UNIVERSIDADE FEDERAL DA GRANDE DOURADOS – UFGD
FACULDADE DE CIÊNCIAS EXATAS E TECNOLÓGICAS – FACET

WILHELM DOS SANTOS PAES

CRIPTOGRAFIA EM BLOCOS: UM ENFOQUE EM SUA APLICAÇÃO NO ENSINO DE MATRIZES

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM MATEMÁTICA

DOURADOS – MS
DEZEMBRO – 2014

WILHELM DOS SANTOS PAES

CRIPTOGRAFIA EM BLOCOS: UM ENFOQUE EM SUA APLICAÇÃO NO ENSINO DE MATRIZES

ORIENTADOR: PROF. DR. LINO SANABRIA

Dissertação apresentada ao final do Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT da Universidade Federal da Grande Dourados (UFGD) como exigência parcial para obtenção do título de Mestre em Matemática.

DOURADOS – MS
DEZEMBRO – 2014

Dados Internacionais de Catalogação na Publicação (CIP).

P126c Paes, Wilhelm dos Santos

Criptografia em blocos: um enfoque em sua aplicação no ensino de matrizes. / Wilhelm dos Santos Paes – Dourados: UFGD, 2014.

65f. il.;

Orientador: Prof. Dr. Lino Sanabria.

Dissertação (Mestrado Profissional em Matemática) FACET, Faculdade de Ciências Exatas e Tecnologia – Universidade Federal da Grande Dourados.

1. Criptografia em bloco. 2. Matrizes. 3. Problema. I. Título.

CDD – 004.6

Ficha catalográfica elaborada pela Biblioteca Central – UFGD.

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DA GRANDE DOURADOS
FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Termo de Aprovação

Após a apresentação, arguição e apreciação pela banca examinadora, foi emitido o parecer APROVADO, para a dissertação intitulada: **"Criptografia em Blocos: Um Enfoque em sua Aplicação no Ensino de Matrizes"**, de autoria de Wilhelm dos Santos Paes, apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal da Grande Dourados.

Prof. Dr. Lino Sanabria (Orientador-UFGD)
Presidente da Banca Examinadora

Prof. Dr. Sérgio Rodrigues
Membro Examinador (UFGD)

Prof. Dr. Vando Narciso
Membro Examinador (UEMS)

Dourados/MS, 15 de dezembro de 2014

Dedico este trabalho primeiramente a Deus, por ter me dado o bem mais precioso a vida.
E a minha esposa Luciana e meu filho Kevin que me ajudaram do começo ao fim.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado saúde e força para superar as dificuldades. Mas existem situações na vida que é fundamental contar com o apoio e a ajuda de algumas pessoas.

Para realização deste trabalho de conclusão e decorrer do curso, pude contar com várias. E a essas pessoas prestarei, através de poucas palavras, os mais sinceros agradecimentos:

Aos professores do Curso do Mestrado Profissional em Matemática - PROFMAT da Universidade Federal da Grande Dourados (UFGD), com os quais pude aprofundar meus conhecimentos matemáticos. Agradeço pelas ideias, sugestões e pelo olhar cuidadoso em toda a minha caminhada no decorrer do curso.

O professor Lino Sanabria, orientador deste trabalho, pelos seus conhecimentos, sua atenção, sua boa vontade e paciência.

A meu colega e amigo Rubens, pelas inúmeras horas de estudo em conjunto, pelo acolhimento, pelo apoio, pelo reconhecimento e pelas dicas que sempre me ajudaram no período da realização do mestrado.

A Luciana, minha esposa, por acreditar em mim e por acreditar que esta conquista seria possível, além de sua compreensão e apoio nos momentos de dificuldade.

Agradeço também a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

Este trabalho trata da criptografia em blocos no ensino de matrizes, mostrando de forma prática uma aplicação que relaciona a criptografia com as matrizes. Vamos estudar a criptografia; enunciar as definições e operações com matrizes; descrever a criptografia em blocos; problemas relacionados com a criptografia em blocos; e na parte final deste trabalho propor atividades a serem aplicadas em sala de aula.

Palavras chaves: Criptografia. Matrizes. Problemas.

ABSTRACT

This work deals of the encryption in block in the teaching of matrices, showing practically an application relating to encryption with the matrices. We will study the encryption; state the definitions and matrix operations; describe the encryption in block; problems related with the encryption in block; and in the end of this work to propose activities to be implemented in the classroom.

Keywords: Encryption. Matrices. Problems.

Sumário

INTRODUÇÃO

A criptografia - do grego: kryptos (escondido, oculto) e grapho (grafia, escrita) - surgiu a partir da necessidade de manter o sigilo nas comunicações a distância, protegendo-as contra a ação de espiões.

Essa ciência consiste de um conjunto de métodos que permitem codificar um texto, tornando-o ininteligível, de modo que apenas seu destinatário legítimo consiga decodificá-lo.

A criptografia é um assunto importante no contexto atual, acredita-se que a utilização em sala de aula possa ser um fator que motive os alunos, já que a tecnologia está presente de maneira intensa na vida dos jovens. Trazendo a criptografia em blocos para sala de aula podemos associa-la às matrizes fazendo com que o aluno sinta motivação no momento de aprender ou aplicar tal conteúdo.

O objetivo geral deste trabalho é fornecer um conhecimento sobre criptografia em blocos de modo que o Professor de Matemática possa introduzi-la em sala de aula, relacionando este tema com as matrizes, tornando a prática docente mais dinâmica e motivante, pois os alunos ficarão frente a frente com atividades de codificação e decodificação.

Os objetivos específicos são:

- Introduzir a criptografia.
- Relacionar a criptografia em blocos ao ensino das matrizes.
- Problemas relacionados a criptografia em blocos.

A fim de proporcionar uma visão geral do nosso trabalho, apresentamos uma breve descrição do que iremos tratar em cada um dos Capítulos.

No primeiro Capítulo apresentamos a criptografia de forma bem simples e objetiva; cifra de César e aritmética dos restos.

No segundo Capítulo faremos um estudo resumido das matrizes, apresentando definições e operações.

No terceiro Capítulo apresentamos a criptografia em blocos, descrevendo sua utilização com uso de matrizes.

No quarto Capítulo vamos abordar alguns problemas relacionados com a criptografia em blocos.

No último capítulo, vamos propor atividades que relacionam criptografia em blocos com matrizes utilizando o software Criptomat2, que podem ser utilizados pelo Professor de Matemática do Ensino Médio.

1 CRIPTOGRAFIA

A palavra criptografia origina-se das palavras gregas Kriptós e gráphein, que significam escondido e grafia, respectivamente, seu surgimento ocorreu devido às necessidades de proteção e sigilo na troca de informações.

Existem registros de criptografia na escrita hieroglífica dos egípcios, há cerca de 4000 anos. Mas foram os militares, com as necessidade de transmitir mensagens com segurança, que desenvolveram essa técnica.

Atualmente a criptografia está presente em diversas situações do nosso dia a dia: quando utilizamos o celular, fazemos operações bancárias e utilizamos o computador. Na telefonia celular, a criptografia evita que suas conversas sejam ouvidas por intrusos. Nos bancos, para que a segurança das movimentações financeiras possa ser preservada, ou seja, para que dados de cartões de crédito por exemplo, se mantenham sigilosos. E em computadores, de maneira que as informações armazenadas ou transmitidas não possam ser acessadas. A partir da evolução dos computadores, a criptografia foi amplamente divulgada, empregada e ainda modificada, passando a receber algoritmos matemáticos. Além de manter a segurança do usuário, a criptografia preserva a integridade do site, a autenticação do usuário bem como a do remetente, do destinatário e da atualidade da mensagem ou do acesso.

Temos a criptografia simétrica,ou de chave privada, e criptografia assimétrica, ou de chave pública:

A criptografia simétrica (ou criptografia de chave privada) é o modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a

mensagem numa ponta, como pelo destinatário para decodificá-la na outra.

Dado um texto antes de criptografá-lo, nos referimos a ele como texto claro, ou mensagem clara em oposição a texto cifrado ou mensagem cifrada.

Essencialmente, quando a origem (ALFA) cifra uma mensagem, ele utiliza um algoritmo de ciframento para transformar o texto claro da mensagem em texto cifrado. Quando o destino (BRAVO) decifra uma mensagem, ele utiliza o algoritmo de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara. Se um intruso (CHARLIE) conhecer o algoritmo de ciframento, ele poderia decifrar uma mensagem cifrada tão facilmente quanto o destino (BRAVO). A solução no uso da criptografia de chave privada propõe que quando a origem (ALFA) cifra uma mensagem, ele utilize um algoritmo de ciframento e uma chave secreta para transformar uma mensagem clara em um texto cifrado. O destino (BRAVO), por sua vez, ao decifrar a mensagem, utiliza o algoritmo de deciframento correspondente e a mesma chave para transformar o texto cifrado em uma mensagem clara. O intruso (CHARLIE), por não possuir a chave secreta, mesmo conhecendo o algoritmo, não conseguirá decifrar a mensagem. A segurança do sistema passa a residir não mais no algoritmo e sim na chave empregada. É ela (chave privada) que agora, no lugar do algoritmo, deverá ser mantida em segredo pela origem (ALFA) e destino (BRAVO).

A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Entenda que se as chaves utilizadas forem complexas a elaboração de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação.

O principal problema residente na utilização deste sistema de criptografia é que quando a chave de ciframento é a mesma utilizada para deciframento, ou de que a chave de deciframento pode ser facilmente obtida a partir do conhecimento da chave de ciframento, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento, este independente do destinado à comunicação sigilosa, uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem. Outras lacunas são interpostas a este sistema:

• Como cada par necessita de uma chave para se comunicar de forma segura, para um uma rede de n usuários precisaríamos de $\frac{n\cdot(n-1)}{2}$ chaves, quantidade esta que dificulta a gerência das chaves;

• A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido;

•A criptografia simétrica não garante a identidade de quem está enviando a mensagem e nem preveni que alguém negue o envio e/ou recebimento de uma mensagem.

Na criptografia assimétrica (ou criptografia de chave pública) são utilizados duas chaves diferentes uma para encriptar e outra para decriptar. O criptossistema com chave pública é mais seguro no sentido de manter oculta a chave decodificadora. A razão para o nome chave pública é que a informação necessária para enviar mensagens secretas - a chave codificadora K_E - pode ser uma informação pública (conhecida por todos) sem permitir com isso, que qualquer pessoa possa ler a mensagem.

Por definição um criptossitema com chave pública tem a propriedade que

alguém que sabe apenas como codificar não pode usar a chave codificadora para encontrar a chave decodificadora sem um cálculo extremamente longo. Em outras palavras, a função codificadora $f : \alpha \to \beta$ é fácil de ser calculada uma vez que a chave codificadora K_E é conhecida, mas é muito difícil calcular a função inversa $f^{-1} : \beta \to \alpha$. Isto significa, do ponto de vista computacional, que a função f não é invertível sem alguma informação extra - a chave decoficadora K_D. Tal função é chamada de "trapdoor".

Há um conceito parecido com a função trapdoor, que é a "função com sentido único". Esse tipo de função, é fácil de ser calculada. A noção função "trapdoor", aparentemente, apareceu pela primeira vez em 1978 junto com a invenção do criptossistema de chave pública RSA. Já, a noção de função com sentido único é mais velha. O que parece ter sido o primeiro uso de funções com sentido único em criptografia foi descrito no livro de Wilkes que foi publicado em 1968.

Observe que em um sistema com chave pública é possível que duas pessoas se comuniquem secretamente sem terem tido nenhum contato prévio, sem trocar nenhuma informação preliminar. Toda as informações necessárias para emitir uma mensagem cifrada estão disponíveis publicamente.

Na criptografia com chave pública, há uma maneira especialmente fácil de identificar-se de modo que ninguém possa fingir ser você. Sejam Ana (A) e Bernardo (B) dois usuários do sistema. Seja f_A a transformação codificadora que qualquer usuário deve usar para enviar mensagens a Ana, e seja f_B o mesmo para Bernardo. Para simplificar, vamos assumir que o conjunto de todas as unidades de mensagens pura (α) e o conjunto de todas as possíveis unidades de mensagem cifrada (β) são iguais, e o mesmo para todos os usuários do sistema. Seja P a assinatura de Ana (talvez incluindo um número de identificação, ou qualquer informação que garanta que a mensagem é mesmo

de Ana). Não é suficiente que Ana Envie para Bernardo a mensagem cifrada $f_B(P)$, já que todos sabem como fazer isso e assim não haveria nenhuma maneira de saber que a assinatura não foi forjada. Então no começo (ou no fim) da mensagem, Ana Transmite $f_B \cdot f_A^{-1}(P)$. Assim, quando Bernardo decodificar toda mensagem, incluindo essa parte, aplicando f_B^{-1}, ele verá que tudo foi transformado em unidade de mensagem pura, exceto uma pequena parte, que é $f_A^{-1}(P)$. Como Bernardo sabe que a mensagem é, supostamente, de Ana ele aplica f_A (que ele conhece, pois a chave codificadora de Ana é pública), e obtém P. Como ninguém além de Ana poderia ter aplicado a função f_A^{-1}, que é invertida aplicando f_A, ele finalmente tem certeza que a mensagem veio de Ana.

1.1 CIFRA DE CÉSAR

A cifra de César é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra representada no mesmo alfabeto. A substituição ocorre alterando a posição definida. Por exemplo para que a substituição ocorra no valor de 3 posições teríamos:

TEXTO SIMPLES	A	B	C	D	E	F	G	H	I	J	K	L	M
CIFRA	D	E	F	G	H	I	J	K	L	M	N	O	P

TEXTO SIMPLES	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CIFRA	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Os primeiros passos para cifrar um criptossistema é identificar todas as possíveis unidades de mensagem de texto puro e cifrado com objetos matemáticos para que as funções possam ser construídas. Esses objetos normalmente são simplesmente números inteiros em alguma ordem.

Por exemplo, se nossas unidades de mensagem de texto puro e cifrado são letras simples e tomamos como nosso alfabeto o alfabeto tradicional com 26 letras A-Z, nós podemos identificar as letras usando os inteiros 0, 1, 2, . . . , 25, os quais chamamos de números equivalentes. Logo teríamos:

TEXTO PURO	A	B	C	D	E	F	G	H	I	J	K	L	M
NÚMERO	0	1	2	3	4	5	6	7	8	9	10	11	12

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

Convertendo a mensagem SECRETO para a forma numérica mostrada acima, obtemos:

S	E	C	R	E	T	O
18	4	2	17	4	19	14

1.2 CONGRUÊNCIAS

1.2.1 Aritmética dos Restos

Segundo (HEFEZ, 2011: 110). Seja m um número natural diferente de zero. Diremos que dois números inteiros a e b são congruentes módulo m, se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b(mod\ m)$$

Por exemplo, $21 \equiv 13(mod\ 2)$, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Quando a relação $a \equiv b(mod\ m)$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso, $a \not\equiv b(mod\ m)$.

Como os restos da divisão de um número natural qualquer por 1 é sempre nulo, temos que $a \equiv b(mod\ 1)$, quaisquer que sejam a, $b \in \mathbb{N}$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $m > 1$.

Decorre, imediatamente, da definição que a congruência, módulo um número inteiro fixado m, é uma relação de equivalência. Vamos enunciar isto explicitamente abaixo.

Proposição 1 *Seja $m \in \mathbb{N}$. Para todos a, b, $c \in \mathbb{Z}$, tem-se que*

(i) $a \equiv a\ mod\ m$,

(ii) se $a \equiv b\ mod\ m$, então $b \equiv a\ mod\ m$,

(iii) se $a \equiv b\ mod\ m$ e $b \equiv c\ mod\ m$, então $a \equiv c\ mod\ m$.

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 2 *Suponha que a, b, $m \in \mathbb{Z}$ com $m > 1$. Tem-se que $a \equiv b(mod\ m)$ se, e somente se, $m \mid b - a$.*

Demonstração: Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, $a \equiv b(mod\ m)$ se, e somente se, $r = r'$, o que, em vista da igualdade acima é equivalente a dizer que $m \mid b - a$, já que $\mid r - r' \mid < m$.

Proposição 3 *Sejam a, b, c, d, $m \in \mathbb{Z}$ com $m > 1$.*

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

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

Demonstração: Suponhamos que $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$. Logo temos que $m \mid b - a$ e $m \mid d - c$

(i) Basta observar que $m \mid (b-a)+(d-c)$ e, portanto, $m \mid (b+d)-(a+c)$, o que prova essa parte do resultado.

(ii) Basta notar que $bd-ac = d(b-a)+a(d-c)$ e concluir que $m \mid (bd-ac)$.

1.3 ARITMÉTICA DAS CLASSES RESIDUAIS

As congruências módulo natural $m > 1$ permitem definir novas aritméticas que transcendem a própria teoria dos números, encontrando inúmeras e profundas aplicações em várias outras partes da matemática. Atualmente, essas aritméticas são a base de quase todos os procedimentos de cálculo dos computadores e possuem muitas aplicações tecnológicas.

Seja dado um número inteiro $m > 1$. Vamos repartir o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m. Isto nos dá a seguinte partição de $\mathbb{Z}$:

$$\begin{aligned} [0] &= \{x \in \mathbb{Z};\ x \equiv 0 \ mod \ m\}, \\ [1] &= \{x \in \mathbb{Z};\ x \equiv 1 \ mod \ m\}, \\ &\vdots \\ [m-1] &= \{x \in \mathbb{Z};\ x \equiv m-1 \ mod \ m\}. \end{aligned}$$

Paramos em $[m-1]$, pois tem-se que $[m] = [0],\ [m+1] = [1],\ \ldots$.

O conjunto

$$[a] = \{x \in \mathbb{Z};\ x \equiv a \ mod \ m\}$$

é chamado de *classe residual módulo* m do elemento a de $\mathbb{Z}$. O conjunto de todas as classes residuais módulo m será representado por $\mathbb{Z}_m$. Portanto,

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

Corolário 1 *Existem exatamente m classes residuais módulo m distintas, a saber,* $[0],\ [1],\ [2],\ \ldots,\ [m-1]$.

É fácil verificar que $\{a_1,\ \ldots,\ a_m\}$ é um sistema completo de resíduos módulo m se,e somente se,

$$[a_1],\ \ldots,\ [a_m] = \mathbb{Z}_m.$$

Uma vantagem das classes residuais é que transformam a congruência $a \equiv b(mod\ m)$ na igualdade $[a] = [b]$.

Em $\mathbb{Z}_m$ definimos as seguintes operações:

Adição: $[a] + [b] = [a + b]$

Multiplicação: $[a] \cdot [b] = [a \cdot b]$

Note que, tendo sido definidas estas operações usando os representantes a e b para classes residuais $[a]$ e $[b]$, respectivamente, temos que verificar que ao mudarmos os representantes das classes $[a]$ e $[b]$, não mudam os valores de $[a + b]$ e de $[a \cdot b]$.

Para verificar que isto acontece, basta notar que se $a \equiv a'(mod\ m)$ e $b \equiv b'(mod\ m)$, então $[a + b] = [a' + b']$ e $[a \cdot b] = [a' \cdot b']$, o que segue diretamente da Proposição 3.

As operações que acabamos de definir, acima gozam das seguintes propriedades.

Propriedades da Adição

Para todos $[a]$, $[b]$, $[c] \in \mathbb{Z}_m$, temos

A_1) **Associatividade**: $([a] + [b]) + [c] = [a] + ([b] + [c])$;

A_2) **Comutatividade**: $[a] + [b] = [b] + [a]$;

A_3) **Existência de zero**: $[a] + [0] = [a]$ para todo $[a] \in \mathbb{Z}_m$;

A_4) **Existência de simétrico**: $[a] - [a] = [0]$.

Propriedades da Multiplicação

Para todos $[a]$, $[b]$, $[c] \in \mathbb{Z}_m$, temos

M_1) **Associatividade**: $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$;

M_1) **Comutatividade**: $[a] \cdot [b] = [b] \cdot [a]$;

M_1) **Existência de unidade**: $[a] + [1] = [a]$.

AM **Distributividade**: $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$.

Todas estas propriedades são fáceis de verificar. Por exemplo, prova-se AM como se segue:

$$[a]\cdot([b]+[c]) = [a]\cdot[b+c] = [a\cdot(b+c)] = [a\cdot b+a\cdot c] = [a\cdot b]+[a\cdot c] = [a]\cdot[b]+[a]\cdot[c]$$

Um conjunto munido de um operação de adição e de uma operação de multiplicação, com as propriedades acima, será chamado de *anel*. Portanto, $\mathbb{Z}_m$, com as operações acima, é um anel, chamado *anel das classes residuais módulo* m.

Um elemento $[a] \in \mathbb{Z}_m$ será dito *invertível*, quando existir $[b] \in \mathbb{Z}_m$ tal que $[a][b] = 1$. Neste Caso, diremos que $[b]$ é o inverso de $[a]$.

Proposição 4 *$[a] \in \mathbb{Z}_m$ é invertível se, e somente se, $mdc(a, m) = 1$.*

Demonstração: Se $[a]$ é invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $[1] = [a] \cdot [b] = [a \cdot b]$. Logo, $a \cdot b \equiv 1 \ mod \ m$, isto é, existe um inteiro t tal que $a \cdot b + t \cdot m = 1$ e, consequentemente, $mdc(a, m) = 1$.

Reciprocamente, se $mdc(a, m) = 1$, existem inteiros b e t tais que $a\cdot b+m\cdot t = 1$ e, consequentemente, $[1] = [a\cdot b+m\cdot t] = [a\cdot b]+[m\cdot t] = [a]\cdot[b]+[0] = [a]\cdot[b]$. Portanto, $[a]$ é invertível.

Na classe residual módulo 26, temos que

$$\mathbb{Z}_{26} = \{[0],\ [1],\ [2],\ \ldots,\ [24],\ [25]\}.$$

E a seguir temos a tabela dos invertíveis em $\mathbb{Z}_{26}$:

1	3	5	7	9	11	15	17	19	21	23	25
25	9	21	15	3	19	7	23	11	5	17	1

2 MATRIZES

2.1 DEFINIÇÃO

A definição conforme (CALLIOLI, 1998: 16). Sejam $m \geq 1$ e $n \geq 1$ dois números inteiros. Uma matriz $m \times n$ real é uma dupla sequência de números reais, distribuídos em m linhas e n colunas, formando uma tabela.

As matrizes costumam ser representadas por letras maiúsculas e seus elementos por letras minúsculas, acompanhadas de dois índices que indicam, respectivamente, a linha e a coluna ocupadas pelo elemento. Algebricamente, uma matriz A do tipo $m \times n$ é representada por:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

Assim:

a_{11} é o elemento da 1^a linha e 1^a coluna.

a_{32} é o elemento da 3^a linha e 2^a coluna.

a_{23} é o elemento da 2^a linha e 3^a coluna.

Abreviadamente, podemos representar essa matriz A tomando-se um elemento genérico a_{ij}, onde $1 \leq i \leq m$ e $1 \leq j \leq n$.

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

Notações - Indicaremos por $M_{m \times n}(\mathbb{R})$ o conjunto das matrizes reais $m \times n$. Se $m = n$, ao invés de $M_{m \times n}(\mathbb{R})$, usa-se a notação $M_n(\mathbb{R})$. Cada matriz de $M_n(\mathbb{R})$ chama-se *matriz quadrada de ordem n*. Em contraposição,

quando $m \neq n$, uma matriz $m \times n$ se diz uma *matriz retangular*. Uma matriz 1×1 (a_{11}) se identifica com o número real a_{11}.

Exemplo 1 *Construa a matriz* $A = a_{ij} \in M_{2\times 3}(\mathbb{R})$*, sendo* $a_{ij} = i + j$*.*

$$a_{11} = 1 + 1 = 2 \qquad a_{21} = 2 + 1 = 3$$

$$a_{12} = 1 + 2 = 3 \qquad a_{22} = 2 + 2 = 4$$

$$a_{13} = 1 + 3 = 4 \qquad a_{23} = 2 + 3 = 5$$

Logo: $A = \begin{pmatrix} 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$

Linhas e Colunas

Dada uma matriz:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

as m sequências horizontais

$$A^{(1)} = (a_{11}, a_{12}, a_{13}, \dots, a_{1n}), \dots, A^{(m)} = (a_{m1}, a_{m2}, a_{m3}, \dots, a_{mn})$$

são chamadas *linhas* da matriz A, enquanto que as n sequências verticais

$$A_{(1)} = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \vdots \\ a_{m1} \end{pmatrix}, \dots, A_{(n)} = \begin{pmatrix} a_{1n} \\ a_{2n} \\ a_{3n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

são as *colunas* de A. É de se notar que cada $A^{(i)} \in M_{1\times n}(\mathbb{R})$ e cada $A_{(j)} \in M_{m\times 1}(\mathbb{R})$.

Exemplo 2 *Na matriz* 2×3

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 6 & -5 \end{pmatrix}$$

as linhas são $(1, 0, 1)$ *e* $(0, 6, -5)$ *ao passo que as colunas são* $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 6 \end{pmatrix}$ *e* $\begin{pmatrix} 1 \\ -5 \end{pmatrix}$.

Igualdade de matrizes

Consideremos duas matrizes reais $m \times n : A = (a_{ij})$ e $B = (b_{ij})$, dizemos que:

$$A = B \Longleftrightarrow a_{ij} = b_{ij}$$

para todo $1 \leq i \leq m$ e $1 \leq j \leq n$.

Exemplo 3 *Dadas as matrizes* $A = \begin{pmatrix} \frac{1}{2} & 5 \\ \sqrt[3]{8} & 0,25 \\ 2^0 & 0 \end{pmatrix}$ *e* $B = \begin{pmatrix} 0,5 & 6-1 \\ 2 & \frac{1}{4} \\ 1 & 3-3 \end{pmatrix}$, *temos que* $A = B$.

Exemplo 4 *Se as matrizes* $A = \begin{pmatrix} 2 & 0 \\ -1 & b \end{pmatrix}$ *e* $B = \begin{pmatrix} 2 & c \\ -1 & 3 \end{pmatrix}$, *são iguais, então* $c = 0$ *e* $b = 3$.

2.2 OPERAÇÕES COM MATRIZES

Para que seja possível aplicar o conceito de matrizes em diversas situações de resolução de problemas práticos é necessário que sejam definidos os processos de operações com matrizes.

2.2.1 Adição de matrizes

Sejam $A = (a_{ij})$ e $B = (b_{ij})$ matrizes $m \times n$. Indicamos por $A + B$ e chamamos soma de A com B a matriz $m \times n$ cujo termo geral é $a_{ij} + b_{ij}$, ou seja

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ \dots\dots\dots & \dots\dots\dots & \dots & \dots\dots\dots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

A operação que transforma cada par (A, B) de matrizes do mesmo tipo na matriz $A+B$ Chama-se adição de matrizes. É uma operação no conjunto $M_{m\times n}(\mathbb{R})$.

Exemplo 5 *Se* $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$ *e* $B = \begin{pmatrix} 0 & 1 & -2 \\ 2 & 4 & 7 \end{pmatrix}$, *então*

$$A + B = \begin{pmatrix} 1 & 3 & -1 \\ 2 & 5 & 9 \end{pmatrix}$$

Para a adição de matrizes acima definida valem as seguintes propriedades:

(i) $A + (B + C) = (A + B) + C,\ \forall\ A,\ B,\ C \in M_{m\times n}(\mathbb{R})$ (*associativa*);

(ii) $A + B = B + A,\ \forall\ A,\ B \in M_{m\times n}(\mathbb{R})$ (*comutativa*);

(iii) Existe uma matriz $O \in M_{m\times n}(\mathbb{R})$ tal que $A + O = A,\ \forall\ A \in M_{m\times n}(\mathbb{R})$ (existe *elemento neutro*);

(iv) Dada matriz $A \in M_{m\times n}(\mathbb{R})$, existe uma matriz $(-A)$, também $m\times n$, tal que $A + (-A) = 0$ (existe a *oposta* de qualquer matriz).

A verificação da propriedade associativa se faz assim:

Se $A = (a_{ij})$, $B = (b_{ij})$ e $C = (c_{ij})$, então

$(A + B) + C = (a_{ij} + b_{ij}) + (c_{ij}) = ((a_{ij} + b_{ij}) + c_{ij}) \stackrel{*}{=} (a_{ij} + (b_{ij} + c_{ij})) = (a_{ij}) + (b_{ij} + c_{ij}) = A + (B + C)$.

$*$ Usamos nesta passagem a propriedade associativa da adição de números reais.

Quanto a (iii) é fácil ver que:

$$O = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

Esta matriz chama-se *matriz nula* $m \times n$.

Por último, se $A = (a_{ij})$, é evidente que $(-A) = (-a_{ij})$. Por exemplo, se $A = \begin{pmatrix} 1 & a & -2 \\ -2 & 1 & 0 \end{pmatrix}$, então $-A = \begin{pmatrix} -1 & -a & 2 \\ 2 & -1 & 0 \end{pmatrix}$.

2.2.2 Multiplicação de uma matriz por um número

Dada uma matriz real $A = (a_{ij})$, $m \times n$, e dado um número real α o produto de α por A é a matriz $m \times n$ dada por:

$$\alpha A = \begin{pmatrix} \alpha a_{11} & \dots & \alpha a_{1n} \\ \dots\dots & \dots & \dots\dots \\ \alpha a_{m1} & \dots & \alpha a_{mn} \end{pmatrix}$$

Para essa operação que transforma cada par (α, A) de $(\mathbb{R}) \times M_{m\times n}(\mathbb{R})$ na matriz real $\alpha A \in M_{m\times n}(\mathbb{R})$, valem as seguintes propriedades:

(i) $(\alpha\beta)A = \alpha(\beta A)$;

(ii) $(\alpha + \beta)A = \alpha A + \beta A$;

(iii) $\alpha(A + B) = \alpha A + \alpha B$;

(iv) $1A = A$.

quaisquer que sejam as matrizes A e B e quaisquer que sejam os números reais α e β.

Provemos (ii).

Suponhamos $A = (a_{ij})$. Então:

$$(\alpha+\beta)\cdot A = ((\alpha+\beta)\cdot a_{ij}) = (\alpha\cdot a_{ij}+\beta\cdot a_{ij}) = (\alpha\cdot a_{ij})+(\beta\cdot a_{ij}) = \alpha A+\beta A.$$

Exemplo 6 *Dadas as matrizes* $A = \begin{pmatrix} 3 & -4 & 1 \\ 0 & 7 & 8 \end{pmatrix}$ *e* $B = \begin{pmatrix} 8 & -1 & 3 \\ 0 & 9 & 5 \end{pmatrix}$, *calcule* $3A + 2B$*:*

$$3\cdot\begin{pmatrix} 3 & -4 & 1 \\ 0 & 7 & 8 \end{pmatrix} + 2\cdot\begin{pmatrix} 8 & -1 & 3 \\ 0 & 9 & 5 \end{pmatrix} =$$

$$= \begin{pmatrix} 9 & -12 & 3 \\ 0 & 21 & 24 \end{pmatrix} + \begin{pmatrix} 16 & -2 & 6 \\ 0 & 18 & 10 \end{pmatrix} = \begin{pmatrix} 25 & -14 & 9 \\ 0 & 39 & 34 \end{pmatrix}$$

2.2.3 Multiplicação de matrizes

Consideremos a matriz $A = (a_{ij})$ de tipo $m \times n$ e a matriz $B = (b_{jk})$ de tipo $n \times p$. O *produto* de $A \cdot B$ (também indicado por AB) é a matriz do tipo $m \times p$ cujo termo geral é dado por:

$$c_{ik} = \sum_{j=1}^{n} a_{ij} + b_{jk} = a_{i1} + b_{1k} \ldots + a_{in} + b_{nk}$$

Usando a notação de matriz linha e a de matriz coluna a definição acima significa que

$$AB = \begin{pmatrix} A^{(1)}\cdot B_{(1)} & \ldots & A^{(1)}\cdot B_{(p)} \\ A^{(2)}\cdot B_{(1)} & \ldots & A^{(2)}\cdot B_{(p)} \\ \ldots\ldots\ldots & \ldots & \ldots\ldots\ldots \\ A^{(m)}\cdot B_{(1)} & \ldots & A^{(m)}\cdot B_{(p)} \end{pmatrix}$$

Nas condições acima, a operação que transforma cada par de matrizes (A, B) na matriz AB chama-se *multiplicação* de matrizes.

Exemplo 7 *Sejam* $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ *e* $B = \begin{pmatrix} 3 & 4 & 5 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, *então:*

$$AB = \begin{pmatrix} 2 \cdot 3 + 1 \cdot 0 + 0 \cdot 1 & 2 \cdot 4 + 1 \cdot 0 + 0 \cdot 0 & 2 \cdot 5 + 1 \cdot 0 + 0 \cdot 1 \\ 0 \cdot 3 + 1 \cdot 0 + 2 \cdot 1 & 0 \cdot 4 + 1 \cdot 0 + 2 \cdot 0 & 0 \cdot 5 + 1 \cdot 0 + 2 \cdot 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 6 & 8 & 10 \\ 2 & 0 & 2 \end{pmatrix}$$

Agora vamos mostrar um exemplo de aplicação da multiplicação de matrizes.

Exemplo 8 *Suponha que um pecuarista crie na sua chácara duas espécies de animais* A_1 *e* A_2 *e os alimente com dois tipos de vitaminas* R_1 R_2.

A seguir apresentamos duas tabelas (matrizes). A primeira mostra quanto cada espécie de animal come em kg do tipo de ração durante uma semana:

	R_1	R_2
A_1	*4*	*3*
A_2	*5*	*6*

A segunda tabela mostra a quantidade de unidades da vitamina (A e B) por kg do tipo de ração:

	Vitamina A	*Vitamina B*
R_1	*10*	*15*
R_2	*12*	*10*

Montemos agora uma terceira tabela que indique ao pecuarista quanto cada espécie de animal consome de cada vitamina por semana na alimentação:

	Vitamina A	*Vitamina B*
A_1		
A_2		

Cada elemento da tabela é encontrada por meio dos seguintes cálculos:

$$e_{11} = 4 \cdot 10 + 3 \cdot 12 = 40 + 36 = 76$$
$$e_{12} = 4 \cdot 15 + 3 \cdot 10 = 60 + 30 = 90$$
$$e_{21} = 5 \cdot 10 + 6 \cdot 12 = 50 + 72 = 122$$
$$e_{22} = 5 \cdot 15 + 6 \cdot 10 = 75 + 60 = 135$$

Obtemos, então a seguinte tabela:

	Vitamina A	*Vitamina B*
A_1	*76*	*90*
A_2	*122*	*135*

Representamos as duas primeiras tabelas pelas matrizes $A = \begin{pmatrix} 4 & 3 \\ 5 & 6 \end{pmatrix}$ *e* $B = \begin{pmatrix} 10 & 15 \\ 12 & 10 \end{pmatrix}$ *e a terceira tabela pela matriz* $C = \begin{pmatrix} 76 & 90 \\ 122 & 135 \end{pmatrix}$ *tem-se que* $A \cdot B = C$.

Proposição 5 - *Sejam* $A = (a_{ij})$, $B = (b_{jk})$ *e* $C = (c_{kr})$ *matrizes reais* $m \times n$, $n \times p$ *e* $p \times q$, *respectivamente. Então* $A(BC) = (AB)C$.

Demonstração - O termo geral de $A(BC)$ é dado por:

$$\sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{p} b_{jk} c_{kr} \right) \tag{1}$$

ao passo que o termo geral de $(AB)C$ é dado por:

$$\sum_{k=1}^{n} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) c_{kr} \tag{2}$$

As propriedades da adição e da multiplicação de números reais nos ensinam, contudo que (1) = (2). Então a proposição está demonstrada.

Proposição 6 - *Sejam A, B e C matrizes reais $m \times n$, $n \times p$ e $n \times p$, respectivamente. Então $A(B + C) = AB + AC$.*

Demonstração - Usa-se o mesmo tipo de raciocínio da demonstração anterior.

Nota: Analogamente, se A e B são matrizes $m \times n$ e C é $n \times p$, então $(A + B)C = AC + BC$.

2.2.4 Matriz inversa

Seja uma matriz quadrada A de ordem n. Quando existe uma matriz B também de ordem n, tal que $A \cdot B = B \cdot A = I_n$, B é chamada de matriz inversa de A, a qual indicamos por A^{-1}.

Se existir a matriz inversa de uma matriz dada dizemos que está é invertível ou não singular. Nesse caso, dizemos que a matriz A é invertível e sua inversa A^{-1} é única.

Se não existir a inversa de uma matriz dada dizemos que está não é invertível ou singular.

Exemplo 9 *Caso exista, determine a inversa da matriz* $A = \begin{pmatrix} 7 & 4 \\ 5 & 3 \end{pmatrix}$.

Se existir, a inversa da matriz A é do tipo $A^{-1} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, tal que $A \cdot A^{-1} = I_2$, ou seja:

$$\begin{pmatrix} 7 & 4 \\ 5 & 3 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 7x+4z & 7y+4w \\ 5x+3z & 5y+3w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Da igualdade de matrizes, temos os seguintes sistemas:

$$\begin{cases} 7x+4z=1 \\ 5x+3z=0 \end{cases} \quad \text{e} \quad \begin{cases} 7y+4w=0 \\ 5y+3w=1 \end{cases}$$

Resolvendo os sistemas temos: $x=3,\ z=-5,\ y=-4 \quad \text{e} \quad w=7.$

Em seguida, verificamos se $A^{-1}\cdot A = I_2$.

$$A^{-1}\cdot A = \begin{pmatrix} 3 & -4 \\ -5 & 7 \end{pmatrix} \cdot \begin{pmatrix} 7 & 4 \\ 5 & 3 \end{pmatrix} =$$

$$= \begin{pmatrix} 3\cdot 7-4\cdot 5 & 3\cdot 4-4\cdot 3 \\ -5\cdot 7+7\cdot 5 & -5\cdot 4+7\cdot 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Como $A\cdot A^{-1} = A^{-1}\cdot A = I_2$, segue que a matriz A é invertível, e sua inversa é $A^{-1} = \begin{pmatrix} 3 & -4 \\ -5 & 7 \end{pmatrix}$.

2.3 CARACTERIZAÇÃO DAS MATRIZES INVERTÍVEIS

A maneira mais popularizada de caracterizar a invertibilidade de uma matriz é por meio do seu determinante, conforme o

Teorema 2 *A matriz quadrada M é invertível se, e somente se, $det\ M \neq 0$.*

A metade da demonstração deste fato consiste no uso imediato da fórmula $det\ (MN) = det\ M \cdot det\ N$. Com efeito, se a matriz M possui a inversa M^{-1}, da igualdade $M\cdot M^{-}1 = I_3$ se conclui que $det\ M\cdot det\ (M^{-1}) = 1$, logo $det\ M \neq 0$ e, mais ainda, $det\ M^{-1} = 1/det\ M$.

Suponhamos agora que, reciprocamente, se tenha $det\ M \neq 0$. Procuremos uma matriz P tal que $MP = I_3$. Escrevamos

$$M = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}, \quad P = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} \quad \text{e} \quad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

A equação matricial $MP = I_3$ significa que os vetores-coluna da matriz procurada P são soluções (x_1, x_2, x_3), (y_1, y_2, y_3) e (z_1, z_2, z_3)dos sistemas abaixo:

$$\begin{cases} a_1x_1 + b_1x_2 + c_1x_3 = 1 \\ a_2x_1 + b_2x_2 + c_2x_3 = 0 \\ a_3x_1 + b_3x_2 + c_3x_3 = 0 \end{cases}, \begin{cases} a_1y_1 + b_1y_2 + c_1y_3 = 0 \\ a_2y_1 + b_2y_2 + c_2y_3 = 1 \\ a_3y_1 + b_3y_2 + c_3y_3 = 0 \end{cases} \quad \text{e}$$

$$\begin{cases} a_1z_1 + b_1z_2 + c_1z_3 = 0 \\ a_2z_1 + b_2z_2 + c_2z_3 = 0 \\ a_3z_1 + b_3z_2 + c_3z_3 = 1 \end{cases}.$$

Como $det\ M \neq 0$, segue-se que as linhas da matrizes M são linearmente independentes, logo cada um dos sistemas acima admite uma única solução. Noutras palavras, existe uma única matriz P, do tipo 3×3 tal que $MP = I_3$.

Num argumento inteiramente análogo, têm-se 3 sistemas com a matriz M (cujo determinante é o mesmo de M). As soluções desses 3 sistemas são as linhas de uma matriz Q, do tipo 3×3 tal que $QM = I_3$. Mas é claro que

$$Q = QI_3 = Q(MP) = (QM)P = I_3P = P.$$

Logo $PM = MP = I_3$, isto é, $P = M^{-1}$ é a matriz inversa de M. Assim, $m \neq 0 \Rightarrow m$ invertível.

Vemos portanto que as seguintes afirmações a respeito de uma matriz M do tipo 3×3 são equivalentes:

1. As linhas de M são linearmente independentes;

2. Todo sistema de equações lineares $MX = D$ tem solução única, seja qual for a matriz D, do tipo 3×1;

3. $det\ M = detM \neq 0$;

4. As colunas de M são linearmente independentes;

5. Existe uma única matriz M^{-1} tal que $M^{-}1M = MM^{-1} = I_3$ (M é invertível).

Observações

1. A restrição a matrizes 3×3 é meramente uma conveniência didática. Todos os resultados deste capítulo continuam válidos, com as mesmas demonstrações, para matrizes $n \times n$ em geral.

2. Se M e P são matrizes do tipo $n \times n$ tais que $MP = I_n$ então vale necessariamente $MP+ = I_n$ então vale necessariamente $PM = I_n$. Com efeito, se $MP = I_n$ então $det\ M \cdot det\ P = 1$, logo $det\ M \neq 0$, logo $det\ M \neq 0$. Então M possui uma inversa M^{-1}. Multiplicando à esquerda ambos os membros da igualdade $MP = I_n$ por M^{-1} obtemos $P = M^{-1}$, portanto $PM = M^{-1}M = I_n$.

2.4 MATRIZ INVERSA EM $\mathbb{Z}_{26}$

Considere a matriz $A = \begin{bmatrix} 4 & 2 \\ 1 & 1 \end{bmatrix}$ com $detA = 4 \cdot 1 - 2 \cdot 0 = 2 \neq 0$.

Poderíamos inicialmente pensar que deve existir A^{-1}, mas em $\mathbb{Z}_{26}$, 2 não é invertível.

Questão: existe B tal que $A \cdot B = I_2$ em $\mathbb{Z}_{26}$?

Por definição, devemos ter $A \cdot A^{-1} = I_2$, ou seja:

$$\begin{pmatrix} 4 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 4x+2z & 4y+2w \\ x+z & y+w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Pela igualdade de matrizes, construímos dois sistemas.

Resolvendo o primeiro sistema temos:

$$\begin{cases} 4x+2z=1 \\ x+z=0 \end{cases}$$

Mas analisando a primeira equação $4x+2z=1$ temos que o 1º membro é par e o 2º membro é ímpar, portanto em $\mathbb{Z}_{26}$ não há solução pois o lado esquerdo é congruente a zero *mod* 2.

A condição para que A seja invertível em $\mathbb{Z}_{26}$ e que $mdc(detA, 26) = 1$, isto é, o determinante de A deve ser invertível em $\mathbb{Z}_{26}$.

Como determinar a matriz inversa em $\mathbb{Z}_{26}$ da matriz $A = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$ com $detA = 7 \in \mathbb{Z}_{26}$. Para fazer isso vamos utilizar a tabela dos invertíveis no $\mathbb{Z}_{26}$:

1	3	5	7	9	11	15	17	19	21	23	25
25	9	21	15	3	19	7	23	11	5	17	1

(i) Determinar A^{-1} por substituição:

A inversa da matriz $A = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$, se existir, deve ser do tipo 2×2, ou seja, $A^{-1} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$.

Por definição, devemos ter $A \cdot A^{-1} = I_2$, ou seja:

$$\begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3x+2z & 3y+2w \\ 4x+5z & 4y+5w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Pela igualdade de matrizes, construímos dois sistemas.

Resolvendo o primeiro sistema temos:

$$\begin{cases} 3x+2z=1 & \cdot 9 \\ 4x+5z=0 \end{cases}$$

$$\begin{cases} x+18z=9 \\ 4x+5z=0 \end{cases}$$

Da primeira equação obtemos que:

$$x+18z=9$$
$$x=9-18z$$
$$x=9+8z$$

Substituindo-se o valor de x na segunda equação:

$$4x+5z=0$$
$$4\cdot(9+8z)+5z=0$$
$$36+32z+5z=0$$
$$10+11z=0 \quad \cdot 19$$
$$190+z=0$$
$$8+z=0$$
$$z=-8$$
$$z=18$$

Substituindo-se $z = 18$ em $x = 9 + 8z$,vem:

$$x = 9 + 8z$$
$$x = 9 + 8 \cdot 18$$
$$x = 9 + 144$$
$$x = 9 + 14$$
$$x = 23$$

Resolvendo o segundo sistema temos:

$$\begin{cases} 3y + 2w = 0 \\ 4y + 5w = 1 \qquad \cdot 21 \end{cases}$$

$$\begin{cases} 3y + 2w = 0 \\ 6y + w = 21 \end{cases}$$

Da segunda equação obtemos que:

$$6y + w = 21$$
$$w = 21 - 6y$$
$$w = 21 + 20y$$

Substituindo-se o valor de w na primeira equação:

$$3y + 2w = 0$$
$$3y + 2 \cdot (21 + 20y) = 0$$
$$3y + 42 + 40y = 0$$
$$43y + 42 = 0$$
$$17y + 16 \quad \cdot 23$$
$$y + 368 = 0$$
$$y + 4 = 0$$
$$y = -4$$
$$y = 22$$

Substituindo-se $y = 22$ em $w = 21 + 20y$,vem:

$$w = 21 + 20y$$
$$w = 21 + 20 \cdot 22$$
$$w = 21 + 440$$
$$w = 21 + 24$$
$$w = 45$$
$$w = 19$$

Portanto temos: $x = 23,\ z = 18,\ y = 22$ e $w = 19$. Logo temos que,

$$A^{-1} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 23 & 22 \\ 18 & 19 \end{pmatrix}$$

(ii) Determinar A^{-1} por escalonamento:

$$\left(\begin{array}{cc|cc} 3 & 2 & 1 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right) \begin{array}{c} \cdot 9 \\ \cdot 21 \end{array} \sim \left(\begin{array}{cc|cc} 1 & 18 & 9 & 0 \\ 6 & 1 & 0 & 21 \end{array}\right) \begin{array}{c} \\ 20 \cdot L_1 + L_2 \end{array} \sim$$

$$\sim \left(\begin{array}{cc|cc} 1 & 18 & 9 & 0 \\ 0 & 23 & 24 & 21 \end{array}\right) \begin{array}{c} \\ \cdot 17 \end{array} \sim \left(\begin{array}{cc|cc} 1 & 0 & 23 & 22 \\ 0 & 1 & 18 & 19 \end{array}\right) \begin{array}{c} \\ 8 \cdot L_2 + L_1 \end{array}$$

Portanto

$$A^{-1} = \begin{pmatrix} 23 & 22 \\ 18 & 19 \end{pmatrix}$$

3 CRIPTOGRAFIA EM BLOCOS

A criptografia em blocos utiliza matrizes para criptografar as mensagens, é um método que consiste transformar um texto original em um texto cifrado, de maneira a permitir que somente o receptor seja capaz de decifrar a mensagem utilizando a inversa da matriz chave.

Logo o primeiro passo que devemos tomar na criptografia em blocos para criptografar uma palavra ou frase é fazer a divisão dos blocos, do seguinte modo:

$$\text{Texto} \quad CRIPTOGRAFIA$$
$$\text{Bloco de tamanho } 2 : [CR][IP][TO][GR][AF][IA]$$
$$\text{Bloco de tamanho } 3 : [CRI][PTO][GRA][FIA]$$
$$\text{Bloco de tamanho } 4 : [CRIP][TOGR][FIAX]$$

Vamos definir que quando faltar letras para completar os blocos, completaremos com a letra X.

Situação geral com blocos de tamanho 2:

Cada unidade do texto puro $P = \begin{pmatrix} x \\ y \end{pmatrix}$ é transformada em um texto cifrado $C = \begin{pmatrix} x' \\ y' \end{pmatrix}$ do seguinte modo:

$C = A \cdot P$, isto é $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$

Para decodificar uma mensagem, se A for invertível basta aplicar a matriz inversa:

$P = A^{-1} \cdot A \cdot P = A^{-1} \cdot C$, isto é $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \end{pmatrix}$

Agora vamos criptografar dois exemplos:

Para criptografar a palavra CRIPTOGRAFIA, devemos multiplicar os

blocos de 2 pela matriz chave $A = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix}$. Para fazer isso devemos transformar a palavra em blocos:

- $\begin{bmatrix} C \\ R \end{bmatrix} \longleftrightarrow \begin{bmatrix} 2 \\ 17 \end{bmatrix}$
- $\begin{bmatrix} I \\ P \end{bmatrix} \longleftrightarrow \begin{bmatrix} 8 \\ 15 \end{bmatrix}$
- $\begin{bmatrix} T \\ O \end{bmatrix} \longleftrightarrow \begin{bmatrix} 19 \\ 14 \end{bmatrix}$
- $\begin{bmatrix} G \\ R \end{bmatrix} \longleftrightarrow \begin{bmatrix} 6 \\ 17 \end{bmatrix}$
- $\begin{bmatrix} A \\ F \end{bmatrix} \longleftrightarrow \begin{bmatrix} 0 \\ 5 \end{bmatrix}$
- $\begin{bmatrix} I \\ A \end{bmatrix} \longleftrightarrow \begin{bmatrix} 8 \\ 0 \end{bmatrix}$

Devemos multiplicar os blocos pela matriz chave A:

- $\begin{bmatrix} C \\ R \end{bmatrix} \longleftrightarrow \begin{bmatrix} 2 \\ 17 \end{bmatrix}$

$$A \cdot \begin{bmatrix} C \\ R \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 17 \end{bmatrix} = \begin{bmatrix} 4+119 \\ 10+306 \end{bmatrix} = \begin{bmatrix} 123 \\ 316 \end{bmatrix}$$

Logo temos que,

$$123 \equiv 19 (mod\ 26) \quad \text{e} \quad 316 \equiv 4 (mod\ 26)$$

Portanto:

$$\begin{bmatrix} 123 \\ 316 \end{bmatrix} = \begin{bmatrix} 19 \\ 4 \end{bmatrix} \longleftrightarrow \begin{bmatrix} T \\ E \end{bmatrix}$$

- $\begin{bmatrix} I \\ P \end{bmatrix} \longleftrightarrow \begin{bmatrix} 8 \\ 15 \end{bmatrix}$

$$A \cdot \begin{bmatrix} I \\ P \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 15 \end{bmatrix} = \begin{bmatrix} 16+105 \\ 40+270 \end{bmatrix} = \begin{bmatrix} 121 \\ 310 \end{bmatrix}$$

Logo temos que,

$$121 \equiv 17(mod\ 26) \quad \text{e} \quad 310 \equiv 24(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 121 \\ 310 \end{bmatrix} = \begin{bmatrix} 17 \\ 24 \end{bmatrix} \longleftrightarrow \begin{bmatrix} R \\ Y \end{bmatrix}$$

- $\begin{bmatrix} T \\ O \end{bmatrix} \longleftrightarrow \begin{bmatrix} 19 \\ 14 \end{bmatrix}$

$$A \cdot \begin{bmatrix} T \\ O \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 14 \end{bmatrix} = \begin{bmatrix} 38+98 \\ 95+252 \end{bmatrix} = \begin{bmatrix} 136 \\ 347 \end{bmatrix}$$

Logo temos que,

$$136 \equiv 6(mod\ 26) \quad \text{e} \quad 347 \equiv 9(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 136 \\ 347 \end{bmatrix} = \begin{bmatrix} 6 \\ 9 \end{bmatrix} \longleftrightarrow \begin{bmatrix} G \\ J \end{bmatrix}$$

- $\begin{bmatrix} G \\ R \end{bmatrix} \longleftrightarrow \begin{bmatrix} 6 \\ 17 \end{bmatrix}$

$$A \cdot \begin{bmatrix} G \\ R \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 17 \end{bmatrix} = \begin{bmatrix} 12+119 \\ 30+306 \end{bmatrix} = \begin{bmatrix} 131 \\ 336 \end{bmatrix}$$

Logo temos que,

$$131 \equiv 1(mod\ 26) \quad \text{e} \quad 336 \equiv 24(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 131 \\ 336 \end{bmatrix} = \begin{bmatrix} 1 \\ 24 \end{bmatrix} \longleftrightarrow \begin{bmatrix} B \\ Y \end{bmatrix}$$

- $\begin{bmatrix} A \\ F \end{bmatrix} \longleftrightarrow \begin{bmatrix} 0 \\ 5 \end{bmatrix}$

$$A \cdot \begin{bmatrix} A \\ F \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 5 \end{bmatrix} = \begin{bmatrix} 0+35 \\ 0+90 \end{bmatrix} = \begin{bmatrix} 35 \\ 90 \end{bmatrix}$$

Logo temos que,

$$35 \equiv 9(mod\ 26) \quad \text{e} \quad 90 \equiv 12(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 35 \\ 90 \end{bmatrix} = \begin{bmatrix} 9 \\ 12 \end{bmatrix} \longleftrightarrow \begin{bmatrix} J \\ M \end{bmatrix}$$

- $\begin{bmatrix} I \\ A \end{bmatrix} \longleftrightarrow \begin{bmatrix} 8 \\ 0 \end{bmatrix}$

$$A \cdot \begin{bmatrix} I \\ A \end{bmatrix} = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 0 \end{bmatrix} = \begin{bmatrix} 16+0 \\ 40+0 \end{bmatrix} = \begin{bmatrix} 16 \\ 40 \end{bmatrix}$$

Logo temos que,

$$40 \equiv 14(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 16 \\ 40 \end{bmatrix} = \begin{bmatrix} 16 \\ 14 \end{bmatrix} \longleftrightarrow \begin{bmatrix} Q \\ O \end{bmatrix}$$

Então a palavra CRIPTOGRAFIA depois de cifrada é TERYGJBYJMQO.

Para decriptografar a mensagem é necessário conhecer a matriz chave, pois assim devemos determinar a inversa e decodificar a mensagem.

No exemplo temos a matriz chave $A = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix}$ e $detA = 2 \cdot 18 - 7 \cdot 5 = 1$.

A inversa da matriz $A = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix}$, se existir, deve ser do tipo 2×2, ou seja, $A^{-1} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$.

Por definição, devemos ter $A \cdot A^{-1} = I_2$, ou seja:

$$\begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2x + 7z & 2y + 7w \\ 5x + 18z & 5y + 18w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Pela igualdade de matrizes, construímos os seguintes sistemas:

$$\begin{cases} 2x + 7z = 1 \\ 5x + 18z = 0 \end{cases} \quad \text{e} \quad \begin{cases} 2y + 7w = 0 \\ 5y + 18w = 1 \end{cases}$$

Resolvendo os sistemas temos: $x = 18$, $z = 21$, $y = 19$ e $w = 2$. Portanto:

$$A^{-1} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix}$$

Como vimos a inversa da matriz $A = \begin{bmatrix} 2 & 7 \\ 5 & 18 \end{bmatrix}$ é a matriz $A^{-1} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix}$. Agora vamos decriptografar a mensagem TERYGJBYJMQO, para fazer isso vamos transformar a palavra em blocos de 2 e multiplicar pela inversa da matriz chave:

- $\begin{bmatrix} T \\ E \end{bmatrix} \longleftrightarrow \begin{bmatrix} 19 \\ 4 \end{bmatrix}$

$$A^{-1} \cdot \begin{bmatrix} T \\ E \end{bmatrix} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 4 \end{bmatrix} = \begin{bmatrix} 342 + 76 \\ 399 + 8 \end{bmatrix} = \begin{bmatrix} 418 \\ 407 \end{bmatrix}$$

Logo temos que,

$$418 \equiv 2(mod\ 26) \quad \text{e} \quad 407 \equiv 17(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 418 \\ 407 \end{bmatrix} = \begin{bmatrix} 2 \\ 17 \end{bmatrix} \longleftrightarrow \begin{bmatrix} C \\ R \end{bmatrix}$$

- $\begin{bmatrix} R \\ Y \end{bmatrix} \longleftrightarrow \begin{bmatrix} 17 \\ 24 \end{bmatrix}$

$$A^{-1} \cdot \begin{bmatrix} R \\ Y \end{bmatrix} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 24 \end{bmatrix} = \begin{bmatrix} 306 + 456 \\ 357 + 48 \end{bmatrix} = \begin{bmatrix} 762 \\ 405 \end{bmatrix}$$

Logo temos que,

$$762 \equiv 8(mod\ 26) \quad \text{e} \quad 405 \equiv 15(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 762 \\ 405 \end{bmatrix} = \begin{bmatrix} 8 \\ 15 \end{bmatrix} \longleftrightarrow \begin{bmatrix} I \\ P \end{bmatrix}$$

- $\begin{bmatrix} G \\ J \end{bmatrix} \longleftrightarrow \begin{bmatrix} 6 \\ 9 \end{bmatrix}$

$$A^{-1} \cdot \begin{bmatrix} G \\ J \end{bmatrix} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 9 \end{bmatrix} = \begin{bmatrix} 108 + 171 \\ 126 + 18 \end{bmatrix} = \begin{bmatrix} 279 \\ 144 \end{bmatrix}$$

Logo temos que,

$$279 \equiv 19(mod\ 26) \quad \text{e} \quad 144 \equiv 14(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 279 \\ 144 \end{bmatrix} = \begin{bmatrix} 19 \\ 14 \end{bmatrix} \longleftrightarrow \begin{bmatrix} T \\ O \end{bmatrix}$$

- $\begin{bmatrix} B \\ Y \end{bmatrix} \longleftrightarrow \begin{bmatrix} 1 \\ 24 \end{bmatrix}$

$$A^{-1} \cdot \begin{bmatrix} B \\ Y \end{bmatrix} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 24 \end{bmatrix} = \begin{bmatrix} 18 + 456 \\ 21 + 48 \end{bmatrix} = \begin{bmatrix} 474 \\ 69 \end{bmatrix}$$

Logo temos que,

$$474 \equiv 6(mod\ 26) \quad \text{e} \quad 69 \equiv 17(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 474 \\ 69 \end{bmatrix} = \begin{bmatrix} 6 \\ 17 \end{bmatrix} \longleftrightarrow \begin{bmatrix} G \\ R \end{bmatrix}$$

- $\begin{bmatrix} J \\ M \end{bmatrix} \longleftrightarrow \begin{bmatrix} 9 \\ 12 \end{bmatrix}$

$$A^{-1} \cdot \begin{bmatrix} J \\ M \end{bmatrix} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix} \cdot \begin{bmatrix} 9 \\ 12 \end{bmatrix} = \begin{bmatrix} 162 + 228 \\ 189 + 24 \end{bmatrix} = \begin{bmatrix} 390 \\ 213 \end{bmatrix}$$

Logo temos que,

$$390 \equiv 0(mod\ 26) \quad \text{e} \quad 213 \equiv 5(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 390 \\ 213 \end{bmatrix} = \begin{bmatrix} 0 \\ 5 \end{bmatrix} \longleftrightarrow \begin{bmatrix} A \\ F \end{bmatrix}$$

- $\begin{bmatrix} Q \\ O \end{bmatrix} \longleftrightarrow \begin{bmatrix} 16 \\ 14 \end{bmatrix}$

$$A^{-1} \cdot \begin{bmatrix} Q \\ O \end{bmatrix} = \begin{bmatrix} 18 & 19 \\ 21 & 2 \end{bmatrix} \cdot \begin{bmatrix} 16 \\ 14 \end{bmatrix} = \begin{bmatrix} 288 + 266 \\ 336 + 28 \end{bmatrix} = \begin{bmatrix} 554 \\ 364 \end{bmatrix}$$

Logo temos que,

$$554 \equiv 8(mod\ 26) \quad \text{e} \quad 364 \equiv 0(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 554 \\ 364 \end{bmatrix} = \begin{bmatrix} 8 \\ 0 \end{bmatrix} \longleftrightarrow \begin{bmatrix} I \\ A \end{bmatrix}$$

Então a mensagem TERYGJBYJMQO decriptografada é CRIPTOGRAFIA.

No segundo exemplo vamos criptografar a palavra PROFMAT utilizando como matriz chave $A = \begin{bmatrix} 0 & 0 \\ 1 & 3 \end{bmatrix}$, a matriz A não possui inversa.

- $\begin{bmatrix} P \\ R \end{bmatrix} \longleftrightarrow \begin{bmatrix} 12 \\ 14 \end{bmatrix}$

$$A \cdot \begin{bmatrix} P \\ R \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 14 \end{bmatrix} = \begin{bmatrix} 0 + 0 \\ 12 + 42 \end{bmatrix} = \begin{bmatrix} 0 \\ 54 \end{bmatrix}$$

Logo temos que,

$$54 \equiv 2(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 0 \\ 54 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix} \longleftrightarrow \begin{bmatrix} D \\ F \end{bmatrix}$$

Não iremos continuar codificando a mensagem porque vamos mostrar que está codificação não é injetiva.

- $\begin{bmatrix} E \\ M \end{bmatrix} \longleftrightarrow \begin{bmatrix} 1 \\ 9 \end{bmatrix}$

$$A \cdot \begin{bmatrix} E \\ M \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 9 \end{bmatrix} = \begin{bmatrix} 0+0 \\ 1+27 \end{bmatrix} = \begin{bmatrix} 0 \\ 28 \end{bmatrix}$$

Logo temos que,

$$28 \equiv 2(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 0 \\ 28 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix} \longleftrightarrow \begin{bmatrix} D \\ F \end{bmatrix}$$

- $\begin{bmatrix} H \\ L \end{bmatrix} \longleftrightarrow \begin{bmatrix} 4 \\ 8 \end{bmatrix}$

$$A \cdot \begin{bmatrix} H \\ L \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 8 \end{bmatrix} = \begin{bmatrix} 0+0 \\ 4+24 \end{bmatrix} = \begin{bmatrix} 0 \\ 28 \end{bmatrix}$$

Logo temos que,

$$28 \equiv 2(mod\ 26)$$

Portanto:

$$\begin{bmatrix} 0 \\ 28 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix} \longleftrightarrow \begin{bmatrix} D \\ F \end{bmatrix}$$

Observação: Temos da álgebra linear que dada a matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, com a, b, c e d são números reais, a matriz é invertível se, e somente, se o determinante $D = ad - bc$ é diferente de zero. Quando trabalhamos em um anel arbitrário $\mathbb{R}$, temos uma situação análoga. De fato, suponha que

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$$

e $D = det(A) = ad - bc \in \mathbb{R}^*$. Seja D^{-1} o inverso multiplicativo de D em $\mathbb{R}$. Então:

$$\begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} D^{-1}(da - bc) & 0 \\ 0 & D^{-1}(-cb + ad) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Se multiplicarmos na ordem inversa, vamos obter o mesmo resultado.

Além dessa, temos outras condições suficientes para que uma matriz seja invertível. Isso pode ser visto no seguinte resultado:

Proposição 7 *Sejam* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_{26})$ *e* $D = ad - bc$. *As seguintes condições são equivalentes:*

(i) $mdc(detA, 26) = 1$;

(ii) A tem uma matriz inversa;

(iii) Se x e y não são ambos zero em $\mathbb{Z}_{26}$, então $A \begin{pmatrix} x \\ y \end{pmatrix} \neq A \begin{pmatrix} 0 \\ 0 \end{pmatrix}$;

(iv) A determina uma correspondência injetora do conjunto $(\mathbb{Z}_{26})^2$ nele mesmo.

DEMONSTRAÇÃO: Já provamos que (i) $\Rightarrow$ (ii). Agora vamos provar que

$$\text{(ii)} \Rightarrow \text{(iv)} \Rightarrow \text{(iii)} \Rightarrow \text{(i)}$$

Suponha que (ii) é verdadeira. Então (iv) também vale, pois A nos dá uma aplicação que leva $\begin{pmatrix} x \\ y \end{pmatrix}$ em $\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ e A^{-1} nos dá a aplicação inversa que leva $\begin{pmatrix} x' \\ y' \end{pmatrix}$ em $\begin{pmatrix} x \\ y \end{pmatrix}$.

Agora, se vale (iv), temos que $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ implica $A \begin{pmatrix} x \\ y \end{pmatrix} \neq A \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Logo (iii) também é verdadeira.

Agora suponhamos que (i) é falsa. Suponha também que $m = mdc(D, 26) > 1$ e que $m' = \frac{26}{m}$. Temos três casos possíveis.

• Se todas as quatro entradas de A são divisíveis, por m, tome $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} m' \\ m' \end{pmatrix}$ e temos uma contradição com (iii).

• Se a e b não são ambos divisíveis por m, tome $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -bm' \\ am' \end{pmatrix}$. Assim,

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -bm' \\ am' \end{pmatrix} = \begin{pmatrix} -abm' + bam' \\ -cbm' + dam' \end{pmatrix} = \begin{pmatrix} 0 \\ Dm' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

pois como m divide D, segue que $26 = mm'$ divide Dm'.

• Se c e d não são ambos divisíveis por m, tome $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} dm' \\ -cm' \end{pmatrix}$ e proceda como no caso anterior.

Logo, em todos os casos temos uma contradição, o que implica que (iii) $\Rightarrow$ (i).

4 PROBLEMAS

Seja $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ e $f(x) = ax+b$. f é injetiva se, e somente se, $mdc(a, 26) = 1$. Quando f não é injetiva, a imagem inversa de cada elemento da imagem de f é um conjunto com 2 elementos quando a é par ou com 13 elementos quando $a = 13$. Para criptografar usando uma função afim em um alfabeto com N letras e com parâmetros $a \in \mathbb{Z}_{26}^*$ e $b \in \mathbb{Z}_{26}$ consiste das seguintes regras:

$$y \equiv ax + b(modN), \qquad x \equiv a'x + b'(modN)$$

onde

$a' = a^{-1}$ em $\mathbb{Z}_{26}^*$ e $b' = -a^{-1}b$ em $\mathbb{Z}_{26}$.

Agora suponha a função $y = 4x+5$, como $mdc = (4, 26) = 2$, temos que a função não é injetiva, logo a imagem inversa de um elemento é um conjunto com 2 elementos.

Então temos que:

Para $x = 0$, $f(0) \equiv 4 \cdot 0 + 5 \equiv 5 \quad mod26$.

Para $x = 1$, $f(1) \equiv 4 \cdot 1 + 5 \equiv 9 \quad mod26$.

Para $x = 2$, $f(2) \equiv 4 \cdot 2 + 5 \equiv 13 \quad mod26$.

Para $x = 14$, $f(14) \equiv 4 \cdot 14 + 5 \equiv 9 \quad mod26$.

Portanto temos que para $x = 1$ e $x = 14$ temos a mesma imagem $y = 9$, logo não é injetiva.

No trabalho CriptoMat2 para implementação de um software educativo de criptografia, no qual o usuário interage com o programa, escolhendo as matrizes surge a necessidade de conhecer a imagem inversa dos elementos de $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ que estão na imagem da transformação A. O conhecimento da imagem inversa permite ao programa sugerir palavras ao usuário para que

este perceba que sua escolha não encripta de modo apropriado.

Seja $A : (\mathbb{Z}_{26})^2 \to (\mathbb{Z}_{26})^2$, A não invertível.

Sejam $\begin{pmatrix} a \\ b \end{pmatrix} \in Im(A)$ e

$$\left[A^{-1}\right] \begin{pmatrix} a \\ b \end{pmatrix} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in (\mathbb{Z}_{26})^2 \;\middle|\; A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \right\}$$

Problema: Quantos e quais são os elementos de $[A^{-1}] \begin{pmatrix} a \\ b \end{pmatrix}$.

Como A é linear, basta responder para $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

A resposta para esta questão está no seguinte teorema.

Teorema 3 *Quando o* $mdc(detA, 26) \neq 1$ *não possui uma única solução, vamos analisar os seguintes casos:*

(i) Quando $mdc(detA, 26) = 13$*, então a imagem inversa de* $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ *possui* 169 *elementos, a saber*

$$f^{-1} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \;\middle|\; x \text{ e } y \text{ são pares} \right\}$$

(ii) Quando $mdc(detA, 26) = par$*.*

Vamos representar respectivamente por p *e* i*, as entradas da matriz que são números pares e as que são números impares.*

(ii.a) Se A for a matriz $\begin{bmatrix} p & p \\ p & p \end{bmatrix}$*, temos para esse sistema temos quatro*

soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 13 \end{bmatrix}$, $\begin{bmatrix} 13 \\ 0 \end{bmatrix}$ *e* $\begin{bmatrix} 13 \\ 13 \end{bmatrix}$.

(ii.b) Se A for a matriz for da forma $\begin{bmatrix} p & p \\ p & i \end{bmatrix}$, $\begin{bmatrix} p & i \\ p & p \end{bmatrix}$ *ou* $\begin{bmatrix} p & i \\ p & i \end{bmatrix}$*, vamos*

ter duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ *e* $\begin{bmatrix} 13 \\ 0 \end{bmatrix}$.

(ii.c) Se A for a matriz $\begin{bmatrix} i & p \\ p & p \end{bmatrix}$, $\begin{bmatrix} p & p \\ i & p \end{bmatrix}$ *ou* $\begin{bmatrix} i & p \\ i & p \end{bmatrix}$*, vamos ter duas*

soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ *e* $\begin{bmatrix} 0 \\ 13 \end{bmatrix}$.

(ii.d) Se A for a matriz $\begin{bmatrix} i & i \\ p & p \end{bmatrix}$ *ou* $\begin{bmatrix} p & p \\ i & i \end{bmatrix}$ *, vamos ter duas soluções:*

$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ *e* $\begin{bmatrix} 13 \\ 13 \end{bmatrix}$.

Prova:

Caso (i) $mdc(detA, 26) = 13$.

Logo $detA = ad - bc = 13$, daí

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\left\{\begin{array}{ll|l} ax+by=0 & (d) & (c) \\ cx+dy=0 & (b) & (a) \end{array}\right.$$

$$\left\{\begin{array}{l} adx+bdy=0 \\ bcx+bdy=0 \end{array}\right.$$

$$\left\{\begin{array}{lllll} (ad-bc)x=0 & \Rightarrow x=0 & \text{ou} & x & \text{é par} \\ (ad-bc)y=0 & \Rightarrow y=0 & \text{ou} & y & \text{é par} \end{array}\right.$$

Se a é ímpar e $a \neq 13$, temos:

$$ax+by=0$$
$$a^{-1}ax+a^{-1}by=0$$
$$x=-a^{-1}by$$

Portanto quando $mdc(detA, 26) = 13$ temos que a imagem inversa de $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ possui 169 elementos, logo não é injetiva.

Caso (ii.a) $mdc(detA, 26) = par$.

Então se A for a matriz $\begin{bmatrix} p & p \\ p & p \end{bmatrix}$, temos:

$$\begin{bmatrix} p & p \\ p & p \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\left\{\begin{array}{l} px+py=0 \\ px+py=0 \end{array}\right.$$

Portanto, para esse sistema temos quatro soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 13 \end{bmatrix}$, $\begin{bmatrix} 13 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 13 \end{bmatrix}$.

Caso (ii.b) $mdc(detA, 26) = par$.

Então se A for a matriz $\begin{bmatrix} p & p \\ p & i \end{bmatrix}$, temos:

$$\begin{bmatrix} p & p \\ p & i \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} px + py = 0 \\ px + iy = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 0 \end{bmatrix}$.

Então se A for a matriz $\begin{bmatrix} p & i \\ p & p \end{bmatrix}$, temos:

$$\begin{bmatrix} p & i \\ p & p \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} px + iy = 0 \\ px + py = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 0 \end{bmatrix}$.

Então se A for a matriz $\begin{bmatrix} p & i \\ p & i \end{bmatrix}$, temos:

$$\begin{bmatrix} p & i \\ p & i \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} px + iy = 0 \\ px + iy = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 0 \end{bmatrix}$.

Portanto, se A for a matriz $\begin{bmatrix} p & p \\ p & i \end{bmatrix}$, $\begin{bmatrix} p & i \\ p & p \end{bmatrix}$ ou $\begin{bmatrix} p & i \\ p & i \end{bmatrix}$, vamos ter duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 0 \end{bmatrix}$.

Caso (ii.c) $mdc(detA, 26) = par$.

Então se A for a matriz $\begin{bmatrix} i & p \\ p & p \end{bmatrix}$, temos:

$$\begin{bmatrix} i & p \\ p & p \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} ix + py = 0 \\ px + py = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 0 \\ 13 \end{bmatrix}$.

Então se A for a matriz $\begin{bmatrix} p & p \\ i & p \end{bmatrix}$, temos:

$$\begin{bmatrix} p & p \\ i & p \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} px + py = 0 \\ ix + py = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 0 \\ 13 \end{bmatrix}$.

Então se A for a matriz $\begin{bmatrix} i & p \\ i & p \end{bmatrix}$, temos:

$$\begin{bmatrix} i & p \\ i & p \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} ix + py = 0 \\ ix + py = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 0 \\ 13 \end{bmatrix}$.

Portanto, se A for a matriz $\begin{bmatrix} i & p \\ p & p \end{bmatrix}$, $\begin{bmatrix} p & p \\ i & p \end{bmatrix}$ ou $\begin{bmatrix} i & p \\ i & p \end{bmatrix}$, vamos ter duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 0 \\ 13 \end{bmatrix}$.

Caso (ii.d) $mdc(detA, 26) = par$.

Então se A for a matriz $\begin{bmatrix} i & i \\ p & p \end{bmatrix}$, temos:

$$\begin{bmatrix} i & i \\ p & p \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} ix + iy = 0 \\ px + py = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 13 \end{bmatrix}$.

Então se A for a matriz $\begin{bmatrix} p & p \\ i & i \end{bmatrix}$, temos:

$$\begin{bmatrix} p & p \\ i & i \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{cases} px + py = 0 \\ ix + iy = 0 \end{cases}$$

Para esse sistema temos duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 13 \end{bmatrix}$.

Portanto, se A for a matriz $\begin{bmatrix} i & i \\ p & p \end{bmatrix}$ ou $\begin{bmatrix} p & p \\ i & i \end{bmatrix}$, vamos ter duas soluções: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ e $\begin{bmatrix} 13 \\ 13 \end{bmatrix}$.

5 PROPOSTA METODOLÓGICA

5.1 SOBRE A PROPOSTA

Este capítulo trata de uma proposta a ser apresentada aos alunos do ensino médio após terem trabalhado com matrizes para que apliquem o que aprenderam de forma prática com a criptografia em blocos.

5.2 PLANO DE AULA

Quantidade de aulas: 5 aulas de 50 minutos.

Ano: 2º ano.

Etapa de Ensino: Ensino Médio.

2º Bimestre.

5.2.1 Primeira Aula

Objetivos Gerais:

•Relacionar a criptografia com assuntos de matemática vistos no ensino básico.

• Apresentar a criptografia, associando cada letra do alfabeto a uma única letra.

Objetivo Específico:

• Introduzir a definição de criptografia;

• Criptografar e decriptograr utilizando a cifra de César.

Conteúdos:

História da criptografia e cifra de César.

Metodologia:

Recursos: Data show, lousa e giz.

Mostrar que a criptografia está relacionada às ideias de função, visto que cada letra do alfabeto foi associada a uma única outra letra. É importante que os alunos percebam que uma mensagem codificada possui apenas uma mensagem original correspondente e, para obtê-la é necessário conhecer a chave decodificadora.

Organizar os alunos em duplas para realizar a leitura e responder as questões.

Atividade 1

a) De acordo com o texto, porque a criptografia é importante?

b) De acordo com o exemplo apresentado, decodifique a mensagem FULS-WRJUDILD?

c) Junte-se a um colega, elabore uma chave de criptografia e decodifiquem algumas mensagens.

Na questão *c*), as duplas terão 15 minutos para que tentem decodificar as mensagens sem as chaves. Em seguida, pedir para as duplas forneçam as chaves e decodifiquem as mensagens.

5.2.2 Segunda Aula

Objetivos Gerais:

• Introduzir a criptografia em sala de aula como fator motivacional para verificar a aprendizagem dos alunos com respeito a multiplicação de matrizes e matriz inversa.

Objetivo Específico:

• Identificar quando o produto de matrizes é possível;

• Calcular o produto entre matrizes;

• Obter a matriz identidade de ordem n;

• Calcular a matriz inversa de uma matriz;

• Resolver problemas envolvendo matrizes utilizando sistemas lineares;

• Relacionar matrizes com a codificação e decodificação de mensagens.

Conteúdos:

Criptografia em blocos.

Metodologia:

Recursos: Data show, lousa e giz.

Apresentar aos alunos a relação entre o alfabeto e os números, em que cada algarismo do sistema decimal é associado a um único algarismo com base nesse sistema codificar e decodificar alguns exemplos na lousa. Nessa atividade vamos relacionar a criptografia com multiplicação de matrizes, mas o diferencial é que vamos envolver matriz inversa nesses cálculos, o que permite fazer uma avaliação sobre o aprendizado dos alunos com relação a esse conteúdo de modo instigante, pois obter a real mensagem será motivante para os discentes. Isso será feito através da resolução de um exemplo prático de aplicação, com a participação dos alunos.

5.2.3 Terceira Aula e Quarta Aula

Objetivos Gerais:

• Identificar regularidades em situações semelhantes para estabelecer regras, algoritmos e propriedades.

Objetivo Específico:

• Identificar quando o produto de matrizes é possível;

• Calcular o produto entre matrizes;

• Obter a matriz identidade de ordem n;

• Calcular a matriz inversa de uma matriz;

• Resolver problemas envolvendo matrizes utilizando sistemas lineares;

• Relacionar matrizes com a codificação e decodificação de mensagens.

Conteúdos:

Criptografia em blocos.

Metodologia:

Recursos:lápis, borracha e a folha contendo a atividade.

Esta atividade será aplicada em sala de aula ao final do conteúdo de matrizes para a verificação da aprendizagem dos alunos com relação a esse conteúdo. Os alunos responderão a atividade e, ao término da discussão, o docente responderá a atividade utilizando o software CriptoMat2 no site http://ivitu.com.br/criptomat/criptomat2/modulo07/ com a participação dos alunos.

Atividade 2

1) Criptografar e decriptografar a palavra MATEMATICA utilizando a matriz chave $A = \begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$.

2) Utilizar a matriz chave $B = \begin{bmatrix} 3 & 8 \\ 1 & 5 \end{bmatrix}$ criptografar as palavras:

a) amor;

b) felicidade;

c) respeito.

3) Decriptografar as matrizes $\begin{bmatrix} A \\ N \end{bmatrix}, \begin{bmatrix} A \\ E \end{bmatrix}, \begin{bmatrix} R \\ Y \end{bmatrix}, \begin{bmatrix} B \\ Y \end{bmatrix}, \begin{bmatrix} M \\ R \end{bmatrix}, \begin{bmatrix} O \\ G \end{bmatrix}, \begin{bmatrix} N \\ A \end{bmatrix}, \begin{bmatrix} C \\ Z \end{bmatrix}, \begin{bmatrix} G \\ J \end{bmatrix}, \begin{bmatrix} Q \\ Q \end{bmatrix}, \begin{bmatrix} W \\ S \end{bmatrix}, \begin{bmatrix} S \\ T \end{bmatrix}, \begin{bmatrix} S \\ N \end{bmatrix}, \begin{bmatrix} A \\ W \end{bmatrix}, \begin{bmatrix} S \\ M \end{bmatrix}, \begin{bmatrix} D \\ D \end{bmatrix}, \begin{bmatrix} B \\ K \end{bmatrix}, \begin{bmatrix} L \\ K \end{bmatrix}, \begin{bmatrix} H \\ A \end{bmatrix}, \begin{bmatrix} C \\ O \end{bmatrix}, \begin{bmatrix} H \\ A \end{bmatrix}, \begin{bmatrix} K \\ O \end{bmatrix}, \begin{bmatrix} R \\ H \end{bmatrix},$

$\begin{bmatrix} B \\ Y \end{bmatrix}$, sabendo que a matriz chave utilizada para criptografar é $A = \begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix}$.

5.2.4 Quinta Aula

Objetivos Gerais:

- Como fazer a multiplicação de matrizes.
- Como aplicar esse conhecimento em criptografia em bloco.

Objetivo Específico:

- Calcular o produto entre matrizes;
- Relacionar matrizes com a codificação e decodificação de mensagens.

Conteúdos:

Criptografia em blocos.

Metodologia:

Recursos: Data show, lousa e giz.

O aluno vai interagir com o software CriptoMat2 escolhendo matrizes para codificar e decodificar frases e assim vai perceber que algumas matrizes não encriptam de modo apropriado, devido $mdc(detA, 26) \neq 1$ não possuir uma única solução. Com essa atividade o aluno vai observar uma aplicação do conteúdo de matrizes.

CONCLUSÃO

Neste trabalho apresentamos uma proposta de atividade para o 2º ano do Ensino Médio, envolvendo a criptografia em blocos ao ensino de matrizes, de forma a aplicar o conhecimento obtido sobre criptografia no ambiente escolar.

Geralmente a contextualização do conteúdo de matrizes utilizada nos livros de Ensino Médio diz respeito à multiplicação de matrizes. Mas no trabalho relacionamos a criptografia com multiplicação de matrizes e envolvemos a matriz inversa nesses cálculos, o que permite fazer uma avaliação sobre o aprendizado dos alunos com relação a este conteúdo de modo instigante, pois obter a real mensagem é motivante para os alunos.

No primeiro e segundo capítulos trabalhamos com o conceito e definições de criptografia, cifra de César, congruências, aritmética das classes residuais e matrizes.

No terceiro capítulo definimos a criptografia em blocos e mostramos exemplos de como criptografar e decriptografar mensagens utilizando matrizes, utilizando uma aplicação prática para o cálculo da matriz inversa.

No quarto capítulo exploramos duas situações particulares do que acontece quando $mdc(detA, 26) = 13$ e de quando $mdc(detA, 26) = par$, devido o trabalho CriptoMat2 para implementação de um software educativo de criptografia, no qual o usuário interage com o programa, escolhendo as matrizes surge a necessidade de conhecer a imagem inversa dos elementos de $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ que estão na imagem da transformação A.

No último capítulo propomos atividades que podem ser utilizados pelo Professor em sala de aula utilizando o software CriptoMat2, para tornar a aula mais interessante e motivante.

Acredita-se que o tema criptografia em blocos pode ser utilizado como

gerador de atividades didáticas que permitem revisar, exercitar, fixar e aprofundar o conteúdo de matrizes desenvolvido no Ensino Médio.

Referências

[1] CALLIOLI, Carlos A. e outros. **Álgebra linear e aplicações**. 6 ed. rev. São Paulo: Atual, 1993.

[2] CRIPTOMAT2. **Sistema para ensino de Matemática utilizando conceitos de Criptografia – em bloco e RSA**. Disponível em: < http://cbie2014.ufgd.edu.br/msie/criptomat2/>. Acesso em: 30 nov. 2014.

[3] DANTE, Luiz Roberto. **Matemática, volume único**. 1 ed. São Paulo: Ática, 2005.

[4] HEFEZ, Abramo. **Elementos de aritmética**. 2 ed. Rio de Janeiro: SBM, 2011.

[5] LIMA, Elon Lages et. al. **A Matemática do Ensino Médio – volume 2**. 6. ed. Rio de Janeiro: SBM, 2006