

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

Aluno (a): _____	Turma: _____
------------------	--------------

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

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

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

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



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

Frase original:

Frase codificada:

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

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

Aluno(a):

Turma:

Atividade 2 - Matrizes e Determinantes



Considere o texto para as questões 1 e 2:

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

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

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

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

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

- a) Somente Carlos.
- b) Somente Beto.
- c) Somente André.
- d) André ou Beto.
- e) Beto ou Carlos.

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

- a) eles comeram no Mc' Ronalds.
- b) eles comeram no Burguer-Ring.
- c) eles comeram no Rob's.
- d) eles não comeram no Mc' Ronalds.
- e) eles não comeram no Burguer-Ring.

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

3. Calcule o valor dos determinantes das matrizes:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Apêndice 4 – Exercícios de congruência modular

Aluno(a): _____

Turma: _____

Atividade 3 - Congruência Modular



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

2. Resolva a congruência

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

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

3. Qual é o valor de $5^{103} \pmod{4}$?

- a) 0
- b) 1
- c) 2
- d) 3
- e) 4

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

- a) 10
- b) 11
- c) 12
- d) 13
- e) 14

5. Se $a \equiv 2 \pmod{5}$ e $b \equiv 3 \pmod{5}$, então $a+b$ é congruente a:

- a) 0 mod 5
- b) 1 mod 5
- c) 2 mod 5
- d) 3 mod 5
- e) 4 mod 5

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

Aluno(a):

Turma:

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



1. Vamos codificar uma palavra?

Para codificação ou decodificação, utilize a tabela a seguir:

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

Passo 1 : Escolha a matriz-chave $A_{2 \times 2}$ para a codificação. Lembre-se que o determinante d da matriz A deve satisfazer $\text{mdc}(d, 26) = 1$ e $d \neq 0$.

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad d = \det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

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

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

(,)

(,)

(,)

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

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

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

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

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

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

2. Agora vamos decodificar a palavra anterior?

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

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

a)

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

b)

$$\text{cof}(A) = \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$$

c)

$$\text{adj}(A) = \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$$

d)

$$A^{-1} = \frac{1}{\square} \cdot \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$$

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

(,)

(,)

(,)

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

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

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

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

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

Gabaritos das Atividades 2 e 3



Atividade 2

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

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

b) Não admite inversa.

c)

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

5. E

Atividade 3

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

Portanto:

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

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

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

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

Testando os valores de 1 a 6:

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

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

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

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

Reduzindo:

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

Assim:

$$x \equiv 6 \pmod{7}$$

3. B
4. A
5. B