2 Criptografia na Educação Básica

A criptografia permite ao professor de matemática da Educação Básica desenvolver atividades didáticas de codificação e decodificação para introduzir conteúdos matemáticos, revisar, reforçar e aprofundar os conteúdos matemáticos. O ensino e aprendizagem da matemática deve ter uma abordagem de assuntos de interesse do aluno, que estimulem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos. O ensino da matemática torna-se interessante quando é desenvolvido de forma integrada e relacionada a outros conhecimentos, trazendo o desafio de desenvolver competências e habilidades formadoras do pensamento matemático. Seguindo esta linha, temos em Olgin (2011) que a criptografia pode ser um recurso didático para trabalhar conteúdos matemáticos, desenvolvidos em sala de aula dentro de um contexto que envolve segurança de dados.

Dessa forma, entendemos que não é possível que a matemática seja trabalhada de forma descontextualizada, fragmentada e repetitiva. E a temática da criptografia pode ser usada como aplicação de conteúdos da Educação Básica de matemática, explorada e adaptada a atividades na sala de aula, e possibilitar ao professor a liberdade de realizar diversas atividades contextualizadas e torna o aluno autônomo

durante o seu processo de ensino e aprendizagem.

Como a criptografia é um assunto importante e interessante no contexto atual, acredita-se que seu uso possa motivar os alunos, ajudando o professor a contornar dificuldades ao tentar estimular seus alunos, no aprendizado e conceitos relacionados com o ensino da matemática. Conforme pode ser evidenciado através dos autores abaixo:

Segundo Tamarozzi (2001), o tema criptografia possibilita o desenvolvimento de atividades didáticas, envolvendo o conteúdo de funções e matrizes que se constituem em material útil para exercícios, atividades e jogos de codificação, onde o professor pode utilizá-los para fixação de conteúdos.

Segundo Groenwald e Franke (2008), esse tema permite interligar os conteúdos matemáticos à situações do mundo real, e ajuda a desenvolver habilidades e competências na resolução de problemas, a criar estratégias de resolução, a ter autonomia durante o processo de aprendizagem e, com isso, tornando-os mais autoconfiantes e concentrados na realização das atividades.

De acordo com Cantoral et al (2000), esse tema pode ser um recurso o qual permitirá ao professor desenvolver atividades didáticas, que proporcionem aulas as quais despertem a atenção e o interesse dos alunos para os conteúdos trabalhados em sala de aula.

Nesse sentido, este trabalho apresenta uma atividade didática com o tema criptografia, que podem ser desenvolvidas no Ensino Médio, levando os alunos a revisitarem conteúdos já estudados, aprimorando seus conhecimentos e ampliando-

os, pois, ao desenvolverem as atividades os estudantes se deparam com novas situações de aprendizagem.

Capítulo 4

Fundamentação Matemática

Nesta seção, vamos abordar as matrizes, determinantes e a aritmética modular, de modo a compreendermos a criptografia com matrizes e cifra de Hill, que serão estudadas no próximo capítulo. Deste modo, não abordaremos o estudo desses conteúdos de uma forma generalizada e alguns resultados terão a demonstração omitida, pois foge ao objetivo deste trabalho.

4.1 Matriz

Nesta seção, serão apresentadas as principais definições e propriedades das matrizes, e determinante segundo Boldrini et al (1984), e Iezzi e Hazzan(2005), que serão usados ao longo desta dissertação para subsidiar criptografia utilizando matrizes.

Chamamos de matriz uma tabela de elementos dispostos em linhas e colunas. Por exemplo, ao recolhermos dados referentes às notas de matemática, física e química de três alunos, podemos dispô-las na tabela 4.1:

	MATEMÁTICA	FÍSCA	QUÍMICA
ALUNO 1	5	8	7,5
ALUNO 2	6,5	6	4
ALUNO 3	10	9,5	7

Tabela 4.1: Quadro de Notas.

Ao abstrairmos os significados das linhas e colunas, temos a matriz:

$$\begin{bmatrix} 5 & 8 & 7,5 \\ 6,5 & 6 & 4 \\ 10 & 9,5 & 7 \end{bmatrix}$$

Os elementos de uma matriz podem ser números(reais ou complexos), funções, ou ainda outras matrizes. Representação de uma matriz de m linhas de n colunas.

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

Usamos sempre letras maiúsculas para denotar matrizes, e quando quisermos especificar a ordem de uma matriz A (isto é, o número de linhas e colunas), escrevemos $A_{m\times n}$.

Para localizar um elemento de uma matriz, dizemos a linha e a coluna (nesta ordem) em que ele está. Por exemplo, na matriz:

$$A_{3\times 2} = \begin{bmatrix} 3 & 5 \\ -7 & 9 \\ 15 & 4 \end{bmatrix}$$

O elemento que está na primeira linha e segunda coluna é 5, isto é, $a_{12} = 5$. Os demais elementos são determinados por $a_{11} = 3, a_{21} = -7, a_{22} = 9, a_{31} = 15, a_{32} = 4$.

Definição 4.1.1 *Duas matrizes* $A_{m\times n} = [a_{ij}]_{m\times n}$ *e* $B_{r\times s} = [b_{ij}]_{r\times s}$ *são iguais,* $A = B$*, se elas têm o mesmo número de linhas* $(m = r)$ *e colunas* $(n = s)$*, e todos os seus elementos correspondentes são iguais* $(a_{ij} = b_{ij})$

4.1.1 Tipos Especiais de Matrizes

Existem algumas matrizes que, pela sua quantidade de linhas ou colunas, ou pela natureza de seus elementos, têm propriedades que as diferenciam de uma matriz qualquer. Além disso, elas aparecem frequentemente na prática e, por isso, recebem nomes especiais. Consideremos uma matriz com m linhas e n colunas que denotamos por $A_{m\times n}$.

- **Matriz Quadrada** é aquela cujo número de linhas é igual ao número de colunas $(m = n)$.

  Exemplo:

$$\begin{bmatrix} -10 & 7 \\ 34 & 101 \end{bmatrix}$$

  No caso de matrizes quadradas $A_{m\times n}$, costumamos dizer que A é uma matriz de ordem m.

- **Matriz Nula** é aquela em que $a_{ij} = 0$, para todo i e j.

Exemplo:

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

- **Matriz Coluna** é aquela que possui uma única coluna ($n = 1$).

  Exemplo:

$$\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

- **Matriz Linha** é aquela em que possui uma única linha ($m = 1$).

  Exemplo:

$$\begin{bmatrix} -16 & 100 \end{bmatrix}$$

- **Matriz Diagonal** é uma matriz quadrada onde $a_{ij} = 0$, para $i \neq j$, isto é, os elementos que não estão na diagonal são nulos.

  Exemplo:

$$\begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 93 \end{bmatrix}$$

- **Matriz Identidade Quadrada** é aquela em que $a_{ii} = 1$ e $a_{ij} = 0$, para $i \neq j$.

  Exemplo:

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

- **Matriz Simétrica** é aquela onde $m = n$ e $a_{ij} = a_{ji}$.

  Exemplo:

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

4.1.2 Operações com Matrizes

Adição

Definição 4.1.2.1 *A soma de duas matrizes de mesma ordem* $A_{m\times n} = [a_{ij}]$ *e* $B_{m\times n} = [b_{ij}]$*, é uma matriz* $m \times n$*, que denotaremos por* $A + B$*, cujos elementos são somas dos elementos correspondentes de* A *e* B*. Isto é,*

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

Exemplo:

$$\begin{bmatrix} -3 & 4 \\ 10 & 17 \end{bmatrix} + \begin{bmatrix} 10 & 0 \\ 8 & 15 \end{bmatrix} = \begin{bmatrix} 7 & 4 \\ 18 & 32 \end{bmatrix}$$

Multiplicação por Escalar

Definição 4.1.2.2 *Seja* $A = [a_{ij}]_{m\times n}$ *e* p *um número, então definimos uma nova matriz*

$$p \cdot A = [pa_{ij}]_{m\times n}$$

Exemplo:

$$-3\begin{bmatrix} 4 & -8 \\ 0 & 13 \end{bmatrix} = \begin{bmatrix} -12 & 24 \\ 0 & -39 \end{bmatrix}$$

Propriedades: Dadas as matrizes A e B de mesma ordem $m \times n$ e números p_1, p_2 e p_3, temos:

(i) $p_1(A + B) = p_1A + p_1B$;

(ii) $(p_1 + p_2)A = p_1A + p_2A$;

(iii) $0 \cdot A = 0$, isto é, se multiplicarmos o número zero por qualquer matriz A, teremos a matriz nula;

(iv) $p_1(p_2A) = (p_1p_2)A$.

Multiplicação de Matrizes

Definição 4.1.2.3 *Sejam* $A = [a_{ij}]_{m\times n}\mathrm{e}B = [b_{rs}]_{n\times p}$. *Definimos* $AB = [c_{uv}]_{m\times p}$. *Onde* $c_{uv} = \sum_{k=1}^{n} a_{uk}b_{kv} = a_{u1}b_{1v} + \ldots + a_{un}b_{nv}$

Observação:

(i) Só podemos efetuar o produto de duas matrizes $A_{m\times n}$ e $B_{l\times p}$ se o número de colunas da primeira for igual ao número de linhas da segunda, isto é, $n = l$. Além disso, a matriz resultado $C = AB$ será de ordem $m \times p$;

(ii) O elemento c_{ij} é obtido, multiplicando os elementos da i-ésima linha da primeira matriz pelos elementos correspondentes de j-ésima coluna da segunda matriz, e somando estes produtos.

Exemplo:

$$\begin{bmatrix} 1 & -2 \\ 5 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 5 & 0 \\ 4 & 7 \end{bmatrix} = \begin{bmatrix} 3 & 8 & -13 \\ 30 & -8 & 19 \\ 3 & -12 & 21 \end{bmatrix}$$

Propriedades:

(i) Em geral $AB \neq BA$;
(ii) $A(B+C) = AB + AC$ (distributividade a esquerda da multiplicação, em relação à soma);
(iii) $(A+B)C = AC + BC$ (distributividade a direita da multiplicação, em relação à soma);
(iv) $(AB)C = A(BC)$ (associatividade).

Transposta

Definição 4.1.2.4 *Dada a matriz* $A = [a_{ij}]_{m\times n}$*, podemos obter uma outra matriz* $A' = [b_{ij}]_{n\times m}$*, cujas linhas são colunas de A, isto é,* $b_{ij} = a_{ji}$*. A′ é denominada transposta de A.*

Exemplo:

$$A = \begin{bmatrix} 1 & 3 & 9 \\ -15 & 7 & 0 \end{bmatrix} \quad \mathrm{A}' = \begin{bmatrix} 1 & -15 \\ 3 & 7 \\ 9 & 0 \end{bmatrix}$$

4.1.3 Matrizes Inversíveis

Esta seção é restrita às matrizes quadradas, e será descrito a noção que corresponde à recíproca de um número real não nulo.

Definição 4.1.3.1 *Uma matriz A de ordem n se diz inversível se, e somente se, existe uma matriz B, também de ordem n, de modo que:*

$$AB = BA = I_n$$

A matriz B, caso exista, é única e chama-se inversa de A, indica-se por A^{-1}.

Exemplo:

A matriz $A = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix}$ é inversível e $A^{-1} = \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix}$ pois:

$$AA^{-1} = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = I_2$$

$$A^{-1}A = \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

Teorema 4.1.3.1 *Se uma matriz tem inversa, então a inversa é única.*

Demonstração:

Sejam B e C inversas de A. Então $BA = AC = I_n$.

Assim, $B = BI_n = B(AC) = (BA)C = I_nC = C$.

C.q.d.

4.2 Determinante

Definição de determinante ($n \leq 3$)

Seja A uma matriz de ordem n. Chamamos determinante da matriz A e indicamos por $detA$ o número que podemos obter operando com os elementos de A da seguinte forma:

1) Se A é de ordem $n = 1$, então $detA$ é o único elemento de A.

$A = [a_{11}] \Rightarrow \det A = a_{11}$.

Exemplo:

$A = [14] \Rightarrow \det A = 14$.

2) Se A é de ordem $n = 2$, o determinante, $detA$, é definido por:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \Rightarrow \det A = a_{11}a_{22} - a_{12}a_{21}$$

Exemplo:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \Rightarrow \det A = 1 \cdot 4 - 2 \cdot 3 = -2.$$

3) Se A é de ordem $n = 3$, o determinante, $detA$ é definido por:

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

Exemplo:

$$A = \begin{bmatrix} 1 & 3 & 4 \\ 5 & 2 & -3 \\ 1 & 4 & 2 \end{bmatrix} \Rightarrow \det A = 4 - 9 + 80 - 8 + 12 - 30 = 49$$

Propriedades:

(i) Se todos os elementos de uma linha (coluna) de uma matriz A são nulos,

$\det A = 0$;

(ii) $\det A = \det A'$;

(iii) Se multiplicarmos uma linha de uma matriz por uma constante, o determinante fica multiplicado por esta constante;

(iv) Uma vez trocada a posição de duas linhas, o determinante troca de sinal;

(v) O determinante de uma matriz que tem duas linhas (colunas) iguais é zero;

(vi) O determinante não se altera se somarmos a uma linha outra linha multiplicada por uma constante;

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

Supondo que $A_{m\times n}$ tenha inversa, isto é, existe A^{-1} tal que $AA^{-1} = I_n$. Usando o determinante temos

$$\det(AA^{-1}) = \det A \cdot \det A^{-1} \text{ e } detI_n = 1$$

Então:

$$\det A \cdot \det A^{-1} = 1$$

Desse produto concluímos que se A tem inversa,

(i) $\det A \neq 0$;

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

4.2.1 Menor Complementar e Complementar Algébrico

Definição 4.2.1 *Consideremos uma matriz A de ordem $n \geq 2$; seja a_{ij} um elemento de A. Definimos menor complementar do elemento a_{ij}, e indicamos por D_{ij}, como sendo o determinante da matriz que se obtém, suprimindo a linha i e a coluna j de A.*

Exemplo:

Seja $A = \begin{bmatrix} 0 & 1 & 7 \\ 3 & 12 & 6 \\ -3 & 2 & 4 \end{bmatrix}$, calcular D_{21}

$$D_{21} = \begin{vmatrix} 1 & 7 \\ 2 & 4 \end{vmatrix} = -10$$

Definição 4.2.2 *Consideremos uma matriz de ordem $n \geq 2$; seja a_{ij} um elemento de A. Definimos complementar algébrico do elemento a_{ij} (ou cofator de a_{ij}), e indicamos por A_{ij}, como sendo o número $(-1)^{i+j} \cdot D_{ij}$.*

Exemplo: Seja $A = \begin{bmatrix} 1 & 2 & 5 \\ 10 & 0 & 6 \\ 3 & 2 & 4 \end{bmatrix}$, calcular A_{32}

$$A_{32} = (-1)^{3+2} \cdot D_{32} = -1 \cdot \begin{vmatrix} 1 & 5 \\ 10 & 6 \end{vmatrix} = 44$$

4.2.2 Matriz Adjunta

Definição 4.2.3 *Seja A uma matriz quadrada de ordem n e $\overline{A}$ a matriz dos cofatores de A. Chamamos de matriz adjunta de A, e indicamos por $adjA$, a transposta da matriz $\overline{A}$, isto é, $adjA = \overline{A}'$*

Teorema Uma matriz quadrada A admite uma inversa se, e somente se $\det A \neq 0$ Neste caso:

$$A^{-1} = \frac{1}{\det A}(adjA) \tag{4.1}$$

Com esse teorema temos um novo modo de calcular a inversa de uma matriz.

4.3 Aritmética Modular

Nesta seção, serão apresentados exemplos de aplicação da aritmética modular extraído das Olimpíadas Brasileira de Matemática das Escolas Públicas, definições e propriedades das congruências, segundo Hefez (1993), que serão usados ao longo desta dissertação para subsidiar as Cifras de Hill.

Antes de apresentarmos as definições e propriedades relacionadas à congruência, vamos introduzir o assunto com uma questão, retirada do banco de questões do nível 2 de 2010, no site da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), que pode ser colocado aos alunos da Educação Básica, ainda não familiarizados com a aritmética modular.

Exemplo:
A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura 4.1. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?
(a) B
(b) D
(c) E
(d) G
(e) H

Solução:
Construindo uma tabela com os números que estão sobre a teia, obtemos:

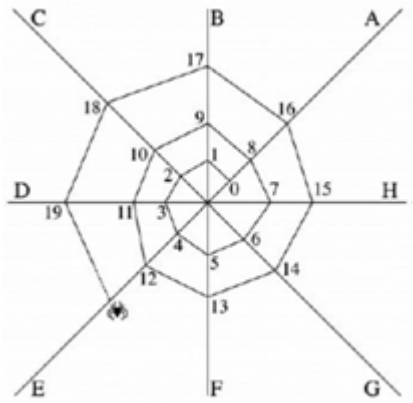


Figura 4.1: Teia

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
...	...	...	...	...	...	...	...

Para responder esta questão, algum aluno, bem paciente, poderia continuar a tabela até que aparecesse o número 118. Desse modo ele saberia em qual fio a aranha iria estar. No entanto, essa opção não seria muito prática e nem rápida.

Podemos perceber que os fios se repetem a cada oito números, e essa periodicidade faz com que os números de cada fio formem uma progressão aritmética de razão igual a 8, ou seja, aumentem de oito em oito. Observamos também que cada fio pode ser representado a partir dos múltiplos de 8. Dessa forma, o fio A corresponde aos números que são múltiplos de 8, ou seja, números que divididos por 8 deixam resto zero ($8n$, com $n \in \mathbb{Z}$). O fio B corresponde aos números que são múltilos de 8, mais um, ou seja, números que divididos por 8 deixam resto 1

($8n+1$, com $n \in \mathbb{Z}$). O fio C corresponde aos números que são múltiplos de 8, mais dois, ou seja, números que divididos por 8 deixam resto 2 ($8n+2$, com $n \in \mathbb{Z}$), e essa lógica se mantém até o fio H. Logo, para saber sobre qual fio estará o número 118, basta verificarmos a qual dessas famílias tal número pertence, e isso é obtido dividindo 118 por 8. Nessa divisão temos 14 como quociente e 6 como resto. E, podemos escrever 118 como sendo $118 = 8 \cdot 14 + 6$, ou seja, pertence a família dos números que estão no fio G.

Todos os números que estão no mesmo fio, tem uma particularidade em comum, deixam o mesmo resto ao serem divididos por 8, portanto são congruentes módulo 8. Para exemplificar, temos que o número 22 é congruente ao número 30, módulo 8, pois $22 \equiv 30 \bmod 8$.

O exemplo acima corresponde a um fenômeno cíclico que resulta em uma aritmética peculiar. A aritmética dos fenômenos cíclicos é denominada de aritmética modular.

4.4 Congruências

Definição 4.4.1 *Seja m um inteiro não nulo. Dois inteiros a e b serão ditos congruentes módulo m se os restos de a e b por m forem iguais. Quando a e b são congruentes módulo m, escrevemos $a \equiv b \bmod m$.*

Exemplo:

$$9 \equiv 2 \bmod 7$$

Uma forma mais simples de verificar se dois números são congruentes é dada pela seguinte proposição.

Proposição 4.4.1 *Tem-se que $a \equiv b \bmod m$ se e somente se $m|(a-b)$.*

Demonstração:

Se $a \equiv b \bmod m$, então existem inteiros r, q e $q^{'}$ tais que $a = mq + r$ e $b = mq^{'} + r$, logo $a - b = m(q - q^{'})$ e consequentemente $m|(a-b)$.
Reciprocamente, suponha que $m|(a-b)$. Pela divisão euclidiana temos que
$a = mq + r$ e $b = mq^{'} + r^{'}$ com $0 \leq r < m$ e $0 \leq r^{'} < m$, logo
$a - b = m(q - q^{'}) + r - r^{'}$. Como $m|m(q - q^{'})$, seque que $m|(r - r^{'})$, logo $r = r^{'}$ pois $\left|r - r^{'}\right| < m$. Portanto $a \equiv b \bmod m$.

Propriedades

A congruência modular satisfaz algumas propriedades que a tornam muito semelhante a igualdade usual. As propriedades mais elementares da igualdade são as seguintes:

Proposição 4.4.2 *Sejam a, b, c, d, m e n inteiros com $m > 1$ e $n \geq 1$.*

Sejam a, b, c, d, m e n inteiros com $m > 1$ e $n \geq 1$.

(i) (Reflexiva) $a \equiv a \bmod m$;
(ii) (Simétrica) Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$;
(iii) (Transitiva) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$;

Demonstração:

(i) Temos que $m|0$ ou $m|(a-a)$, então $a \equiv a \bmod m$.
(ii) Se $a \equiv b \bmod m$, então $a - b = km$, com $k \in \mathbb{Z}$. Portanto,
$b - a = -(km) = (-k)m$, então $b \equiv a \bmod m$.
(iii) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $m|(a-b)$ e $m|(b-c)$, logo
$m|(a - b + b - c)$, donde $m|(a-c)$ e portanto $a \equiv c \bmod m$.

Propriedades relativas a adição e multiplicação

Proposição 4.4.3 *Sejam a, b, c, d, m e n inteiros com* $m > 1$ *e* $n \geq 1$.

(i) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$;

(ii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$;

(iii) Se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$.

Demonstração:

(i) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, segue que $m|(a-b)$ e $m|(c-d)$, logo $m|(a-b+c-d)$ e portanto $a + c \equiv b + d \bmod m$.

(ii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, segue que $m|(a-b)$ e $m|(c-d)$. Como

$$ac - bd = a(c-d) + d(a-b)$$

seque que $m|(ac-bd)$ e consequentemente $ac \equiv bd \bmod m$.

(iii) Por indução a proposição é verdadeira para $n = 1$, e supondo verdadeira para um inteiro positivo k, temos: $a^k \equiv b^k \bmod m$ e $a \equiv b \bmod m$.

Portanto, pelo item (ii): $a^k \cdot a \equiv b^k \cdot b \bmod m$ ou $a^{k+1} \equiv b^{k+1} \bmod m$. Logo a proposição é verdadeira para o inteiro positivo $k + 1$. Portanto, a proposição é verdadeira para todo inteiro positivo n.

4.4.1 Classes Residuais

Dado um módulo m, qualquer inteiro a é equivalente, módulo m a exatamente um dos inteiros 0,1,2,3,...,m-1 Este inteiro é chamado resíduo de a módulo m e denotamos por

$$\mathbb{Z}_m = \{0, 1, 2, 3, ..., m-1\}$$

para representar o conjunto dos resíduos de a módulo m.

Proposição 4.4.1.1 *Sejam a e $m > 1$ números inteiros e r o resto da divisão de $|a|$ por m, então o resíduo de a módulo m é igual a:*

- 0 se $r = 0$;
- r se $r \neq 0$ e $a \geq 0$;
- $m - r$ se $r \neq 0$ e $a < 0$.

4.4.2 Inversos Modulares

Na aritmética usual, cada número não-nulo a tem um inverso multiplicativo denotado por a^{-1}, tal que

$$aa^{-1} = a^{-1}a = 1$$

Na aritmética modular temos o seguinte conceito correspondente:

Definição 4.4.2.1 *Dado um número a em $\mathbb{Z}_m$, dizemos que um número a^{-1} em $\mathbb{Z}_m$ é um recíproco, ou inverso multiplicativo de a módulo m se $aa^{-1} = a^{-1}a \equiv 1 \bmod m$.*

Proposição 4.4.2.1 *Seja a um elemento não nulo de $\mathbb{Z}_m$. Então a é inversível, se e somente se, $mdc(a, m) = 1$.*

Capítulo 5

Criptografia através de Matrizes

Entre outros autores, Howard e Rorres (2001), Boldrini et al (1984) e Leon (2008), foram usados para fundamentação desse capítulo, no qual faremos uma abordagem de dois métodos para criptografar mensagens: Criptografia com matrizes e Cifra de Hill. Apresentaremos detalhes para a criptografia e decifragem de mensagens utilizando matrizes e cifra de Hill. Através de exemplos, buscamos as soluções com orientações precisas e detalhadas, pois é um tema pouco explorado nos livros de matemática e professores e alunos não estão familiarizados com essa temática.

As cifras de substituição preservam as frequências de letras individuais, tornando relativamente fácil quebrar o código por métodos estatísticos. Uma das formas de superar este problema é dividir o texto em grupos de letras e criptografar o texto comum por grupo, em vez de uma letra de cada vez. Neste capítulo, estudaremos uma classe de sistemas poligráficos, chamados cifras de Hill, como motivador de situações problema para alunos no Ensino Médio. As cifras de Hill será uma aplicação para a utilização da matrizes no Ensino Médio de forma contextualizada.

5.1 Criptografia com Matrizes

Um modo simples de cifrar uma mensagem é associar um valor inteiro a cada letra do alfabeto, conforme a tabela 5.1, e mandar a mensagem como uma lista de números. Por exemplo, a mensagem CONGRUENTE poderia ser codificada por 2 14 13 6 17 20 4 13 19 4. No entanto, este tipo de criptografia é fácil de quebrar. Para dificultar a decifragem da mensagem, por pessoas não autorizadas, podemos disfarçar a mensagem usando multiplicação de matrizes. Usando o conhecimento de matrizes inversas, apresentado no capítulo IV, na seção matriz inversa. Usando a expressão 4.1 do capítulo IV. Se A é uma matriz cujos elementos são todos inteiros e cujo determinante é ± 1, então os elementos de A^{-1} serão todos inteiros. Podemos usar tal matriz como chave para transformar a mensagem em outra mais difícil de quebrar.

Para exemplificar essa técnica, considere as matrizes

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

Exemplo 1

Criptografar a mesagem CONGRUENTE

O remetente vai usar uma matriz A para codificar a mensagem, e o destinatário vai usar a matriz B para decodificar a mensagem.

Devemos agrupar a mensagem em pares de letras da seguinte forma

CO NG RU EN TE

ou equivalentemente, usando a tabela 5.1,

$$2\ 14 \quad 13\ 6 \quad 17\ 20 \quad 4\ 13 \quad 19\ 4$$

Uma vez que a matriz codificadora A é uma matriz 2 x 2, arranjamos nossa sequência de números disposta em coluna, formando uma matriz com duas linhas:

$$X = \begin{bmatrix} 2 & 13 & 17 & 4 & 19 \\ 14 & 6 & 20 & 13 & 4 \end{bmatrix}$$

5.1.1 Criptografando Mensagem

Para criptografar da mensagem, multiplicamos a matriz X à esquerda pela matriz A:

$$Y = A \cdot X$$

$$Y = A \cdot X = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 13 & 17 & 4 & 19 \\ 14 & 6 & 20 & 13 & 4 \end{bmatrix}$$

Tal que

$$Y = \begin{bmatrix} 34 & 51 & 91 & 38 & 65 \\ 16 & 19 & 37 & 17 & 23 \end{bmatrix}$$

Os elementos de Y constituem a mensagem cifrada

$$34\ 16 \quad 51\ 19 \quad 91\ 37 \quad 38\ 17 \quad 65\ 23$$

5.1.2 Decifrando Mensagem

Quando esta mensagem codificada chega, o destinatário utiliza a matriz decodificadora B para reverter os passos acima, sabendo que

$$B \cdot Y = B \cdot A \cdot X = I \cdot X = X$$

$$B \cdot Y = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} \begin{bmatrix} 34 & 51 & 91 & 38 & 65 \\ 16 & 19 & 37 & 17 & 23 \end{bmatrix}$$

$$B \cdot Y = \begin{bmatrix} 2 & 13 & 17 & 4 & 19 \\ 14 & 6 & 20 & 13 & 4 \end{bmatrix}$$

Pela tabela 5.1, pode-se ver que os equivalentes alfabéticos destes vetores coluna são

CO NG RU EN TE

Que corresponde a palavra CONGRUENTE.

5.2 Técnica de Hill

Como criptografar uma mensagem utilizando a técnica de Hill?

Para criptografar uma mensagem devemos inicialmente associar cada letra do alfabeto a um número inteiro de 0 a $n-1$ de forma biunívoca (onde n é o número de letras do alfabeto). No caso do alfabeto latino, como temos 26 letras, obtemos a tabela 5.1 formada por 26 caracteres e chegamos ao conjunto $\mathbb{Z}_{26}$.

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

Tabela 5.1: Relação entre letras e números.

No entanto, para tornar a criptografia de mensagens mais realista incluímos na tabela 5.1 letras, com seus respectivos acentos e alguns sinais de pontuação de acordo com a norma ortografia da língua portuguesa, segundo Azeredo (2008). Dessa forma,

passamos a trabalhar com o $\mathbb{Z}_{44}$. Para maior clareza usamos o símbolo #, indicando um espaço. Daí obtemos a tabela 5.2.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
W	X	Y	Z	Á	É	Í	Ó	Ú	Â	Ê	Ô	Ã	Õ	À	Ç	.	,	:	!	?	#
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43

Tabela 5.2: Relação entre caracteres e números.

Para criptografar uma mensagem utilizando a técnica de Hill, devemos inicialmente associar cada letra do alfabeto um número inteiro de 0 a $n-1$ de forma biunívoca (onde n é o número de letras e sinais do alfabeto), conforme a tabela 5.2.
Observação: Não faremos distinção entre letra maiúscila e minúscula.

Escolhe-se uma matriz quadrada inversível em $\mathbb{Z}_{44}$

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

cujas entradas a_{ij} são números inteiros em $\mathbb{Z}_{44}$. Esta matriz é a chave do método. Dado um texto x para criptografar, deve-se quebrá-lo em blocos de n caracteres

$$x_1 x_2 x_3 ... x_n$$

e efetuar o produto matricial

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

onde as operações são efetuadas módulo 44, para obter o bloco criptografado

$$y_1 y_2 y_3 ... y_n.$$

Caso o último bloco de caracteres do texto comum não possua exatamente n letras, ele pode ser completado com letras escolhidas ao acaso.

Para recuperar a mensagem original, basta inverter a matriz A em $\mathbb{Z}_{44}$ e efetuar o produto matricial

$$X = A^{-1}Y$$

onde $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ e $Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$ são matrizes coluna.

A matriz A deve ser inversível em $\mathbb{Z}_{44}$. Uma matriz quadrada A com elementos em $\mathbb{Z}_{44}$ é inversível em $\mathbb{Z}_{44}$ se existir outra matriz B com elementos em $\mathbb{Z}_{44}$ tal que $AB = I$

5.2.1 Codificando Mensagem

Exemplo 1 Use a matriz

$$A = \begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix}$$

Cujas entradas são números inteiros em $\mathbb{Z}_{44}$. Esta matriz é a chave do método.

Para obter a cifra de Hill da mensagem de texto comum

RIO#SÃO#FRANCISCO.

Associando os caracteres da mensagem com seus equivalentes numérico da tebela 5.2.

R	I	O	#	S	Ã	O	#	F	R	A	N	C	I	S	C	O	.
17	8	14	43	18	34	14	34	5	17	0	13	2	8	18	2	14	38

Tabela 5.3: Representação dos caracteres da mensagem em números.

Agora, agrupe os caracteres sucessivos do texto puro em ternos e substitua cada caracter pelo seu equivalente numérico pela tabela 5.2.

Para codificar RIO nós convertemos seus respectivos números em um vetor coluna

$$\begin{bmatrix} 17 \\ 8 \\ 14 \end{bmatrix}$$

efetuamos o seguinte produto matricial módulo 44

$$\begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 8 \\ 14 \end{bmatrix} = \begin{bmatrix} 111 \\ 215 \\ 174 \end{bmatrix} \tag{5.1}$$

como os números 111, 215 e 174 não possuem equivalente alfabético na tabela 5.2, devemos calculá-los módulo 44, onde obtemos

$$111 \equiv 23 \bmod 44$$
$$215 \equiv 39 \bmod 44$$
$$174 \equiv 42 \bmod 44$$

como o resto da divisão é um dos inteiros 0, 1, 2, ..., 43, este procedimento sempre fornece um inteiro da tabela 5.2. Assim, nós substituímos 111 por 23, 215 por 39 e 174 por 42, e o produto matricial 5.1 pode ser reescrito da seguinte forma

$$\begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 8 \\ 14 \end{bmatrix} = \begin{bmatrix} 111 \\ 215 \\ 174 \end{bmatrix} = \begin{bmatrix} 23 \\ 39 \\ 42 \end{bmatrix} \bmod 44$$

que fornece o texto cifrado X,? pela tabela 5.2.

Os cálculos para codificar os demais ternos são

$$\begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix} \begin{bmatrix} 43 \\ 18 \\ 34 \end{bmatrix} = \begin{bmatrix} 267 \\ 525 \\ 414 \end{bmatrix} = \begin{bmatrix} 3 \\ 41 \\ 18 \end{bmatrix} \bmod 44$$

$$\begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix} \begin{bmatrix} 14 \\ 43 \\ 5 \end{bmatrix} = \begin{bmatrix} 168 \\ 277 \\ 303 \end{bmatrix} = \begin{bmatrix} 36 \\ 13 \\ 39 \end{bmatrix} \bmod 44$$

$$\begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 82 \\ 176 \\ 117 \end{bmatrix} = \begin{bmatrix} 38 \\ 0 \\ 29 \end{bmatrix} \bmod 44$$

$$\begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix} \begin{bmatrix} 2 \\ 8 \\ 18 \end{bmatrix} = \begin{bmatrix} 116 \\ 168 \\ 210 \end{bmatrix} = \begin{bmatrix} 28 \\ 36 \\ 34 \end{bmatrix} \text{ mod } 44$$

$$\begin{bmatrix} 1 & 3 & 5 \\ 5 & 4 & 7 \\ 0 & 6 & 9 \end{bmatrix} \begin{bmatrix} 2 \\ 14 \\ 38 \end{bmatrix} = \begin{bmatrix} 234 \\ 332 \\ 426 \end{bmatrix} = \begin{bmatrix} 14 \\ 24 \\ 30 \end{bmatrix} \text{ mod } 44$$

resultando nos ternos de textos cifrados D!S,ÀN,, .AÓ, ÍÀÃ, OYÚ respectivamente. Coletando os ternos, obtemos a mensagem cifrada completa
X,?D!SÀN,.AÓÍÀÃOYÚ

Como o texto comum foi agrupado em ternos e criptografado por uma matriz 3x3, dizemos que a cifra de Hill, do exemplo acima, é uma 3-cifra de Hill. Em geral, para uma n-cifra de Hill agrupamos o texto comum em conjuntos de n letras e codificamos com uma matriz codificadora nxn de entradas inteiras.

5.2.2 Decifrando Mensagem

Para decifrar cifras de Hill, usamos a inversa módulo 44 da matriz codificadora. Se m é um inteiro positivo, dizemos que a matriz A com entradas em $\mathbb{Z}_m$ é inversível módulo m se existir uma matriz B com entradas em $\mathbb{Z}_m$ tal que

$$AB = BA = I \text{ mod } m$$

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

É inversível módulo 44 e que esta matriz é usada para uma 3-cifra de Hill. Se

$$p = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

É um vetor comum, então

$$c = Ap$$

É o correspondente vetor cifrado e

$$p = A^{-1}c$$

Assim, cada vetor comum pode ser recuperado do correspondente vetor cifrado pela multiplicação por A^{-1} mod 44.

Para garantir a existência da inversa da matriz A, será necessária a aplicação de alguns resultados, enunciados a seguir, cuja demonstração deles será omitida, pois foge ao objetivo deste trabalho.

Em criptografia é importante saber quais matrizes são inversíveis módulo m e como obter suas inversas. Em aritmética comum, uma matriz quadrada A é inversível se, e somente se, $\det(A) \neq 0$ ou, equivalentemente, $\det(A)$ tem um recíproco.
O teorema a seguir é o análogo deste resultado em aritmética modular.

Teorema 5.2.2.1 *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é inversível módulo m se, e somente se, o resíduo de* $\det(A)$ *módulo m tem um recíproco módulo m.*

Como o resíduo de $\det(A)$ módulo m terá um recíproco módulo m se, e somente se, este resíduo e m não tiverem fator primo comum, temos o seguinte corolário.

Corolário 5.2.2.1 *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é inversível módulo m se, e somente se, m e o resíduo de* $\det(A)$ *módulo m não têm fatores primos comuns.*

Como os únicos fatores primos de $m = 44$ são 2 e 11, temos o seguinte corolário que é útil em criptografia com módulo 44.

Corolário 5.2.2.2 *Uma matriz quadrada A com entradas em $\mathbb{Z}_{44}$ é inversível módulo 44 se, e somente se, o resíduo de* $\det(A)$ *módulo 44 não é divisível por 2 ou 11.*

Teorema 5.2.2.2 *Uma matriz quadrada A em $\mathbb{Z}_m$ é inversível módulo m se, e somente se,* $\det(A)$ *módulo m tem um inverso módulo m.*

Um número m terá inverso módulo 44 se e somente se $mdc(m, 44) = 1$, ou seja, m e 44 são co-primos (não têm fatores em comum). Assim, só existirá inversa módulo 44 se o $det(A)$ não for divisível por 2 ou 11.

Sendo assim, se na matriz $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ o $\det(A)$ não divisível por 2 ou 11 podemos obter a inversa de A módulo 44 pela expressão:

$$A^{-1} = [\det(A)]^{-1} \cdot Adj(A) \bmod 44 \tag{5.2}$$

Onde $[\det(A)]^{-1}$ é o inverso multiplicativo de $det(A)$ módulo 44.

Abaixo temos uma tabela com os inversos multiplicativos do módulo 44:

a	1	3	5	7	9	13	15	17	19	21	23	25	27	29	31	35	37	39	41	43
a^{-1}	1	15	9	19	5	17	3	13	7	21	23	37	31	41	27	39	25	35	29	43

Tabela 5.4: Inversos multiplicativos módulo 44.

Exemplo 2:

Decifrar a 3-cifra de Hill, que foi dada no exemplo 2:

X,? D!S ÀN, .AÓ ÍÀÃ OYÚ

Solução: Pela Tabela 5.2, encontramos o equivalente numérico do texto cifrado

X	,	?	D	!	S	À	N	,	.	A	Ó	Í	À	Ã	O	Y	Ú
23	39	42	3	41	18	36	13	39	38	0	29	28	36	34	14	24	30

Tabela 5.5: Representação dos caracteres da mensagem cifrada em números.

Para obter a mensagem decifrada, multiplicamos cada terno vetor coluna cifrado pela inversa de A do exemplo 1.

Temos que $\det(A) = 9$ e que o inverso de 9 módulo 44 é igual a 5, ou seja, $9 \cdot 5 \equiv 1 \bmod 44$. Assim, por 5.2,

$$A^{-1} = 5\begin{bmatrix} -6 & 3 & 1 \\ -45 & 9 & 18 \\ 30 & -6 & -11 \end{bmatrix} = \begin{bmatrix} -30 & 15 & 5 \\ -225 & 45 & 90 \\ 150 & -30 & -55 \end{bmatrix} = \begin{bmatrix} 14 & 15 & 5 \\ 39 & 1 & 2 \\ 18 & 14 & 33 \end{bmatrix}$$

Para decifrar X,? nós convertemos seus respectivos números em um vetor coluna

$$\begin{bmatrix} 23 \\ 39 \\ 42 \end{bmatrix}$$

efetuamos o seguinte produto matricial módulo 44

$$\begin{bmatrix} 14 & 15 & 5 \\ 39 & 1 & 2 \\ 18 & 14 & 33 \end{bmatrix}\begin{bmatrix} 23 \\ 39 \\ 42 \end{bmatrix} = \begin{bmatrix} 1117 \\ 1020 \\ 2346 \end{bmatrix} = \begin{bmatrix} 17 \\ 8 \\ 14 \end{bmatrix} \text{ mod } 44$$

que corresponde ao terno descriptografado RIO pela tabela 5.2.

Os cálculos para decifrar os demais ternos são

$$\begin{bmatrix} 14 & 15 & 5 \\ 39 & 1 & 2 \\ 18 & 14 & 33 \end{bmatrix}\begin{bmatrix} 3 \\ 41 \\ 18 \end{bmatrix} = \begin{bmatrix} 747 \\ 194 \\ 1222 \end{bmatrix} = \begin{bmatrix} 43 \\ 18 \\ 34 \end{bmatrix} \text{ mod } 44$$

$$\begin{bmatrix} 14 & 15 & 5 \\ 39 & 1 & 2 \\ 18 & 14 & 33 \end{bmatrix}\begin{bmatrix} 36 \\ 13 \\ 39 \end{bmatrix} = \begin{bmatrix} 894 \\ 1495 \\ 2117 \end{bmatrix} = \begin{bmatrix} 14 \\ 43 \\ 5 \end{bmatrix} \text{ mod } 44$$

$$\begin{bmatrix} 14 & 15 & 5 \\ 39 & 1 & 2 \\ 18 & 14 & 33 \end{bmatrix} \begin{bmatrix} 38 \\ 0 \\ 29 \end{bmatrix} = \begin{bmatrix} 677 \\ 1540 \\ 1641 \end{bmatrix} = \begin{bmatrix} 17 \\ 0 \\ 13 \end{bmatrix} \text{ mod } 44$$

$$\begin{bmatrix} 14 & 15 & 5 \\ 39 & 1 & 2 \\ 18 & 14 & 33 \end{bmatrix} \begin{bmatrix} 28 \\ 36 \\ 34 \end{bmatrix} = \begin{bmatrix} 1102 \\ 1196 \\ 2130 \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \\ 18 \end{bmatrix} \text{ mod } 44$$

$$\begin{bmatrix} 14 & 15 & 5 \\ 39 & 1 & 2 \\ 18 & 14 & 33 \end{bmatrix} \begin{bmatrix} 14 \\ 24 \\ 30 \end{bmatrix} = \begin{bmatrix} 706 \\ 630 \\ 1578 \end{bmatrix} = \begin{bmatrix} 2 \\ 14 \\ 38 \end{bmatrix} \text{ mod } 44$$

Pela tabela 5.2, pode-se ver que os equivalentes alfabéticos destes vetores são RIO#SÃO#FRANCISCO.

Capítulo 6

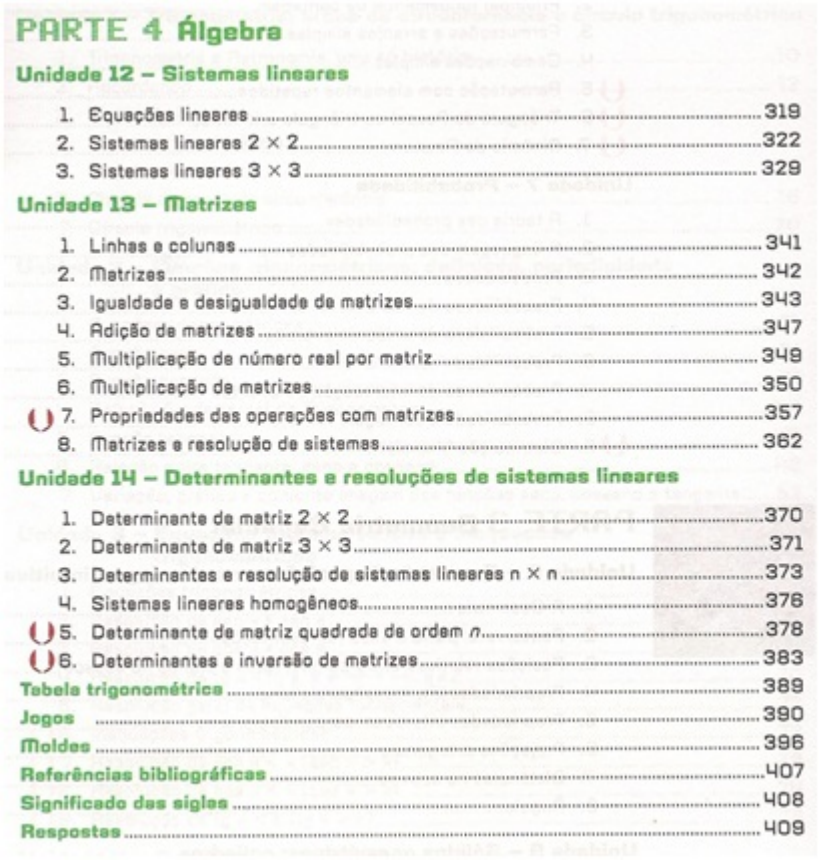
Sequência Fedathi

6.1 O Ensino de Matrizes

No que concerne ao processo de ensino-aprendizagem de matrizes, podemos inferir que este se caracteriza pela utilização de regras que, de um modo geral, apresentam-se completamente desvinculadas da realidade dos alunos. Para Sanches (2002), o ensino de matrizes apresenta-se em total descompasso com os avanços tecnológicos. Percebemos ainda, que poucos são os livros didáticos adequados para auxiliar o ensino de matemática, particularmente de matrizes, dado que muitos apresentam confusões conceituais, linguagem inadequada, raras contextualizações e exercícios repetitivos, o que prejudica o desenvolvimento do raciocínio lógico-matemático dos educandos.

Para efeito da análise, selecionei o livro de Smole e Diniz (2010), escolhido pela escola que leciono. O objetivo desta análise é levantar dados referentes à abordagem do conteúdo de Matrizes para subsidiar a análise da metodologia didática. Dessa forma, descrevo e analiso o livro considerando sua apresentação e os conteúdos de matrizes no segundo volume.

É uma coleção composta por três volumes cada um referente a uma série do Ensino Médio. Sendo que o objeto de nosso estudo foi o volume 2, pois aborda o conteúdo de matrizes. Esse volume é composto por quatro partes. Na parte 1 Trigonometria; na parte 2, Estatística, contagem e probabilidade; na parte 3, Geometria Espacial e na parte 4, Álgebra. Nesta última parte é que temos o desenvolvimento do assunto de matrizes. O conteúdo é desenvolvido com explanação e definição dos conceitos, exemplos e exercícios resolvidos. Segue abaixo, na figura 6.1 o índice referente a Álgebra, que possui três unidades.

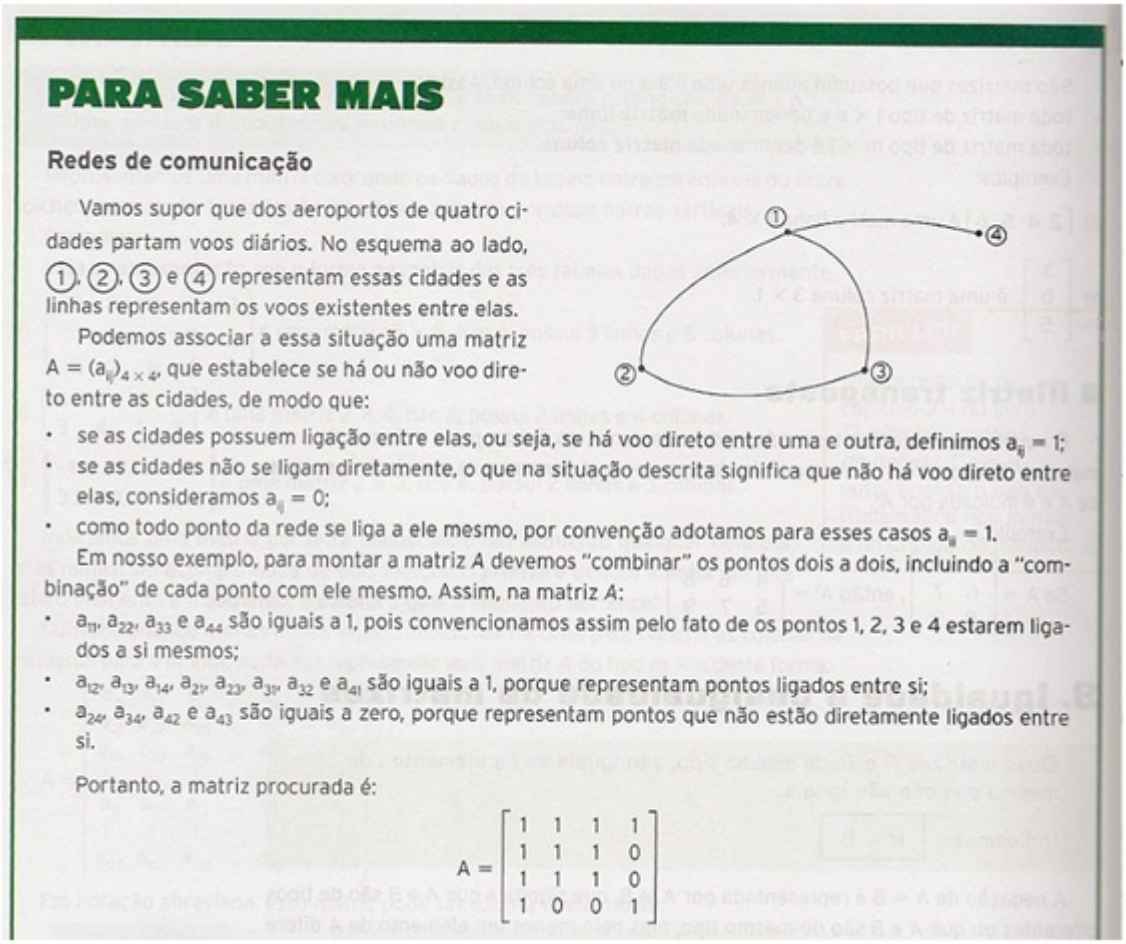


PARTE 4 Álgebra

Figura 6.1: Índice referente ao Livro Matemática: Ensino Médio. Fonte: Smole e Diniz (2010)

O conteúdo de matrizes é introduzido no referido livro com considerações sobre 3 situações, que podem ser organizadas em tabelas numéricas. No primeiro caso, o número de carros vendidos por uma agência durante uma semana, no caso 2 temos a quantidade de livros que um aluno deve ler em um certo ano letivo. E no último caso, uma tabela é apresentada no programa Excel.

Seguindo essa linha, as autoras demonstram uma preocupação em contextualizar o conteúdo de matrizes, através de exemplo do dia a dia, antes de mostrar a definição de matriz. Depois seguem os conteúdos tradicionais de matrizes como tipo de matrizes, igualdade de matrizes, operações com matrizes e exercícios. No entanto, intercalado a esses conteúdos, temos as seções "Para Saber Mais"e "No Computador", que abordam as aplicações com matrizes. Na primeira seção, temos como exemplo a conexão de vôos entre quatro cidades, representadas em uma figura, conforme se observa na figura 6.2.



PARA SABER MAIS

Redes de comunicação

Vamos supor que dos aeroportos de quatro cidades partam voos diários. No esquema ao lado, ①, ②, ③ e ④ representam essas cidades e as linhas representam os voos existentes entre elas.

Podemos associar a essa situação uma matriz $A = (a_{ij})_{4 \times 4}$, que estabelece se há ou não voo direto entre as cidades, de modo que:

- se as cidades possuem ligação entre elas, ou seja, se há voo direto entre uma e outra, definimos $a_{ij} = 1$;
- se as cidades não se ligam diretamente, o que na situação descrita significa que não há voo direto entre elas, consideramos $a_{ij} = 0$;
- como todo ponto da rede se liga a ele mesmo, por convenção adotamos para esses casos $a_{ii} = 1$.

Em nosso exemplo, para montar a matriz *A* devemos "combinar" os pontos dois a dois, incluindo a "combinação" de cada ponto com ele mesmo. Assim, na matriz *A*:

- a_{11}, a_{22}, a_{33} e a_{44} são iguais a 1, pois convencionamos assim pelo fato de os pontos 1, 2, 3 e 4 estarem ligados a si mesmos;
- a_{12}, a_{13}, a_{14}, a_{21}, a_{23}, a_{31}, a_{32} e a_{41} são iguais a 1, porque representam pontos ligados entre si;
- a_{24}, a_{34}, a_{42} e a_{43} são iguais a zero, porque representam pontos que não estão diretamente ligados entre si.

Portanto, a matriz procurada é:

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Figura 6.2: Seção "Para Saber Mais". Fonte: Smole e Diniz (2010, p. 344)

De acordo com o texto, a figura pode parecer mais simples que matriz, mas numa situação de se representar conexões entre muitas cidades, as matrizes possibilitariam consultas mais fáceis, sobretudo se elas estiverem armazenadas em computadores.

No outro exemplo, da seção "Para Saber Mais", descreve um modelo que representa três conjuntos de semáforos de um cruzamento, em que as matrizes indicam o tempo, em minutos em que o semáforo se mantêm simultaneamente abertos, segundo uma sequência dada, conforme a figura 6.3. Para isto, são efetuados cálculos com matrizes (multiplicação de um número real por uma matriz).

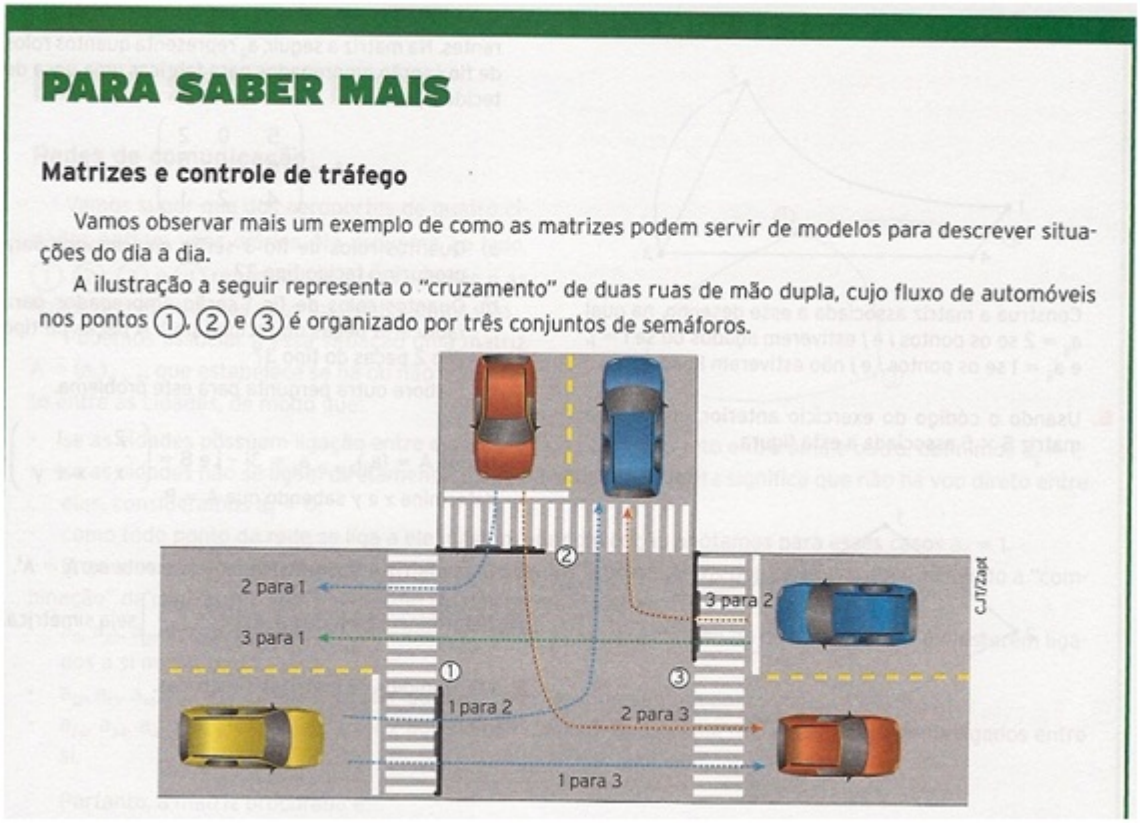


Figura 6.3: Seção "Para Saber Mais". Fonte: Smole e Diniz (2010, p. 346)

A partir dessas análises, é possível dizer que os dois exemplos acima apresentam situações contextualizadas com o foco na aplicabilidade, porém o livro carece de exemplos práticos, no qual é abordado diversos conteúdos de matrizes. Nessa perspectiva, a Sequência Fedathi, exposta neste trabalho, abordou os conteúdos de matriz de forma mais abrangente, pois com a utilização da criptografia foi possível trabalhar com produto de matriz, matriz transposta, matriz inversível e determinante. Dessa forma, a proposta apresentada na sequência didática consegue complementar o conteúdo do livro.

Lima (2001, p. 462) reforça nosso argumento ao caracterizar o hábito do professor, quando declara que:

> O livro didático é o instrumento essencial utilizado pelo professor para realizar o seu trabalho. Dele

são tiradas as listas de exercícios, é nele que estão as definições, os exemplos, as observações, as demonstrações e a linguagem a ser usada na comunicação com a classe.

Dai a importância de se trabalhar a Sequência Fedathi como uma complementação para os conteúdos de matrizes utilizados nos livros didáticos de matemática.

6.2 Aplicação de Sequência Fedathi no Ensino de Matrizes com o Auxílio da Criptografia

Apresentaremos abaixo, uma situação de ensino delineada sob um modelo de aplicação da Sequência Fedathi, voltada para o ensino de matrizes para alunos do Ensino Médio, tendo como foco, o trabalho com criptografia para facilitar o ensino aprendizado.

1° Estágio Tomada de Posição

Inicialmente, recomenda-se que o professor explique o que é criptografia, abordando assim, seus conceitos; faça uma breve introdução da história mostrando sua evolução ao longo dos anos; suas aplicações no dia a dia; a importância da comunicação para a sociedade e a necessidade, surgida com o tempo, de uma linguagem secreta que permitisse sigilo entre as comunicações.

Em seguida, são sugeridos alguns passos para o professor nortear o processo de ensino de matrizes, utilizando a criptografia como facilitador do processo de ensino aprendizagem.

Primeiro Passo: O professor poderá abordar os conhecimentos prévios dos alunos através de algumas perguntas.

Dada as matrizes $A = \begin{bmatrix} 6 & 2 \\ 11 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} -5 & 13 \\ 7 & 8 \end{bmatrix}$

Qual a inversa da matriz A? Qual o determinante da matriz A? Qual a adjunta da matriz B? Qual o produto da A por B? Qual a relação entre matriz inversível e determinante? Qual a transposta da matriz B? Qual a relação entre matriz adjunta e matriz inversível?

As perguntas expostas acima não precisam necessariamente seguir essa ordem, e nem serem somente essas, pois a condução de outros questionamentos poderá ocorrer dependendo das respostas dadas pelos alunos. Essa sondagem é primordial para a continuidade da situação, pois através dela o professor estará fazendo um diagnóstico a respeito dos conhecimentos prévios dos alunos, em relação ao conteúdo que será abordado.

Segundo Passo: Em seguida, o professor poderá propor a seguinte situação problema:

Considere a seguinte mensagem: CRIPTOGRAFIA COM MATRIZES.

Questões

1. Como crifrar e decifrar uma mensagem utilizando matrizes?
2. Qual informação será enviada para o destinatário após a cifragem da mensagem?
3. Como transformar a mensagem cifrada no texto original?

4. Se a chave para cifrar a matriz não foi uma matriz inversível, será possível decifrar a mensagem? Dê exemplo e justifique.

Para direcionar o raciocínio dos alunos, o professor poderá dar alguns exemplos de como cifrar e decifrar uma mensagem conforme a explicação feita em criptografia com matrizes no capítulo cinco na seção 5.1, que se refere a criptografia com matrizes, sem mencionar para os alunos que devemos trabalhar com matriz quadrada e que ele deve ser inversível.

E ao final o professor pode propor que a atividade deve ser feita em grupo, para que tenhamos uma divisão das tarefas e uma maior interação entre os alunos.

2° Estágio Maturação

Após apresentar a criptografia, a relação dela com matrizes e estimular o interesse dos alunos, o professor deverá observar as estratégias usadas pelos alunos e as dificuldades apresentadas por eles. Deverá também mediar a atividade, estimulando a interação entre eles para a resolução dos problemas. Nesta fase, o processo de algoritmização ainda não teve início. Para a realização das tarefas pertinentes a este estágio se faz necessário que o professor dê tempo suficiente aos alunos para suas discussões e experimentações, o tempo vai variar de acordo com a evolução do trabalho realizado pelos alunos.

Os grupos deverão descrever textualmente, ou através de algum esquema gráfico, como ocorre a cifragem e decifragem de mensagens utilizando matrizes. Também deverão criar suas próprias chaves, para em seguida transformar a mensagem em uma matriz de números, com um auxílio de uma tabela de conversão, que relaciona cada caractere da escrita com um número. Nesta fase, os alunos devem perceber que existe uma relação entre a matriz da mensagem e a chave, pois para que possamos

multiplicar essas matrizes deve-se verificar se o número de colunas da primeira matriz é igual ao número de linhas da segunda matriz. Uma vez codificada, será enviada ao destinatário em forma de texto numérico.

Caso eles tenham escolhida uma matriz não inversível, como chave, eles não conseguirão decifrar a mensagem. Neste momento, o professor poderá perguntar ao grupo se a matriz chave escolhida é inversível? Qual a relação entre a matriz inversa e a decifragem da mensagem? Nesta fase os alunos deverão testar suas hipóteses, discutir com seus colegas e considerar as opiniões de todos quanto à resolução do problema. O professor, deve permanecer com uma postura passiva e observar as estratégias utilizadas pelos alunos com o objetivo de discuti-las posteriormente.

3° Estágio - Solução

A terceira etapa, os alunos são convidados a realizarem duas ações: expor suas resoluções e discuti-las com os outros alunos e o professor.

Nesta fase temos um momento de interação entre professor e alunos, e embora seja o docente responsável pela mediação, sugere-se que os alunos sejam estimulados a assumirem um papel ativo, revendo seus resultados na medida em que opina sobre os resultados expostos pelos colegas.

Durante a exposição dos alunos, o professor terá a oportunidade de verificar quais foram as estratégias adotada pelos grupos para a resolução da situação problema.

No caso dos grupos que usaram como chave uma matriz inversível, poderemos acompanhar a técnica usada para determinação da inversa, se foi utilizando a definição, ou através de matriz elementar ou por meio da matriz adjunta e utilizando os conhecimentos de determinante. No caso do grupo que por ventura não tenha

usado uma matriz inversível como chave, pode ocorrer de a mensagem não ser decifrável, pois sem a condição da chave ser inversível não podemos garantir que a decifragem da mensagem. Diante desta situação, o professor terá a oportunidade de analisar as estratégias do aluno para conseguir decifrar a mensagem, analisar suas conjecturas e suas observações. Nesta fase, os alunos poderão usar seu repertório de conhecimentos adquiridos durante as aulas de matrizes e determinante.

O professor deve considerar todas as soluções dadas pelos alunos, inclusive as que contiveram erros. Nesta etapa também deve ser dada ênfase ao raciocínio dos alunos e suas estratégias para resolver a situação problema.

4° Estágio - Prova:

Neste momento, sugere-se ao professor que formalize o conceito matriz inversível e seus teoremas, pois tais conteúdos são essenciais para o entendimento da situação problema. Depois, explique o processo de criptografia utilizando matrizes, partindo dos casos particulares propostos para o caso geral, e, a partir desta representação, construir com os alunos a formalização dos conteúdos abordados ao longo do trabalho. Nesse último estágio, os alunos deverão ter adquirido subsídios teóricos para entenderem e estabelecerem relações entre os resultados das discussões, e o modelo científico do conhecimento a ser aprendido. Nesse momento, os alunos serão conduzidos pelo professor, a compreenderem o modelo de criptografia utilizando matrizes. Para enriquecer e tornar este estudo mais significativo para os alunos, o professor poderá estabelecer uma relação e uma explanação sobre criptografia com matrizes utilizando as Cifras de Hill. Ao final da situação, os alunos deverão exercitar e aprofundar o conhecimento aprendido através do estudo, e exploração de outras situações que abordem o conceito de criptografia com matrizes.

Para aprofundar os conceitos de matrizes, podemos posteriormente a esta Sequência Fedathi, propor outra sequência didática, desta vez utilizando as cifras de Hill. No entanto faz-se necessário, inicialmente, passar para os alunos os conceitos da aritmética modular, que serão utilizado na cifra de Hill. A descrição das etapas são similares às apresentadas acima, porém com a inclusão de conteúdos relativos a congruência. E tendo como fundamentação o que fora exposto no capítulo cinco na seção 5.2, na qual são abordas as técnicas utilizadas para criptografar e decifrar mensagens.

6.2.1 Considerações Finais

Matrizes são úteis em diversos campos como na economia, na engenharia, na física, na tecnologia (grafos) e também pode ser aplicada em criptografia. A área da criptografia é bem abrangente, e usa diversos métodos para transformar texto puro em texto cifrado.

A Sequência Fedathi implementada na seção anterior, teve por objetivo revisar o conceito de matriz, multiplicação de matrizes, operações com matrizes, matriz transposta, matriz adjunta, cálculo de matriz inversa e determinante, visando reforçar e ampliar o conhecimento dos alunos. Para Tamarozzi (2001), a criptografia possibilita o desenvolvimento de atividades didáticas envolvendo o conteúdo de funções e matrizes, os quais se constituem em material útil para exercícios, atividades e jogos de codificação, em que o professor pode utilizá-los para fixação de conteúdos. Nesse contexto, a criptografia possibilita o desenvolvimento de atividades didáticas, que podem ser desenvolvidas no Ensino Médio, levando os alunos a aprofundarem seus conhecimentos. Além da atividade em grupo que de acordo com o que preconiza em Brasil (1998), destaca a importância de trabalhos em grupos favorecendo o desenvolvimento de capacidades como:

- perceber que além de buscar a solução para uma situação proposta devem cooperar para resolvê-la e chegar a um consenso;
- saber explicitar o próprio pensamento e procurar compreender o pensamento do outro;
- discutir as dúvidas, supor que as soluções dos outros podem fazer sentido e persistir na tentativa de construir suas próprias idéias;
- incorporar soluções alternativas, reestruturar e ampliar a compreensão acerca dos conceitos envolvidos nas situações e, desse modo, aprender.

Portanto, a metodologia didática do trabalho possibilita aos alunos uma abordagem de conteúdos novos, por exemplo, o conteúdo de Aritmética Modular. Também possibilita trabalhar com um tema de interesse dos estudantes, aliando os conteúdos matemáticos a um tema atual, tornando possível ampliar e revisar conteúdos já desenvolvidos. A atividade didática proporciona um trabalho em grupo e cooperativo. Além disso, os alunos passam a conhecer aplicações da matemática, na vida Moderna, como a codificação e decodificação de mensagem.

Capítulo 7

Conclusão

Neste trabalho, observou-se que o estudo da criptografia possibilita aos alunos do Ensino Médio uma interação com os conteúdos de matrizes de forma contextualizada, pois aliam os conteúdos matemáticos a um tema atual, apresentando diferentes situações e aplicações.

O Currículo de Matemática, utilizado no Ensino Médio precisa despertar o interesse dos alunos, para motivar e incentivá-lo no estudo dos conteúdos. E, principalmente, deve proporcionar a compreensão do uso da matemática em assuntos da vida moderna. Fatores, que podem ser observados no tema criptografia, desenvolvido ao longo desta dissertação.

Nesse trabalho, a proposta de trabalhar com a Sequência Fedathi como metodologia as aulas de matrizes associada com criptografia demonstrou ser uma excelente ferramenta para o ensino-aprendizagem de matemática, pois trabalhou situações que valorizam a construção de conhecimentos matemáticos pelo aluno, através de situações conjecturais que viabilizem a lógica do desenvolvimento matemático do aluno.

A temática apresentada neste trabalho está vinculada a um contexto histórico e tecnológico, além de apropriar-se de conceitos matemáticos que podem ser desenvolvidos em atividades para alunos do Ensino Médio, possibilitando trabalhar com o ensino aprendizado da matemática com aplicações condizentes com a realidade.

Entendemos que o tema criptografia pode e deve ser incluído nos currículos do Ensino Médio, pois no ensino de matrizes, a criptografia apresenta-se com muita aplicabilidade coerente, interessante e atual da matemática, o que proporciona aos estudantes uma maior motivação para o aprendizado desses conceitos.

Espera-se que este trabalho possa ser uma contribuição que possibilite discussões e reflexões, junto aos professores que lecionam matemática na Educação Básica, em relação ao processo de ensino aprendizagem, por meio de um processo em que o aluno é o construtor do seu próprio conhecimento, sendo o professor um mediador entre o conhecimento e o aluno.

E como sugestão de trabalho futuro, desenvolver um aplicativo que possibilite cifrar e decifrar mensagens através de matrizes.

Bibliografia

[Azeredo 2008] AZEREDO, José Carlos de. *Escrevendo pela nova ortografia: como usar as regras do novo acordo ortográfico da Língua Portuguesa.* Rio de Janeiro: Instituto Antônio Houaiss. 1ª edição, Publifolha, 2008.

[Boldrini et al. 1984] BOLDRINI, José L. et al.: Álgebra Linear, Ed Harbra, 3a edição, São Paulo, SP, 1984.

[Borges Neto 2001] BORGES NETO, Hermínio e outros. A Sequência Fedathi como proposta metodológica no ensino de Matemática e sua aplicação no ens ino de retas paralelas. XV EPENN Encontro de Pesquisa Educacional do Norte e Nordeste. São Luiz/MA: UFMA, 2001.

[Borges Neto 2003] BORGES NETO, Hermínio e SANTANA, J. Rogério. Sequência Fedathi: uma proposta de mediação pedagógica na relação ensino/aprendizagem. In:VASCONCELOS, José Gerardo (Org.). Filosofia, Educação e realidade. Fortaleza: EUFC, 2003

[Brasil 1996] BRASIL. Ministério de Educação e Cultura. LDB - Lei nº 9394/96, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da Educação Nacional. Brasília: MEC, 1996.

[Brasil 1998] BRASIL. Secretaria de Educação Fundamental. Parâmetros curriculares nacionais : Matemática / Secretaria de Educação Fundamental. Brasília : MEC, 1998.

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

[Coutinho 2011] COUTINHO, S. C. *Números Inteiros e Criptografia RSA.* Rio de Janeiro: IMPA, 2001.

[Du Sautoy 2007] DU SAUTOY, Marcus. *A música dos números primos* - a história de um problema não resolvido na matemática. Rio de Janeiro: Jorge Zahar Editor Ltda., 2007.

[Faleiros 2011] FALEIROS, Antonio Cândido. *Criptografia.* São Carlos: SBMAC, 2011, 138 P, (Notas em Matemática Aplicada; v. 52). Disponível em: http://www.sbmac.org.br/arquivos/notas/livro_52.pdf. Acessado em 19 de jan 2013.

[Groenwald e Franke 2008] GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber. Currículo de Matemática e o tema Criptografia no Ensino Médio. Educação Matemática em Revista, Rio Grande do Sul, p. 51-57, 2008.

[Hefez 1993] HEFEZ, Abramo.*Curso de Álgebra, Volume 1* Rio de Janeiro: IMPA, CNPQ, 1993.

[Howard e Rorres 2001] HOWARD, Anton; RORRES, Chris. *Álgebra Linear com Aplicações.* 8. ed. Porto Alegre: Bookman, 2001.

[Iezzi 2005] IEZZI, Gelson, HAZZAN, Samuel. Fundamentos da Matemática Elementar: sequências, matrizes, determinante, sistemas. Atual Editora Ltda: 4 ed. São Paulo, 2005

[Leon 2008] LEON, Steven J. *Álgebra Linear com Aplicações.* Rio de Janeiro: LTC, 2008.

[Lima 1999] LIMA, E. *Conceituação, Manipulação e Aplicação - Os Três Componentes de Ensino da Matemática.* Revista do Professor de Matemáica.São Paulo: Sociedade Brasileira de Matemática, n. 41, p. 1-6, 1999.

[Lima 2001] LIMA, E. *Exame de Textos - Análise de Livros de Matemática para o Ensino Médio.* Rio de Janeiro: IMPA/SBM, 2001.

[Malagutti et al. 2010] MALAGUTTI, Pedro Luiz; BEZERRA, Débora de Jesus; RODRIGUES, Vânia Cristina da Silva. *Aprendendo criptologia de forma divertida.* Paraíba, 2010. Disponível em: http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas$_C$*ompletos*/*O*1*Completo.pdf*. *Acessoem* : 05*dez*.2012.

[Moreno et al. 2005] MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. *Criptografia em software e hardware.* São Paulo: Novatec, 2005.

[Olgin 2011] OLGIN, Clarissa de Assis. *Currículo no ensino médio: Uma experiência com o tema criptografia.* Canoas: ULBRA, 2011. Dissertação (Mestrado) Programa de Pós - Graduação em Ensino de Ciências e Matemática da Universidade Luterana do Brasil, 2011.

[Pigatto 2012] PIGATTO, Daniel Fernando. *Segurança em sistemas embarcados críticos utilização de criptografia para comunicação segura.* São Carlos: USP, 2012. 88 p. Dissertação (Mestrado) Programa de Pós-Graduação em Ciências de Computação e Matemática Computacional, Universidade de São Paulo, 2012.

[Polya 1978] POLYA, George. A arte de resolver problemas: Um novo aspecto do método matemático. Tradução: Lisboa de Araújo. Rio de Janeiro-RJ: Interciência, 1978.

[Sanches 2002] SANCHES, Maria Helena Figueiredo. *Efeitos de uma estratégia diferenciada do ensino dos conceitos de matrizes.* CampinaS: SP, 2002. Dissertação (Mestrado) - Universidade Estadual de Campinas. Faculdade de Educação., 2002.

[Shokranian 2012] SHOKRANIAN, Salahoddin. *Criptografia para Iniciantes 2ª Edição.* Rio de Janeiro: Editora Ciência Moderna Ltda., 2012.

[Singh 2003] SINGH, Simon. *O Livro dos Códigos*: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro: Record, 2003.

[Smole e Diniz 2010] SMOLE, Kátia Cristina Stocco; DINIZ, Maria Ignez de Souza Vieira. *Matemática: Ensino Médio, vol 2.* 6. ed. São Paulo: Saraiva, 2010.

[Stallings 2008] STALLINGS, William. *Criptografia e Segurança de Redes:* Princípios e práticas. 4. ed. Pearson Prentice-Hall, 2008.

[Tamarozzi 2001] TAMAROZZI, Antônio Carlos. Codificando e decifrando mensagens. Revista do Professor de Matemática, São Paulo: Sociedade Brasileira de Matemática, n. 45, 2001.

[Tkotz 2005] TKOTZ, Viktoria. *Criptografia, Segredos Embalados para Viagem.* São Paulo: Novatec Editora, 2005.