Universidade Federal de Sergipe
Mestrado Profissional em Matemática
Curso de Pós-graduação em Matemática

Dayane Silva dos Santos

Uso da Criptografia como Motivação para o Ensino Básico de Matemática

Itabaiana
2015

Dayane Silva dos Santos

Uso da Criptografia como Motivação para o Ensino Básico de Matemática

Trabalho de conclusão apresentado ao Corpo Docente do Curso de Pós-Graduação em Matemática em Rede Nacional PROFMAT - UFS - Campus Alberto Carvalho, como requisito parcial para obtenção do título de Mestre em Matemática, sobre orientação do Profº Dr. Éder Mateus de Souza.

Itabaiana
2015

FICHA CATALOGRAFICA ELABORADA PELA BIBLIOTECA PROFESSOR ALBERTO CARVALHO
UNIVERSIDADE FEDERAL DE SERGIPE

Santos, Dayane Silva dos
S237u Uso da criptografia como motivação para o ensino básico de matemática / Dayane Silva dos Santos; orientador Éder Mateus de Souza. – Itabaiana, 2016.
63 f.

Dissertação (Mestrado em Matemática) – Universidade Federal de Sergipe, 2016.

1. Matemática – estudo e ensino. 2. Criptografia. I. Souza, Éder Mateus de, orient. II. Título.

CDU 51:37

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Uso da Criptografia como Motivação para o Ensino Básico de Matemática

por

Dayane Silva dos Santos

Aprovada pela Banca Examinadora:

Prof. Dr. Eder Mateus de Souza- UFS
Orientador

Prof. Dr. Naldisson dos Santos- UFS
Primeiro Examinador

Prof. Dr. Filipe Dantas dos Santos - UFS
Segundo Examinador

Itabaiana, 27 de Agosto de 2015.

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Cristóvão. Tel. (00 55 79) 2105-6887
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat.ufs@gmail.com

Resumo

O objetivo deste trabalho é apresentar um contexto no qual a matemática pode ser vislumbrada de forma mais atrativa e dinâmica. Para isso, serão apresentados conhecimentos sucintos, mas regulares, para a compreensão básica da criptografia. Citaremos exemplos de cifras e de como funcionam algumas delas, mostraremos algumas definições, teoremas e demonstrações sobre assuntos, tais como, divisibilidade, congruência, funções e matrizes. Por fim, faremos sugestões de um conjunto de atividades que proporcionam a interligação de conhecimento matemático e conhecimento diário do aluno, visto que essa combinação é um fator atrativo para melhor assimilação do conteúdo. No entanto, o professor tem o discernimento para realizar escolhas e julgar o que achar mais interessante.

Palavras Chaves: Criptografia, divisibilidade, congruência, funções e matrizes.

Abstract

The objective of this paper is to present a context in which mathematics can be glimpsed in a more attractive and dynamic way. For this, succinct but regular knowledge will be presented to the basic understanding of cryptography. We will cite examples of figures and how some of them work, in addition to some definitions, theorems and demonstrations on topics such as divisibility, congruence, functions and arrays. Finally, we will make suggestions of a set of activities that provide the interconnection of mathematical and daily knowledge of the student, since this combination is an attractive factor for a better assimilation of content. However, the teacher has the insight to make choices and to judge what he thinks it's most interesting.

Keywords: Encryption, divisibility, congruence, functions and matrix.

Sumário

Introdução

Como nos diz a própria história, a matemática surge da necessidade humana de contabilizar objetos, medir áreas, entre outras coisas, sendo assim, conceituada como uma disciplina de números e formas, das relações e das medidas.

De acordo com os próprios PCN's, a matemática se apresenta como uma ciência de muita aplicabilidade, um utensílio importante para os diferentes campos do conhecimento e indispensável para o crescimento da nação. À medida que a sociedade evolui, mais o ser humano precisa de conhecimentos matemáticos para exercer sua cidadania, tornando assim um sujeito crítico, com atitudes, responsável e acima de tudo ético.

Dessa forma, o ensino de matemática nas escolas se caracteriza pela forma peculiar, constituída pela aplicação de regras, desencadeadas em uma sequência de formas mecanizadas que são utilizadas para resolução e aparentemente "compreensão"de um determinado conteúdo. Assim, ela passa a ser compreendida por muitos como uma disciplina complicada, onde suas teorias não são necessárias para nossa sobrevivência, sendo vista muitas vezes como o "bicho-papão". Seu ensino tem sido percebido por muitos como algo monótono e abstrato, em que o professor transfere conceitos fundamentais através de aulas tediosas e o aluno é um mero receptor de informação.

Grande parte dos alunos não consegue entender a matemática que lhe é atribuída, reprovam constantemente, ou pior, são aprovados, mas não conseguem ter acesso a essa aprendizagem, de vital importância, de forma satisfatória e produtiva. Trabalhar a matemática de forma mais contextualizada e lúdica pode ser uma maneira de aproximar mais o aluno do conhecimento matemático desmitificando o fato de que a matemática é um bicho de sete cabeças, para isso, as metodologias podem ser uma grande ferramenta.

Vivemos em uma sociedade bem diversificada, onde cada ser tem suas próprias crenças, individualidades e isso não é diferente com os nossos professores. Cada um deles tem sua metodologia, sua crença, suas reflexões com relação ao que é melhor para seus alunos e diante de cada circunstância podem vivenciar situações de desilusões, de erros, acertos e é através delas que adquirimos maturidade e construímos nosso próprio conceito de vida.

Diante de tais observações, o foco deste trabalho é mostrar algumas atividades que servirão de subsídio para sistematizar alguns conteúdos específicos de matemática, tais como, divisibilidade, funções, matrizes, entre outros, a fim de estreitar a relação de conteúdos matemáticos com situações cotidianas.

É imprescindível que o professor busque, incansavelmente, novas formas de abordar os conteúdos, de forma atrativa para tentar amenizar o desinteresse e as dificuldades apresentadas pelos estudantes. Pensando nisso, a criptografia neste trabalho é usada para fundamentar essa prática de impulsionar o interesse de nossos alunos.

A criptografia serve de fundamento para possibilitar professores de Matemática do

Ensino Fundamental e Médio pesquisar e desenvolver atividades didáticas que facilite, incentive, aprimore a interpretação de conteúdos desenvolvidos em sala de aula, através de atividades de codificação e decodificação envolvendo os conteúdos matemáticos.

No primeiro capítulo, serão apontados além do conceito de criptografia, algumas técnicas de codificação que visam sistematizar uma informação de forma que somente o emissor e o receptor possam entendê-la, além de exemplos de cifras de transposição e substituição. No segundo capítulo, serão definidos conceitos básicos de funções, matrizes e determinantes que servirão de pré-requisitos para o desenvolvimento das atividades propostas. No terceiro capítulo, serão demostrados teoremas e apresentados exemplos sobre divisibilidade e congruência.

É importante frisar que todo embasamento teórico dos capítulos anteriores serão utilizado como suporte para execução das atividades que mesclam tais conteúdos com a criptografia, sendo apresentadas no quarto capítulo. No quinto e último, exibiremos uma lista de atividades, um questionário sobre o uso da criptografia na educação básica e relatos da aplicação desse questionário e de algumas atividades desenvolvidas em sala de aula.

Capítulo 1

Criptografia

A criptografia é um conjunto de conceitos e técnicas que visam codificar uma informação de forma que somente o emissor e o receptor possam entendê-la, evitando que um intruso consiga interpretá-la. A palavra criptografia ainda evoca imagens de agentes secretos sorrateiramente transferindo informações sigilosas a nações rivais. Entretanto, a principal missão da moderna criptografia é proteger as informações referentes as transações bancárias e comerciais que transitam entre computadores numa rede.

"CRIPTOGRAFIA"deriva da fusão das palavras gregas

kryptós = oculto e Gráphein = escrever

A escrita por meio de códigos começou a surgir mediante alguns conflitos entre a Grécia e Roma e era usada como estratégia secreta para formular os ataques. Um método bastante conhecido é a Cifra de César, que recebeu esse nome porque foi criada para ser usada nas Guerras de Gália de Júlio César. Ele substituía cada letra na mensagem por outra que estivessem três casas à frente no alfabeto. A cifra é de fácil acesso tanto de codificação quanto de decodificação. É chamada de cifras monoalfabéticas, pois é um tipo de criptografia por substituição, que emprega um único alfabeto.

Novas técnicas de codificação têm sido desenvolvidas de tal forma que a decodificação por intermédio de computadores é praticamente inviável. Todo sistema criptográfico pode ser descrito num modelo matemático, no qual, o que difere são as funções de codificação e decodificação.

Vale ressaltar que quando usamos uma chave para decodificar e a mesma é usada também para decodificar, dizemos que o método de criptografia é simétrico. Caso contrário, ou seja, quando usamos chaves distintas o método é definido como assimétrico, uma dessas chaves, especificamente a de codificação, é de conhecimento público, e a outra, a de decodificação é de conhecimento privado.

Duas técnicas são bastante utilizadas na arte de codificar mensagens: a substituição e a transposição. Observe abaixo a diferença entre elas.

i) Cifras de Substituição

O valor normal das letras do texto original é mudado sem que a posição seja mudada. É um criptograma, ou seja, um texto cifrado que obedece a um código e a uma lógica pré-determinados para decifrar a mensagem. Essa é a arte de escrita secreta, na qual as letras originais do texto original, tratadas individualmente ou em grupos de comprimento constante, são substituídas por letras, figuras, símbolos ou uma combinação destes de acordo com um sistema definido e uma chave.

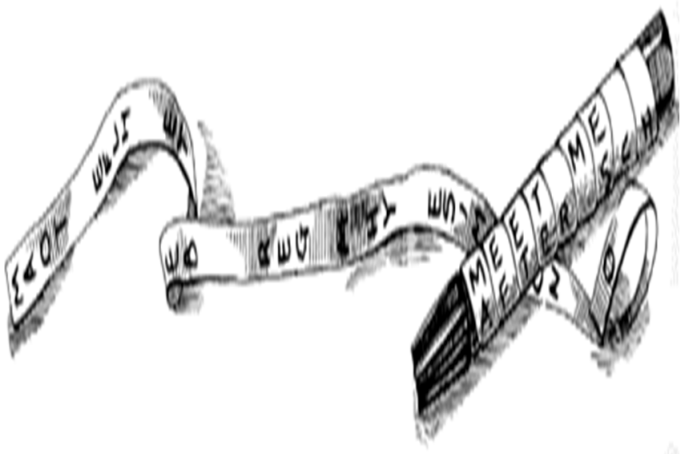
ii) Cifras de Transposição

Apenas a posição das letras do texto original é mudada, sem qualquer alteração no seu valor normal ou convencional. É um criptograma no qual as letras originais são apenas reorganizadas de acordo com um sistema definido. Em outras palavras, o texto cifrado é obtido através da permutação do texto original.

Vejamos alguns exemplos dessas cifras!

1.1 Bastão de Licurgo

Segundo algumas fontes históricas, uma das cifras de transposição mais antiga é a do bastão de Licurgo ou scytalae. Ele consiste em um bastão de madeira ao redor do qual se enrolava firmemente uma tira de couro ou pergaminho, longa e estreita. Escrevia-se a mensagem no sentido do comprimento do bastão e depois a tira era desenrolada, contendo a mensagem cifrada.



Esse método era bastante usado pelos gregos de Esparta em 475 a.C. É uma cifra de transposição, cuja segurança é baixíssima e hoje é apenas utilizado com interesse histórico por ser o primeiro "dispositivo mecânico"de criptografia.

1.2 Cifras Hebraicas

É um método de cifra de substituição simples, bastante usadas pelos religiosos, em especial os Hebreus. Atbash, Albam e Atbah são cifras hebraicas mais conhecidas que surgiram nos primórdios de 600 anos a.C. Vejamos um exemplo básico de como eram usadas uma dessas cifras.

CIFRA DE ALBAM

Para cifrar com Albam, inicialmente dividimos o alfabeto em duas metades. A segunda metade do alfabeto é alocada abaixo da primeira metade. A cifragem se dá pela troca da primeira letra do alfabeto normal pela primeira letra deste alfabeto trocado; a segunda letra do alfabeto normal pela segunda do alfabeto trocado, a terceira letra normal pela terceira do alfabeto trocado e assim sucessivamente.

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

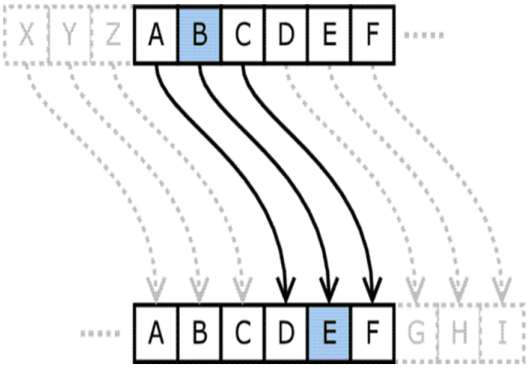
i) Texto Original: CRIPTOGRAFIA NUMA BOA

ii) Texto Cifrado: PEVCGBTENSVN AHZN OBN

1.3 Cifra de César

Como supracitado, a Cifra de César é um tipo de criptografia por substituição, no qual trocava cada letra na mensagem por outra que estivessem três casas à frente no alfabeto. Além disso, também é considerada monoalfabética porque usa apenas um alfabeto cifrante e ficou conhecida assim, pois surgiu durante conflitos nas Guerras da Gália de Júlio César.

Esse processo se resume a figura abaixo:



i) Texto Original: “NÃO HÁ ENSINO SEM PESQUISA E PESQUISA SEM ENSINO”.

ii) Texto Codificando: “QDR KD HQVLQR VHP SHVTXLVD H SHVTXLVD VHP HQVLQR”.

1.4 Cifra de Vigenère

A cifra recebeu esse nome em homenagem a Blaise de Vigenère, um diplomata e criptógrafo francês. Mesmo não sendo ele o responsável por sua criação, foi ele quem modificou a cifra para torná-la mais vigorosa.

Além disso, segundo Fonseca (2011, p. 179) essa cifra "é um método de encriptação que usa uma série de diferentes cifras de César baseadas em letras de uma senha. Trata-se de uma versão simplificada de uma mais geral cifra de substituição polialfabética, inventada por Leone Battista Alberti a cerca de 1465."

O artifício incide basicamente em substituir cada letra na mensagem por outra que estivessem deslocadas algumas "casas à frente no alfabeto. Ele versa de 26 alfabetos, sendo que na primeira linha está o alfabeto na ordem correta e nas linhas seguintes utiliza-se a Cifra de César deslocando uma casa em comparação com a linha anterior, como mostra o quadro abaixo:

Alfabeto correto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Suponhamos que queremos cifrar a palavra DESEJO.

i) Criar uma chave, ou seja, uma palavra qualquer e repetir sucessivamente até obter o mesmo comprimento da palavra ou texto a ser cifrado. Por exemplo, se a chave escolhida fosse UVA, teríamos

DESEJO = UVAUVA

ii) A primeira letra do texto, D, é cifrada usando o alfabeto na linha 20, que corresponde ao U, que é a primeira letra da chave. Basta olhar para a letra na linha U e coluna D, na tabela de Vigenère, que verás a correspondência com a letra X. Para a segunda letra do texto, ver a segunda letra da chave: linha 21 (V) e coluna E, que é Z, continuando sempre até obter toda a cifra.

DESEJO = UVAUVA = XZSYEO

Observação: A decifração segue de maneira inversa.

1.5 Cifra de Hill

É uma cifra de substituição, ganhou esse nome em homenagem ao matemático norte americano Lester S. Hill. Ela é um sistema poligráfico no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas. O método utiliza como suporte o conteúdo de matrizes quadradas invertíveis as quais são utilizadas para codificar e decodificar mensagens. Uma desvantagem desse método é o fácil acesso de quebrar o código por métodos estatísticos.

1.6 Correspondência Biunívoca

Esse método de criptografia é muito utilizado no dia a dia. Desde a educação infantil quando a criança aprende a desenvolver habilidade de combinar números à quantidade que eles representam, até a fase adulta na prática de jogos, tal como, batalha naval, onde o jogador irá dar as coordenadas de seu tiro fornecendo o número e letra equivalentes ao quadrado que atirou.

A essência dessa operação é a comparação e equiparação entre dois conjuntos. Uma correspondência entre os elementos de dois conjuntos é considerada biunívoca, quando a cada elemento de um corresponde a um único elemento do outro.

Observe a seguinte tabela:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	Q	L	M	N	O
4	P	R	S	T	U
5	V	W	X	Y	Z

i) Texto Original: A P L I C A Ç Õ E S / D A / M A T E M Á T I C A

ii) Texto Cifrado: 11 41 32 24 13 11 13 35 15 43 / 14 11 / 33 11 44 15 33 11 44 24 13 11

Com base em algumas técnicas de criptografia e em conteúdos matemáticos que constituirão este trabalho, serão indicadas algumas atividades que poderão ser explorada por professores do ensino fundamental e médio. Essas têm como fundamento colaborar, enfatizar, motivar, incrementar e aprimorar algumas de suas aulas, tornando-as mais dinâmicas e atrativas.

Capítulo 2

Conceitos Básicos

2.1 Funções

O assunto principal deste capítulo é o estudo de funções. Abordaremos, de início, as funções reais de uma variável real, isto é, funções $f : X \to \mathbb{R}$ que têm como domínio um subconjunto $X \subset \mathbb{R}$ e cujo valores $f(x)$, para todo $x \in X$, são números reais.

Definição 2.1.1 *Sejam X e Y dois conjuntos quaisquer*

Uma função é uma relação $f : X \to Y$ que, a cada elemento $x \in X$, associa a um, e somente um, elemento $y \in Y$.

Além disso,

i) Os conjuntos X e Y são chamados domínio e contradomínio de f, respectivamente;

ii) O conjunto $f(X) = \{y \in Y;\ \exists x \in X,\ f(x) = y\} \subset Y$ é chamado imagem de f;

iii) Dado $x \in X$, o (único) elemento $y = f(x) \in Y$ correspondente é chamado imagem de x.

Para que uma relação $f : X \to Y$ seja uma função, deve satisfazer a duas condições fundamentais.

i) Está definida em todo elemento do domínio;

ii) A cada elemento do domínio, não associar a mais de um elemento do contradomínio.

2.2 Funções Injetiva, Sobrejetiva e Bijetiva

Definição 2.2.1 *Consideremos uma função $f : X \to Y$.*

i) f é sobrejetiva se para todo $y \in Y$, existe $x \in X$, tal que, $f(x) = y$;

ii) f *é injetiva se* $x_1, x_2 \in X$, $x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)$;

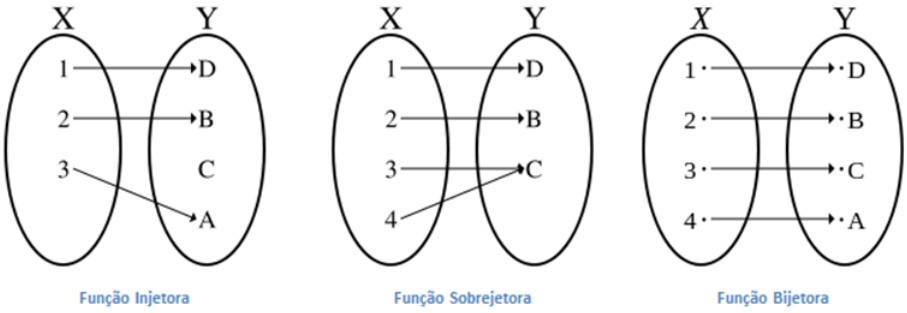
iii) f *é bijetiva se é sobrejetiva e injetiva.*

Exemplo 2.2.2 *A função* $f : \mathbb{R} \rightarrow \mathbb{R}$ *dada por* $f(x) = 2x$ *é injetiva, pois faz corresponder a cada número real* x *o seu dobro* $2x$*, e não existem dois números reais diferentes que tenham o mesmo dobro. Simbolicamente: Para quaisquer* $x_1, x_2 \in R$, $x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)$.

Exemplo 2.2.3 *A função sucessora* $f : \mathbb{N} \rightarrow \mathbb{N}$ *definida por* $f(n) = n + 1$ *não é sobrejetiva, pois* $Im(f) = \mathbb{N}^*$ *e* $\mathbb{N}^* \neq \mathbb{N}$*. Em outras palavras, dado* $0 \in \mathbb{N}$*, não há natural algum que seja transformado em 0 pela função* f*, isto é, 0 não é sucessor de nenhum número natural.*

Exemplo 2.2.4 *A função* $f : \mathbb{R} \rightarrow \mathbb{R}_+$ *dada por* $f(x) = x^2$ *não é bijetiva, pois, embora seja sobrejetiva, ela não é injetiva:* $3 \neq -3$*, mas* $f(3) = f(-3) = 9$.

Observe abaixo alguns anagramas que representa cada tipo de função descrita acima:



2.3 Função Afim

Definição 2.3.1 *Uma função $f : \mathbb{R} \to \mathbb{R}$, chama-se afim quando existem constantes a, $b \in \mathbb{R}$ tais que $f(x) = ax + b$ para todo $x \in \mathbb{R}$.*

Exemplo 2.3.2 *A função identidade $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x$ para todo $x \in \mathbb{R}$, é afim. Também são afins as translações $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x + b$. São ainda casos particulares de funções afins as funções lineares, $f(x) = ax$ e as funções constantes $f(x) = b$.*

2.4 Composição de Funções

Sejam $f : X \to Y$ e $g : U \to V$ duas funções, com $Y \subset U$. A função composta de g com f é a função denotada por $g \circ f$, com domínio em X e contradomínio em V, em que cada elemento de $x \in X$ faz corresponder a um elemento de $y = g \circ f(x) = g(f(x)) \to V$. Isto é:

$$\begin{gathered} gof : X \to Y \subset U \to V \\ x \mapsto f(x) \mapsto g(f(x)) \end{gathered}$$

2.5 Função Inversa

Definição 2.5.1 *Uma função $f : X \to Y$ é invertível se existe uma função $g : Y \to X$ tal que:*

i) $f \circ g = I_Y$;

ii) $g \circ f = I_X$.

Seja $f : X \to Y$ uma função e $f^{-1} : Y \to X$ sua relação inversa.

i) f é sobrejetiva $\iff$ f^{-1} está definida em todo elemento do domínio Y;

ii) f é injetiva $\iff$ f^{-1} não associa, a cada elemento do domínio Y, mais de um elemento do contradomínio X.

Observamos que I_A denota a função identidade do conjunto A, ou seja, $I_A : x \in A \mapsto x \in A$.
Neste caso, a função g é dita função inversa de f e denotada por $g = f^{-1}$.

Teorema 2.5.2 *Uma função $f : X \to Y$ é invertível se, e somente se, é bijetiva.*

Demonstração:
($\Rightarrow$)Por hipótese, existe $g : Y \to X$ tal que: (i) $f \circ g = I_Y$ e $g \circ f = I_X$. Tomemos $y \in Y$, qualquer. Seja $x = g(y)$, por (i), segue que $f(x) = f(g(y)) = f \circ g(y) = I_Y(y) = y$. Então, f é sobrejetiva. Tomemos $x_1, x_2 \in X$, tais que, $f(x_1) = f(x_2)$. Logo, $g \circ f(x_1) = g \circ f(x_2)$. Da condição (ii), segue que $I_X(x_1) = I_X(x_2)$, logo $x_1 = x_2$. Então, f é injetiva.

($\Leftarrow$) Por hipótese, f é bijetiva. Desejamos construir uma função $g : Y \to X$ satisfazendo as condições (i) e (ii) da defnição de função invertível. Dado $y \in Y$ qualquer, como f é sobrejetiva, existe $x \in X$, tal que, $f(x) = y$ e, como f é injetiva, o elemento x com esta propriedade é único. Assim, definimos $g(y)$ como o único $x \in X$, tal que, $f(x) = y$. As duas condições desejadas decorrem imediatamente da construção de g. ■

2.6 Determinantes

A noção de determinante desempenha um papel importante na matemática, aparecendo em alguns teoremas fundamentais. Desta maneira, faremos então uma abordagem mais simples e elementar, de modo a tornar o texto acessível aos alunos. Vejamos:

Dado um sistema linear 2 x 2 nas incógnitas x e y, por exemplo,

$$\begin{cases} ax + by = e \\ cx + dy = f \end{cases}$$

é notável que se $ad - bc \neq 0$, as soluções desse sistema são dadas pelas fórmulas

$$x = \frac{ed - fb}{ad - bc} \text{ e } y = \frac{af - ce}{ad - bc}.$$

Os numeradores e os denominadores que apareceram nas soluções são os determinantes, definição a seguir, de certas matrizes associadas ao sistema linear.

Se $A[a_{ij}]$ é uma matriz 2 x 2, definimos o determinante da matriz A como

$$DetA = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} = a_1b_2 - a_2b_1$$

O termo determinante foi introduzido pela primeira vez por Gauss em 1801.

No caso de sistemas lineares 3 x 3, assim como no caso 2 x 2, se o determinante da matriz dos coeficientes é não nulo, é possível determinar a solução do sistema.

Faremos agora o estudo do determinante de uma matriz 3 x 3. O caso geral, de matriz nxn, pode ser tratado de modo análogo, com uma notação mais complexa.

O determinante da matriz

$$m = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}$$

é o número

$$\triangle = detm = a_1b_2c_3 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1 + a_2b_3c_1 - a_1b_3c_2.$$

Ele é a soma de $6 = 3!$ parcelas, cada uma das quais é um produto de três fatores, pertencendo esses 3 fatores a linha e colunas diferentes. Assim, cada uma das seis parcelas é um produto do tipo abc, com índices $1, 2, 3$ aparecendo, cada um uma vez, em todas as parcelas. A ordem em que os índices aparecem é relevante. Ela corresponde às permutações de $1, 2, 3$. As permutações $123, 312 e 231$ aparecem nas parcelas precedidas do sinal $+$ enquanto as permutações $213, 321 e 132$ correspondem às parcelas precedidas do sinal $-$. As três primeiras são chamadas as permutações pares. Elas são obtidas quando se tomam três números consecutivos quaisquer na sequência

$$123123123123\ldots$$

As outras são as permutações ímpares, que se obtêm trocando as posições de 2 elementos numa permutação par ou então escolhendo três números consecutivos quaisquer na sequência

$$321321321321\ldots$$

Sejam $u = (a_1, b_1, c_1)$, $v = (a_2, b_2, c_2)$ e $w = (a_3, b_3, c_3)$ os três vetores de $\mathbb{R}^{\not 4}$ que correspondem às três linhas da matriz m acima. Para enfatizar a dependência do determinante de m em relação a esses vetores, escrevemos

$$detm = det[u, v, w].$$

A seguir, faremos uma lista das propriedades básicas do determinante.

1. O determinante muda de sinal quando se trocam as posições de duas quaisquer de suas linhas. Assim, tem-se

$$\begin{gathered} det[v, u, w] = -det[u, v, w], \\ det[w, v, u] = -det[u, v, w] \text{ e} \\ det[u, w, v] = -det[u, v, w]. \end{gathered}$$

2. Se uma matriz tem duas linhas iguais, seu determinante é igual a zero. Assim, $det[u, u, w] = det[u, v, u] = det[u, v, v] = 0$.

3. Se multiplicarmos uma linha da matriz por um número, o determinante fica multiplicado por aquele número. Assim, $det[u, v, w] = det[u, v, \alpha.w] = \alpha det[u, v, w]$.

4. Se uma linha da matriz é soma de duas parcelas (vetoriais) seu determinante é soma de dois outros, em cada um dos quais aquela linha é substituída por uma das parcelas. Assim, $det[u + u', v, w] = det[u, v, w] + det[u', v, w]$.

5. Se uma linha da matriz é combinação linear das outras duas, o determinante dessa matriz é zero. assim, $det[\alpha.v + \beta.w, v, w] = det[u, v, \alpha.u + \beta.v] = 0$.

6. Tem-se $det[u, v, w] = 0$ se, e somente se, os vetores u, v, w são linearmente dependentes, isto é, um deles é combinação linear dos demais.

7. O determinante não se altera se substituirmos uma de suas linhas pela soma dela com um múltiplo de outra. Assim, por exemplo, $det[u + \alpha.v, v, w] = det[u, v, w]$.

8. O determinante não se altera quando se trocam as linhas pelas colunas e vice-versa. Podemos reformular a última propriedade acima do seguinte modo. As matrizes

$$m = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix} \text{ e } m^T = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

são tais que as linhas da segunda coincidem com as colunas da primeira, na mesma ordem. Diz-se então que m^T é a transposta da matriz m. A propriedade 8 significa que as matrizes m e m^T têm o mesmo determinante.

2.7 Matrizes

O estudo de matrizes é de suma importância ao nosso cotidiano e está intimamente ligada ao ser humano, desde os mais diversos meios de comunicação, a engenharia civil, elétrica, mecânica, meteorologia, oceanografia entre outras inúmeras áreas. Neste tópico será explorado um pouco do conteúdo básico de matrizes o qual, mais tarde, será correlacionado com a criptografia.

Uma matriz $m \times n$ é uma lista de números a_{ij}, com índices duplos, onde $1 \leq i \leq m$ e $1 \leq j \leq n$. A matriz M é representada por um quadro numérico com m linhas e n colunas, no qual o elemento a_{ij} situa-se no cruzamento de i-ésima linha com a j-ésima coluna:

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

A lista ordenada $(a_{i1}, a_{i2}, \ldots, a_{in})$ chama-se i-ésima linha da matriz M, enquanto $(a_{1j}, a_{2j}, \ldots, a_{mj})$ chama-se j-ésima coluna da matriz M. O elemento a_{ij} chama-se ij-ésimo elemento de M e escreve-se $M = [a_{ij}]$.

2.8 Matriz Quadrada

Definição 2.8.1 *Diz-se que a matriz M é quadrada quando tem o mesmo número de linhas e colunas.*

Exemplo 2.8.2

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

é uma matriz quadrada de ordem 3.

Numa matriz quadrada M de ordem n, os elementos a_{ij} tais que $i = j$ formam a diagonal principal da matriz, e os elementos a_{ij} tais que $i + j = n + 1$ formam a diagonal secundária.

2.9 Matriz Nula

Definição 2.9.1 *Diz-se que a matriz M é nula quado todos os seus elementos são iguais a zero, ou seja, $a_{ij} = 0$, quaisquer que sejam i e j, com $1 \leq i \leq m$ e $1 \leq j \leq n$.*

Exemplo 2.9.2

$$M = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}$$

2.10 Matriz Identidade

Definição 2.10.1 *Diz-se matriz identidade, a matriz quadrada de ordem n em que todos os elementos da diagonal principal são iguais a 1 e os outros elementos são iguais a zero e representamos por I_n.*

Exemplo 2.10.2

$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Sendo $a_{ij} = 1$ para $i = j$ e $a_{ij} = 0$ para $i \neq j$.

2.11 Matriz Inversa

Seja A uma matriz quadrada de ordem n. A matriz A é dita inversível, se existe uma matriz B (quadrada de ordem n), tal que, $A \cdot B = B \cdot A = I_n$. Nesse caso, B é dita inversa de A e é indicada por A^{-1}.

Exemplo 2.11.1 *A inversa de* $A = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$ *é* $A^{-1} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$, *pois:*

$$A \cdot A^{-1} = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \quad . \quad \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

$$A^{-1} \cdot A = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} \quad \cdot \quad \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

2.12 Igualdade de Matrizes

Definição 2.12.1 *Duas matrizes, A e B, são iguais se, e somente se, têm o mesmo tipo e seus elementos correspondentes são iguais.*

Dadas as matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{m\times n}$, temos simbolicamente:

$$A = B \Leftrightarrow a_{ij} = b_{ij}, \text{ com } 1 \leq i \leq m \text{ e } 1 \leq j \leq n.$$

2.13 Adição de Matrizes

Dadas duas matrizes, A e B, do mesmo tipo, $m \times n$, denomina-se soma de matriz A com a matriz B, que representamos por $A + B$, a matriz C do tipo $m \times n$ na qual cada elemento é obtido adicionando-se os elementos correspondentes de A e B.

Se $A = (a_{ij})$ e $B = (b_{ij})$ são matrizes do tipo $m \times n$, a soma $A+B$ é a matriz $C = (c_{ij})$ do tipo $m \times n$ tal que:

$$c_{ij} = a_{ij} + b_{ij}, \text{ com } 1 \leq i \leq m \text{ e } 1 \leq j \leq n.$$

2.14 Matriz Oposta

Definição 2.14.1 *Denomina-se matriz oposta de uma matriz A (representa-se por $-A$) a matriz que somada com A resulta em uma matriz nula.*

Exemplo 2.14.2 *Dada a matriz* $A = \begin{bmatrix} 2 & 0 \\ 7 & -8 \end{bmatrix}$ *, sua oposta é* $-A = \begin{bmatrix} -2 & 0 \\ -7 & 8 \end{bmatrix}$ *, pois:*

$$A + (-A) = \begin{bmatrix} 2 & 0 \\ 7 & -8 \end{bmatrix} + \begin{bmatrix} -2 & 0 \\ -7 & 8 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Observação: Os elementos correspondente de A e $-A$ são números opostos. Obtemos $-A$ mudando os sinais de todos os elementos de A.

2.15 Subtração de Matrizes

Sendo A e B duas matrizes do tipo $m \times n$, denomina-se diferença entre A e B (representada por $A - B$) a soma da matriz A com a matriz oposta de B.

$$A - B = A + (-B)$$

Dadas as matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{m\times n}$, $A - B = (c_{ij})_{m\times n}$ tal que $c_{ij} = a_{ij} - b_{ij}$, com $1 \leq i \leq m$ e $1 \leq j \leq n$.

2.16 Matriz Transposta

Seja A uma matriz $m \times n$, denomina-se matriz transposta de A (indica-se por A^t) a matriz $m \times n$ cujas linhas são, ordenadamente, as colunas de A, ou seja, se $A = (a_{ij})$ é do tipo $m \times n$, então $A^t = (b_{ij})$ é do tipo $n \times m$ e $b_{ij} = a_{ij}$.

2.17 Multiplicação de Matrizes

Dada uma matriz $A = (a_{ij})$ do tipo $m \times n$ e uma matriz $B = (b_{ij})$ do tipo $n \times p$, o produto da matriz A pela matriz B é a matriz $C = (c_{ij})$ do tipo $m \times p$, tal que, o elemento c_{ij} é calculado multiplicando-se ordenadamente os elementos da linha i, da matriz A, pelos elementos da coluna j, da matriz B, e somando-se os produtos obtidos. Para dizer que a matriz C é o produto de A por B, vamos indicá-lo por AB.

$$A_{m\times n} \cdot B_{n\times p} = AB_{m\times p}$$

Observações: O produto de matrizes é associativo: $(MN)P = M(NP)$ e distributivo: $(M+N)P = MP+NP$, $M(N+P) = MN+MP$. Mas, há quatro diferença fundamentais entre o produto de matrizes e o produto de números.

i) Primeira diferença: O produto MN não está definido para quaisquer matrizes M e N; pois só faz sentido quando o número de colunas de M é igual ao número de linhas de N.

ii) Segunda diferença: O produto MN não é comutativo. Mesmo que MN e NM existam, não se tem necessariamente $MN = NM$.

Exemplo 2.17.1

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 1 & 4 & 5 \end{bmatrix} \quad . \quad \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} = \begin{bmatrix} 30 & 36 & 42 \\ 41 & 49 & 57 \\ 52 & 62 & 73 \end{bmatrix}$$

Enquanto que,

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \quad . \quad \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 1 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 6 & 20 & 26 \\ 15 & 47 & 62 \\ 24 & 74 & 98 \end{bmatrix}$$

Portanto, multiplicamos as matrizes na ordem inversa e o resultado não foi o mesmo, concluindo assim que o produto de matrizes realmente não é comutativo.

iii) Terceira diferença: O produto de duas matrizes não nulas pode ser uma matriz nula: de $M \neq 0$ e $N \neq 0$ não se infere que $MN \neq 0$. Pode até ocorrer que $M \neq 0$ seja tal que $M^2 = 0$, como no exemplo abaixo.

Exemplo 2.17.2 *Se*

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

então, $M^2 = 0$.

iv) Quarta diferença: Todo número a diferente de zero possui o inverso multiplicativo a^{-1} pois, $aa^{-1} = a^{-1}a = 1$. Por outro lado, dada a matriz quadrada M, do tipo $m \times n$, nem sempre existe uma matriz P, do tipo $n \times p$, tal que, $MP = PM = I_n$. Quando uma tal matriz P existe, a matriz M se diz invertível e P chama-se matriz inversa de M. Escreve-se então $P = M^{-1}$.

Dada uma matriz quadrada A, cujo $det(A) \neq 0$, a sua inversa é dada por $A^{-1} = \dfrac{1}{det(A)} \cdot \overline{A}$, onde $\overline{A}$ é a matriz adjunta de A, ou seja, a transposta da matriz dos cofatores de A.

Diate dessas afirmações, temos a seguinte preposição:

Proposição 2.17.3 *Seja A uma matriz quadrada. A inversa de A existe, se e somente se, $det(A) \neq 0$.*

Demonstração:

Se $det(A) \neq 0$, temos que existe a inversa $A^{-1} = \dfrac{1}{det(A)} \cdot \overline{A}$;

Se a inversa de A^{-1} existe, então, $A \cdot A^{-1} = I$ e, pelo teorema de Binet, $det(A) \times det(A^{-1}) = 1 \neq 0$, portanto $det(A) \neq 0$.

■

Exemplo 2.17.4 *Determine, caso exista, a matriz inversa de* $A = \begin{bmatrix} 1 & 0 & 1 \\ 5 & 4 & 1 \\ 0 & 2 & 2 \end{bmatrix}$.

Como $det(A) = 16 \neq 0$, a inversa dessa matriz existe. Então, vamos calculá-la!

i) Inicialmente devemos calcular a matriz dos cofatores e para definir cofator é necessário primeiro definir o menor principal ou menor complementar, associado a um elemento qualquer de uma matriz quadrada.

Seja a matriz quadrada $M = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, *definimos como menor principal (ou complementar) ao determinante da matriz que se obtém eliminando a linha i e a coluna j da matriz A, representamos o menor principal por D.*

Neste caso temos, $A = \begin{bmatrix} 1 & 0 & 1 \\ 5 & 4 & 1 \\ 0 & 2 & 2 \end{bmatrix}$, *e iremos determinar o menor principal D_{11}, associado ao elemento a_{11}.*

O menor principal associado ao elemento a_{11} é a matriz que se obtém eliminando a linha e a coluna em que está o elemento a_{11}, ou seja,

$$D_{11} = \begin{bmatrix} 4 & 1 \\ 2 & 2 \end{bmatrix}$$

O menor principal será portanto o determinante de A_{11}. Assim, temos que $D_{11} = Det\ (A_{11}) = 4 \cdot 2 - 2 \cdot 1 = 6$.

Agora vamos determinar o menor principal D_{12}, associado ao elemento a_{12}, isto é, a matriz que se obtém eliminando a linha e a coluna em que está o elemento a_{12}, ou seja,

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

O menor principal será portanto o determinante de A_{12}. Assim, temos que $D_{12} = Det\ (A_{12}) = 5 \cdot 2 - 0 \cdot 1 = 10$.

Analogamente, calculamos os demais, então

$D_{13} = Det\ (A_{13}) = 5 \cdot 2 - 0 \cdot 4 = 10.$
$D_{21} = Det\ (A_{21}) = 0 \cdot 2 - 2 \cdot 1 = -2.$
$D_{22} = Det\ (A_{22}) = 1 \cdot 2 - 0 \cdot 1 = 2.$
$D_{23} = Det\ (A_{23}) = 1 \cdot 2 - 0 \cdot 0 = 2.$
$D_{31} = Det\ (A_{31}) = 0 \cdot 1 - 4 \cdot 1 = -4.$
$D_{32} = Det\ (A_{32}) = 1 \cdot 1 - 5 \cdot 1 = -4.$
$D_{313} = Det\ (A_{33}) = 1 \cdot 4 - 5 \cdot 0 = 4.$

ii) Uma vez definido o menor principal, podemos então definir cofator como $A_{ij} = (-1)^{i+j} \cdot D_{ij}$, desta forma, a matriz dos cofatores é do tipo $Cof(A) = \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}$.

Fazendo os devidos cálculos, temos

$A_{11} = (-1)^{1+1} \cdot D_{11} = 1 \cdot 6 = 6$
$A_{12} = (-1)^{1+2} \cdot D_{12} = (-)1 \cdot 10 = -10$
$A_{13} = (-1)^{1+3} \cdot D_{13} = 1 \cdot 10 = 10$
$A_{21} = (-1)^{2+1} \cdot D_{21} = (-1) \cdot (-2) = 2$
$A_{22} = (-1)^{2+2} \cdot D_{22} = 1 \cdot 2 = 2$
$A_{23} = (-1)^{2+3} \cdot D_{23} = (-1) \cdot 2 = -2$
$A_{31} = (-1)^{3+1} \cdot D_{31} = 1 \cdot (-4) = -4$
$A_{32} = (-1)^{3+2} \cdot D_{32} = (-1) \cdot (-4) = 4$
$A_{33} = (-1)^{3+3} \cdot D_{33} = 1 \cdot 4 = 4,$

portanto a matriz dos cofatores fica da seguinte forma:

$$Cof(A) = \begin{bmatrix} 6 & -10 & 10 \\ 2 & 2 & -2 \\ -4 & 4 & 4 \end{bmatrix}.$$

iii) Agora calculamos a matriz adjunta $\overline{A}$ *que é dada pela transposta da matriz dos cofatores, logo,*

$$\overline{A} = \begin{bmatrix} 6 & 2 & -4 \\ -10 & 2 & 4 \\ 10 & -2 & 4 \end{bmatrix}.$$

Como citamos anteriormente, dada uma matriz quadrada A*, cujo* $det(A) \neq 0$*, a sua inversa é dada por* $A^{-1} = \dfrac{1}{det(A)} \cdot \overline{A}$*, ou seja,*

$$A^{-1} = \frac{1}{16} \cdot \begin{bmatrix} 6 & 2 & -4 \\ -10 & 2 & 4 \\ 10 & -2 & 4 \end{bmatrix} = \begin{bmatrix} \frac{3}{8} & \frac{1}{8} & -\frac{1}{4} \\ -\frac{5}{8} & \frac{1}{8} & \frac{1}{4} \\ \frac{5}{8} & -\frac{1}{8} & \frac{1}{4} \end{bmatrix}.$$

Capítulo 3

Divisibilidade e Congruência

Divisibilidade e congruência são conteúdos fundamentais da Teoria dos Números. Com eles desencadeamos diversos outros assuntos, tais como, números primos, divisão euclidiana, algoritmos de criptografia, justificamos critérios de divisibilidade, encontramos o máximo divisor comum, entre diversas aplicações.

Um dos objetivos de falar sobre congruência é ajudar os professores e alunos nas atividades baseadas no conceito da aritmética modular, que os levassem a ampliar sua compreensão e promovesse o desenvolvimento do pensamento aritmético e algébrico no campo da criptografia. Desta forma, serão citadas algumas definições, demostrados alguns teoremas e exibidos exemplos, os quais servirão de auxílio para o desenvolvimento de atividades, que correlacionam tais conteúdos com a criptografia.

3.1 Divisibilidade

Definição 3.1.1 *Dizemos que o número inteiro a divide o número inteiro b, o qual representamos por $a|b$, se existe um número inteiro c tal que $b = a \cdot c$. Dizemos então que b é um múltiplo de a ou que a divide b ou que a é um fator de b ou ainda que a é divisor de b. Dizemos também que a divisão de b por a é exata.*

Teorema 3.1.2 *Sejam a e b números inteiros. Se a divide b e b divide a, então $a = b$.*

Demonstração:
Com efeito, se $a \mid b$ então existe um número inteiro c, tal que, $b = a \cdot c$. Se $b \mid a$ existe então um número inteiro d, tal que, $a = b \cdot d$. Segue-se que $b = (bd)c = b(dc) = bdc$, devido a monoticidade dos números inteiros, temos $1 = dc$ implicando assim, $a = b$. ■

Teorema 3.1.3 *Se a, b e c são números inteiro e $a|b$ e $a|c$ então $a|(b + c)$.*

Demonstração: Com efeito, se $a|b$ então existe q_1, tal que, $b = q_1 \cdot a$. Se $a|c$ existe q_2, tal que, $c = q_2 \cdot a$. Assim, $(b+c) = q_1a + q_2a = (q_1 + q_2)a$, donde $a|(b+c)$ como queríamos demonstrar. ■

Observação: A recíproca deste teorema nem sempre é verdadeira. É fácil achar números inteiros a, b e c, tais que, $a|(b + c)$ mas a não divide b e a não divide c, por exemplo, $3|(5 + 4)$, mas $3 \nmid 5$ e nem $3 \nmid 4$.

Teorema 3.1.4 *Se a, b e c são números inteiros, tais que, $a|b$ e $b|c$, então $a|c$.*

Demonstração: Com efeito, se $a|b$ e $b|c$ existem q_1 e q_2, tais que, $b = q_1 \cdot a$ e $c = q_2 \cdot b$. Substituíndo o valor de b na equação $c = q_2 \cdot b$, temos, $c = (q_2 \cdot q_1)a = q_3 \cdot a$ o que implica $a|c$. ■

3.2 Divisão Euclidiana

Em matemática, o algoritmo de Euclides é um método simples e eficiente de encontrar o máximo divisor comum entre dois números inteiros diferentes de zero. Fora da Geometria, Euclides descobriu um teorema o qual nos permite dividir qualquer número natural por outro. Desta forma, mesmo quando um número natural a não divide o número natural b, Euclide, utiliza, sem enunciá-lo explicitamente, o fato de que é sempre possível efetuar a divisão de b por a. Esse afirmação será enunciada no teorema (3.2.2), mas para sua demonstração precisamos primeiro apresentar o Princípio da Boa Ordenação.

Teorema 3.2.1 *Princípio da Boa Ordenação: Todo subconjunto não-vazio $A \subset \mathbb{N}$ possui um menor elemento.*

Demonstração:
Sem perda de generalidade, podemos admitir que 1 não pertence a A, pois caso contrário 1 seria evidentemente o menor elemento de A. O menor elemento de A, cuja existência queremos provar, deverá ser da forma $n + 1$. Desta forma, devemos encontrar um número natural n, tal que, $n + 1 \in A$ e, além disso, todos os elementos de A são maiores do que n, logo maiores do que $1, 2, \ldots, n$. Noutras palavras, procuramos um número natural n, tal que, $I_n \subset \mathbb{N} - A$ e $n + 1 \in A$. Com esse objetivo, consideramos o conjunto

$$X = \{n \in \mathbb{N}; I_n \subset \mathbb{N} - A\}$$

Portanto, X é o conjunto dos números naturais n, tais que, todos os elementos de A são maiores do que n. Como estamos supondo que 1 não pertence a A, sabemos que $1 \in X$. Por outro lado, como A não é vazio, nem todos os números naturais pertencem a X, ou seja, temos $X \neq \mathbb{N}$. Sabemos que um dos axiomas de Peano diz que se um conjunto de números naturais contém o número 1 e, além disso, contém o sucessor de cada um de seus elementos, então esse conjunto coincide com $\mathbb{N}$, isto é, contém todos os números naturais. Desta forma, vemos que o conjunto X não é indutivo, isto é, deve existir algum $n \in X$, tal que, $n + 1$ não pertença a X. Isto significa que todos os elementos de A são maiores do que n mas nem todos são maiores do que $n + 1$. Como não há números naturais entre n e $n + 1$, concluímos que $n + 1$ pertence a A e é o menor elemento de A. ■

Teorema 3.2.2 *Sejam a e b números inteiros, com $0 < a < b$. Existem dois únicos números inteiro q e r tais que*

$$b = aq + r, \text{ com } r < a.$$

Demonstração:
Suponha que $b > a$ e considere, enquanto fizer sentido, os números

$$b, b-a, b-2a, \cdots, b-n\cdot a, \cdots$$

Pelo teorema (3.2.1), o conjunto S formado pelos elementos acima tem um menor elemento $r = b - q.a$. Vamos provar que r tem a propriedade requerida, ou seja, que $r < a$.

Se $a|b$, então $r = 0$ e nada mais temos a provar. Se, por outro lado, $a \nmid b$, então $r \neq a$, e, portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número inteiro $c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - q \cdot a$, teríamos

$$c = b - (q+1)\cdot a \in S, \text{ com } c < r,$$

contradição com o fato de r ser o menor elemento de S.

Portanto, temos que $b = aq + r$, com $r < a$, o que prova a existência de q e r.

Agora vamos provar a unicidade. Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Logo, se $r = b - a.q$ e $r' = b - a \cdot q'$, com $r < r' < a$, teríamos $r' - r \geqslant a$, o que acarretaria $r' \geqslant r + a \geqslant a$, absurdo. Portanto, $r = r'$.

Daí segue-se que $b - a \cdot q = b - a \cdot q'$, o que implica que $a \cdot q = a \cdot q'$ e, portanto, $q = q'$.
■

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de quociente e de resto da divisão b por a.

Note que o resto da divisão acima de b por a é zero se, e somente se, a divide b.

3.3 Máximo Divisor Comum

Dados dois números inteiros a e b, não simultaneamente nulos, diremos que o número inteiro $d \in \mathbb{Z}^*$ é um divisor comum de a e b se $d|a$ e $d|b$.

Exemplo 3.3.1 *Sejam D o conjunto de divisores de um número, então $D(12) = \{1, 2, 3, 4, 6, 12\}$ e $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$, então os divisores comuns de 12 e 30 são $\{1, 2, 3$ e $6\}$.*

Definição 3.3.2 *Dizemos que d é um máximo divisor comum (mdc) de a e b se possuir as seguintes propriedades:*

i) $d|a$ (ou d é divisor de a)

ii) $d|b$

iii) Se d' é divisor de a e b, então $d'|d$

Escrevemos $d = mdc(a, b)$. Se $mdc(a, b) = 1$, dizemos que a e b são primos entre si.

Lema 3.3.3 *Sejam a e b números inteiros positivos. Se existem inteiros g e s, tais que, $a = bg + s$, então $mdc(a, b) = mdc(b, s)$.*

Demonstração:

$$\text{Sejam } d_1 = mdc(a, b) \text{ e } d_2 = mdc(b, s)$$

Afirmamos que $d_1 \leqslant d_2$. De fato, existem inteiros positivos u e v tais que:

$$a = d_1 u \text{ e } b = d_1 v$$

Substituindo a e b na equação $a = bg + s$ obtemos

$$s = d_1 u - d_1 vg = d_1(u - vg).$$

Ou seja, d_1 é um divisor comum de b e s. Mas d_2 é o maior divisor de b e s e portanto (por definição) $d_1 \leqslant d_2$ como queríamos. Seguindo um argumento semelhante, podemos provar o inverso, ou seja, $d_2 \leqslant d_1$. Em outras palavras, $d_1 = d_2$. ■

Podemos verificar um método prático para determinar o MDC, ou seja, dados dois números inteiros positivos a e b, tais que, $a \geqslant b$, divide-se a por b, encontrando resto r_1. Se $r_1 \neq 0$, dividimos b por r_1, obtendo resto r_2. Se $r_2 \neq 0$, dividimos r_1 por r_2 e assim por diante. O último resto diferente de zero dessa sequência de divisões é o $mdc(a, b)$, podemos comprovar através do teorema abaixo.

Teorema 3.3.4 *Dados a e b inteiros positivos, o último resto diferente de zero da sequência de divisões dada pelo algoritmo euclideano para a e b é o máximo divisor comum entre a e b.*

Demonstração:

$$\begin{gathered} a = bq_1 + r_1 \text{ e } 0 \leqslant r_1 < b \\ b = r_1 q_2 + r_2 \text{ e } 0 \leqslant r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 \text{ e } 0 \leqslant r_3 < r_2 \\ r_2 = r_3 q_4 + r_4 \text{ e } 0 \leqslant r_4 < r_3 \\ \vdots \\ r_{n-2} = r_{n-1} q_n \text{ e } r_n = 0 \end{gathered}$$

Da última linha, temos que r_{n-1} divide r_{n-2} e portanto $mdc(r_{n-1},\ r_{n-2}) = r_{n-1}$. Aplicando sucessivamente o lema anterior, temos que $mdc(a, b) = r_{n-1}$.

■

Exemplo 3.3.5

-	1	2	1	1	3
125	90	35	20	15	5
35	20	15	5	0	-

Ou seja, $mdc(125, 90) = 5$

Teorema 3.3.6 *Sejam a e b números inteiros positivos e seja d o máximo divisor comum entre a e b. Existem inteiros α e β tais que*

$$\alpha a + \beta b = d.$$

Demonstração:

Seja B o conjunto de todas as combinações lineares $(\alpha a + \beta b)$ onde α e β são inteiros. Vamos escolher α' e β', tais que, $c = \alpha' a + \beta' b$ seja o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c|a$ e $c|b$ (c divide a e c divide b). A prova será por contradição.

Suponhamos que $c \dagger a$ (c não divide a). Neste caso, pelo algoritmo da divisão, existem q e r tais que $a = q.c + r$, com $0 < r < c$.

Portanto, $r = a - qc = a - q(\alpha' a + \beta' b) = (1 - q\alpha')a + (-q\beta')b$. Isto mostra que $r \in B$, pois $(1 - q\alpha')$ e $(-q\beta')$ são inteiros, o que é um absurdo, uma vez que $0 < r < c$ e c é o menor elemento positivo de B.

Logo, $c \mid a$ e de forma análoga se prova que $c \mid b$.

Como d é um divisor comum de a e b, existem inteiros q_1 e q_2, tais que, $a = q_1 \cdot d$ e $b = q_2 \cdot d$.

Portanto, $c = \alpha' a + \beta' b = \alpha' q_1 \cdot d + \beta' q_2 \cdot d \Rightarrow c = d(\alpha' q_1 + \beta' q_2)$, o que implica que $d \mid c$.

Observe que se $d \mid c$, então $d \leqslant c$, mas d é o máximo divisor comum, então, $d \geqslant c$. Portanto, temos:

$$d = c \text{ e } d = \alpha a + \beta b.$$

■

Exemplo 3.3.7 *Sejam* $a = 1234$ *e* $b = 54$. *Temos que:*

$$1234 = 54 \cdot 22 + 46, \textit{ ou seja, } 46 = 1234 - 54 \cdot 22$$
$$54 = 46 \cdot 1 + 8, \textit{ ou seja, } 8 = 54 - 46 \cdot 1$$

Logo,

$8 = 54 - 46 \cdot 1$
$= 54 - (1234 - 54 \cdot 22) \cdot 1$
$= 54(1 + 22 \cdot 1) + 1234 \cdot (-1)$
$= 54 \cdot (23) + 1234 \cdot (-1)$

Logo,

$46 = 8 \cdot 5 + 6 \rightarrow 6 = 46 - 8 \cdot 5$
$= (1234 - 54.22) - [54 \cdot (23) + 1234 \cdot (-1)] \cdot 5$
$= 1234 \cdot (6) + 54 \cdot [-22 - (23) \cdot 5]$
$= 1234 \cdot (6) + 54 \cdot (-137)$

$8 = 6 \cdot 1 + 2 \rightarrow 2 = 8 - 6$
$= [54 \cdot (23) + 1234 \cdot (-1)] - [1234 \cdot (6) + 54 \cdot (-137)]$
$= 1234(-1 - 6) + 54(23 + 137)$
$= 1234(-7) + 54(160)$

E portanto, $\alpha = -7$ *e* $\beta = 160$.

3.4 Congruência

Congruência significa coerência, harmonia e está intimamente ligada a divisibilidade e restos de uma divisão. É uma tema abrangente e gerador de oportunidades de contextualização. Pode ser trabalhado já no ensino fundamental para ajudar no processo ensino aprendizagem de matemática.

Definição 3.4.1 *Considere* m *um número inteiro 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*

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

Quando a relação $a \equiv b(mod\ m)$ *for falsa, diremos que* a *e* b *não são congruentes, ou que são incongruentes, módulo* m.

Exemplo 3.4.2 $28 \equiv 4(mod\ 3)$*, já que os restos da divisão de* 28 *e de* 4 *por* 3 *são iguais a* 1*. Mas,* 21 *não é congruente a* 4 *módulo* 3*, pois a divisão de* 21 *por* 3 *deixa resto zero, já a divisão de* 4 *por* 3 *deixa resto igual a* 1.

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

Proposição 3.4.3 *Suponha que* a *e* $b \in \mathbb{Z}$ *são, tais que,* $b \geqslant a$*. 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,

$$b - a = m(q' - q) + (r' - r), \text{ se } r' \geqslant r$$
$$\text{ou}$$
$$b - a = m(q' - q) - (r' - r), \text{ se } r \geqslant r'$$

onde $r' - r < m$ ou $r - r' < m$. Portanto, $a \equiv b(\text{mod } m)$ se, e somente se, $r = r'$, o que é equivalente a dizer que $m \mid b - a$. ■

Proposição 3.4.4 *Seja* $m \in \mathbb{Z}$*, com* $m > 1$*. 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* $a \equiv c(mod\ m)$*.*

Demonstração:

i) $m \mid 0$, ou seja, $m \mid a - a$, o que implica que $a \equiv a(\text{mod } m)$.

ii) Se $a \equiv b(\text{mod } m)$, então $b - a = qm$, com $q \in \mathbb{Z}$.

$$a - b = -qm = (-q)m \Rightarrow b \equiv a(\text{mod } m).$$

iii) Se $a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m)$, então existem inteiros q_1 e q_2 tais que

$$b - a = q_1 m \text{ e } c - b = q_2 m$$

Portanto,

$$c - a = (b + q_2 m) - (b - q_1 m) = q_2 m + q_1 m = (q_2 + q_1)m$$

e isto significa que $a \equiv c(\text{mod } m)$. ■

Proposição 3.4.5 *Sejam* a*,* b*,* c*,* d *e* $m \in \mathbb{Z}$*, 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:

Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$ então existem inteiros q_1 e q_2 tais que $a - b = q_1 m$ e $c - d = q_2 m$. Desta forma,

$$(a + c) - (b + d) = (a - b) + (c - d) = (q_1 m + q_2 m) = (q_1 + q_2)m$$

e

$$ac - bd = (b + q_1 m)(d + q_2 m) - bd = (bq_2 + dq_1 + q_1 q_2)m$$

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

Proposição 3.4.6 *Para todo* $n \in \mathbb{N}$*, com* $a, b \in \mathbb{Z}$*, se* $a \equiv b(mod\ m)$*, então* $a^n \equiv b^n(mod\ m)$*.*

Demonstração: Provaremos por indução. A proposição é verdadeira para $n = 1$ e suponha que seja verdadeira para qualquer natural k. Desta forma, temos:

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

Portanto, pela proposição (3.4.5) acima

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

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

■

3.5 Classes de Restos módulo m

Uma relação de equivalência permite dividir um conjunto em classes de equivalência, ou seja, todos os números inteiros com o mesmo resto na divisão por m, podem ser agrupados num único subconjunto, e eles formam uma classe módulo m. Os possíveis restos da divisão por m serão um dos seguintes números inteiros $0, 1, 2, 3, \cdots, m-1$, desta forma, concluímos que existem exatamente m classes módulo m.

Teorema 3.5.1 *O conjunto $S = \{0, 1, 2, \cdots, m-1\}$ é um sistema completo de restos módulo m.*

Demonstração:
Com efeito, o conjunto S tem m elementos e, além disso, qualquer que seja o inteiro a temos, pelo algoritmo da divisão:

$$a = mq + r, \text{ com } 0 \leqslant r < m$$

o que implica $a \equiv r(\text{mod } m)$. Como o resto r só pode assumir os m valores $0, 1, 2, \cdots, m-1$, segue-se que o inteiro a é congruente módulo m a um único desses m inteiros. ■

3.6 Aritmética Módulo m

Seja a um inteiro. Chama-se classe de congruência de a módulo m ($m > 1$) o conjunto formado por todos os inteiros que são congruentes a a módulo m. Denotamos esse conjunto por $\overline{a}$. Temos, então:

$$\overline{a} = \{x \in \mathbb{Z};\ x \equiv a(\text{mod } m)\}$$

Como $x \equiv a(\text{mod } m)$, se e somente se, x é da forma $x = a + k \cdot m$, para algum $k \in \mathbb{Z}$, também podemos escrever:

$$\overline{a} = \{a + km | k \in \mathbb{Z}\}$$

Proposição 3.6.1 *Sejam a e b inteiros. Então $a \equiv b(mod\ m)$, se e somente se, $\overline{a} = \overline{b}$.*

Demonstração:
Suponhamos que $a \equiv b(\text{mod } m)$, queremos provar que $\overline{a} = \overline{b}$, isto é, uma igualdade entre conjuntos. Dado $x \in \overline{a}$, temos por definição que $x \equiv a(\text{mod } m)$. Da propriedade transitiva de congruência e da hipótese, segue imediatamente que $x \in \overline{b}$. Logo, $\overline{a} \subset \overline{b}$. A inclusão $\overline{b} \subset \overline{a}$ em sentido contrário segue de forma análoga.

Reciprocamente, $\overline{a} = \overline{b}$, como $a \in \overline{a}$, temos também que $a \in \overline{b}$, logo, $a \equiv b(\text{mod } m)$.
■

Corolário 3.6.2 *Sejam a e b inteiros. Se $\overline{a} \neq \overline{b}$, então $\overline{a} \cap \overline{b} = \oslash$.*

Demonstração:
Se $\overline{a} \cap \overline{b} \neq \oslash$, consideremos um inteiro c que pertença a ambas as classes. Como $c \in \overline{a}$, temos que $c \equiv a(\text{mod } m)$ e, de forma análoga, $c \equiv b(\text{mod } m)$. Portanto, $a \equiv b(\text{mod } m)$ e, da proposição acima, $\overline{a} = \overline{b}$. ■

Dada uma classe $\overline{a}$, para qualquer inteiro x, tal que, $x \in \overline{a}$, temos que $\overline{x} = \overline{a}$. Por causa disto, cada inteiro pertencente a uma dada classe diz-se um representante daquela classe. Por exemplo, 11 e -3 são representantes da classe $\overline{4}$ módulo 7.

Consideremos um sistema completo de classes ou resíduos módulo m, por exemplo, os inteiros $0, 1, \cdots, m-1$ e suas respectivas classes

$$\begin{gathered}\overline{0} = \{0, \pm m, \pm 2m, \pm 3m, \cdots\} \\ \overline{1} = \{1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \cdots\} \\ \overline{2} = \{2, 2 \pm m, 2 \pm 2m, 2 \pm 3m, \cdots\} \\ \vdots \\ \overline{m-1} = \{m-1, m-1 \pm m, m-1 \pm 2m, m-1 \pm 3m, \cdots\}\end{gathered}$$

Conforme já foi considerado, cada inteiro pertence a uma e apenas uma das m classes. Por exemplo, se $m = 5$, todas as classes possíveis, módulo 5, são as seguintes:

$$\begin{gathered}\overline{0} = \{0, \pm 5, \pm 10, \pm 15, \cdots\} \\ \overline{1} = \{1, 1 \pm 5, 1 \pm 10, 1 \pm 15, \cdots\} \\ \overline{2} = \{2, 2 \pm 5, 2 \pm 10, 2 \pm 15, \cdots\} \\ \overline{3} = \{3, 3 \pm 5, 3 \pm 10, 3 \pm 15, \cdots\} \\ \overline{4} = \{4, 4 \pm 5, 4 \pm 10, 4 \pm 15, \cdots\}\end{gathered}$$

Denotaremos pelo símbolo $\mathbb{Z}_m$ o conjunto das classes de congruências módulo m e o chamaremos de Conjunto dos Inteiros Módulo m. Assim, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{m-1}\}$.

3.7 Adição e Multipicação em $\mathbb{Z}_m$

Definição 3.7.1 *Para adicionar duas classes resto, tomamos um elemento de cada classe e os adicionamos. A classe a qual pertence a soma será a soma dessas duas classes resto.*

Exemplo 3.7.2 *Exemplificando a adição em uma "tabuada"módulo 5 teremos:*

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Definição 3.7.3 *Para achar o produto de duas classes resto, multiplicaremos um elemento qualquer de uma das classes por um elemento qualquer da outra. A classe a qual pertence o produto é o produto das classes.*

Exemplo 3.7.4 *Obtemos assim, a seguinte tabela de multiplicação módulo 5.*

$\times$	*0*	*1*	*2*	*3*	*4*
0	*0*	*0*	*0*	*0*	*0*
1	*1*	*2*	*3*	*4*	*0*
2	*0*	*2*	*4*	*1*	*3*
3	*0*	*3*	*1*	*4*	*2*
4	*0*	*4*	*3*	*2*	*1*

Observações: Observe, na tabela de adição, o conceito de inverso aditivo módulo m. Dizemos que dois elementos de $\mathbb{Z}_m$ são inversos aditivos, se e somente se, $\overline{a+b} \equiv 0(\text{mod } m)$. Assim, por exemplo, 4 e 3 são inversos aditivos módulo 7, uma vez que $\overline{4+3} \equiv 0(\text{mod } 7)$.

Portanto, para efetuar a soma de duas classes módulo m, tomamos representantes (quaisquer) a e b dessas classes, efetuamos a soma $a+b$ em $\mathbb{Z}$ e consideramos como resultado da soma a classe de $a+b$ módulo m. A operação de produto se faz de forma análoga. Surge agora uma pergunta natural: será que o resultado das operações não depende dos representantes escolhidos? Sabemos que em $\mathbb{Z}_7$, $\overline{3}+\overline{6} = \overline{9} = \overline{2}$, será que poderíamos tomar 38 como um representante de $\overline{3}$ e 27 como representante de $\overline{6}$. Será que $\overline{38} + \overline{27} = \overline{65}$ é o mesmo resultado que aquele obtido acima, $\overline{3} + \overline{6} = \overline{9} = \overline{2}$? A resposta é afirmativa. Como $65 \equiv 2(\text{mod } 7)$, felizmente o resultado é o mesmo.

3.8 Divisão em $\mathbb{Z}_m$

Dividir um número a por b nada mais é que multiplicarmos a pelo inverso multiplicativo de b, ou seja, b^{-1}, com $b \neq 0$, isto é, o número, tal que, $b \cdot b^{-1} = 1$.

Analogamente, digamos que $a \in \mathbb{Z}_m$. Diremos que a classe $a^{-1} \in \mathbb{Z}_m$ é o inverso de $a \in \mathbb{Z}_m$ se a equação $a \cdot a^{-1} = 1$ é verificada em $\mathbb{Z}_m$.

Obviamente, $\overline{1}$ e $\overline{-1}$ são sempre inversíveis em $\mathbb{Z}_m$, mas há outros exemplos. Em $\mathbb{Z}_5$ temos que $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$ e $\overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$, logo $\overline{2}$, $\overline{3}$ e $\overline{4}$ são também inversíveis de $\mathbb{Z}_5$, $\overline{2}$ é o inverso de $\overline{3}$ e, reciprocamente, $\overline{4}$ é o seu próprio inverso.

Por outro lado, é claro que $\overline{0}$ não é inversível em $\mathbb{Z}_m$, para nenhum valor de m. De fato, para qualquer $\overline{a} \in \mathbb{Z}_m$ temos que $\overline{0} \cdot \overline{a} = \overline{0} \neq \overline{1}$.

A proposição abaixo estabelece as condições necessárias para que um elemento de $\mathbb{Z}_m$ seja inversível e sua demonstração fornece um algoritmo para determinação do inverso de um elemento inversível.

Proposição 3.8.1 *Seja $\overline{a}$ um elemento não nulo de $\mathbb{Z}_m$. Então, $\overline{a}$ é inversível se, e somente se, $mdc(a, m) = 1$.*

Demonstração:

Suponhamos que $mdc(a, m) = 1$. Sendo a e b inteiros se $d = mdc(a, b)$, então existem q_1 e q_2 tais que $d = q_1a + q_2b$. Também existem q_1 e q_2 tais que $aq_1 + q_2m = 1$. Tomando classes temos:

$$\overline{1} = \overline{aq_1 + q_2m} = \overline{aq_1} + \overline{mq_2} = \overline{aq_1} + \overline{0q_2} = \overline{aq_1} = \overline{a} \ . \ \overline{q_1}$$

Logo, $\overline{q_1}$ é o inverso de $\overline{a}$.

Reciprocamente, se $mdc(a, m) \neq 1$, então $\overline{a}$ é divisor de zero e existe $\overline{b} \neq 0$, tal que $\overline{a} \cdot \overline{b} = \overline{0}$. Mostraremos que, nesse caso, $\overline{a}$ não pode ser inversível. Com efeito, suponhamos que existe $\overline{a'}$ tal que $\overline{a} \cdot \overline{a'} = \overline{1}$. Teríamos então:

$\overline{b} = \overline{b} \cdot \overline{1} = \overline{b} \cdot (\overline{a.a'}) = (\overline{b} \ . \ \overline{a}) \cdot \overline{a'} = (\overline{a} \ . \ \overline{b}) \cdot \overline{a'} = \overline{0}$, uma contradição. ■

Um exemplo bastante notório que envolve congruência é a famosa "aritmética do relógio". É um exemplo de aritmética módulo m, neste caso, $m = 24$. Se for $6h$ e se passarem $20h$, teremos $6 + 20 = 26h$ que nada mais é que 2 módulo 24, ou seja, $2h$ do dia seguinte. Usaremos como base esse método para trabalharmos com divisibilidade em sala de aula.

3.9 Cripto-sistema

Como já mencionamos anteriormente, na criptografia a mensagem para ser enviada é chamada de texto-original e a mensagem codificada é chamada de texto-cifrado. O texto-original e o texto-cifrado são escritos em algum alfabeto F consistindo de um certo número m de símbolos; isto é,

$$\neq (F) = m.$$

O processo de converter um texto-original para um texto-cifrado é chamado de codificação ou cifragem, e o processo de reverter é chamado de decodificação ou decifragem.

O texto-original e texto-cifrado são divididos em mensagens unitárias. Uma mensagem unitária pode ser um bloco de k símbolos do alfabeto F. O processo de codificação é uma função que associa cada mensagem unitária u do texto-original a uma mensagem unitária c do texto-cifrado. Mais precisamente, sejam P o conjunto de todas as possíveis mensagens unitárias u do texto-original e C o conjunto de todas as possíveis mensagens unitárias c do texto-cifrado. Então a correspondência biunívoca

$$f : P \to C, \text{ tal que, } f(u) = c$$

é o processo de codificação. A correspondência biunívoca

$$f^{-1} : C \to P, \text{ tal que, } f^{-1}(c) = u$$

o processo de decodificação. Assim, temos o seguinte diagrama, denominado Cripto-Sistema

$$\begin{array}{c} f \ f^{-1} \\ P \to C \to P \end{array}$$

Um Cripto-sistema é qualquer bijeção de P sobre C.
É útil substituir os símbolos de um alfabeto F por números inteiros 1, 2, . . ., para tornar mais fácil a construção do cripto-sistema f. Para decodificar a mensagem cifrada, temos que aplicar a propriedade inversa, daí, precisamos de alguns resultados que nos ajudará a definir melhor nossa função codificadora. Observem o seguinte teorema:

Teorema 3.9.1 *Sejam $m \in \mathbb{N}$ e $a, b \in \mathbb{Z}_m$ fixados. Se $mdc(a, m) = 1$, então a função*

$$f : \mathbb{Z}_m \to \mathbb{Z}_m \text{ dada por } f(x) = ax + b$$

é um cripto-sistema.

Demonstração:
Como $mdc(a, m) = 1$ temos que existe $a' = a^{-1} \in \mathbb{Z}_{m\cdot}$, tal que, $a \cdot a' = 1$. Assim,

$$f^{-1}(x) = a'x + b'$$

onde $b' = -a'b$ é tal que

$$f \circ f^{-1} = f^{-1} \circ f = I_{\mathbb{Z}_m},$$

isto é, f^{-1} é a função inversa de f. De fato,

$f \circ f^{-1}(x) = f(f^{-1}) = a \cdot f^{-1} + b = a \cdot (a'x + b') + b = aa'x + ab' + b = aa'x + a(-a'b) + b = aa'x + (-a'a)b + b = x - b + b = x$.

■

O cripto-sistema

$$f(x) = ax + b$$

é chamado de transformação afim. O par (a, b) é chamado de chave de codificação ou chave secreta. Quando $m = 26$, $a = 1$ e $b \in \mathbb{Z}_{26}$ o cripto-sistema

$$f(x) = x + b$$

é chamado de Cifra de César, pois Júlio César a utilizava. Quando $b = 0$ o cripto-sistema

$$f(x) = ax$$

é uma transformação linear.

Para decodificar a mensagem cifrada, temos que aplicar a propriedade inversa, lembrando que a inversa também tem que está em $\mathbb{Z}_{26}$. Para isso, calculamos $f^{-1}(x) = a'x+b'$, onde $a \cdot a' = 1$ e $b' = -a'b$.

Diante do que apresentamos, devemos sempre ter o cuidado de buscar uma função bijetora, pois do contrário poderemos ter um mesmo valor relacionado a duas letras distintas. Como vamos trabalhar em $\mathbb{Z}_{26}$, não será problema já que nosso domínio é um conjunto discreto com número finito de elementos, neste caso, 26 elementos. Portanto, no caso de funções do 1º grau, seu gráfico é um conjunto de 26 pontos sobre uma reta.

3.10 Inversa de Matrizes em $\mathbb{Z}_m$

Quando tratamos de matrizes também devemos nos alertar quanto a importância de sua inversa está em $\mathbb{Z}_m$. Fiquemos atentos a seguinte resultado.

Uma matriz A é inversível em $\mathbb{Z}_m$ se, e somente se, $mdc(detA, m) = 1$.

Desta maneira, para encontrar a matriz inversa em $\mathbb{Z}_{26}$, temos que garantir que seu determinante seja diferente de zero e, além disso, esse valor deve ser primo com 26, ou seja, $mdc(detA, 26) = 1$.

Vamos agora mostrar, através de um exemplo, como determinar a inversa de uma matriz em $\mathbb{Z}_{26}$.

Exemplo 3.10.1 *Determine em $\mathbb{Z}_{26}$ a inversa, caso exista, da matriz $M = \begin{bmatrix} 1 & 3 \\ -1 & 6 \end{bmatrix}$.*

Primeiro calculamos o valor do determinante de M. Como $det(M) = 9 \neq 0$ e, além disso, $mdc(detM, 26) = mdc(9, 26) = 1$, a definição acima garante a existência da matriz inversa. Como o determinante da matriz M é igual a 9, temos que seu inverso multiplicativo em $\mathbb{Z}_{26}$ é igual a 3, já que é o número que multiplicado por 9 deixa resto 1 quando dividido por 26, isso nada mais é que a solução da seguinte congruência, $9X \equiv 1 (mod\ 26)$.

Agora encontramos a matriz transposta da matriz dos cofatores, indicada por $\overline{M}$, e, em seguida, multiplicamos por 3, obtendo assim M^{-1}.

$$M^{-1} = \frac{1}{detM} \cdot \overline{M} = 3 \cdot \begin{bmatrix} 6 & -3 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 18 & -9 \\ 3 & 3 \end{bmatrix}$$

Em seguida, converteremos cada m_{ij} da matriz M^{-1} em termos pertencentes a $\mathbb{Z}_{26}$, usando assim as técnicas de congruência. Desta maneira,

$$M^{-1} = \begin{bmatrix} 18 & -9 \\ 3 & 3 \end{bmatrix} = \begin{bmatrix} 18 & 17 \\ 3 & 3 \end{bmatrix} (mod\ 26)$$

é a matriz inversa em $\mathbb{Z}_{26}$, da matriz M.

Capítulo 4

Criptografia e Aplicações

Neste capítulo serão desenvolvidas algumas atividades nas quais interligamos conteúdos matemáticos ao estudo de criptografia, mesclando esses conhecimentos a fim de tornar o ensino de matemática mais atrativo.

4.1 Atividade 1

A primeira atividade consiste em codificar uma mensagem e pode ser aplicada a qualquer série do ensino fundamental maior.

De ante mão, para o desenrolar da atividade considere a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

1. Tomando $y = 15$ vamos criptografar a seguinte frase: "CRIPTOGRAFIA TORNA A MATEMÁTICA MAIS DIVERTIDA"

   Primeiro devemos fazer a correspondência devida de cada letra da mensagem baseado na tabela apresentada. Em seguida, para o processo de codificação, basta adicionarmos a cada valor o número 15 que é a chave escolhida. Então teremos:

   Se C corresponde a 3, codificado teremos: $3 + 15 = 18$ que corresponde a letra R na nossa tabela.

   Se R corresponde a 18, codificando teremos: $18 + 15 = 33$. Como nossa correspondência está em $\mathbb{Z}_{26}$, para validar o processo vamos utilizar a congruência e aderir o resto da divisão de 33 por 26, ou seja, 7. Portanto, a G é a codificação da letra R.

Este processo deve ser feito com todas as letras e consequentemente, no final, teremos a mensagem completamente codificada.

Em termo de função teríamos, $f(x) = x + b$, onde x seria o valor correspondente a letra e b seria o valor correspondente da chave. Nesse exemplo, ficaríamos com $f(x) = x + 15$. Sendo assim:

$C \to 3$, então, $f(3) = 3 + 15 = 18 \to R$

$R \to 18$, então, $f(18) = 18 + 15 = 33$, mas $33 \equiv 7 (\text{mod } 26)$ e $7 \to G$

$I \to 9$, então, $f(9) = 9 + 15 = 24 \to X$

$\vdots$

$D \to 4$, então, $f(4) = 4 + 15 = 19 \to S$

$A \to 1$, então, $f(1) = 1 + 15 = 16 \to P$

Desta maneira, a mensagem criptografada ficaria: "RGXEIDVGPUXP IDGCP P BPITBPIXRP SXKTGIXSP"

2. Agora, sabendo que a chave de criptografia foi $b = 7$ vamos decifrar a seguinte mensagem: "HWYLUKP YHWPKV"

   Novamente, devemos fazer a correspondência devida de cada letra da mensagem baseado na tabela apresentada. Em seguida, para o processo de decodificação basta, ao invés de adicionarmos, subtrairmos 7 a cada valor do número na correspondência, ou seja, basta fazermos o processo inverso. Então teremos:

   Se H corresponde a 8, decodificado teremos: $8 - 7 = 1$ que corresponde a letra A na nossa tabela.

   Se W corresponde a 23, decodificado teremos: $23 - 7 = 16$ que corresponde a letra P na nossa tabela.

   Este processo deve ser feito com todas as letras e consequentemente, no final, teremos a mensagem completamente decodificada.

   Em termo de função teríamos, $f(x) = x - b$, onde x seria o valor correspondente a letra e b seria o valor correspondente da chave. Nesse exemplo ficaríamos com $f(x) = x - 7$. Sendo assim:

   $H \to 8$, então, $f(8) = 8 - 7 = 1 \to A$

   $W \to 23$, então, $f(23) = 23 - 7 = 16 \to P$

$\vdots$

$K \to 11$, então, $f(11) = 11 + 7 = 4 \to D$

$V \to 22$, então, $f(22) = 22 - 7 = 15 \to O$

Desta maneira, a mensagem decodificada ficaria: "APRENDI RÁPIDO"

3. Vamos agora construir um algoritmo de codificação e de decodificação, através da congruência módulo m.

   O algoritmo de codificação seria $x + b \equiv r(\text{mod } 26)$, onde x é o valor da letra correspondente na tabela, b o valor correspondente a chave de codificação e r o resto da divisão inteira de $x + b$ por 26.

   Usando o algoritmo da divisão, temos que:

   $$x + b = 26 \cdot q + r \Leftrightarrow x = 26 \cdot q + (r - b) \Leftrightarrow x - (r - b) = 26 \cdot q \Leftrightarrow x \equiv r - b(\text{mod } 26).$$

   Portanto, teríamos:

   $$x + b \equiv r(\text{mod } 26), \text{ como algoritmo de codificação}$$
   $$\text{e}$$
   $$x \equiv r - b(\text{mod } 26), \text{ como algoritmo de decodificação.}$$

   Vale ressaltar que, se aos invés de somarmos o valor de b ao valor correspondente de cada letra tentássemos multiplicar, o método não surtiria efeito, diante da justificativa de que se tomarmos $b = 0$, todos os valores encontrados seriam nulos e a mensagem não teria sentido.

4.2 Atividade 2

Uma correspondência natural entre o alfabeto $F = \{ A, B, C, ..., K, ..., X, Y, Z \}$ e o conjunto de números inteiros $\mathbb{Z}_{26} = \{ 1, 2, ..., 10, ..., 23, 24, 25, 26 \}$ é dada pela tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Considerando $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ dada por $f(x) = 2x + 1$, utilizando a tabela acima, vamos codificar a seguinte mensagem:

MESTRADO PROFISSIONALIZANTE

Para isso, calculamos $f(13) = 27$, $f(5) = 11$, . . . , $f(20) = 41$, $f(5) = 11$. Depois convertemos cada valor correspondente em seu equivalente alfabético. Quando necessário, deveremos substituir os inteiros maiores que 26 pelo resto da divisão deles por 26, utilizando a aritmética modular. Desta forma, a mensagem cifrada é

AKMOKCIE GKEMSMMSECCYSACCOK

Para decodificar a mensagem cifrada, temos que aplicar a propriedade inversa, calculando $f^{-1}(x) = \dfrac{x-1}{2}$. Tomando como base a função, teremos:

$$f^{-1}(1) = 0,\ f^{-1}(11) = 5,\ ...,\ f^{-1}(15) = 7,\ f^{-1}(11) = 5,$$

Sendo assim, ficaríamos com o seguinte texto:

"0"EFGEADB CEBFIFFIBAALI"0"AAGE

Como vocês podem notar, o processo de decodificação não surtiu o efeito desejado, já que o primeiro problema surgi com o aparecimento do zero que não possui letra para ser representado de acordo com nossa tabela. O segundo problema é que podemos encontrar uma mesma letra com significados distintos, tudo isso fez e fará com que o nosso texto fique sem nexo algum. Isto acontece porque estamos trabalhando com uma correspondência natural entre o alfabeto $F = \{\ A, B, C, ..., K, ..., X, Y, Z\ \}$ e o conjunto de números inteiros em $\mathbb{Z}_{26} = \{\ 1, 2, ..., 10, ..., 23, 24, 25, 26\ \}$. Desta forma, iremos utilizar o resultado do teorema (4.2.1) que nos ajudará a definir melhor nossa função codificadora.

Se tomarmos $a = 3$ e $b = 2$, temos que a função

$$f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \text{ dada por } f(x) = 3x + 2$$

é um cripo-sistema. Desta forma, para codificar o texto-original

MESTRADO PROFISSIONALIZANTE

primeiro calculamos $f(13) = 15$, $f(5) = 17$, . . . , $f(20) = 10$, $f(5) = 17$, logo a mensagem cifrada é

OQGJDENUXDU TCGGCURELCBERJQ

Para decodificar a mensagem cifrada, temos que aplicar a propriedade inversa, lembrando que a inversa também tem que está em $\mathbb{Z}_{26}$. Para isso, calculamos $f^{-1}(x) = a'x + b'$, onde $a \cdot a' = 1$ e $b' = -a'b$. Neste caso $a' = 9$, pois $9 \cdot 3 \equiv 1 (\text{mod } 26)$ e $b' = 8$, pois $b' = -9 \cdot 2 = -18 \equiv 8 (\text{mod } 26)$. Tomando como base a função $f^{-1}(x) = 9x + 8$, teremos:

$$f^{-1}(15) = 13, f^{-1}(17) = 5, \cdots, f^{-1}(10) = 20, f^{-1}(17) = 5,$$

voltando assim para mensagem original.

MESTRADO PROFISSIONALIZANTE

4.3 Atividade 3

Vamos a mais uma aplicação, desta vez usando o conteúdo de matrizes.

Consideremos a tabela abaixo e vamos aos procedimentos básicos para codificar e decodificar a seguinte mensagem: "O TEMPO É REI".

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

CODIFICAÇÃO

1. Escolhemos uma matriz quadrada que será nossa chave, e esta, tem por obrigação ser invertível em $\mathbb{Z}_{26}$. Tomemos

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

2. Agrupamos letras sucessivas do texto que será cifrado em pares, caso o mesmo tenha um número ímpar de letras, adicionamos uma letra fictícia para completar o último par. Em seguida, trocamos cada letra pelo seu valor numérico correspondente na tabela.

OT - EM - PO - ER - EI
1520 - 513 - 1615 - 518 - 59

3. Feito isso, converteremos cada par de letras em vetor coluna e efetuaremos o produto da matriz chave com a matriz referente a mensagem inicial. Obtendo assim, $C = A \cdot B$, onde C será a matriz codificada.

$$C = \begin{bmatrix} 5 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 15 & 5 & 16 & 5 & 5 \\ 20 & 13 & 15 & 18 & 9 \end{bmatrix} = \begin{bmatrix} 115 & 51 & 110 & 61 & 43 \\ 35 & 18 & 31 & 23 & 14 \end{bmatrix}$$

4. Agora convertemos cada valor correspondente em seu equivalente alfabético. Quando necessário, deveremos substituir os inteiros maiores que 26 pelo resto da divisão deles por 26, utilizando assim a aritmética modular.

$$C = \begin{bmatrix} 115 & 51 & 110 & 61 & 43 \\ 35 & 18 & 31 & 23 & 14 \end{bmatrix} = \begin{bmatrix} 11 & 25 & 6 & 9 & 17 \\ 9 & 18 & 5 & 23 & 14 \end{bmatrix} \pmod{26}$$

Logo,a mensagem codificada fica da seguinte maneira:

"K IYRFE I WQN"

DECODIFICAÇÃO

Para decifrar aplicamos a operação inversa. Se para cifrarmos uma mensagem efetuamos o produto $C = A \times B$, para decifrar basta multiplicarmos, à esquerda dessa equação, a matriz inversa da matriz de cifragem, ou seja, $A^{-1} \times C = A^{-1} \times A \times B$, obtendo assim, $B = A^{-1} \times C$.

Vale ressaltar que para garantir a existência da inversa da matriz A precisamos da definição (3.9.2), logo, como nossa matriz chave é dada por:

$$\begin{bmatrix} 5 & 2 \\ 1 & 1 \end{bmatrix}$$

Temos que, $detA = 3 \neq 0$ e o $mdc(3, 26) = 1$ o que garante a inversa da matriz A em $\mathbb{Z}_{26}$.

A mensagem decodificada é dada por $B = A^{-1} \times C$. Vamos ver passo a passo o procedimento para a decodificação da mensagem: "K WYRFI I GQE"

1. Como o determinante da matriz A é igual a 3, temos que seu inverso multiplicativo em $\mathbb{Z}_{26}$ é igual a 9, já que é o número que multiplicado por 3 deixa resto 1 quando dividido por 26, isso nada mais é que a solução da seguinte congruência, $3X \equiv 1 (\text{mod } 26)$.

2. Agora devemos encontrar a matriz transposta da matriz dos cofatores, indicada por $\overline{A}$, e, em seguida, multiplicar por 9, obtendo assim A^{-1}.

$$A^{-1} = \frac{1}{detA} \cdot \overline{A} = 9 \cdot \begin{bmatrix} 1 & -2 \\ -1 & 5 \end{bmatrix} = \begin{bmatrix} 9 & -18 \\ -9 & 45 \end{bmatrix}$$

3. Em seguida, devemos converter cada a_{ij} da matriz A^{-1} em termos pertencentes a $\mathbb{Z}_{26}$, usando assim as técnicas de congruência. Desta maneira,

$$A^{-1} = \begin{bmatrix} 9 & -18 \\ -9 & 45 \end{bmatrix} = \begin{bmatrix} 9 & 8 \\ 17 & 19 \end{bmatrix} (\text{mod } 26)$$

4. Encontrada a matriz inversa em $\mathbb{Z}_{26}$, para decodificar a mensagem (para encontramos B) basta calcularmos o produto de A^{-1} com a matriz codificada, indicada por C, ou seja, $B = A^{-1} \times C$.

$$B = \begin{bmatrix} 9 & 8 \\ 17 & 19 \end{bmatrix} \cdot \begin{bmatrix} 11 & 25 & 6 & 9 & 17 \\ 9 & 18 & 5 & 23 & 14 \end{bmatrix} = \begin{bmatrix} 171 & 369 & 94 & 265 & 265 \\ 358 & 767 & 197 & 590 & 555 \end{bmatrix}$$

5. Para finalizar, convertemos cada valor correspondente em seu equivalente alfabético. Quando necessário, deveremos substituir os inteiros maiores que 26 pelo resto da divisão deles por 26, utilizando mais uma vez a aritmética modular.

$$C = \begin{bmatrix} 171 & 369 & 94 & 265 & 265 \\ 358 & 767 & 197 & 590 & 555 \end{bmatrix} = \begin{bmatrix} 15 & 5 & 16 & 5 & 5 \\ 20 & 13 & 15 & 18 & 9 \end{bmatrix} (\text{mod } 26)$$

Obtendo assim a mensagem inicial: "O TEMPO É REI".

Capítulo 5

Experiência em Sala de Aula

Algumas das atividades e o questionário apontado foram aplicados no Colégio Estadual Prefeito Eduardo Marques de Oliveira, que está situado no município de Pião - Se. As turmas envolvidas foram 7º ano do ensino fundamental, 2º e 3º ano do ensino médio no período da manhã. Esses alunos estão numa faixa etária de 11 aos 18 anos, sendo que a maioria é do sexo feminino e não são alunos repetentes.

Através de observações, foi possível verificar que esses alunos têm perfis diferenciados nas aulas, por exemplo, na maioria das aulas de matemática eles participam questionando o professor para retirarem suas dúvidas e se concentram na explicação dada pelo mesmo. No entanto, em algumas disciplinas, eles conversam o tempo inteiro sobre assuntos alheios, brigam com os colegas, ouvem músicas no celular com o fone de ouvido, enfim, muita desconcentração.

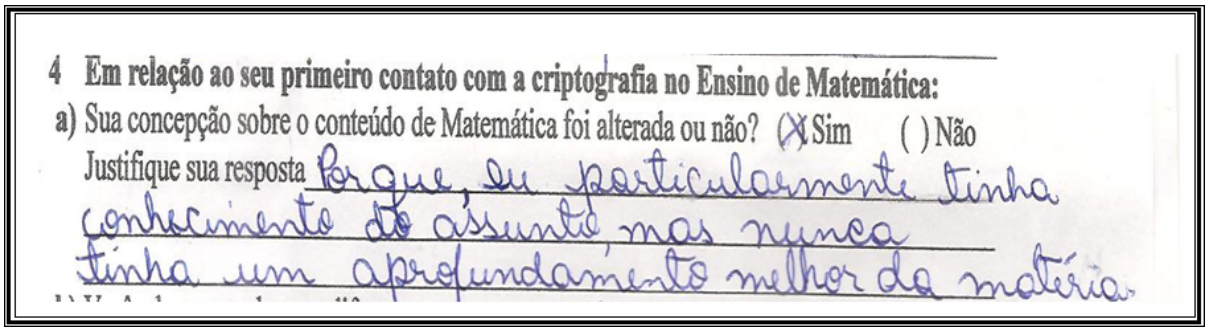
Mas, em geral, os alunos são participativos, trabalham junto com o professor, questionam o porquê das coisas e fazem comentários sobre o assunto abordado. Nas aulas de matemática, a maioria desses comentários são críticos, do tipo: "Não sei pra que estudar isso, não serve pra nada mesmo", "Só tem coisa difícil em matemática". Estes comentários surgem na medida em que o aluno encontra uma dificuldade quando estão resolvendo uma determinada atividade. A dificuldade em interpretar o problema, a "mania"de resolvê-lo mecanicamente e a falta de conhecimentos prévios do aluno são fatores que podem contribuir para formar uma má visão dos alunos em relação ao ensino da matemática.

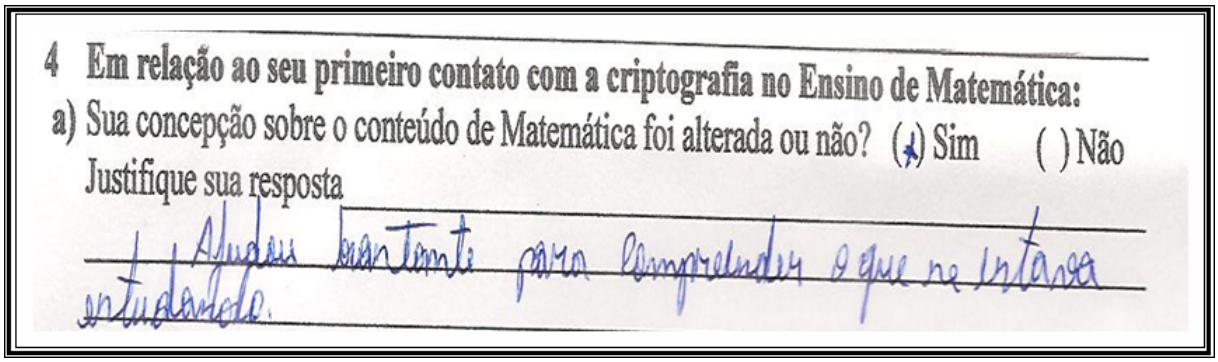
Um fator positivo que deve ser considerado é o respeito que boa parte dos alunos têm pelos professores, e, além disso, eles demonstram gostar bastante do professor de Matemática pela afetividade expressada ao vê-lo, pela companheirismo e a boa relação professor-aluno.

O professor titular, Samuel Brito, possui curso superior de Matemática-Licenciatura e Mestrado também em Matemática. O professor tem domínio de conteúdo, avalia os alunos através de participação, atividades em grupo, listas de exercícios e provas escritas, tudo isso enfrentando dificuldades como o grande número de alunos nas turmas e o desinteresse de alguns. Procura sempre escutar a classe e seu objetivo principal é fazer com que eles assimilem o máximo de conhecimento transmitido durante o ano letivo e que tenham um bom desempenho.

Diante da análise dos questionários e do desenvolver das atividades foi possível perceber que alguns alunos admitem possuir dificuldade com a disciplina e, segundo os mesmos, isso está intimamente ligado ao fato de que se dedicam pouco, não tem noções básicas e não conseguem enxergar a ligação entre o conteúdo e a prática.

Vale salientar que o tema "criptografia"foi novo para esses alunos, instigante e um belo atrativo para desenrolar as atividades.


4 Em relação ao seu primeiro contato com a criptografia no Ensino de Matemática:
a) Sua concepção sobre o conteúdo de Matemática foi alterada ou não? (X) Sim ( ) Não
Justifique sua resposta Porque, eu particularmente tinha conhecimento do assunto mas nunca tinha um aprofundamento melhor da matéria.

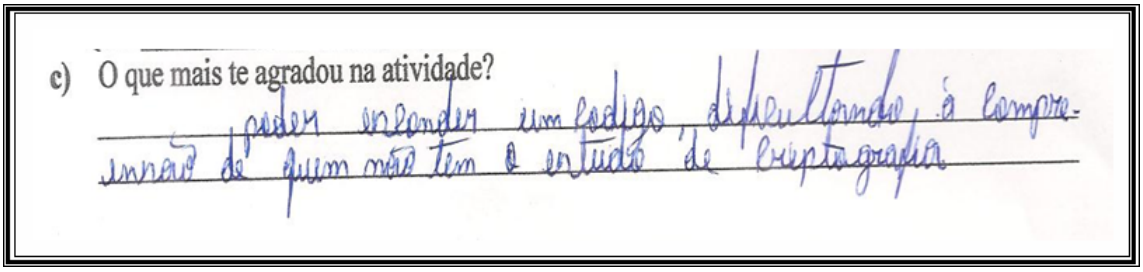

4 Em relação ao seu primeiro contato com a criptografia no Ensino de Matemática:
a) Sua concepção sobre o conteúdo de Matemática foi alterada ou não? (X) Sim ( ) Não
Justifique sua resposta Ajudou bastante para compreender o que se estava estudando.

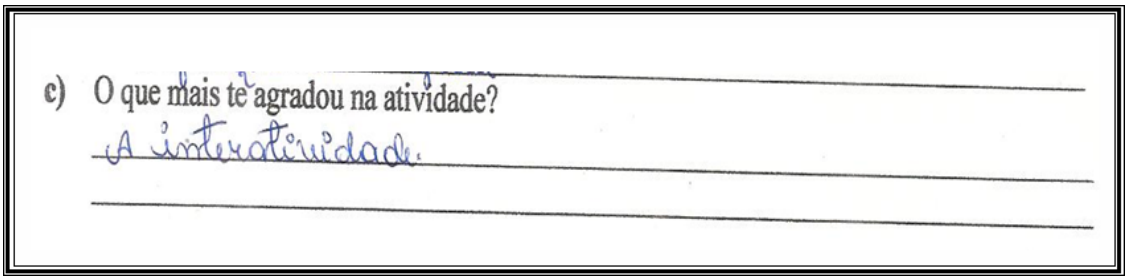
Em todas as turmas, expus aos alunos de forma intuitiva e sucinta, o uso de congruência, pois do contrário a atividade não teria sentido. Como a ideia de congruência está intimamente ligada à divisibilidade a assimilação, pela maioria dos alunos, foi rápida e produtiva.

Na atividade proposta no anexo 1, relacionada à divisibilidade e desenvolvida com os alunos do ensino fundamental, houve um desempenho surpreendente. Os alunos fizeram a correspondência numérica com facilidade e a transposição dos resultados para o módulo 26 não apresentou grave dificuldade, a menos com erros básicos de cálculos, devido a falta de domínio da tabuada e descuido na hora de efetuar a subtração de alguns números. A motivação e a curiosidade eram nítidas.

Na atividade proposta no anexo 3, relacionada a funções afins, houve alguns imprevistos. O primeiro deles foi com relação ao tempo, já que havia planejado desenvolver toda atividade em 2 h/a, o que não foi suficiente e o segundo foi a falta do conhecimento prévio já que nenhum deles lembravam como encontrar a inversa de uma função. Depois de relembrar alguns conteúdos e de ensiná-los como encontrar a inversa de uma função em $\mathbb{Z}_{26}$ a atividade foi concluída, unanimemente, com sucesso.

É importante frisar, que mesmo em meio às dificuldades, mesmo a tarefa sendo extensa (algo que eles reclamaram) a atividade agradou boa parte dos alunos. A ideia de dificultar a compreensão do outro, o fato de camuflar recados, a criptografia em si, excitou o desejo de realizar a atividade por completo, como é possível observar nas figuras:





A atividade proposta no anexo 4, relacionada a matrizes, também surtiu o efeito desejado. Antes de começar a desenvolvê-la foi preciso revisar o conteúdo de matrizes e explicar a classe como encontrar a inversa de uma determinada matriz em $\mathbb{Z}_{26}$,já que este tópico não é algo comum na grade curricular dos alunos.

Feita a revisão a dúvida em proeminência foi quanto a maneira de organizar a matriz, pois mesmo frisando que deveria ser do tipo A_{2xn}, eles não sabiam se deveriam disseminar no sentido horizontal ou vertical, mas depois do esclarecimento a tarefa transcorreu tranquilamente. Um dos alunos enfatizou para toda classe o fato da matriz chave ter seu determinante diferente de zero, pois do contrário a matriz não teria inversa o que me deixou radiante.

Falhas de cálculos foram frequentes em todas as atividades, mas o legal de tudo isso era que os próprios alunos percebiam seus erros, visto que no final de toda a atividade a palavra ou frase não estava fazendo sentido. Daí, eles refaziam as contas e no final da atividade ficavam surpresos e encantados com o resultado.

Diante de que foi proposto e da momentânea experiência em sala de aula, pude perceber que no decorrer desse período alguns pontos positivos e negativos se fizeram presentes.

Dentre os pontos positivos, podemos destacar a satisfação de alunos e do professor durante a execução das atividades. Além disso, os resultados obtidos foram proveitosos e atingiu a expectativa, que era trabalhar conhecimentos de forma dinâmica e atrativa. Além disso, é interessante destacar a relevância das pesquisas, das leituras e dos conhecimentos básicos tanto minha, quanto dos alunos, pois a troca de informações e experiências

é bastante significativa.

Em relação aos pontos negativos, lamenta-se o curto espaço de tempo, a dificuldade e a ausência de conhecimentos prévios necessários para conclusão com êxito de todas as atividades, o que pode ser revisto e reorganizado pelo professor titular da turma.

Torna-se evidente o otimismo e o entusiasmo do professor ao aplicar a atividade aos alunos e perceber o reconhecimento destes em relação ao trabalho.

Anexo 1: Sugestão de Atividade

O nosso cérebro é doido!!! De aorcdo com uma peqsiusade uma uinrvesriddae ignlsea, não ipomtra em qaul odrem as Lteras de uma plravaa etãso, a úncia csioa iprotmatne é que a piremria e útmlia lteras etejasm no lgaur crteo. O rseto pdoe ser uma bçguana ttaol, que vcoê anida pdoe ler sem pobrlmea. Itso é poqrue nós não lmeos cdaa ltera isladoa, mas a plravaa cmoo um tdoo. Sohw de bloa! Fixe seus olhos no texto abaixo e deixe que a sua mente leia corretamente o que está escrito:
35T3 P3QU3N0 T3XTO 53RV3 4P3N45 P4R4 M05TR4R COMO NO554 C4B3Ç4 CONS3GU3 F4Z3R CO1545 1MPR3551ON4ANT35! R3P4R3 N155O! NO COM3ÇO 35T4V4 M310 COMPL1C4DO, M45 N3ST4 L1NH4 SU4 M3NT3 V41 D3C1FR4NDO O CÓD1GO QU453 4UTOM4T1C4M3NT3, S3M PR3C1S4R P3N54R MU1TO, C3RTO? POD3 F1C4R B3M ORGULHO5O D155O! SU4 C4P4C1D4D3 M3R3C3! N0550 CR14DOR M3R3C3 P4R4BÉN5!

Em criptografia, a Cifra de César, também conhecida como cifra de troca, 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, que se apresenta no alfabeto abaixo dela um número fixo de vezes.
Exemplo: Deslocando 3 vezes cada letra do alfabeto teremos:
∗Texto Normal: AULA DE MATEMÁTICA
∗Texto Cifrado: DXOD GH PDWHPDWLFD

Para tornarmos o método um pouco mais seguro vamos escolher um valor fixo, $y \in \mathbb{Z}$(caso a atividade seja desenvolvida com alunos do 6º ano o professor deve orientar os alunos a escolherem $y \in \mathbb{N}$), tal que, para criptografarmos uma mensagem devemos somar o valor correspondente da letra do alfabeto a esse valor fixo, o novo número representará a letra criptografada. Caso o valor seja superior aos valores da tabela o aluno deverá pegar o resto da divisão desse número por 26, quantidade total de letras do nosso alfabeto.
Para o desenrolar da atividade considere a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

1. Tomando $y = 13$ criptografe a seguinte frase: "MATEMÁTICA E SUAS APLICAÇÕES"

2. Agora use $b = 22$ e codifique a PALAVRA: "POSITIVIDADE"

3. Sabendo que a chave de criptografia foi $b = 7$, decifre a seguinte mensagem: "HWY-LUKP YHWPKV"

4. Se ao invés de somarmos o valor de b ao valor correspondente de cada letra tentássemos multiplicar o método surtiria efeito? Faça o teste e verifique!

Anexo 2: Sugestão de Atividade

Essa é uma atividade de divisibilidade e congruência que envolve também o conteúdo de potência.

A atividade consiste na troca de informações entre duplas de alunos em sala de aula, utilizando o método de Diffiel-Hellman. A função que deverá ser utilizada é do tipo: $m^x(modn)$, onde m é considerada base, n o módulo e x o expoente secreto.
1ºPasso: O professor deverá dividir a turma em duplas;
2º Passo: As duplas, com a ajuda do professor, caso necessitem, deverão escolher dois números, um para a base e outro para o módulo, tais que:
A base m precisa ser maior que 1 e menor que o módulo n. O módulo n e $(n-1)/2$ tem que ser números prímos e m dever ser raiz primitiva do módulo n;
Obs.1: O m deve ser analisado pelo professor, já que os alunos da série indicada não tem o conhecimento do que seja raiz primitiva.
3º Passo: Cada integrante da dupla deve escolher um expoente que deverá ser mantido cuidadosamente em segredo;
4º Passo: Feito a escolha dos seus expoentes cada integrante da dupla deverá calcular o resultado da função aplicando, é claro, o expoente escolhido;
5º Passo: Os integrantes da dupla deverão fazer a troca de resultados obtidos;
6º Passo: De ante do resultado repassado pelo colega, cada um deles deverá aplicá-lo na mesma função, só que desta vez a base será o número enviado pelo colega e o expoente continua sendo o número secreto escolhido pelos mesmos;
7º Passo: O resultado obtido pela dupla será absolutamente igual, e este número indica a chave secreta em comum que será usada para criptografar e descriptografar a mensagem.
Após todo o procedimento, cada integrante da dupla deverá criptografar uma mensagem e entregar para seu parceiro que, em seguida, terá que descriptografar e enviar a mesma ao professor.
Obs.2: Tendo em mãos a chave secreta, a cifragem da mensagem se dá pelo deslocamento da letra escolhida y vezes para direita, onde y é o valor da chave secreta.
Obs.3: Caso o deslocamento extrapole o número 26 o aluno deverá aplicar a divisibilidade do mesmo por 26 e considerar o resto da divisão.
Obs.4: Para descriptografar o processo é o inverso da criptografia.

Tome como fundamento a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Anexo 3: Sugestão de Atividade

Você já deve ter ouvido ou lido a palavra empreendedor. É sinônimo de sujeito ativo, arrojado, que se propõe a fazer alguma coisa...e faz mesmo! Não por acaso é uma das palavras mais usadas no meio empresarial, quase sempre ligada a um comerciante de sucesso. Num país de dificuldades econômicas como o Brasil, empreendedores bem sucedidos são alvo de grande admiração. "Como eles conseguiram?", todo mundo se pergunta, enquanto surgem milhares de receitas para explicar o sucesso. Paula é uma grande empreendedora de sucesso e numa determinada entrevista no jornal local assume que não existem receitas prontas, existem sim, algumas qualidades destaques nos empreendedores, tais como:

Criatividade e 78-23-88-93-43-93-98-23-68-13-43-3

Considere a função $C(x) = 5x - 2$ e a seguinte tabela, onde cada letra do alfabeto corresponde a um valor fixo.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

1. Com base na função e na tabela acima, cifre a primeira qualidade citada por Paula que é comum a um empreendedor de sucesso.

2. Como vocês já devem ter notado, uma das qualidades citada está criptografada. Decifre o código para sabermos qual a segunda característica dada por Paula.

3. Determine a função utilizada para a decifração da qualidade acima, o seu domínio e a sua imagem.

Anexo 4: Sugestão de Atividade

Matrizes são utilizadas em diversos áreas como na informática, economia, engenharia, física, entre outras. Com a criptografia não é diferente, utilizamos diversos métodos para transformar dados normais em textos cifrados e as matrizes nesse caso são bastante úteis.

Podemos empregar álgebra linear, mais especificamente matriz a fim de criarmos um sistema de criptografia. O método envolve duas matizes, uma para criptografar e uma para descriptografar, vamos a prática!

Associe cada letra do alfabeto aos números de acordo com a tabela abaixo e utilize como base para a resolução das questões atribuídas.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

1. Criptografe a frase "Sou estudante". Para isso, considere $C = A \cdot B$, onde C é a matriz criptografada, A é a matriz chave, dada por

$$A = \begin{bmatrix} 7 & 1 \\ 2 & 1 \end{bmatrix}$$

   e B é a matriz da mensagem que será criptografada que deve ser escrita da forma $B_{2\times n}$.

2. Amanda está super nervosa com que acabou de descobrir e precisa, urgentemente, contar a alguém que não seja seus pais. Ontem a noite, durante o jantar, estavam presentes seus pais, seu irmão e sua melhor amiga e eufórica ela grita em voz alta.

   2 - 3 - 25 - 3 - 24 - 23 - 22 - 11 - 7 - 1 - 3 - 9

   Utilizando a mesma chave da questão anterior, decifre a mensagem. Qual a técnica utilizada?

Anexo 5: Questionário Aplicado aos Alunos

PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

Estou realizando uma avaliação sobre o uso de Criptografia na Educação Básica. Sua opinião é muito importante, pois por meio desta formularei conclusões sobre a aplicação deste tema em sala de aula. Desde já agradeço sua colaboração e estou à disposição para esclarecimento.

Att.: Dayane Silva

1. Dados de identificação

Nome completo:
Sexo: ( )Masculino ( )Feminino
Idade:
Cidade que reside:
Série:

2. Aspectos relativos à formação

2.1 Ensino fundamental

( ) Pública ( ) Particular

1ª Instituição:
2ª Instituição:
3ª Instituição:

2.2 Ensino Médio

( ) Pública ( ) Particular

1ª Instituição:
2ª Instituição:
3ª Instituição:

3. Aspectos relativos a disciplina matemática

a) Você acha que os alunos realmente tem dificuldade em Matemática ou trata-se de algum tipo de pré-conceito existente?

( ) Sim, os alunos tem dificuldades
( ) Não, trata-se de um pré-conceito existente

b) Porque os alunos apresentam dificuldade na disciplina de Matemática?(pode assinalar mais de um item)

( ) Estudam pouco
( ) Tem pré-conceito com o professor
( ) Tem pré-conceito com a disciplina
( ) Não tem noções básicas(raciocínio lógico matemática,...
( ) Não conseguem fazer a ligação entre o conteúdo e a prática
( ) Não consideram importante a disciplina
( ) Os professores avaliam baseado no resultado e não no processo, causando medo da avaliação e preconceito com a disciplina.
( ) Os professores não tem conhecimento suficiente.
( ) Outro. Qual?

4. Aspectos relativos a alguns conteúdos matemáticos abordados

a) Você teve contato com o conceito de funções no ensino médio?( ) Sim ou ( ) Não.

Se sim, em que(quais) série(s)?

Que tipo de função(funções) foi(foram) trabalhado(s)? (marque todas as que foram)
( ) Função afim
( ) Função quadrática
( ) Função modular
( ) Função exponencial
( ) Função logarítmica
( ) Função trigonométrica
( ) Função polinomial
Como foram trabalhadas?

( ) Muito bem ( ) Pouco ( ) Não lembra

Justifique sua resposta

b) Você teve contato com o conceito de matrizes no ensino médio? ( ) Sim ( ) Não.

Se sim, em que(quais) série(s)?

Que tipo de matriz(matrizes) foi(foram) trabalhado(s)? (marque todas as que foram)
( ) Matriz transposta ( ) Adição e subtração de matriz
( ) Multiplicação de matriz
( ) Matriz oposta
( ) Matriz identidade
( ) Matriz inversa
( ) Igualdade de matriz
Como foram trabalhadas?

( ) Muito bem ( ) Pouco ( ) Não lembra

Justifique sua resposta

5. Em relação ao seu primeiro contato com a criptografia no Ensino de Matemática

a) Sua concepção sobre o conteúdo de Matemática foi alterada ou não? ( ) Sim ( ) Não.

Justifique sua resposta

b) Você observou alguma diferença entre os conteúdos que eram trabalhados quando você estudou Matemática e agora quando você interliga o mesmo conteúdo a outro tema?( ) Não ( ) Sim. Quais?

6. Em relação a atividade aplicada envolvendo matemática e criptografia

a) A atividade foi... (pode marcar mais de uma alternativa)
( ) Produtiva e motivadora
( ) Interessante
( ) Pouco produtiva e desmotivadora
( ) Interessante porém cansativa
( ) Difícil e desinteressante
( ) Outra resposta

b) Você sentiu dificuldade em desenvolver a atividade por não ter visto um determinado conteúdo específico? ( ) Sim ( ) Não. Qual?

c) O que mais te agradou na atividade?

Considerações Finais

O conceito de criptografia tem sua origem desde os tempos remotos da civilização. A necessidade de se esconder mensagens foi algo muito importante para segurança de estados e nações. Com o passar do tempo foi se sofisticando e formalizando com um campo de estudos da matemática ganhando grande destaque na II Guerra Mundial e, mais recentemente, na segurança na transmissão de mensagens via internet.

Neste contexto, este trabalho foi criado com propósito de acentuar conceitos da disciplina matemática na educação básica através do paralelo com o conceito de criptografia. Diante disso, foram apresentados definições, exemplificações, sugestões e resultados que desencadearam a abordagem do mesmo.

Conteúdos como divisibilidade, funções, matrizes são de suma importância na vida acadêmica dos nossos alunos, visto que, são usados como ferramentas capazes de ajudar a detectar e solucionar problemas do mundo real. Então, nada melhor que tentar estreitar a afinidade entre o aprender e o querer, isso de forma pacífica, participativa e construtiva.

Acredito que este trabalho possa contribuir para o ensino aprendizagem, tanto dos nossos alunos, quanto dos professores que resolverem seguir essa linha de indicação. Podendo a cada experiência incrementar e melhorar.

Vale ressaltar que devemos inserir com mais afinco o uso de assuntos ligados à realidade do aluno, que despertem o empenho dos mesmos nas salas de aulas para contribuir de forma mais atrativa no aprendizado do discente com objetivo de aperfeiçoar seu raciocínio, considerando suas ideias e pensamentos. E o mais importante, continuar buscando aprimoramento.

Referências

LIMA, Elon Lages. et al. A Matemática do Ensino Médio. Volume 1 - 9ª ed. Rio de Janeiro, RJ: Sociedade Brasileira de Matemática, 1997. (Coleção do Professor de Matemática).

LIMA, Elon Lages. et al. A Matemática do Ensino Médio. Volume 3 - 6ª ed. Rio de Janeiro, RJ: Sociedade Brasileira de Matemática, 1998. (Coleção do Professor de Matemática).

PAIVA, Manoel. Matemática Paiva. Volume 1. 2ª ed. São Paulo, SP: Moderna, 2013.

PAIVA, Manoel. Matemática Paiva. Volume 2. 2ª ed. São Paulo, SP: Moderna, 2013.

FONSECA, Rubens Vilhena. Teoria dos Números. Belém: UEPA / Centro de Ciências Sociais e Educação. 2011.

LEMOS, Manoel. Criptografia, Números Primos e Algoritmos. 4ª ed. Universidade Federal de Pernambuco - UFPB. Pernambuco: IMPA. 2010.

ANDRADE, A. Números, Relações e Criptografia. UFPB. Paraíba. 2010.

TOMAROZZI, A. C. Codificando e Decifrando Mensagens. Revista do professor de Matemática. Volumes 45. Sociedade Brasileira de Matemática.

FIARRESGA, Victor Manuel Calhabrês. Criptografia e Matemática. 2010. 161 p. Universidade de Lisboa - Faculdade de Ciências, Lisboa, 2010.
Disponível em:
< http://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf >. Acesso em 29/01/2015.

MATTOS, Sergio Ricardo Pereira. Aritmética modular na formação continuada de professores: desenvolvendo o pensamento aritmético e algébrico. 2011. 154p. Universidade do Grande Rio - UNIGRANRIO, Duque de Caxias, Rio de Janeiro, 2011.
Disponível em:
< http://tede.unigranrio.edu.br/tde_busca/arquivo.php?codArquivo=100 >. Acesso em 18/02/2015.

NETO, Luiz Alves de Souza. Aritmética Modular e Criptografia no Ensino Básico. 2014. 60 p. Universidade Federal do Maranhão - UFMA, São Luiz, Maranhão, 2014.
Disponível em:
< http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/1502/2012_01309_LUIZ_ALVES_DE_SOUZA_NETO.pdf-sequence=1 >. Acesso em: 18/02/2015.

SANTOS, José Luiz. A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fon-

tes Motivadoras para Atividades de Matemática Básica. 2013. 81 p. Universidade Federal da Bahia - UFBA, Salvador, Bahia, 2013.
Disponível em:
< `http://bit.profmat-bm.org.br/xmlui/bitstream/handle/123456789/208/2011_00046_JOSE_LUIZ_DOS_SANTOS.pdf-sequence=1` >. Acesso em: 02/03/2015.