UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

ELISANGELA REGINA DIOCESANO DE CASTRO

ÁLGEBRA LINEAR E TEORIA DOS NÚMEROS NA CRIPTOGRAFIA.

MONOGRAFIA DE ESPECIALIZAÇÃO

CAMPO MOURÃO

2012

ELISANGELA REGINA DIOCESANO DE CASTRO

ÁLGEBRA LINEAR E TEORIA DOS NÚMEROS NA CRIPTOGRAFIA.

Monografia apresentada ao Programa de Pós-graduação em Matemática da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Especialista em Ciências" – Área de Concentração: Matemática.

Orientadora: Priscila Amara Patricio de Melo

CAMPO MOURÃO

2012

TERMO DE APROVAÇÃO

Elisangela Regina Diocesano De Castro

Álgebra Linear e Teoria dos Números na Criptografia.

Monografia apresentada ao Programa de Pós-graduação em Matemática da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Especialista em Ciências" – Área de Concentração: Matemática.

Orientadora: Prof. Msc. Priscila Amara
Patricio de Melo

Prof. Msc.Adriana Strieder Philippsen

Prof. Msc. Raquel Polizeli

Campo Mourão, 2012

Dedico este trabalho à Deus e a minha família.

AGRADECIMENTOS

Agradeço a Deus por tudo de bom que fez e tem feito em minha vida, e pela oportunidade de ter concretizado mais um sonho.

Agradeço a minha mãe, Bernardina que sempre foi minha conselheira e amiga, ao meu pai, Jorge que me ensinou que na vida é preciso ter determinação para alcançar os nossos objetivos, as minhas irmãs, Rosangela e Andréia e ao meu irmão, Luiz que sempre torceram por mim e ao meu esposo, Edilson que com muito amor e paciência soube me compreender.

Agradeço as minhas amigas da graduação, Andressa, Luciane Grazieli, Sandra, Vanderléia e Virgínia, por compartilharem seus conhecimentos e estarem sempre presentes nos momentos de alegrias e tristezas.

Agradeço aos professores da Graduação na UEM e aos professores da Especialização UTFPR que me enriqueceram com seus conhecimentos, e em especial a minha orientadora, a professora Priscila Amara Patricio de Melo pelo apoio, paciência e dedicação para realização deste trabalho.

Agradeço a minha amiga Andressa, que esteve comigo durante toda a especialização e me ajudou em todos os momentos.

“Bem-aventurado o homem que encontra sabedoria, e o homem que adquire conhecimento, pois é mais valiosa do que ouro e prata”. Provérbios (3: 13)

RESUMO

CASTRO, Elisangela R. D. de. Álgebra Linear e Teoria dos Números na Criptografia. . 46 f. Monografia – Programa de Pós-graduação em Matemática, Universidade Tecnológica Federal do Paraná. Campo Mourão, 2012.

Neste trabalho, temos por objetivo principal aplicar conceitos da Álgebra Linear e da Teoria de congruências para decodificar mensagens. Iniciaremos estudando a parte de Álgebra Linear que proporciona suporte a Criptografia. Em seguida estudaremos alguns resultados da Teoria de Números. Por fim, apresentaremos as cifras de Hill e utilizaremos a teoria estudada no processo de decodificação de mensagens.

Palavras-chave: matrizes, transformações lineares, congruência, cifras de Hill.

ABSTRACT

CASTRO, Elisangela R. D. de. Title in English. 46 f. Monografia – Programa de Pós-graduação em Matemática, Universidade Tecnológica Federal do Paraná. Campo Mourão, 2012.

In this work, we aim to apply the main concepts of linear algebra and the theory of congruences to decode messages. Begin studying the part of linear algebra that provides support encryption. Then study some results from Number Theory. Finally, we present the figures of Hill and we use the theory studied in the process of decoding messages.

Keywords: matrices, linear transformations, congruence, Hill ciphers.

SUMÁRIO

1 INTRODUÇÃO

A palavra Criptografia vem do Grego kryptós ”escondido” e gráphein ”escrita” é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, o que a torna praticamente impossível de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. Nos dias atuais, em que grande parte dos dados é digital, sendo representados por bits, o processo de Criptografia é basicamente feito por algoritmos que fazem o embaralhamento, tornando assim a Criptografia uma área muito importante. O objetivo deste trabalho é aplicar conceitos de Álgebra Linear e Teoria dos Números no processo de decodificação de mensagens.

No Capítulo 2 listaremos algumas informações básicas sobre matrizes e determinantes. Relembraremos alguns conceitos da Álgebra Linear como espaços vetorias, base, dimensão, dependência e independência linear, transformações lineares, bem como alguns resultados importantes que relacionam tais conceitos. Esses resultados darão base para o andamento dos próximos capítulos.

No Capítulo 3 faremos um estudo sobre congruência. Mais especificamente definiremos inteiros congruentes, sistemas completos de restos e listaremos algumas propriedades das congruências.

No Capítulo 4 temos por objetivo aplicar o que foi estudado num problema da Criptografia. Para facilitar a compreensão do problema começaremos falando brevemente sobre cifras, mais especificamente sobre as cifras de Hill. Em seguida trataremos o problema matricialmente e por fim veremos como quebrar uma cifra de Hill usando a teoria estudada.

2 PRELIMINARES

Este capítulo recorda alguns fatos básicos da Álgebra Linear e estabelece algumas notações que serão utilizadas ao longo deste trabalho. Indicamos os textos (BOLDRINI,1980; ANTON, 2001) para maiores detalhes.

2.1 MATRIZES

Definição 2.1 *Chamamos de matriz uma tabela de elementos dispostos em linhas e colunas. Os elementos de uma matriz podem ser números, reais ou complexos, funções ou ainda outras matrizes. Representaremos uma matriz de m linhas e n colunas por:*

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

Usaremos sempre letras maiúsculas para denotar matrizes, e quando quisermos especificar a ordem de uma matriz A, isto é, o número de linhas e colunas, escreveremos $A_{m\times n}$. Também são utilizadas outras notações para matriz, além de colchetes, como parênteses ou duas barras.

Definição 2.2 *Matriz Identidade Quadrada: É aquela em que $a_{ii} = 1$ e $a_{ij} = 0$, para $i \neq j$. Denotada por I.*

Exemplo 2.1

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Definição 2.3 *Dada uma matriz $A = [a_{ij}]_{m\times n}$, podemos obter uma outra matriz $A^t = [b_{ij}]_{n\times m}$, cujas linhas são as colunas de A, isto é, $b_{ij} = a_{ji}$. A^t é denominada transposta de A.*

Exemplo 2.2 *a) Seja* $A = \begin{bmatrix} 2 & 1 \\ 0 & 3 \\ -1 & 4 \end{bmatrix}_{3\times 2}$ *então* $A^t = \begin{bmatrix} 2 & 0 & -1 \\ 1 & 3 & 4 \end{bmatrix}_{2\times 3}$

b) $\begin{bmatrix} 1 \\ 2 \end{bmatrix}^t = \begin{bmatrix} 1 & 2 \end{bmatrix}$

Propriedades:

i) Uma matriz é simétrica se, e somente se, ela é igual á sua transposta, isto é, $A = A^t$.

ii) $(A^t)^t = A$. Isto é, a transposta da transposta de uma matriz é ela mesma.

iii) $(A+B)^t = A^t + B^t$. Em outras palavras, a transposta de uma soma é igual à soma das transpostas.

iv) $(kA)^t = kA^t$, em que k é qualquer escalar.

Definição 2.4 *Sejam* $A=[a_{ij}]_{m\times n}$ *e* $B=[b_{rs}]_{n\times p}$. *Definimos o produto da matriz A pela matriz B por* $AB = [c_{uv}]_{m\times p}$ *onde*

$$c_{uv} = \sum_{k=1}^{n} a_{uk}b_{kv} = a_{u1}b_{1v} + \ldots + a_{un}b_{nv}$$

Observação 2.1 .

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* $C = AB$ *será de ordem* $m \times p$.

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

Exemplo 2.3 *a) Seja* $A = \begin{bmatrix} 2 & 1 \\ 4 & 2 \\ 5 & 3 \end{bmatrix}_{3\times 2}$ *e* $B = \begin{bmatrix} 1 & -1 \\ 0 & 4 \end{bmatrix}_{2\times 2}$. *Então*

$$AB = \begin{bmatrix} 2.1+1.0 & 2(-1)+1.4 \\ 4.1+2.0 & 4(-1)+2.4 \\ 5.1+3.0 & 5(-1)+3.4 \end{bmatrix}_{3\times 2} = \begin{bmatrix} 2 & 2 \\ 4 & 4 \\ 5 & 7 \end{bmatrix}_{3\times 2}$$

b) Seja $A = \begin{bmatrix} 1 & -1 \\ 0 & 4 \end{bmatrix}_{2\times 2}$ *e* $B = \begin{bmatrix} 2 & 1 \\ 4 & 2 \\ 5 & 3 \end{bmatrix}_{3\times 2}$.

Note que não é possível efetuar multiplicação AB, porque o número de colunas da primeira matriz é diferente do número de linhas da segunda matriz .

Propriedades:
i) Em geral $AB \neq BA$, podendo mesmo um dos membros estar definido e o outro não.
Desde que sejam possíveis as operações, as seguintes propriedades são válidas:
ii) $AI = IA = A$ (Isto justifica o nome da matriz identidade.)
iii) $A(B+C) = AB + AC$(distributividade à esquerda da multiplicação, em relação à soma)
iv) $(A+B)C = AC + BC$ (distributividade à direita da multiplicação, em relação à soma)
v) $(AB)C = A(BC)$ (associatividade)
vi) $(AB)^t = B^t A^t$
vii) $0 \cdot A = 0$ e $A \cdot 0 = 0$

2.2 DETERMINANTE

No Ensino Médio você deve ter se deparado com o cálculo de determinante de matrizes 2 x 2 e 3 x 3, fazendo o uso de algumas regras e fórmulas. No entanto, nesta seção verificaremos que o "determinante"é um certo tipo de função, que associa a cada matriz quadrada um número real, independente da ordem da matriz quadrada. Para isso necessitamos de alguns conceitos.

Definição 2.5 *Uma permutação do conjunto de inteiros* $\{1,2,...,n\}$ *é um rearranjo destes inteiros em alguma ordem sem omissões ou repetições.*

Exemplo 2.4 *Existem 6 permutações distintas do conjunto de inteiros* $\{1,2,3\}$.

Permutação	Número de inversões
(1 2 3)	0
(1 3 2)	1
(2 1 3)	1
(2 3 1)	2
(3 1 2)	2
(3 2 1)	3

Definição 2.6 *Denotando por* $(j_1, j_2, ..., j_n)$ *uma permutação arbitrária do conjunto* $\{1,2,...,n\}$ *dizemos que ocorre uma inversão numa permutação sempre que um inteiro maior precede um menor.*

Observação 2.2 *Para calcular o número de inversões de uma permutação* $(j_1, j_2, ..., j_n)$ *devemos:*
(1) encontrar a quantia de números menores que j_1 *e que estão depois de* j_1 *na permutação;*
(2) encontrar a quantia de números menores que j_2 *e que estão depois de* j_2 *na permutação.*
(3) Continuar esse processo até j_{n-1} *e somar estas quantias. A soma destes números será o número de inversões de uma permutação.*

Exemplo 2.5 *Determine o número de inversões nas seguintes permutações.*
a) Considerando o conjunto $\{1,2,3,4,5,6\}$ *o número de inversões em* $(6,1,3,4,5,2)$ *é dado por:*
$5+0+1+1+1=8$
b) Considerando o conjunto $\{1,2,3,4\}$ *o número de inversões em* $(2,4,1,3)$ *é dado por:*
$1+2+0=3$

Definição 2.7 *Uma permutação é chamada par se o número de inversões é um inteiro par e é chamado ímpar se o número de inversões é ímpar.*

Definição 2.8 *Seja* $A = [a_{ij}]_{n\times n}$ *uma matriz quadrada e* $(j_1, j_2, ..., jn)$ *uma permutação arbitrária do conjunto* $\{1,2,...,n\}$. *O produto*

$$a_{1j_1}, a_{2j_2}, ..., a_{nj_n}$$

é dito um produto elementar de A.

Definição 2.9 *Seja A uma matriz quadrada. A função determinante é denotada por det e definida por:*

$$det(A) = \sum(-1)^k a_{1j_1} \cdot a_{2j_2}...a_{nj_n}$$

onde k é o número de inversões de $(j_1, j_2, ..., j_n)$ *ou seja, det(A) é definido como a soma de todos os produtos elementares de A acompanhados do sinal:* $(+)$ *se a permutação* $(j_1, j_2, ..., j_n)$ *é par ou* $(-)$ *se* $(j_1, j_2, ..., j_n)$ *é ímpar.*

Exemplo 2.6 *Cálculo do determinante de uma matriz de* 2^a *ordem.*

$$detA = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

Exemplo 2.7 *Cálculo do determinante de uma matriz de* 3^a *ordem.*

$$detA = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$$

Definição 2.10 *Dada uma matriz A quadrada se pudermos encontrar uma matriz B de mesma ordem tal que* $A_{n\times n}.B_{n\times n} = B_{n\times n}.A_{n\times n} = I_{n\times n}$ *então diremos que* $A_{n\times n}$ *é invertível e que* $B_{n\times n}$ *é a inversa de* $A_{n\times n}$*. Se não puder ser encontrada tal matriz B, então diremos que A é não invertível ou singular.*

Teorema 2.1 *A inversa de uma matriz quadrada A é única e será denotada por* A^{-1}*.*
Demonstração:
Suponhamos que B e C são inversas da matriz A. Então:

$$(BA) = I$$

Multiplicando ambos os lados da igualdade pela direita por C têm-se:

$$(BA)C = IC = C$$

Por outro lado,

$$(BA)C = B(AC) = B \cdot I = B$$

Portanto, $B = C$*.*

Teorema 2.2 *A matriz* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *é invertível se* $ad - bc \neq 0$*, caso em que a inversa é dada por*

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Demonstração:
Basta verificar que $A \cdot A^{-1} = A^{-1} \cdot A = I_{2\times 2}$*.*

2.3 ESPAÇO VETORIAL

Definição 2.11 *Um espaço vetorial real é um conjunto V, não vazio, com duas operações: soma,* $V \times V \to V$ *e multiplicação por escalar,* $\mathbb{R} \times V \to V$*, tais que, para quaisquer* $u, v, w \in V$ *e* $\alpha, \beta \in \mathbb{R}$*, as seguintes propriedades sejam satisfeitas:*

i) $(u+v)+w = u+(v+w)$

ii) $u+v = v+u$

iii) Existe $0 \in V$ tal que $u+0 = u$, 0 é chamado vetor nulo.

iv) Existe $-u \in V$ tal que $u+(-u) = 0$

v) $\alpha(u+v) = \alpha u + \alpha v$

vi) $(\alpha+\beta)v = \alpha v + \beta v$

vii) $(\alpha\beta)v = \alpha(\beta v)$

viii) $1 \cdot u = u$

Exemplo 2.8 *Verifique se o conjunto* $\{(a,2a,3a); a \in \mathbb{R}\}$ *é espaço vetorial real com as operações usuais.*

i) Sejam $u = (a_1,2a_1,3a_1), v = (a_2,2a_2,3a_2)$ *e* $w = (a_3,2a_3,3a_3) \in V = \mathbb{R}^3$. *Então*
$(u+v)+w = [(a_1,2a_1,3a_1)+(a_2,2a_2,3a_2)]+(a_3,2a_3,3a_3) = [(a_1+a_2,2a_1+2a_2,3a_1+3a_2)]+$
$(a_3,2a_3,3a_3) = [(a_1+a_2)+a_3,(2a_1+2a_2)+2a_3,(3a_1+3a_2)+3a_3]$ *como IK é corpo real, vale a associativa* $= [a_1+(a_2+a_3),2a_1+(2a_2+2a_3),3a_1+(3a_2+3a_3)] = (a_1,2a_1,3a_1)+[(a_2+$
$a_3),(2a_2+2a_3),(3a_2+3a_3)] = (a_1,2a_1,3a_1)+[(a_2,2a_2,3a_2)+(a_3,2a_3,3a_3)] = u+(v+w)$
$\therefore (u+v)+w = u+(v+w)$

ii) Sejam $u = (a_1,2a_1,3a_1)$ *e* $v = (a_2,2a_2,3a_2) \in V = \mathbb{R}^3$. *Então*
$u+v = (a_1,2a_1,3a_1)+(a_2,2a_2,3a_2) = (a_1+a_2,2a_1+2a_2,3a_1+3a_2)$ *como IK é corpo real, vale a comutativa* $= (a_2+a_1,2a_2+2a_1,3a_2+3a_1) = [(a_2,2a_2,3a_2)+(a_1,2a_1,3a_1)] = v+u$
$\therefore u+v = v+u$

iii) $(0,0,0) \in \mathbb{R}^3$ *é o valor nulo de* $\mathbb{R}^3$, *pois se* $u = (a_1,2a_1,3a_1) \in \mathbb{R}^3$ *então*
$0+u = (0,0,0)+(a_1,2a_1,3a_1) = (0+a_1,0+2a_1,0+3a_1) = (a_1,2a_1,3a_1) = u$
$\therefore 0+u = u$

iv) Se $u = (a_1,2a_1,3a_1) \in \mathbb{R}^3$, *então* $-u = (-a_1,-2a_1,-3a_1)$ *pois*
$u+(-u) = (a_1,2a_1,3a_1)+(-a_1,-2a_1,-3a_1) = (a_1-a_1,2a_1-2a_1,3a_1-3a_1) = (0,0,0)$
$\therefore u+(-u) = 0$

v) Sejam $u = (a_1,2a_1,3a_1)$ *e* $v = (a_2,2a_2,3a_2) \in \mathbb{R}^3$ *e* $\alpha \in \mathbb{R}$
$\alpha(u+v) = \alpha[(a_1,2a_1,3a_1)+(a_2,2a_2,3a_2)] = \alpha(a_1+a_2,2a_1+2a_2,3a_1+3a_2) = [\alpha(a_1+a_2),\alpha(2a_1+$
$2a_2),\alpha(3a_1+3a_2)] = [\alpha a_1+\alpha a_2,\alpha 2a_1+\alpha 2a_2,\alpha 3a_1+\alpha 3a_2] = (\alpha a_1,\alpha 2a_1,\alpha 3a_1)+\alpha a_2,\alpha 2a_2+$
$\alpha 3a_2] = [\alpha(a_1,2a_1,3a_1)+\alpha(a_2,2a_2,3a_2)] = \alpha u+\alpha v$
$\therefore \alpha(u+v) = \alpha u+\alpha v$

vi) Sejam $u = (a_1,2a_1,3a_1) \in \mathbb{R}^3$ *e* $\alpha,\beta \in \mathbb{R}$. *Então*
$(\alpha+\beta).u = (\alpha+\beta).(a_1,2a_1,3a_1) = [(\alpha+\beta).a_1,(\alpha+\beta).2a_1),(\alpha+\beta).3a_1] = [\alpha a_1+\beta a_1,\alpha 2a_1+$
$\beta 2a_1,\alpha 3a_1+\beta 3a_1] = [(\alpha a_1,\alpha 2a_1,\alpha 3a_1)+(\beta a_1,\beta 2a_1,\beta 3a_1)] = [\alpha(a_1,2a_1,3a_1)+\beta(a_1,2a_1,3a_1)] =$
$\alpha u+\beta u$

$\therefore (\alpha+\beta).u = \alpha u + \beta u$

vii) Sejam $\alpha, \beta \in \mathbb{R}, u = (a_1, 2a_1, 3a_1) \in \mathbb{R}^3$. *Então*

$(\alpha\beta).u = (\alpha\beta).(a_1, 2a_1, 3a_1) = [(\alpha\beta)a_1, (\alpha\beta)2a_1, (\alpha\beta)3a_1] = [\alpha(\beta a_1), \alpha(\beta 2a_1), \alpha(\beta 3a_1)] =$
$\alpha[\beta(a_1, 2a_1, 3a_1)] = \alpha(\beta u)$

$\therefore (\alpha\beta).u = \alpha(\beta u)$

viii) Se $u = (a_1, 2a_1, 3a_1) \in \mathbb{R}^3$ *então*

$1.u = 1.(a_1, 2a_1, 3a_1) = (1.a_1, 1.2a_1, 1.3a_1) = (a_1, 2a_1, 3a_1) = u$

$\therefore 1.u = u$

2.4 DEPENDÊNCIA E INDEPENDÊNCIA LINEAR

Definição 2.12 *Sejam V um espaço vetorial e* $v_1, ...v_n \in V$. *Dizemos que o conjunto* $\{v_1, ...v_n\}$ *é linearmente independente (LI) ou que os vetores* $v_1, ...v_n$ *são LI, se a equação*

$$a_1 v_1 + ... + a_n v_n = 0$$

implica que $a_1 = a_2 = ... = a_n = 0$. *No caso em que exista algum escalar* $a_i \neq 0$ *dizemos que* $\{v_1, ..., v_n\}$ *é linearmente dependente ou que os vetores* $v_1, ...v_n$ *são LD.*

Teorema 2.3 *Um conjunto* $\{v_1, ..., v_n\}$ *de vetores é LD se, e somente se, um destes vetores for uma combinação linear dos outros.*

Demonstração:

$(\Rightarrow)$ *Suponhamos que* $\{v_1, ..., v_n\}$ *é LD sendo assim:*

$$a_1 v_1 + ... + a_j v_j ... + a_n vn = 0 \Rightarrow v_j = -\frac{1}{a_j}(a_1 v_1 + ... + a_{j-1} v_{j-1} + a_{j+1} v_{j+1} ... + a_n vn)$$

então

$$v_j = -\frac{a_1}{a_j} v_1 - ... - \frac{a_{j-1}}{a_j} v_{j-1} - \frac{a_{j+1}}{a_j} v_{j+1} - ... - \frac{a_n}{a_j} v_n$$

Logo v_j *é uma combinação linear dos outros vetores.*

$(\Leftarrow)$ *Suponhamos sem perda de generalidade que* $v_j = b_1 v_1 + ... + b_{j-1} v_{j-1} + b_{j+1} v_{j+1} ... +$ $b_n vn$ *para algum j. Então temos,* $b_1 v_1 + ... - 1 v_j + ... + b_n vn = 0$ *com* $b_j = -1$.

Portanto, $\{v_1, ..., v_n\}$ *é LD.*

Exemplo 2.9 *Sejam* $V = \mathbb{R}^2, e_1 = (1,0)$ *e* $e_2 = (0,1)$. *Então* e_1 *e* e_2 *são LI, pois* $a_1 e_1 + a_2 e_2 = 0 \Rightarrow a_1(1,0) + a_2(0,1) = (0,0) \Rightarrow (a_1, a_2) = (0,0) \Rightarrow a_1 = 0$ *e* $a_2 = 0$

Exemplo 2.10 *Sejam* $V = \mathbb{R}^2$ *e* $A = \{(1,-1), (1,0), (1,1)\}$. *O conjunto A é linearmente dependente, pois* $\frac{1}{2}(1,-1) - 1(1,0) + \frac{1}{2}(1,1) = (0,0)$.

Definição 2.13 *Seja V um espaço vetorial e* $B = \{v_1, ..., v_n\}$ *um conjunto de V. Dizemos que B é um conjunto gerador de V se todos os elementos de V puderem ser escritos como combinação linear dos elementos de B. Denotamos* $V = [v_1, ..., v_n]$.

2.5 BASE DE UM ESPAÇO VETORIAL

Definição 2.14 *Um conjunto* $\{v_1, ...v_n\}$ *de vetores de V será uma base de V se,*
i) $\{v_1, ...v_n\}$ *é LI*
ii) $[v_1, ..., v_n] = V$

Exemplo 2.11 *O conjunto* $\{(1,1),(0,1)\}$ *é uma base de* $V = \mathbb{R}^2$.
De fato,
$(0,0) = a(1,1) + b(0,1)$
$(0,0) = (a, a+b)$
$\begin{cases} a = 0 \\ a+b = 0 \end{cases} \Rightarrow b = 0$
Logo $\{(1,1),(0,1)\}$ *é LI.*
Ainda $[(1,1),(0,1)] = V$ *pois dado* $v = (x,y) \in V$, *temos*
$(x,y) = x(1,1) + (y-x)(0,1)$, *ou seja, todo vetor de* $\mathbb{R}^2$ *é uma combinação linear dos vetores* $(1,1)$ *e* $(0,1)$.

Exemplo 2.12 *Consideremos* $V = \mathbb{R}^3$ *e* $B = \{(1,0,0),(0,1,0),(0,0,1)\}$. *B é uma base de* $\mathbb{R}^3$, *chamada base canônica de* $\mathbb{R}^3$.
De fato,
$(0,0,0) = a(1,0,0) + b(0,1,0) + c(0,0,1)$
$(0,0,0) = (a,b,c)$
$a = 0,\ b = 0,\ c = 0$
Logo B é LI.
Além disso, $(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$
Portanto, B é base de $\mathbb{R}^3$.

Teorema 2.4 *Sejam* $v_1, v_2, ..., v_n$ *vetores não-nulos que geram um espaço vetorial V. Então dentre estes vetores podemos extrair uma base de V.*
Demonstração:
Se $v_1, v_2, ..., v_n$ *são linearmente independentes, satisfazem a definição para uma base, logo não há nada a fazer.*

Se $v_1, v_2, ..., v_n$ são linearmente dependentes, então existe uma combinação linear deles, com algum coeficiente diferente de zero, dando o vetor nulo.

$$x_1v_1 + x_2v_2 + ... + x_nv_n = 0$$

Suponha sem perda de generalidade que $x_n \neq 0$. Então podemos escrever:

$$v_n = \frac{-x_1}{x_n}v_1 + \frac{-x_2}{x_n}v_2 + ... + \frac{-x_{n-1}}{x_n}v_{n-1},$$

ou seja, v_n é uma combinação linear de $v_1, ..., v_{n-1}$ e, portanto $v_1, v_2, ..., v_{n-1}$ ainda geram V. Se $v_1, v_2, ..., v_{n-1}$ for LD então existe uma combinação linear deles dando o vetor nulo e com algum coeficiente diferente de zero, portanto, poderemos extrair aquele vetor que corresponde a este coeficiente. Seguindo desta forma, após uma quantidade finita de estágios, chegaremos a um subconjunto de $\{v_1, ..., v_r\}$, formado por $(r \leq n)$ vetores LI $v_1, v_2, ..., v_r$, que ainda geram V, ou seja, formaremos uma base.

Teorema 2.5 *Seja um espaço vetorial V gerado por um conjunto finito de vetores $v_1, v_2, ..., v_n$. Então, qualquer conjunto com mais de n vetores é necessariamente LD (e portanto, qualquer conjunto LI tem no máximo n vetores).*

Demonstração:

Visto que $[v_1, ..., v_n] = V$, pelo Teorema 2.4, podemos extrair uma base para V de $v_1, ..., v_n$.

Seja $\{v_1, ..., v_r\}$, $r \leq n$ esta base. Consideremos agora $w_1, w_2, ..., w_m$, m vetores de V, com $m > n$.

Existem, então constantes a_{ij}, tais que

$$\begin{aligned} w_1 &= a_{11}v_1 + a_{12}v_2 + \quad \dots \quad + a_{1r}v_r \\ w_2 &= a_{21}v_1 + a_{22}v_2 + \quad \dots \quad + a_{2r}v_r \\ &\vdots \\ w_m &= a_{m1}v_1 + a_{m2}v_2 + \quad \dots \quad + a_{mr}v_r \end{aligned} \tag{1}$$

Consideremos agora

$$x_1w_1 + x_2w_2 + ... + x_mw_m = 0 \tag{2}$$

Substituindo (1) em (2) e coletando os termos, obtemos

$x_1(a_{11}v_1 + a_{12}v_2 + ... + a_{1r}v_r) + x_2(a_{21}v_1 + a_{22}v_2 + ... + a_{2r}v_r) + ... + x_m(a_{m1}v_1 + a_{m2}v_2 + ... + a_{mr}v_r) = 0$

$x_1a_{11}v_1 + x_1a_{12}v_2 + ... + x_1a_{1r}v_r + x_2a_{21}v_1 + x_2a_{22}v_2 + ... + x_2a_{2r}v_r + ... + x_ma_{m1}v_1 + x_ma_{m2}v_2 +$

$... + x_m a_{mr} v_r = 0$

$(a_{11}x_1 + a_{21}x_2 + ... + a_{m1}x_m)v_1 + (a_{12}x_1 + a_{22}x_2 + ... + a_{m2}x_m)v_2 + ... + (a_{1r}x_1 + a_{2r}x_2 + ... + a_{mr}x_m)v_r$.

Como $v_1, v_2, ..., v_r$ são LI, então

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \quad \dots \quad + a_{m1}x_m &= 0 \\ \qquad\qquad\qquad\quad \ddots & \\ a_{1r}x_1 + a_{2r}x_2 + \quad \dots \quad + a_{mr}x_r &= 0 \end{cases}$$

Temos então um sistema linear homogêneo com r equações e m incógnitas $x_1, ..., x_m$ e como $r \leq n < m$, ele admite uma solução não trivial, ou seja, existe uma solução com algum x_i não nulo. Portanto $w_1, ..., w_m$ são LD.

Corolário 2.1 *Qualquer base de um espaço vetorial tem sempre o mesmo número de elementos. Este número é chamado dimensão de V, e denotado por dim V.*

Demonstração:

Considere $\{v_1, ..., v_n\}$ e $\{w_1, ..., w_m\}$ duas bases de V. Como $v_1, ..., v_n$ geram V e $w_1, ..., w_m$ são LI pelo Teorema 2.5, $m \leq n$.

Por outro lado, como $w_1, ..., w_m$ geram V e $v_1, ..., v_n$ são LI, ainda pelo Teorema 2.5, $n \leq m$. Portanto $n = m$.

Teorema 2.6 *Qualquer conjunto de vetores LI de um espaço vetorial V de dimensão finita pode ser completado de modo a formar uma base de V.*

Demonstração:

Sendo $dimV = n$ e $v_1, ..., v_r$ vetores LI (pelo Teorema 2.5, $r \leq n$). Se $[v_1, ..., v_r] = V$ então $\{v_1, ..., v_r\}$ forma uma base $(n = r)$, não temos mais nada a fazer.

Se existe $v_{r+1} \in V$ tal que $v_{r+1} \notin [v_1, ..., v_r]$, isto é, v_{r+1} não é uma combinação linear de $v_1, ..., v_r$, então $\{v_1, v_2, ..., v_r, v_{r+1}\}$ é LI.

Se $[v_1, v_2, ..., v_r, v_{r+1}] = V$, então $\{v_1, ..., v_{r+1}\}$ é a base procurada. Caso contrário, existe $v_{r+2} \notin [v_1, ..., v_{r+1}]$ e então $\{v_1, ..., v_{r+1}, v_{r+2}\}$ é LI.

Se $[v_1, ..., v_{r+1}, v_{r+2}]$ nossa demonstração esta concluída. Se não prosseguimos usando o mesmo argumento. Como não podemos ter mais do que n vetores LI em V pelo Teorema 2.5, após um número finito de passos teremos obtido uma base de V que contém os vetores dados.

Corolário 2.2 *Se $dimV = n$, qualquer conjunto de n vetores LI formará uma base de V.*

Demonstração: Se o conjunto de n vetores não formasse uma base, poderíamos completá-lo até formá-la e dessa forma teríamos uma base com mais de n vetores em V o que é um absurdo pelo Corolário 2.1.

Teorema 2.7 *Dada uma base $\beta = \{v_1, v_2, ..., v_n\}$ de V, cada vetor de V é escrito de maneira única como combinação linear de $v_1, v_2, ..., v_n$.*
Demonstração:
Seja $v \in V$. Como β é base sabemos que β gera V e β é LI.
Então

$$v = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$$

Suponha que existam $\beta_1, \beta_2, ..., \beta_n \in IK$ tal que

$$v = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + ... + \beta_n v_n$$

$$= \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n - \beta_1 v_1 - \beta_2 v_2 - ... - \beta_n v_n = 0$$

$$= (\alpha_1 - \beta_1) v_1 + (\alpha_2 - \beta_2) v_2 + ... + (\alpha n - \beta_n) v_n = 0$$

Como β é LI temos que

$$\begin{cases} \alpha_1 - \beta_1 = 0 \Rightarrow \alpha_1 = \beta_1 \\ \alpha_2 - \beta_2 = 0 \Rightarrow \alpha_2 = \beta_2 \\ \vdots \\ \alpha_n - \beta_n = 0 \Rightarrow \alpha_n = \beta_n \end{cases}$$

Portanto, v se escreve de maneira única.

Definição 2.15 *Sejam $\beta = \{v_1, ..., v_n\}$ base de V e $v \in V$ onde $v = a_1 v_1 + ... + a_n v_n$. Chamamos estes números $a_1, ..., a_n$ de coordenadas de v em relação a base β e denotamos por:*

$$[v]_\beta = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

Observação 2.3 *: É importante notar que a ordem dos elementos de uma base também influência na matriz das coordenadas de um vetor em relação a esta base.*

2.6 TRANSFORMAÇÕES LINEARES

Definição 2.16 *Sejam V e W dois espaços vetoriais. Uma transformação linear é uma função de V em W, $T : V \to W$, que satisfaz as seguintes condições:*

i) $T(u+v) = T(u) + T(v)$, $u, v \in V$.
ii) $T(kv) = kT(v)$, $k \in \mathbb{R}$ *e* $v \in V$.

Exemplo 2.13 *Seja* $T : \mathbb{R} \to \mathbb{R}$ *dada por* $T(u) = u^2$. *Então T não é uma transformação linear. De fato, como* $T(u+v) = (u+v)^2 = u^2 + 2uv + v^2$ *e* $T(u) + T(v) = u^2 + v^2$. *Logo,* $T(u+v) \neq T(u) + T(v)$. *Portanto não há necessidade de verificar a segunda condição da definição, já que não satisfaz a primeira.*

Exemplo 2.14 *Consideremos* $V = \mathbb{R}^2$ *e* $W = \mathbb{R}^3$ *espaços vetoriais e* $T : \mathbb{R}^2 \to \mathbb{R}^3$ *dada por* $T(x,y) = (2x,\ 0,\ x+y)$. *Então T é uma transformação linear.*
De fato, dados $u, v \in \mathbb{R}^2$, *temos* $u = (x_1, y_1)$ *e* $v = (x_2, y_2)$ *com* $x_i, y_i \in \mathbb{R}$. *Logo*
$T(u+v) = T((x_1,y_1)+(x_2,y_2)) = T(x_1+x_2, y_1+y_2) = (2((x_1+x_2), 0, (x_1+x_2)+(y_1+y_2)) =$
$(2x_1, 0, x_1+y_1) + (2x_2, 0, x_2+y_2) = T(u) + T(v)$
Assim, a primeira condição é satisfeita. Mais ainda,
$T(ku) = T(k(x,y)) = T(kx,ky) = (2kx, 0, kx+ky) = k(2x, 0, x+y) = kT(u)$
e a segunda condição é satisfeita. Então T é uma transformação linear.

Teorema 2.8 *Dados dois espaços vetoriais reais V e W e* $\{v_1, ..., v_n\}$ *uma base de V. Sejam* $w_1, ..., w_n$ *elementos arbitrários de W. Então existe uma única transformação linear* $T : V \to W$ *tal que* $T(v_1) = w_1, ..., T(v_n) = w_n$.
Demonstração:
Seja $v \in V$. *Então existem* $\lambda_1, \lambda_2, ..., \lambda_n \in IK$ *tais que*

$$v = \lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n$$
$$T(v) = \lambda_1 w_1 + \lambda_2 w_2 + ... + \lambda_n w_n$$

Vamos mostrar que T é uma transformação linear.
Considere

$$v = \beta_1 v_1 + \beta_2 v_2 + ... + \beta_n v_n = \sum_{i=1}^{n} \beta_i v_i$$

e

$$u = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = \sum_{i=1}^{n} \alpha_i v_i$$

dois vetores de V, onde $\beta_i's$ *e* $\alpha_i's$ *e* $\lambda \in IK$. *Então:*
$T(\lambda v + u) = T(\lambda(\sum \beta_i v_i) + (\sum \alpha_i v_i)) = T(\sum \lambda \beta_i v_i + \sum \alpha_i v_i) = T(\sum(\lambda \beta_i + \alpha_i) v_i) = \sum(\lambda \beta_i +$

$\alpha_i)w_i = \lambda \sum \beta_i w_i + \sum \alpha_i w_i = \lambda T(\sum \beta_i v_i) + T(\sum \alpha_i v_i) = \lambda T(v) + T(u)$.
Portanto, T é transformação linear.
Resta mostrar que T é única. Para isto suponhamos que exista uma transformação linear $S : V \to W$ *tal que:*

$$S(v_i) = w_i, \forall\, v_i \in V$$

Seja $v \in V$*, então:*
$v = \lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n$
$S(v) = S(\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n) = \lambda_1 S(v_1) + \lambda_2 S(v_2) + ... + \lambda_n S(v_n)$
$= \lambda_1 w_1 + \lambda_2 w_2 + ... + \lambda_n w_n = T(V)$.
Logo S e T são iguais.
Portanto, a transformação linear é única.

Este Teorema nos mostra que a definição de uma transformação linear depende basicamente da definição de T nos elementos de uma base de V.

Definição 2.17 *Seja* $T : V \to W$ *uma transformação linear. Chamamos de imagem de T o conjunto dos vetores* $w \in W$ *tais que existe um vetor* $v \in V$*, que satisfaz* $T(v) = w$*. Ou seja,* $Im(T) = \{w \in W; T(v) = w \text{ para algum } v \in V\}$.

Observação 2.4 *Im(T) é um subconjunto de W, e ainda, um subespaço vetorial de W. Por vezes Im(T) é escrita como T(V).*

Definição 2.18 *Seja* $T : V \to W$ *uma transformação linear. O conjunto de todos os vetores* $v \in V$ *tais que* $T(v) = 0$ *é chamado núcleo de T, sendo denotado por* $ker(T)$*. Isto é*

$$kert(T) = \{v \in V; T(v) = 0\}$$

Observe que $kert(T) \subset V$ *é um subconjunto de V e, mais, é um subespaço vetorial de V.*

Definição 2.19 *Dada uma função* $T : V \to W$*, diremos que T é injetora se dados* $u \in V, v \in V$ *com* $T(u) = T(v)$*, tivermos* $u = v$*. Ou equivalentemente, T é injetora se dados* $u, v \in V$ *com* $u \neq v$*, então* $T(u) \neq T(v)$*. Em outras palavras, T é injetora se as imagens de vetores distintos são distintas.*

Definição 2.20 *A transformação* $T : V \to W$ *será sobrejetora se a imagem de T coincidir com W, ou seja* $T(V) = W$*. Em outras palavras, T será sobrejetora se* $\forall w \in W$ *, existir* $v \in V$ *tal que* $T(v) = w$.

Teorema 2.9 *Seja $T : V \to W$ uma transformação linear. Então $ker(T) = \{0\}$, se e somente se, T é injetora.*

Demonstração:

$(\Rightarrow)$ *Vamos mostrar que se $kerT = \{0\} \Rightarrow$ T é injetora.*

Suponhamos que $u, v \in V$ tais que $T(u) = T(v)$. Então $T(u) - T(v) = T(u - v) = 0$, isto é, $u - v \in ker(T)$. Mas por hipótese o único elemento do núcleo é 0. Então $u - v = 0$, isto é $u = v$, logo T é injetora.

$(\Leftarrow)$ *Agora mostremos que se T é injetora $\Rightarrow ker(T) = \{0\}$.*

Seja $v \in ker(T)$, isto é $T(v) = 0$. Como necessariamente $T(0) = 0, T(v) = T(0)$. Logo $v = 0$, pois T é injetora. Portanto, o único elemento do núcleo é 0, ou seja, $ker(T) = \{0\}$.

3 ARITMÉTICA MODULAR

O conceito de números inteiros congruentes é devido a Gauss, um dos estudiosos da Teoria dos Números. Nesta seção vamos estudar alguns resultados sobre congruências que serão utilizados no próximo capítulo. Indicamos (FILHO, 1988) para maiores detalhes.

3.1 INTEIROS CONGRUENTES

Definição 3.1 *Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que a é congruente a b módulo m se, e somente se, m divide a diferença $a-b$.*

Em outros termos, a é *congruente* a b *módulo m* se, e somente se, existe um inteiro k tal que $a-b=km$.
Com a notação

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

indica-se que a é congruente a b *módulo m*. Portanto, simbolicamente:

$$a \equiv b(mod.m) \Leftrightarrow m|(a-b)$$

ou seja

$$a \equiv b(mod.m) \Leftrightarrow \exists\, k\ \in \mathbb{Z} \text{ tal que } a-b=km$$

Por exemplo:

$$3 \equiv 24(mod.7), \text{ pois } 7|(3-24)$$

$$-31 \equiv 11(mod.6), \text{ pois } 6|(-31-11)$$

$$-15 \equiv -63(mod.8), \text{ pois } 8|(-15-(-63))$$

Se m não divide a diferença $a-b$, então diz-se que a é *incongruente* a b *módulo m*, e denotamos

$$a \not\equiv b(mod.m)$$

Por exemplo

$$25 \not\equiv 12(mod.7), \text{ pois } 7 \not| (25-12)$$

$$-21 \not\equiv 10(mod.5), \text{ pois } 5 \not| (-21-10)$$

$$16 \not\equiv 9(mod.4), \text{ pois } 4 \not| (16-9))$$

Note que dois inteiros quaisquer são congruentes *módulo 1*, enquanto que dois inteiros são congruentes *módulo 2* se ambos são *pares* ou se ambos são *ímpares*.
Em particular, $a \equiv 0(mod.m)$ se, e somente se, o *módulo m divide* a $(m|a)$.

Exemplo 3.1 *Mostremos que*

$$n \equiv 7(mod.12) \Rightarrow n \equiv 3(mod.4), \forall n \in \mathbb{Z}$$

Com efeito:

$$n \equiv 7(mod.12) \Rightarrow n-7 = 12k \Rightarrow n-3-4 = 12k \Rightarrow n-3 = 12k+4 \Rightarrow n-3 = 4(3k+1)$$

$$4|(n-3) \Rightarrow n \equiv 3(mod.4)$$

Exemplo 3.2 *Mostremos que*

$$n^2 \equiv 0(mod.4) \text{ } ou \text{ } n^2 \equiv 1(mod.4), \forall n \in \mathbb{Z}$$

Com efeito:
(i) Se n par temos

$$n = 2k \Rightarrow n^2 = 4k^2 \Rightarrow n^2 - 0 = 4k^2 \Rightarrow 4|n^2 \Rightarrow n^2 \equiv 0(mod.4)$$

(ii) Se n ímpar temos

$$n = 2k+1 \Rightarrow n^2 = (2k+1)^2 \Rightarrow n^2 = 4k^2+4k+1 \Rightarrow n^2 = (4k^2+4k)+1$$

$$\Rightarrow n^2 = 4(k^2+k)+1 \Rightarrow n^2-1 = 4(k^2+k) \Rightarrow 4|(n^2-1) \Rightarrow n^2 \equiv 1(mod.4)$$

3.2 CARACTERIZAÇÃO DE INTEIROS CONGRUENTES

Teorema 3.1 *Dois inteiros a e b são congruentes módulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m.*
Demonstração:
($\Rightarrow$) *Suponhamos que* $a \equiv b(mod.m)$. *Então, por definição*

$$a - b = km, \text{ com } k \in \mathbb{Z}$$

Seja r o *resto* da divisão de b por m. Então, pelo *Algoritmo da Divisão*:

$$b = mq + r, \text{ onde } 0 \leq r < m$$

Portanto

$$a = km + b = km + mq + r = (k+q)m + r$$

e isto significa que r é o *resto* da divisão de a por m, isto é, os inteiros a e b divididos por m deixam o mesmo *resto* r.
($\Leftarrow$) Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo *resto* r. Então podemos escrever

$$a = mq_1 + r \text{ e } b = mq_2 + r, \text{ onde } 0 \leq r < m$$

e, portanto

$$a - b = mq_1 + r - mq_2 - r = m(q_1 - q_2) \Rightarrow m|(a-b) \Rightarrow a \equiv b(mod.m)$$

Exemplo 3.3 *Sejam os inteiros -56 e -11. Pelo Algoritmo da Divisão:*

$$-56 = 9(-7) + 7 \; e \; -11 = 9(-2) + 7$$

isto é, -56 *e* -11 *divididos por* 9 *deixam o mesmo resto* 7. *Logo, pelo Teorema 3.1:*

$$-56 \equiv -11(mod.9).$$

Sejam, agora, os inteiros -31 *e* 11. *Temos a congruência:*

$$-31 \equiv 11(mod.7)$$

de modo que, pelo Teorema 3.1, -31 e 11 divididos por 7 deixam o mesmo resto. Realmente, é o que mostram as igualdades:

$$-31 = 7(-5)+4 \text{ e } 11 = 7.1+4$$

3.3 PROPRIEDADES DAS CONGRUÊNCIAS

Teorema 3.2 *Seja m um inteiro positivo fixo $(m > 0)$ e sejam a, b, e c inteiros quaisquer. São satisfeitas as seguintes propriedades:*
(1) $a \equiv a(mod.m)$
(2) *Se* $a \equiv b(mod.m)$, *então* $b \equiv a(mod.m)$
(3) *Se* $a \equiv b(mod.m)$ *e se* $b \equiv c(mod.m)$, *então* $a \equiv c(mod.m)$
Demonstração:
(1) $m|0$ *ou* $m|(a-a) \Rightarrow a \equiv a(mod.m)$
(2) *Se* $a \equiv b(mod.m)$, *então* $a-b = km$, *com* $k \in \mathbb{Z}$.
Portanto $b-a = -(km) = (-k)m \Rightarrow b \equiv a(mod.m)$
(3) *Se* $a \equiv b(mod.m)$ *e se* $b \equiv c(mod.m)$, *então existem inteiros h e k tais que*

$$a-b = km \text{ e } b-c = km$$

Portanto

$$a-c = a+b-b-c = (a-b)+(b-c) = hm+km = (h+k)m$$

isto é, $a \equiv c(mod.m)$.

Observação 3.1 *: Consoante este Teorema, a relação R do conjunto $\mathbb{Z}$ dos inteiros definida por*

$$aRb \Leftrightarrow a \equiv b(mod.m)$$

é reflexiva, simétrica e transitiva, ou seja, R é uma relação de equivalência em $\mathbb{Z}$.
Esta relação de equivalência R em $\mathbb{Z}$ é denominada "congruência módulo m".

Teorema 3.3 *Seja m um inteiro positivo fixo $(m > 0)$ e sejam a e b dois inteiros quaisquer. Então*
(1) *Se* $a \equiv b(mod.m)$ *e se* $n|m$, *com* $n > 0$, *então* $a \equiv b(mod.n)$
(2) *Se* $a \equiv b(mod.m)$ *e se* $c > 0$, *então* $ac \equiv bc(mod.mc)$.
(3) *Se* $a \equiv b(mod.m)$ *e se* a, b, m *são todos divisíveis pelo inteiro* $d > 0$, *então* $a/d \equiv b/d(mod.m/d)$.
Demonstração:
(1) *Com efeito,*

$$a \equiv b(mod.m) \Rightarrow a - b = km \; e \; n|m \Rightarrow m = nq$$

onde k e $q > 0$ *são inteiros.*
Portanto

$$a - b = (kq)n \Rightarrow a \equiv b(mod.n)$$

(2) *De fato*

$$a \equiv b(mod.m) \Rightarrow a - b = km \Rightarrow ac - bc = k(mc) \Rightarrow ac \equiv bc(mod.mc)$$

(3) *Com efeito*

$$a \equiv b(mod.m) \Rightarrow a - b = km \Rightarrow a/d - b/d = k(m/d) \Rightarrow a/d \equiv b/d(mod.m/d)$$

Assim por exemplo

$$-15 \equiv 9(mod.8) \Rightarrow -15 \equiv 9(mod.4)$$

$$7 \equiv -8(mod.3) \Rightarrow 35 \equiv -40(mod.15)$$

$$36 \equiv -24(mod.12) \Rightarrow 9 \equiv -6(mod.3)$$

Teorema 3.4 *Seja m um inteiro positivo fixo* $(m > 0)$ *e sejam* a, b, c, d *inteiros quaisquer. As seguintes propriedades são válidas:*
(1) *Se* $a \equiv b(mod.m)$ *e se* $c \equiv d(mod.m)$ *então* $a + c \equiv b + d(mod.m)$ *e* $ac \equiv bd(mod.m)$
(2) *Se* $a \equiv b(mod.m)$ *então* $a + c \equiv b + c(mod.m)$ *e* $ac \equiv bc(mod.m)$
(3) *Se* $a \equiv b(mod.m)$ *então* $a^n \equiv b^n(mod.m)$ *para todo inteiro positivo n.*
Demonstração:
(1) *Se* $a \equiv b(mod.m)$ *e se* $c \equiv d(mod.m)$*, então existem inteiros h e k tais que* $a - b = hm$ *e* $c - d = km$*.*
Logo

$$(a + c) - (b + d) = (a - b) + (c - d) = hm + km = (h + k)m$$

e

$$ac - bd = (b + hm)(d + km) - bd = bd + bkm + dhm + hkm^2 - bd = (bk + dh + hkm).m$$

o que implica

$$a+c \equiv b+d(mod.m) \text{ e } ac \equiv bd(mod.m)$$

(2) *Se* $a \equiv b(mod.m)$*, como* $c \equiv c(mod.m)$ *temos, pela Propriedade* (1)*, que*

$$a+c \equiv b+c(mod.m) \text{ e } ac \equiv bc(mod.m)$$

(3) *Usando o "Teorema da Indução Matemática", a proposição é verdadeira para* $n = 1$*, e suposta verdadeira para um inteiro positivo k, então*

$$a^k \equiv b^k(mod.m) \text{ e } a \equiv b(mod.m)$$

Portanto pela Propriedade (1)*:*

$$a^k \cdot a \equiv b^k \cdot b(mod.m) \text{ e } a^{k+1} \equiv b^{k+1}(mod.m)$$

isto é, a proposição é verdadeira para o inteiro positivo $k+1$*. Logo, a proposição é verdadeira para todo inteiro positivo n.*

Por exemplo:
(i) $12 \equiv 22(mod.5)$ e $8 \equiv 13(mod.5)$ então

$$12+8 \equiv 22+13(mod.5) \text{ ou } 20 \equiv 35(mod.5)$$

e

$$12.8 \equiv 22.13(mod.5) \text{ ou } 96 \equiv 286(mod.5)$$

(ii) Como $12 \equiv 5(mod.7)$ temos

$$12+6 \equiv 5+6(mod.7) \text{ ou } 18 \equiv 11(mod.7)$$

e

$$12(-9) \equiv 5(-9)(mod.7) \text{ ou } -108 \equiv -45(mod.7)$$

(iii) $-5 \equiv 2(mod.7)$ então

$$(-5)^3 \equiv 2^3(mod.7) \text{ ou } -125 \equiv 8(mod.7)$$

Exemplo 3.4 *Mostraremos que* $a \equiv b(mod.m)$ *implica*

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

Com efeito, multiplicando ordenadamente as congruências

$$a \equiv b(mod.m) \; e \; -1 \equiv -1(mod.m)$$

obtemos

$$a(-1) \equiv b(-1)(mod.m) \; ou \; -a \equiv -b(mod.m)$$

Exemplo 3.5 *Mostraremos que se* $a+b \equiv c(mod.m)$ *temos que* $a \equiv c-b(mod.m)$
Com efeito, somando ordenadamente as congruências

$$a+b \equiv c(mod.m) \; e \; -b \equiv -b(mod.m)$$

obtemos

$$a+b+(-b) \equiv c+(-b)(mod.m) \; ou \; a \equiv c-b(mod.m)$$

Portanto, como nas equações, também nas congruências podemos passar um termo de um membro para o outro trocando apenas o sinal.

Teorema 3.5 *Se* $ac \equiv bc(mod.m)$ *e se o* $mdc(c,m) = d$, *então* $a \equiv b(mod.m/d)$.
Demonstração:
Se $ac \equiv bc(mod.m)$. *Então* $ac-bc = (a-b)c = km$, *com* $k \in \mathbb{Z}$
E se o $mdc(c,m) = d$, *existem inteiros* r *e* s *tais que* $c = dr$ *e* $m = ds$, *onde* r *e* s *são primos entre si. Portanto,* $(a-b)dr = kds$ *ou* $(a-b)r = ks$ *o que implica que* $s|(a-b)r$, *com o* $mdc(r,s) = 1$. *Logo, pelo Teorema de Euclides:* $s|(a-b)$ *e* $a \equiv b(mod.s)$ *ou, por ser* $s = m/d, a \equiv b(mod.m/d)$.

Corolário 3.1 *Se* $ac \equiv bc(mod.m)$ *e se o* $mdc(c,m) = 1$ *então* $a \equiv b(mod.m)$.
Este corolário mostra que é permitido cancelar fatores de ambos os membros de uma congruência que são primos com o módulo.

Corolário 3.2 *Se* $ac \equiv bc(mod.p)$, *com p primo, e se p não divide c* $(p \nmid c)$, *então* $a \equiv b(mod.p)$.
Demonstração:
Basta notar que as condições p não divide c $(p \nmid c)$ *e p é primo, implicam que o* $mdc(c,p) = 1$.

Exemplo 3.6 *Consideremos a congruência:*

$$33 \equiv 15(mod.9) \text{ ou } 3.11 \equiv 3.5(mod.9)$$

Como o $mdc(3,9) = 3$ *pelo Teorema 3.5, temos:*

$$11 \equiv 5(mod.3)$$

.

Exemplo 3.7 *Consideremos a congruência:*

$$-35 \equiv 45(mod.8) \text{ ou } 5(-7) \equiv 5.9(mod.8)$$

Como o $mdc(5,8) = 1$*, podemos cancelar o fator 5 de ambos os membros da congruência, o que dá a nova congruência*

$$-7 \equiv 9(mod.8).$$

Na congruência $4.11 \equiv 4.15(mod.8)$ *não podemos cancelar o fator 4, porque o* $mdc(4,8) = 4 \neq 1$*. Realmente,* $11 \not\equiv 15(mod.8)$*. Mas, temos* $11 \equiv 15(mod.2)$

3.4 SISTEMA COMPLETO DE RESTO

Definição 3.2 *Chama-se sistema completo de restos módulo m todo conjunto* $S = \{r_1, r_2, ..., r_m\}$ *de m inteiros tal que um inteiro qualquer a é congruente módulo m a um único elemento de S.*

Assim, por exemplo, cada um dos conjuntos:

$$\{1,2,3\}, \{0,1,2\}, \{-1,0,1\}, \{1,5,9\}$$

é um *sistema completo de restos módulo 3*.

Teorema 3.6 *O conjunto* $S = \{0,1,2,...,m-1\}$ *é um sistema completo de restos módulo m.*
Demonstração:
Seja a um inteiro qualquer e sejam q e r o quociente e o resto na divisão de a pelo inteiro positivo m, isto é:

$$a = mq + r, \text{ onde } 0 \leq r < m$$

Então, pela definição de inteiros congruentes módulo m, temos:

$$a \equiv r(mod.m)$$

e como r só pode assumir os valores $0,1,2,...,m-1$*, segue-se que o inteiro a é congruente módulo m a um único elemento do conjunto S, e por conseguinte este conjunto é um sistema completo de restos módulo m.*

Por exemplo, o conjunto $S = \{0,1,2,3,4\}$ é um *sistema completo de restos módulo 5.*

Corolário 3.3 *Se* $S = \{r_1, r_2, ..., r_m\}$ *é um sistema completo de restos módulo m, então os elementos de S são congruentes módulo m aos inteiros* $0,1,2,...,m-1$*, tomados numa certa ordem.*
Demonstração:
Qualquer que seja o inteiro a, temos

$$a \equiv r_i(mod.m), \text{ com } r_i \in S$$

$$a \equiv k(mod.m), \text{ com } 0 \leq k \leq m-1$$

Logo, pela propriedade transitiva da "congruência módulo m", temos

$$r_i \equiv k(mod.m)$$

Assim por exemplo, o conjunto:

$$S = \{-12, -4, 11, 13, 22, 82, 91\}$$

é um *sistema completo de restos módulo* 7 e
$-12 \equiv 2(mod.7), -4 \equiv 3(mod.7), 11 \equiv 4(mod.7), 13 \equiv 6(mod.7), 22 \equiv 1(mod.7)$
$32 \equiv 5(mod.7), 91 \equiv 0(mod.7)$
isto é, os elementos de S são *congruentes módulo 7* aos inteiros $2,3,4,6,1,5,0$.

Exemplo 3.8 *Mostrar que o conjunto* $S = \{-2,-1,0,1,2\}$ *é um sistema completo de restos módulo 5.*
Pelo Teorema 3.6, um inteiro qualquer a é congruente módulo 5 a um único elemento do conjunto $0,1,2,3,4$*, tomados numa certa ordem, pois, temos*
$-2 \equiv 3(mod.5), -1 \equiv 4(mod.5), 0 \equiv 0(mod.5), 1 \equiv 1(mod.5), 2 \equiv 2(mod.5)$
Logo, o inteiro a é congruente módulo 5 a um único elemento do conjunto S, e por conseguinte este conjunto é um sistema completo de restos módulo 5.

4 CRIPTOGRAFIA

Neste capítulo vamos aplicar a Teoria apresentada nos capítulos anteriores para examinarmos um método que codifica e decodifica mensagens: a criptografia.

4.1 CIFRAS

O estudo de codificação e decodificação de mensagens secretas é denominado *criptografia*. Embora os códigos secretos remontem aos primórdios da comunicação escrita, tem havido um aumento recente de interesse no assunto devido à necessidade de manter a privacidade da informação transmitida ao longo das linhas públicas de comunicação. Na linguagem da criptografia, os códigos são denominados *cifras*, as mensagens não codificadas são textos comuns e as mensagens codificadas são *textos cifrados* ou *criptogramas*. O processo de converter um texto comum em cifrado é chamado *cifrar* ou *criptografar* e o processo inverso de converter um texto cifrado em comum é chamado *decifrar*.

As cifras mais simples, denominadas *cifras de substituição*, são as que substituem cada letra do alfabeto por uma outra letra. Por exemplo, na cifra de substituição:
Comum

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cifra

DEFGHIJKLMNOPQRSTUVWXYZABC

a letra do texto comum A é substituída por D, a letra de texto comum B por E e assim por diante. Com esta cifra, a mensagem de texto comum

ROMA NÃO FOI CONSTRUÍDA EM UM DIA

fica

URPD QDR IRL FRQVWUXLGD HP XP GLD

Uma desvantagem de cifras de substituição é que elas preservam as frequências de letras individuais, tornando relativamente fácil quebrar o código por métodos estatísticos.
Uma maneira 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. Um sistema que permite isto, é o *sistema poligráfico* em que o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas. Estudaremos uma classe de sistemas poligráficos chamados *cifras de Hill* que são baseados em transformações matriciais.
Vamos supor que cada letra de texto comum e de texto cifrado, exceto o Z, tem um valor numérico que especifica sua posição no alfabeto padrão como mostrado na Tabela 1. Por motivos que ficarão claros mais tarde, damos a Z o valor 0.

Tabela 1

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Nos casos mais simples de cifras de Hill, transformamos *pares* sucessivos de texto comum em texto cifrado pelo seguinte procedimento:

Passo 1. Escolha uma matriz 2×2

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

com entradas inteiras para efetuar a codificação. Condições adicionais sobre A serão impostas mais tarde.

Passo 2. Agrupe letras sucessivas de texto comum em pares, inserindo uma letra adicional fictícia para completar o último par caso o texto comum tenha um número ímpar de letras; substitua cada letra de texto comum por seu valor numérico.

Passo 3. Converta cada par sucessivo $p_1 p_2$ de letras de texto comum em um vetor-coluna

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

e forme o produto Ap. Nós chamamos p de *vetor comum* e Ap o *vetor cifrado*.

Passo 4. Converta cada vetor cifrado em seu equivalente alfabético.

Exemplo 4.1 *Cifra de Hill de uma Mensagem*

Use a matriz

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

para obter a cifra de Hill da mensagem de texto comum (em inglês)

I AM HIDING

Solução:
Se nós agrupamos o texto comum em pares de letras e adicionamos a letra fictícia G para completar o último par, obteremos

IA MH ID IN GG

ou equivalentemente, usando a Tabela 1,

9 1 13 8 9 4 9 14 77

Para codificar o par IA nós efetuamos o produto matricial

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix}$$

que fornece o texto cifrado KC pela Tabela 1.
Para codificar o par MH nós efetuamos o produto matricial

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 8 \end{bmatrix} = \begin{bmatrix} 29 \\ 24 \end{bmatrix} \tag{1}$$

Aqui temos um problema, pois o número 29 não possui equivalente alfabético Tabela 1. Para resolver este problema nós fazemos o seguinte acordo:
Sempre que ocorrer um inteiro maior do que 25, ele será substituído pelo resto da divisão deste inteiro por 26.
Como o resto da divisão é um dos inteiros 0, 1, 2,...,25, este procedimento sempre fornece um inteiro com equivalente alfabético.
Assim, em (1) nós substituímos 29 por 3, que o resto da divisão de 29 por 26, e obtemos o texto cifrado CX da Tabela 1 para MH.
As contas para os demais vetores cifrados são

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 4 \end{bmatrix} = \begin{bmatrix} 17 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 14 \end{bmatrix} = \begin{bmatrix} 37 \\ 42 \end{bmatrix} ou \begin{bmatrix} 11 \\ 16 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 7 \\ 7 \end{bmatrix} = \begin{bmatrix} 21 \\ 21 \end{bmatrix}$$

Estes vetores correspondem aos pares de texto cifrado QL, KP e UU, respectivamente. Coletando os pares, obtemos a mensagem cifrada completa

KC CX QL KP UU

que, normalmente, seria transmitida como uma única cadeia sem espaços

KCCXQLKPUU

Como o texto comum foi agrupado em pares e criptografado por uma matriz 2×2*, dizemos que a cifra de Hill do Exemplo 4.1 é uma 2-cifra de Hill. Evidentemente também é possível agrupar o texto comum em ternos e criptografar com uma matriz* 3×3 *com entradas inteiras; isto é chamado uma 3-cifra de Hill agrupamos o texto comum em conjuntos de n letras e codificamos com uma matriz codificadora* $n \times n$ *de entradas inteiras.*

No Exemplo 4.1 substituímos os inteiros maiores do que 25 pelo seu resto na divisão por 26. Esta técnica de trabalhar com restos é a base de uma parte da Matemática chamada de aritmética modular. Tendo em vista sua importância em criptografia, nós iremos voltar por um momento para relembrar algumas das principais ideias desta área.

Em aritmética modular nós supomos dado um inteiro positivo m, chamado módulo e consideramos "iguais"ou "equivalentes"em relação ao módulo quaisquer dois inteiros cuja diferença é um múltiplo inteiro do módulo.
Relembrando:
Dados um número inteiro positivo m e dois inteiros a e b quaisquer, dizemos que a é equivalente a b módulo m, e escrevemos

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

se $a - b$ *é um múltiplo inteiro de m.*

Exemplo 4.2 *Várias Equivalências*

$$7 \equiv 2 \text{ (mod 5)}$$
$$19 \equiv 3 \text{ (mod 2)}$$
$$-1 \equiv 25 \text{(mod 26)}$$
$$12 \equiv 0 \text{ (mod 4)}$$

Dado um módulo m, pode ser provado que qualquer inteiro a é equivalente, módulo m, a exatamente um dos inteiros

$$0, 1, 2, ..., m-1$$

Este inteiro é chamado o ***resíduo*** *de a módulo m e nós escrevemos*

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

para denotar o conjunto dos resíduos de a módulo m.

Se a é um inteiro não-negativo, então seu resíduo módulo m é simplesmente o resto da divisão de a por m. Para um inteiro a arbitrário, o resíduo que pode ser encontrado usando o seguinte Teorema.

Teorema 4.1 *Dados um inteiro a e um módulo m quaisquer, seja*

$$R = \text{resto de } \frac{|a|}{m}$$

Então o resíduo r de a módulo m é dado por

$$r = \begin{cases} R & se \quad a \geq 0 \\ m - R & se \quad a < 0 \quad e \quad R \neq 0 \\ 0 & se \quad a < 0 \quad e \quad R = 0 \end{cases}$$

Exemplo 4.3 *Resíduos mod 26*
Encontre os resíduos módulo 26 de (a) 87, (b) - 38 e (c) - 26.
Solução:
(a) Dividindo $|87| = 87$ *por 26 dá um resto de R = 9, ou seja, r = 9. Assim,*

$$87 \equiv 9 (mod 26)$$

(b) Dividindo $|-38| = 38$ *por 26 dá um resto de R = 12, ou seja, r = 26 - 12 = 14. Assim,*

$$-38 \equiv 14(mod 26)$$

(c) Dividindo $|-26| = 26$ *por 26 dá um resto de R = 0. Assim,*

$$-26 \equiv 0(mod 26)$$

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

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

Na aritmética modular nós temos o seguinte conceito correspondente:

Definição 4.1 *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* $aa^{-1} = a^{-1}a = 1(modm)$.

Pode ser provado que se a e m não têm fatores primos comuns, então a tem um único recíproco módulo m; reciprocamente, se a e m têm um fator primo comum, então a não tem recíproco módulo m.

Exemplo 4.4 *Recíproco de 3 mod 26*
O número 3 tem um recíproco módulo 26 pois 3 e 26 não têm fatores primos em comum. Este recíproco pode ser obtido encontrado o número x em $\mathbb{Z}_{26}$ *que satisfaz a equação modular*

$$3x \equiv 1(mod 26)$$

Embora existam métodos gerais para resolver tais equações modulares, isto não será abordado pois nos levaria para muito longe do nosso objetivo. Contudo, como 26 é relativamente pequeno, esta equação pode ser resolvida experimentando, uma por uma, cada solução possível de 0 a 25. Desta maneira nós encontramos que $x = 9$ *é a solução, pois*

$$3.9 = 27 \equiv 1(mod 26)$$

Assim,

$$3^{-1} \equiv 9(mod 26)$$

Exemplo 4.5 *Um Número sem Recíproco mod 26*
O número 4 não possui recíproco mod 26 pois 4 e 26 têm 2 como fator primo comum.

Para referência futura, fornecemos a seguinte tabela de recíprocos módulo 26:
Tabela 2 Recíprocos Módulo 26

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

Decifrando cada cifra útil iremos obter um procedimento para decifrar. Para decifrar as cifras de Hill, usamos a inversa (mod 26) da matriz codificadora. Para ser preciso, se m é um inteiro positivo, dizemos que uma matriz A com entradas em $\mathbb{Z}_m$ é invertível módulo m se existir uma matriz B com entradas em $\mathbb{Z}_m$ tal que

$$AB = BA = 1(modm)$$

Suponha agora que

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

é invertível módulo 26 e que esta matriz é usada para uma 2- cifra de Hill. Se

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

é um vetor comum, então

$$c = Ap$$

é o correspondente vetor cifrado e

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

Assim, cada vetor comum pode ser recuperado através do correspondente vetor cifrado pela multiplicação à esquerda por $A^{-1}(mod26)$.

Em criptografia é importante saber quais matrizes são invertíveis módulo 26 e como obter suas inversas. Em seguida nós investigaremos estas questões.

Em aritmética comum, uma matriz quadrada A é invertível se, e somente se, $det(A) \neq 0$ ou, equivalentemente, det(A) tem um recíproco. O teorema seguinte é o análogo deste resultado em aritmética modular.

Teorema 4.2 *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, o resíduo de $det(A)$ módulo m tem um recíproco módulo m.*

Como 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 4.1 *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível 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 = 26 são 2 e 13, temos o seguinte Corolário que é útil em criptografia.

Corolário 4.2 *Uma matriz quadrada A com entradas em $\mathbb{Z}_{26}$ é invertível módulo 26 se, e somente se, o resíduo de $det(A)$ módulo 26 não é divisível por 2 ou 13.*

Ao verificar-se que

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

tem entradas em $\mathbb{Z}_{26}$ e que o resíduo de $det(A) = ad - bc$ módulo 26 não é divisível por 2 ou 13, então a inversa de $det(A)(mod 26)$ é dada por

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (mod 26) \tag{2}$$

onde $(ad - bc)^{-1}$ é o recíproco do resíduo de $ad - bc(mod 26)$.

Exemplo 4.6 *Inversa de uma Matriz mod 26*
Encontre a inversa de

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

módulo 26.
Solução:

$$det(A) = ad - bc = 5.3 - 6.2 = 3$$

de modo que, pela Tabela 2,

$$(ad - bc)^{-1} = 3^{-1} \equiv 9(mod 26)$$

Assim, por (2),

$$A^{-1} = 9\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} (mod 26)$$

Conferindo,

$$AA^{-1} = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} = \begin{bmatrix} 53 & 234 \\ 26 & 105 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod 26)$$

Analogamente, $A^{-1}A = I(mod 26)$.

Exemplo 4.7 *Decifrando uma 2 - cifra de Hill*
Decifre a seguinte 2- cifra de Hill, que foi criptografada pela matriz do Exemplo 4.6:

GTNKGKDUSK

Solução:
Pela Tabela 1, o equivalente numérico do texto cifrado é

7 20 14 11 7 11 4 21 19 11

Para obter os pares de texto, comum, nós multiplicamos cada vetor cifrado pela inversa de A (obtida no Exemplo 4.6):

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 7 \\ 20 \end{bmatrix} = \begin{bmatrix} 487 \\ 436 \end{bmatrix} = \begin{bmatrix} 19 \\ 20 \end{bmatrix} (mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 14 \\ 11 \end{bmatrix} = \begin{bmatrix} 278 \\ 321 \end{bmatrix} = \begin{bmatrix} 18 \\ 9 \end{bmatrix} (mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 7 \\ 11 \end{bmatrix} = \begin{bmatrix} 271 \\ 265 \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \end{bmatrix} (mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 4 \\ 21 \end{bmatrix} = \begin{bmatrix} 508 \\ 431 \end{bmatrix} = \begin{bmatrix} 14 \\ 15 \end{bmatrix} (mod 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 19 \\ 11 \end{bmatrix} = \begin{bmatrix} 283 \\ 361 \end{bmatrix} = \begin{bmatrix} 23 \\ 23 \end{bmatrix} (mod 26)$$

Pela Tabela 1, os equivalentes alfabéticos destes vetores são

ST RI KE NO WW

que fornecem a mensagem

STRIKE NOW

4.2 QUEBRANDO UMA CIFRA DE HILL

Como o objetivo de criptografar mensagens e informações é impedir que "oponentes" descubram seu conteúdo, os criptógrafos têm uma preocupação com a segurança de suas cifras, ou seja, quão facilmente podem ser quebradas (ou decifradas pelos oponentes). Discutiremos agora uma técnica para quebrar cifras de Hill.

Suponha que você consiga algum texto comum e o cifrado correspondente de uma mensagem de seu oponente. Por exemplo, examinando algum texto cifrado interceptado, você talvez seja capaz de deduzir que a mensagem é uma carta que começa com DEAR SIR. Nós iremos mostrar que com alguns poucos destes dados pode ser possível determinar a matriz decodificadora de uma cifra de Hill e consequentemente obter acesso ao resto da mensagem.

Um resultado básico em Álgebra Linear, apresentado no Teorema 2.8, garante que uma transformação fica completamente determinada por seus valores em uma base. Este princípio sugere que se nós tivermos uma n- cifra de Hill e se

$$p_1, p_2, ..., p_n$$

forem vetores comuns linearmente independentes cujos correspondentes vetores cifrados

$$Ap_1, Ap_2, ..., Ap_n$$

são conhecidos então disporemos de informação suficiente para determinar a matriz A e portanto sua inversa $A^{-1}(mod m)$.

O próximo Teorema, fornece uma maneira de fazer isto.

Teorema 4.3 *Determinando a Matriz Decodificadora*
Sejam $p_1, p_2, ..., p_n$ vetores comuns linearmente independentes e sejam $c_1, c_2, ..., c_n$ os corres-

pondentes vetores cifrados de uma n-cifra de Hill. Se

$$P = \begin{bmatrix} p_1^t \\ p_2^t \\ \vdots \\ p_n^t \end{bmatrix}$$

é a matriz $n \times n$ de vetores-coluna $p_1^t, p_2^t, ..., p_n^t$ e se

$$C = \begin{bmatrix} c_1^t \\ c_2^t \\ \vdots \\ c_n^t \end{bmatrix}$$

é a matriz $n \times n$ de vetores-linha $c_1^t, c_2^t, ..., c_n^t$, então a sequência de operações elementares sobre linhas que reduz C a I transforma P em $(A^{-1})^t$.

Este Teorema nos diz que para encontrar a transposta da matriz decodificadora A^{-1} nós deveremos encontrar uma sequência de operações elementares sobre linhas que reduza C a I e então aplicar estas mesmas operações sobre linhas de P. O próximo exemplo ilustra um algoritmo simples para fazer isto.

Exemplo 4.8 *Usando o Teorema 4.3*
Foi interceptada a 2- cifra de Hill

IOSBTGXESPXHOPDE

Decifre esta mensagem, sabendo que ela principia com a palavra DEAR.
Solução:
Pela Tabela 1, o equivalente numérico do texto comum conhecido é

DE AR

4 5 1 18

e o equivalente numérico do texto cifrado correspondente é

IO SB

9 15 19 2

de modo que os vetores comuns e correspondentes vetores cifrados são

$$p_1 = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \leftrightarrow c_1 = \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \leftrightarrow c_2 = \begin{bmatrix} 19 \\ 2 \end{bmatrix}$$

Nós queremos reduzir

$$C = \begin{bmatrix} c_1^t \\ c_2^t \end{bmatrix} = \begin{bmatrix} 9 & 15 \\ 19 & 2 \end{bmatrix}$$

a I por operações elementares sobre linhas e simultaneamente aplicar estas operações a

$$P = \begin{bmatrix} p_1^t \\ p_2^t \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 1 & 18 \end{bmatrix}$$

para obter $(A^{-1})^t$ (a transposta da matriz decodificadora). Isto pode ser obtido adjuntando P a direita de C e aplicando as operações sobre linhas à matriz resultante $[C|P]$ até que o lado esquerdo esteja reduzido a I. A matriz final então terá o formato $[I|(A^{-1})^t]$. As contas podem ser feitas como segue:
Formar a matriz $[C|P]$.

$$\left[\begin{array}{cc|cc} 9 & 15 & 4 & 5 \\ 19 & 2 & 1 & 18 \end{array}\right]$$

Multiplicar a primeira linha por $9^{-1} = 3$.

$$\left[\begin{array}{cc|cc} 1 & 45 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right]$$

Substituir 45 pelo seu resíduo módulo 26.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right]$$

Somar -19 vezes a primeira linha a segunda.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & -359 & -227 & -267 \end{array}\right]$$

Substituir as entradas da segunda linha pelos seus resíduos módulo 26.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 5 & 7 & 19 \end{array}\right]$$

Multiplicar a segunda linha por $5^{-1} = 21$

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 147 & 399 \end{array}\right]$$

Substituir as entradas da segunda linha pelos seus resíduos módulo 26.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 17 & 9 \end{array}\right]$$

Somar -19 vezes a segunda linha à primeira.

$$\left[\begin{array}{cc|cc} 1 & 0 & -311 & -156 \\ 0 & 1 & 17 & 9 \end{array}\right]$$

Substituir as entradas da primeira linha pelos seus resíduos módulo 26.

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 17 & 9 \end{array}\right]$$

Assim,

$$(A^{-1})^t = \left[\begin{array}{cc} 1 & 0 \\ 17 & 9 \end{array}\right]$$

e portanto a matriz decodificadora é

$$A^{-1} = \left[\begin{array}{cc} 1 & 17 \\ 0 & 9 \end{array}\right]$$

Para decifrar a mensagem, primeiro agrupamos o texto cifrado em pares e encontramos os equivalentes numéricos de cada letra:

IO SB TG XE SP XH OP DE

9 15 19 2 20 7 24 5 19 16 24 8 15 16 4 5

Em seguida, multiplicamos os vetores cifrados sucessivamente pela esquerda por A^{-1} e encon-

tramos os equivalentes alfabéticos dos pares de texto comum resultantes

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 9 \\ 15 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \begin{matrix} D \\ E \end{matrix} \ (mod 26)$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \begin{matrix} A \\ R \end{matrix} \ (mod 26)$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 7 \end{bmatrix} = \begin{bmatrix} 9 \\ 11 \end{bmatrix} \begin{matrix} I \\ K \end{matrix} \ (mod 26)$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 19 \end{bmatrix} \begin{matrix} E \\ S \end{matrix} \ (mod 26)$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 5 \\ 14 \end{bmatrix} \begin{matrix} E \\ N \end{matrix} \ (mod 26)$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 4 \\ 20 \end{bmatrix} \begin{matrix} D \\ T \end{matrix} \ (mod 26)$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 1 \\ 14 \end{bmatrix} \begin{matrix} A \\ N \end{matrix} \ (mod 26)$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 11 \\ 19 \end{bmatrix} \begin{matrix} K \\ S \end{matrix} \ (mod 26)$$

Finalmente, construímos a mensagem a partir dos pares de texto comum

DE AR IK ES EN DT AN KS

DEAR IKE SEND TANKS

5 CONCLUSÃO

Podemos observar que para a decodificação de uma mensagem foi essencial o estudo de conceitos da Álgebra Linear como representações matriciais e transformações lineares bem como resultados da Teoria dos Números. Além disso, ficou evidente as facilidades em se trabalhar com problemas na forma matricial.

REFERÊNCIAS

BOLDRINI, J. L. et al. **Álgebra Linear**. 3.ed. São Paulo: Editora HARBRA Ltda, 1980.

FILHO, E. A. **Teoria Elementar dos Números**. 3.ed. São Paulo: Editora Nobel, 1988.

ANTON, H. ; Rorres, C. **Álgebra Linear com Aplicações**. 8.ed. Porto Alegre: Editora Bookman, 2001.