UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Marco Antônio Lopes

Introdução à criptografia usando aritmética modular

São José do Rio Preto

2017

Marco Antônio Lopes

Introdução à criptografia usando aritmética modular

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

Orientador: Prof. Dr. Jéfferson Luiz Rocha Bastos

São José do Rio Preto

2017

Lopes, Marco Antônio.
Introdução à criptografia usando aritmética modular / Marco Antônio Lopes . -- São José do Rio Preto, 2017
56 f. : il.

Orientador: Jéfferson Luiz Rocha Bastos
Dissertação (mestrado profissional) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas

1. Matemática - Estudo e ensino. 2. Criptografia. 3. Funções (Matemática) 4. Aritmética. 5. Internet – Sistemas de segurança. I. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. II. Título.

CDU – 51(07)

Ficha catalográfica elaborada pela Biblioteca do IBILCE
UNESP - Câmpus de São José do Rio Preto

Marco Antônio Lopes

Introdução à criptografia usando aritmética modular

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

Comissão Examinadora

Prof. Dr. Jéfferson Luiz Rocha Bastos
UNESP - São José do Rio Preto/SP
Orientador

Prof. Dr. Marcus Augusto Bronzi
UFU - Uberlândia/MG

Profª. Drª. Michelle Ferreira Zanchetta Morgado
UNESP - São José do Rio Preto/SP

São José do Rio Preto

2017

Agradecimentos

Agradeço inicialmente a Deus pela saúde, força e inspiração que me fizeram superar as dificuldades surgidas nesta jornada.

Agradeço ao Professor Dr. Jéfferson Luiz Rocha Bastos pela serenidade com que me orientou e compartilhou comigo um pouco de sua sabedoria e, em nome do qual, também agradeço a todos os professores do Profmat.

Agradeço aos amigos do Profmat, companheiros dessa caminhada que, apesar de árdua, trouxe momentos de descontração e colaboração, necessários para vencermos os obstáculos à medida em que surgiam. Ao Anderson, companheiro de viagem.

Agradeço aos amigos que, direta ou indiretamente, contribuíram para que eu pudesse alcançar meu objetivo. Em particular à Profa. Ma. Flávia Rossi Rezende Albino pela revisão ortográfica.

E em especial, agradeço às minhas filhas e minha esposa Ana, pelo carinho, compreensão pelas horas dedicadas na execução do presente trabalho, pela paciência e auxílio prestados. O carinho de vocês foi muito importante

À CAPES, pelo apoio financeiro.

Resumo

A troca de informações confidenciais sempre foi um problema que nos desafiou. O conhecimento de técnicas que visam ocultar uma mensagem data de alguns séculos a.C., tais como, a esteganografia e a criptografia. A esteganografia consiste na técnica de ocultar a mensagem que será enviada sem, no entanto, esconder seu significado. Já a criptografia consiste na técnica de ocultar o significado da mensagem através de sua codificação, que pode ser feita de várias maneiras, e cujo conteúdo só pode ser decodificado pelo destinatário, que tem a chave de decodificação. Essas técnicas evoluíram com o tempo, principalmente a criptografia, por ter uma natureza mais complexa na decodificação e que, por isso mesmo, torna-se mais adequada atualmente. Isso porque, com o desenvolvimento de novas tecnologias de comunicação, garantir a segurança das informações tornou-se uma preocupação maior do que já era. Nesse sentido, destacamos a internet, que, além de exigir segurança, é compartilhada pela grande maioria de nossos alunos. Como a segurança da internet faz uso da criptografia, e como esta está associada a modelos matemáticos, podemos então explorar o uso desta, em sala de aula, a fim de despertar no aluno, além de sua curiosidade, seu interesse por temas, muitas vezes de difícil compreensão, dada a maturidade dos mesmos para enfrentá-los. Teorias como funções e suas funções inversas, aritmética das classes residuais, etc., podem ser trabalhados em sala de aula usando o Código de Caesar e permite ao professor lidar de forma mais didática as diferenças existentes em sala de aula.

Palavras-chave: Criptografia. Função. Função Inversa. Classes Residuais.

Abstract

The exchange of confidential information has always been a problem that challenged us. The techniques knowledge that aimed to concealing a message dates back to some centuries BC, such as steganography and cryptography Steganography consists on the technique of hiding the message that will be sent however, without, hide its meaning. However, encryption is the technique of hide the meaning of the message through its coding, which can be done in several ways, whose content can only be decoded by the recipient, who has the decryption key. These techniques have evolved over time, especially cryptography, because it has a more complex decoding nature and, therefore, it is more suitable today. That's because, with the development of new communication technologies, guarantee information security has become a greater concern than it used to be. On this side, we highlight the internet, which, in addition to requiring security, it's shared by the vast majority of our students. As Internet security uses the encryption, and it's associated with mathematical models, we can explore the use of encryption in classroom in order to arouse the student's curiosity, his interest in subjects, often difficult to understand, given their maturity to face them. Theories as functions and their inverse functions, arithmetic of the residual classes, etc., can be worked in classroom using the Caesar Code, and it allows the teacher to deal in a didactic way with the differences existing in the classroom.

Keywords: Cryptography. Function. Reverse function. Residual classes.

Sumário

Introdução

O perfil do aluno da Educação Básica no Brasil mudou consideravelmente nos últimos tempos. Um dos fatores que contribuiu para isso foi a mudança na legislação da Educação Básica, que deu ao aluno mais facilidade para alçar séries superiores, outro, foi o desenvolvimento da tecnologia permitindo obter informações em tempo real.

Em contrapartida, por mais que se tente modificar a maneira de abordar determinados assuntos em sala de aula, o professor acaba por cair na educação tradicional e, por isso mesmo, a maioria das matérias trabalhadas numa aula acabam por ficar desinteressante para o aluno.

Vencer a barreira do desinteresse do aluno durante as aulas fazendo que o mesmo interaja de maneira produtiva, isto é, de forma que o processo ensino-aprendizagem dê resultados no mínimo satisfatórios, é um desafio para aqueles que se propõem a enfrentar uma sala de aula.

A criptografia já é conhecida desde a antiguidade e sofreu ao longo dos anos uma evolução considerável devido à ação dos criptoanalistas. Essa evolução passa a exigir um processo mais científico em detrimento dos métodos empíricos usados em sua fase inicial.

E é aí que se encontra a vantagem de levar a criptografia para a sala de aula uma vez que, os métodos iniciais tais como o Código de Caesar ou Cítala espartana, são métodos que permitem ao professor trabalhar os conceitos de forma mais simples para, depois, ir aprofundando nos conceitos à medida em que o aluno passe a dominar os temas discutidos na aula.

Outro fato importante, é que os métodos utilizados na criptografia atualmente exigem conceitos matemáticos mais avançados e, por isso mesmo, permitem ao

professor discutir com alunos que gostam de um desafio, tais conceitos, pois exigem um maior domínio da matéria, além da paixão pela matemática.

A matemática encontrada na criptografia torna certos assuntos fascinantes, pois permite ao aluno conciliar o tema da aula ao seu dia a dia, uma vez que este usa a internet a todo momento. Temas como funções, aritmética modular, matrizes, geometria, dentre outros, podem ser encontrados nos modelos criptográficos usados atualmente.

Logo, a criptografia é um tema apaixonante e que pode fazer com que o aluno se interesse por temas tais que talvez passasse desapercebidos durante as aulas. Cabe ao professor aprender a utilizá-lo de maneira mais efetiva durante suas aulas.

Capítulo 1

Criptografia, um pouco de história

Criptografia é *a arte de esconder o significado de uma mensagens através dos números.*

Este trabalho pretende abordar, de forma sucinta, alguns momentos do desenvolvimento da criptografia no decorrer do tempo.

O significado da palavra Criptografia em grego é *kryptós,* "escondido, oculto", e *gráphein,* "escrita" e pode ser entendida como o estudo de técnicas ou métodos, através dos quais a informação original pode ser modificada de tal forma a tornar-se ilegível a qualquer outro que não seja seu destinatário (ou alguém autorizado), uma vez que somente este detém a "chave de decodificação".

A preocupação em transmitir secretamente informações importantes não é recente e ao longo da história da humanidade muitos meios já foram buscados, tais como, a *"esteganografia"* (a arte de esconder a mensagem) e a *"criptografia"* sendo esta, dado o avanço da tecnologia, muito utilizada no mundo virtual em face do volume de informações que transitam pela rede.

Num sentido mais técnico, a criptografia apresentava dois ramos, a criptografia de transposição e criptografia de substituição. A diferença entre ambas está no fato de que enquanto nesta a letra mantém a identidade, mas muda de posição, naquela, a letra muda de identidade, mas mantém a posição.

Contudo, em face dos novos métodos utilizados para criptografar uma mensagem, tem-se usado os termos *criptografia simétrica* (ou de chave privada - uma chave que cifra e decifra a mensagem) e *criptografia assimétrica* (ou de chave

pública - um par de chaves criptográficas uma pública e outra privada, matematicamente relacionadas).

Exemplo 1.0.1. ***A criptografia de transposição***

Esse método de criptografar foi utilizado na Grécia por volta do século V a.C. pelo exército espartano e ficou conhecido como a Cítala Espartana. A cítala consiste num bastão (do grego scytale ou skytale) como instrumento de cifragem de determinada largura e uma tira de papiro ou pergaminho no qual era escrito, no comprimento do bastão, a mensagem a ser cifrada. Uma vez escrita a mensagem, a tira era desenrolada e transmitida. Para ser lida, o destinatário da mensagem deveria ter, obrigatoriamente, um bastão semelhante ao qual a mensagem foi escrita.

Figura 1.1: Cítala espartana - CC BY-SA 3.0, [11].

Nota-se que o algoritmo para cifrar e decifrar a mensagem consiste apenas em enrolar a tira num bastão e a chave é a largura deste, o que torna a cítala espartana um método pouco seguro na cifragem de mensagens.

Para criptografar a frase

"ESTAMOS CONTANDO COM A AJUDA DE TODOS PARA ALCANÇARMOS NOSSO OBJETIVO"

usando a cítala espartana transcreve-se inicialmente o enunciado em uma tabela de, por exemplo, seis linhas, logo, o número de colunas necessárias é dado pelo número de caracteres, desprezados os espaços em branco, dividido por seis (que é o número de linhas adotadas) o que resulta em dez colunas.

E	S	T	A	M	O	S	C	O	N
T	A	N	D	O	C	O	M	A	A
J	U	D	A	D	E	T	O	D	O
S	P	A	R	A	A	L	C	A	N
C	A	R	M	O	S	N	O	S	S
O	O	B	J	E	T	I	V	O	K

Tabela 1.1: Tabela para visualização da codificação da mensagem

Observa-se que, ao final, foi acrescentada uma letra "K" para completar a linha. Ao desenrolar a tira a mensagem transmitida será

"ETJSCO SAUPAO TNDARB ADARMJ MODAOE OCEAST SOTLNI CMOCOV OADASO NAONSK".

Exemplo 1.0.2. ***Código de Caesar***

Uma das mais simples e conhecidas técnicas de criptografar é o Código de Julius Caesar. O Código de Caesar, também conhecido como Cifra de Substituição, consiste em substituir uma letra por outra que esteja três posições à frente no alfabeto, isto é, a letra "A"é substituída pela letra "D", a letra "B"pela letra "E", e assim sucessivamente, onde, as três últimas letras seriam substituídas pelas três primeiras letras do alfabeto, ou seja, a letra "X"pela letra "A", a letra "Y"pela letra "B"e a letra "Z", pela letra "C", conforme mostra a tabela abaixo.

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

Tabela 1.2: Cifra de Caesar

Como exemplo a mensagem:

"PARABÉNS A TODOS PELA VITÓRIA"

após cifrada ficaria assim

"SDUDEHQV D WRGRV SHOD YLWRULD"

Como se observa, semelhante à cifra de transposição, a Cifra de Caesar não é de difícil decodificação bastando para isso conhecermos o número de posições deslocadas utilizadas para fazermos a codificação.

Hoje em dia, costuma-se atribuir a denominação de Código de Caesar para qualquer cifra na qual cada letra da mensagem original seja substituída por outra deslocada um número fixo de posições, não necessariamente três, na mensagem cifrada.

1.1 Atribuindo modelos matemáticos

Um detalhe a ser observado é que esses dois métodos, que praticamente deram início à criptografia clássica, não foram construídos sobre modelos matemáticos mas sim empíricos. Porém, sem muito esforço, é possível associá-los a um modelo matemático específico. Essa associação torna-se interessante para ser trabalhada em sala aula com alunos do Ensino Médio.

1.1.1 A Cítala espartana e as matrizes

Conforme visto, esse método tem como algoritmo enrolar uma tira de papiro ou pergaminho num bastão onde escrevemos a mensagem da esquerda para direita (alternativamente de cima para baixo), conforme ilustra as figuras abaixo.

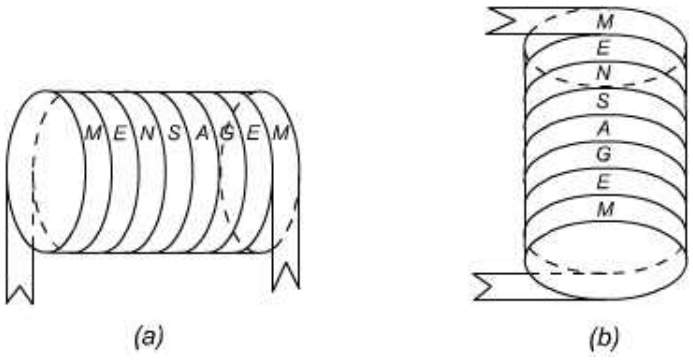


Figura 1.2: Cítala horizontal (a) e vertical (b)

A mensagem cifrada surge em forma de um *cinto* ao desenrolar a tira do bastão

e, por ser este a chave de codificação, o destinatário deve possuir um bastão de largura idêntica. No caso da mensagem ser escrita no sentido horizontal do bastão (da esquerda para direita - figura 1.2 (a)), a cítala espartana pode ser associada a uma matriz $m \times n$ onde m representa o número de linhas da matriz que depende do raio do cilindro, enquanto n representa o número caracteres na linha, ou seja, o número de colunas da matriz (o que vai definir o comprimento do bastão).

Já na figura 1.2 (b) a mensagem é anotada em verticais no bastão (de cima para baixo) e se tomar a mesma mensagem anotada na figura (a), tem-se uma matriz $n \times m$ transposta da matriz anterior. Neste caso, n representa o total de caracteres na mesma vertical, em outras palavras, o número de linhas da matriz (determinando, assim, o comprimento do bastão) e m a quantidade de caracteres na coluna (que depende do raio do bastão).

Criptografando a frase

"MATEMÁTICA, DE MODO ALGUM, SÃO FÓRMULAS, ASSIM COMO A MÚSICA NÃO SÃO NOTAS"

usando cítala espartana (desconsiderando os espaços e caracteres especiais) procede-se da seguinte maneira: inicialmente toma-se uma matriz com, por exemplo $n = 9$ colunas, a quantidade de linhas m será obtida ao final da transcrição da mensagem, nesse caso, $m = 7$ (para o caso da figura 1.2 (b) teremos a matriz transposta com 9 linhas e 7 colunas).

$$\begin{bmatrix} M & A & T & E & M & A & T & I & C \\ A & D & E & M & O & D & O & A & L \\ G & U & M & S & A & O & F & O & R \\ M & U & L & A & S & A & S & S & I \\ M & C & O & M & O & A & M & U & S \\ I & C & A & N & A & O & S & A & O \\ N & O & T & A & S & A & B & C & D \end{bmatrix} \quad ou \quad \begin{bmatrix} M & A & G & M & M & I & N \\ A & D & U & U & C & C & O \\ T & E & M & L & O & A & T \\ E & M & S & A & M & N & A \\ M & O & A & S & O & A & S \\ A & D & O & A & A & O & A \\ T & O & F & S & M & S & B \\ I & A & O & S & U & A & C \\ C & L & R & I & S & O & D \end{bmatrix}$$

Em ambos os casos, desenrolando a tira, tem-se a seguinte decodificação:

"MAGMMIN ADUUCCO TEMLOAT EMSAMNA MOASOAS ADOAAOA TOFSMSB IAOSUAC CLRISOD"

Um fato interessante é que se pode explorar esse método de criptografar para explorar temas como multiplicação de matrizes, determinantes, matriz inversa, dentre outros.

1.1.2 A Cifra de Caesar e a função afim

O Código de Caesar utiliza o método da substituição, ou seja, troca-se, na mensagem, uma letra por outra que esteja três posições à frente e as três últimas são substituídas pelas três primeiras.

Associando cada letra à sua posição no alfabeto tem-se então a oportunidade de explorar dois ramos da matemática: a aritmética modular e as funções.

A	B	C	D	E	F	G	H	I	J	K	L	M
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
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
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
14	15	16	17	18	19	20	21	22	23	24	25	26

Em particular, a função do tipo $f(x) = x + b \ (mod\ 26)$, onde x representa a posição da letra do texto original e b o número de posições que se quer deslocar. O interessante é que não é preciso ficar limitado a um deslocamento de apenas três posições, tal como no Código de Caesar, o que pode ser ilustrado no exemplo abaixo.

Exemplo 1.1.1. *Ana resolveu enviar uma mensagem para duas amigas, Amanda e Lígia. Contudo, para testar o domínio de ambas no campo das funções e aritmética*

modular, criptografou a mensagem "EM FEVEREIRO TEM CARNAVAL" usando a associação acima, para Amanda, codificou segundo o Código de Caesar, já para Lígia, substituiu cada letra da mensagem pela letra que está 15 posições à frente desta . A descrição dos procedimentos realizados por cada uma delas toma como referência o conjunto $A = \{1, 2, 3, ..., 25, 26\}$ *e a função definida por* $f : A \to A$, *tal que* $f(x) = x + b \ (mod\ 26)$.

(i) Os passos a serem seguidos por Ana para codificar a mensagem são: inicialmente trocar cada letra da mensagem a ser enviada pelo número correspondente e após, codificar a mensagem a ser enviada a cada uma delas.

E	M	F	E	V	E	R	E	I	R	O	T	E	M	C	A	R	N	A	V	A	L
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
5	13	6	5	22	5	18	5	9	18	15	20	5	13	3	1	18	14	1	22	1	12

Em seguida definem-se as funções de acordo com o enunciado;

(a) Para Amanda tem-se a função definida por $f(x) = x + 3 \ (mod\ 26)$ *que, aplicada à sequência numérica original gera a seguinte sequência numérica codificada*

8 16 - 9 8 25 8 21 8 12 21 18 - 23 8 16 - 6 4 21 17 4 25 4 15

e traduz na seguinte mensagem a ser enviada para ela

"HP IHYHUHLUR WHP FDUQDYDO"

(b) Para Lígia, a função fica $f(x) = x+15 \ (mod\ 26)$ *que produz a sequência numérica*

20 2 - 21 20 11 20 7 20 24 7 4 - 9 20 2 - 18 16 7 3 16 11 16 1

resultando então na seguinte mensagem a ser enviada

"TB UTKTGTXGD ITB RPGCPKPA"

(ii) Para que ambas possam ler a mensagem original, elas deverão fazer uso de suas "chaves" que são as respectivas funções inversas.

(a) *Inicialmente Amanda deve associar cada letra do texto criptografado à sua posição para, em seguida, utilizar a chave de decodificação, isto é, a função inversa da função* $f(x) = x + 3\,(mod\ 26)$ *que pode ser obtida usando como referência um "relógio codificador/decodificador"de 26 posições no qual o ponteiro de codificação avançou três posições, de acordo com o Código de Caesar.*

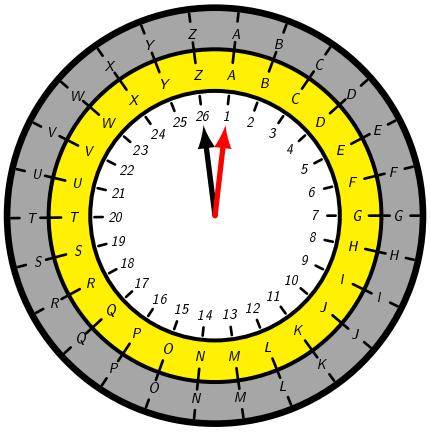


fig. (a) Relógio de codificação

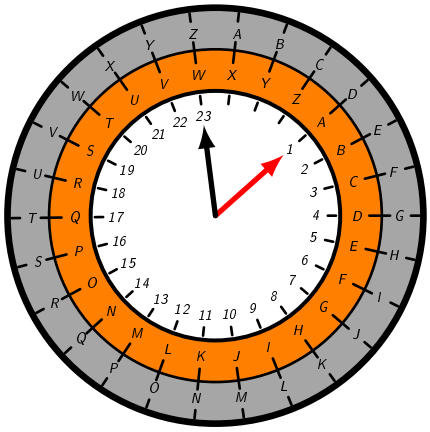


fig. (b) Relógio de decodificação

Observando o relógio nota-se que o ponteiro deverá se deslocar 23 posições para completar a volta, isto é, para chegar em "Z"que é o último símbolo adotado no exemplo, o que fornece $f^{-1}(y) = y + 23\ (mod\ 26)$*, onde* $y = f(x)$*. Logo:*

	H	P	I	H	Y	H	U	H	L	U	R	W	H	P	F	D	U	Q	D	Y	D	O
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	8	16	9	8	25	8	21	8	12	21	18	23	8	16	6	4	21	17	4	25	4	15
f^{-1}	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	5	13	6	5	22	5	18	5	9	18	15	20	5	13	3	1	18	14	1	22	1	12
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	E	M	F	E	V	E	R	E	I	R	O	T	E	M	C	A	R	N	A	V	A	L

Os valores obtidos acima após serem substituídos na função inversa resulta na decodificação da mensagem recebida.

(b) *Procedimento análogo deve ser realizado por Lígia, isto é, usar o "relógio*

codificador/decodificador"deslocado de 15 posições para obter a função inversa.

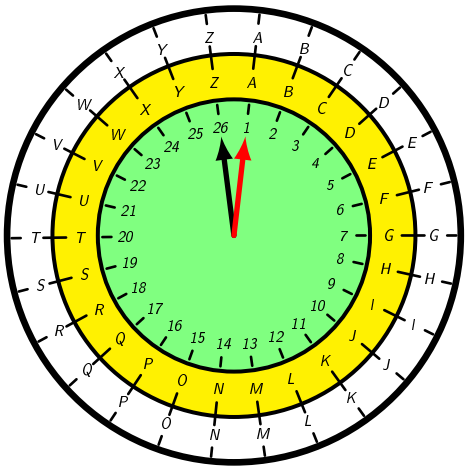


fig. (a) Relógio de codificação

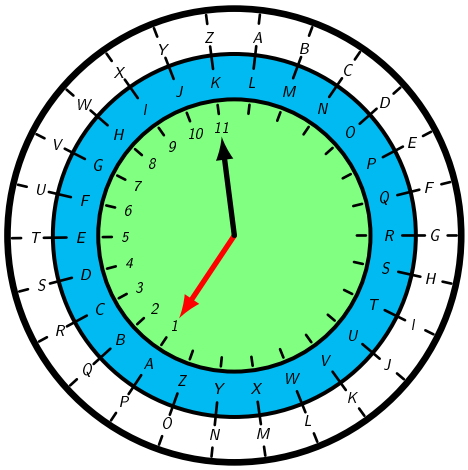


fig. (b) Relógio de decodificação

Que, neste caso, é dada por $f^{-1}(y) = y + 11\,(mod\ 26)$, *onde* $y = f(x)$, *o que resulta em:*

	T	B	U	T	K	T	G	T	X	G	D	I	T	B	R	P	G	C	P	K	P	A
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	20	2	21	20	11	20	7	20	24	7	4	9	20	2	18	16	7	3	16	11	16	1
f^{-1}	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	5	13	6	5	22	5	18	5	9	18	15	20	5	13	3	1	18	14	1	22	1	12
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	E	M	F	E	V	E	R	E	I	R	O	T	E	M	C	A	R	N	A	V	A	L

Neste exemplo trabalha-se com uma função do tipo $f(x) = x + b\ (mod\ 26)$ ficando para o capítulo 3 a abordagem das funções do tipo $f(x) = ax + b$ quando então já terão sido discutidos alguns pontos da **"teoria das funções"**, bem como, da **"aritmética modular"**, o que será feito no capítulo 2.

Conforme observa-se nos modelos de criptografia acima há um vasto campo de trabalho que pode ser explorado no Ensino Médio e leva os alunos a uma discussão prática e não apenas teórica. Fato é que se destaca apenas dois modelos de criptografia. Outros modelos foram surgindo ao longo da história à medida em que se fizeram necessários devido à ação dos criptoanalistas, tais como, a Cifra de Vigenère que, por ser uma cifra de substituição polialfabética, torna a decodificação

da mensagem um pouco mais complexa. Outros modelos criptográficos podem ser encontrados em [11] e [12].

Capítulo 2

Embasamento Teórico

Do exposto no capítulo 1, concluí-se que a *criptografia* permite ao professor trabalhar em sala de aula temas como funções, aritmética modular e até mesmo matrizes de forma bem prática, o que torna a aula mais dinâmica e mais acessível aos alunos, uma vez que se pode aprofundar mais ou menos no assunto de acordo com cada turma.

Nesse trabalho será dado destaque à *criptografia* que faz uso das funções e aritmética modular. As definições, teoremas e proposições terão por base os livros [1], [5] e [3].

2.1 Relações e funções

Tema fundamental do trabalho, a "*criptografia*" está intimamente ligada às funções, bem como, às suas funções inversas. Neste contexto é interessante tecer algum comentário sobre o tema, pois serão explorados na construção do capítulo 3, em que serão destacadas algumas funções e sua aplicação na criptografia para serem trabalhadas em sala de aula no Ensino Médio.

2.1.1 Produto cartesiano

Definição 2.1.1. *Dados dois conjuntos* $\boldsymbol{A}$ *e* $\boldsymbol{B}$*, subconjuntos de um conjunto universo* $\boldsymbol{U}$*, define o produto cartesiano de* $\boldsymbol{A}$ *por* $\boldsymbol{B}$ *e denota-se* $A \times B$ *o conjunto*

formado por todos os pares ordenados (x, y) *com* $x \in A$ *e* $y \in B$*. Em símbolos:*

$$A \times B = \{(x, y) \mid x \in A \text{ e } y \in B\}$$

Observações:

- $A = \varnothing$ *ou* $B = \varnothing$*, por definição,* $A \times B = \varnothing$
- *O conceito de par ordenado é tomado aqui como primitivo, isto é, algo que é aceito sem demonstração.*

Exemplo 2.1.1. *Se* $A = \{1; 2; 3\}$ *e* $B = \{1; 4\}$*, então*

(a) $A \times B = \{(1,1),\ (1,4),\ (2,1),\ (2,4),\ (3,1),\ (3,4)\}$

(b) $B \times A = \{(1,1),\ (1,2),\ (1,3),\ (4,1),\ (4,2),\ (4,3)\}$

Além de enumerarmos seus elementos para representar o produto cartesiano, como foi feito acima, pode-se ainda utilizar o diagrama de flechas ou o diagrama cartesiano. Se aplicado no item (a) do exemplo anterior, suas respectivas representações ficam:

Diagrama de flechas

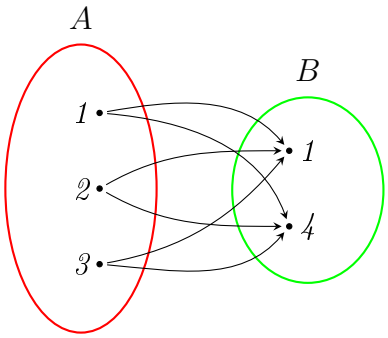
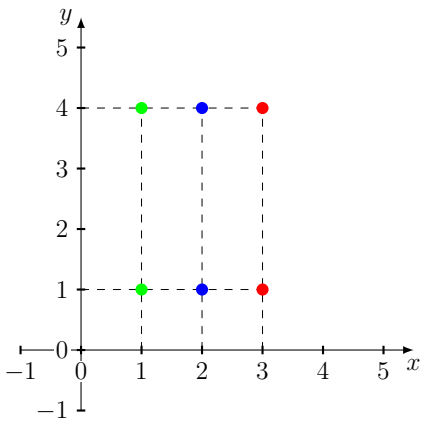


Diagrama Cartesiano



Conforme se observa nas representações acima cada uma têm suas vantagens e desvantagens. Quando queremos fazer a representação de conjuntos com poucos elementos, o diagrama de flechas é uma ótima opção. Porém, quando deseja-se representar intervalos numéricos, a melhor opção é o diagrama cartesiano.

2.1.2 Relação Binária

Definição 2.1.2. *Dados dois conjuntos* $\boldsymbol{A}$ *e* $\boldsymbol{B}$ *quaisquer, não necessariamente distintos, chama-se* ***relação binária*** *de* $\boldsymbol{A}$ *em* $\boldsymbol{B}$ *todo subconjunto* $\boldsymbol{R}$ *de* $A \times B$.

Em símbolos

$$R \text{ é uma relação binária de } A \text{ em } B \iff R \subset A \times B$$

Notação

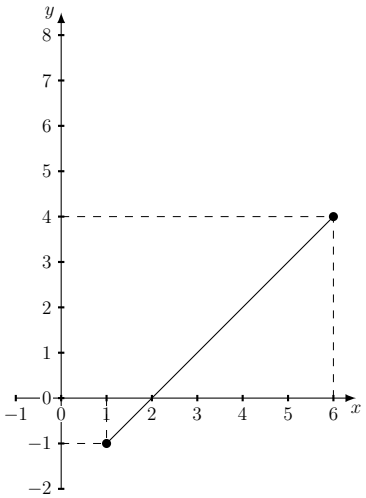
$$xRy \iff (x, y) \in R$$

Exemplos 2.1.1.

1. *Sejam os conjuntos* $A = \{a, b, c\}$ *e* $B = \{m, n, p, q\}$.
   $R_1 = \{(a, q), (b, n)\}$ *é uma relação de* A *em* B.
   $R_2 = \{(b, m), (b, n), (c, p)\}$ *é uma relação de* A *em* B.

2. *Considere os conjuntos* $M = \{2, 3\}$ *e* $N = \{1, 2, 3, 4, 6, 7\}$
   $R_3 = \{(x, y) \in M \times N \mid x \geq y\} = \{(2, 1), (2, 2), (3, 1), (3, 2), (3, 3)\}$.
   $R_4 = \{(x, y) \in M \times N \mid x|y\} = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6)\}$.
   Acima, $x|y$ *significa que* x *divide* y *ou* x *é um divisor de* y.

3. *Considere os conjuntos* $A = [1, 6]$ *e* $B = [-1, 8]$. *Represente no diagrama cartesiano a relação binária definida por* $R = \{(x, y) \in A \times B \mid y = x - 2\}$.



2.1.3 Domínio e Imagem

Seja R uma relação de A em B.

Definição 2.1.3. *Chama-se* ***domínio*** *de R o subconjunto de A constituído pelos elementos x que estão relacionados com algum elemento y de B, isto é, $(x, y) \in R$. Em símbolos,*

$$D(R) := \{x \in A \mid \exists y \in B : (x, y) \in R\}.$$

Definição 2.1.4. *Chama-se* ***imagem*** *de R o subconjunto de B constituído pelos elementos y para cada um dos quais existe algum x pertencente a A tal que $(x, y) \in R$. Em símbolos*

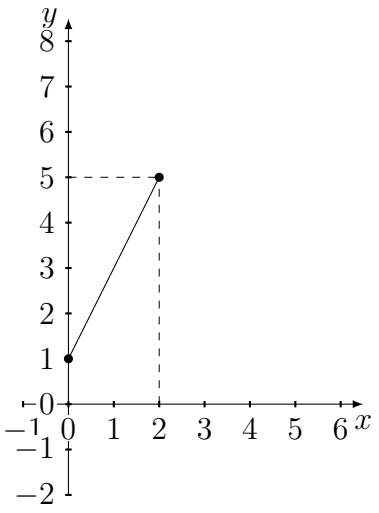
$$Im(R) = \{y \in B \mid \exists x \in A : (x, y) \in R\}.$$

Exemplos 2.1.2.

1. *Considere os conjuntos $A = \{a, e, i, o, u\}$ e $B = \{k, l, m, n, p, q\}$ e a relação binária $R = \{(a, k), (a, q), (i, m), (u, p)\}$. Então:*

$$D(R) = \{a, i, u\} \qquad Im(R) = \{k, m, p, q\}$$

2. *Sejam $A = \{x \in \mathbb{R} \mid 0 \leq x \leq 5\}$ e $B = \{y \in \mathbb{R} \mid 1 \leq y \leq 6\}$. Determine o domínio e imagem da relação $R = \{(x, y) \in A \times B \mid y = 2x + 1\}$.*
   Inicialmente faz-se a representação cartesiana de R.



Logo, $D(R) = [0,\ 2]$ e $Im(R) = [1,\ 5]$.

Propriedades de relações sobre conjuntos

A seguir apresentamos algumas propriedades que uma relação **R** sobre um conjunto **A** pode ter:

(a) **Reflexiva**: Uma relação R é reflexiva quando todo elemento de A se relaciona consigo mesmo, isto é,

$$\forall x \in A, (x, x) \in R,$$

ou ainda

$$xRx.$$

(b) **Simétrica**: Uma relação R é simétrica se

$$\forall x,\ y \in A : (x, y) \in R \Longrightarrow (y, x) \in R$$

(c) **Antissimétrica**: Uma relação R é dita antissimétrica se, para quaisquer

$$x,\ y \in A,\ \textit{se } xRy \textit{ e } yRx \Longrightarrow x = y$$

(d) **Transitiva**: Uma relação R é transitiva se

$$\forall x,\ y,\ z \in A : (x, y) \in R \textit{ e } (y, z) \in R \Longrightarrow (x, z) \in R$$

Definição 2.1.5. *Uma relação R sobre um conjunto A é dita uma relação de equivalência se, e somente se, R é reflexiva, simétrica e transitiva, isto é, R deve cumprir as seguintes propriedades:*

(i) $\forall x,\ x \in A \Longrightarrow (x, x) \in R$,

(ii) $\forall x,\ y \in A,\ (x, y) \in R \Longrightarrow (y, x) \in R$ e

(iii) $\forall x, y, z \in A,\ (x, y) \in R \textit{ e } (y, z) \in R \Longrightarrow (x, z) \in R$

2.1.4 Relações inversas

Definição 2.1.6. *Seja R uma relação de A em B. Chama-se relação inversa de R, e indica-se por R^{-1} a seguinte relação de B em A.*

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$$

Exemplos 2.1.3.

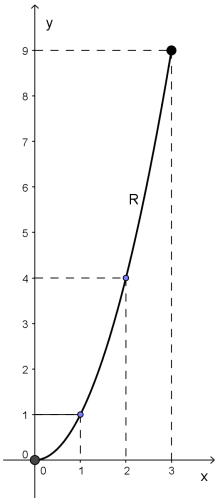
1. *$A = \{6, 8, 10, 12\}$, $B = \{1, 3, 5, 7, 9\}$ e $R = \{(6, 5), (8, 7), (8, 9), (12, 1)\}$. Então:*

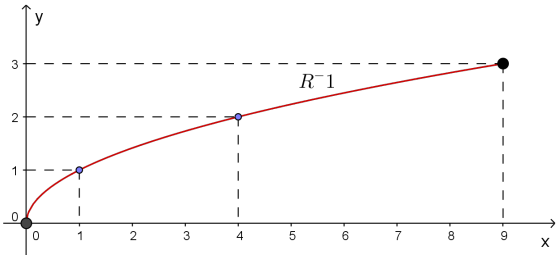
$$R^{-1} = \{(5, 6), (7, 8), (9, 8), (1, 12)\}$$

2. *Dados os conjuntos $A = \{x \in \mathbb{R} \mid 0 \leq x \leq 3\}$ e $B = \{y \in \mathbb{R} \mid 0 \leq y \leq 9\}$, e a relação $R = \{(x, y) \in A \times B \mid y = x^2\}$, representar no plano cartesiano a relação R e sua inversa R^{-1}.*
   Se $R = \{(x, y) \in A \times B \mid y = x^2\}$, então

$$R^{-1} = \{(y, x) \in B \times A \mid y = x^2\} \;=\; \{(x, y) \in B \times A \mid \sqrt{x} = y\}$$

Suas representações no plano cartesiano são mostradas abaixo:





Seguem de maneira direta:

(a) Se $R \subset A \times B$*, então* $R^{-1} \subset B \times A$*.*

(b) $D(R^{-1}) = Im(R)$*.*

(c) $Im(R^{-1}) = D(R)$*.*

(d) $(R^{-1})^{-1} = R$*.*

2.1.5 Funções

Definição 2.1.7. *Sejam* A *e* B *conjuntos não vazios e* f *uma relação de* A *em* B*. Dizemos que* f *é uma* ***aplicação*** *(função ou transformação) de* A *em* B *se, e somente se, para todo* $x \in A$*, existe um único* $y \in B$ *tal que* $(x,\ y) \in f$*. Em símbolos*

$$f \subset A \times B \text{ é uma aplicação de A em B} \iff \forall x \in A,\ \exists!\ y \in B \mid (x, y) \in f$$

Observações: Se f é uma aplicação (função) de A em B, então

(i) Para indicarmos uma função f, definida em A com imagem em B, segundo a lei de correspondência $y = f(x)$ também pode ser usada a seguinte notação

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

(ii) Se $x \in A$ então o único elemento $y \in B$ tal que $(x, y) \in f$ é denotado por $y = f(x)$ e é chamado de **imagem** de x pela função f.

Exemplo 2.1.2. *Considere os conjuntos* $A = \{1,\ 2,\ 3,\ 4\}$ *e* $B = \{5,\ 10,\ 15,\ 20,\ 25\}$ *e as seguintes relações de* A *em* B*:*

$R_1 = \{(1, 10),\ (2, 5),\ (4, 10)\}$*;*

$R_2 = \{(1, 20),\ (2, 5),\ (2, 25),\ (3, 15),\ (4, 20)\}$*;*

$R_3 = \{(1, 5),\ (2, 15),\ (3, 15),\ (4, 5)\}$*;*

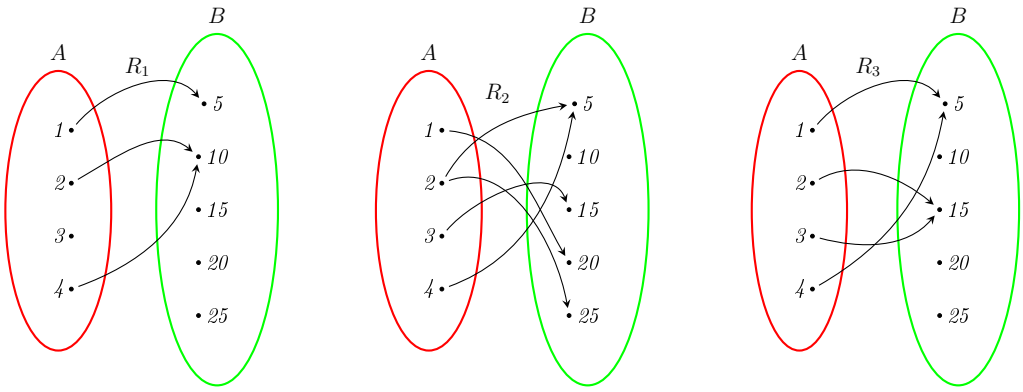
Analisando a definição de função temos:

R_1 *não é função, pois* $D(R_1) = \{1,\ 2,\ 4\} \neq \{1,\ 2,\ 3,\ 4\} = A$*;*

R_2 *não é função, pois* $(2, 5) \in R_2$*,* $(2, 25) \in R_2$ *e* $5 \neq 25$*;*

R_3 é uma função cujo domínio é $D(R_3) = \{1,\ 2,\ 3,\ 4\}$ e conjunto imagem é $Im(R_3) = \{5,\ 15\}$.

Abaixo encontra-se a representação dessas relações nos diagramas de flechas.



2.1.6 Função Composta

Definição 2.1.8. *Sejam $f : A \to B$ e $g : B \to C$ duas funções. Chama-se **função composta** de **g** com **f** a função $g \circ f : A \to C$ e definida por*

$$(g \circ f)(x) = g(f(x));\ \forall x \in A.$$

2.1.7 Funções Sobrejetoras, Injetoras e Bijetoras

Definição 2.1.9. *Uma função f de A em B é **sobrejetora** se, e somente se, para todo **y** pertencente a **B** existe pelo menos um **x** pertencente a **A** tal que **f(x) = y**. Em símbolos,*

$$f : A \to B \quad \text{é sobrejetra} \iff \forall y,\ y \in B,\ \exists\ x \in A \mid f(x) = y.$$

Ou ainda

$$f : A \to B \quad \text{é sobrejetora} \iff Im(f) = B.$$

Definição 2.1.10. *Uma função f de A em B é **injetora** se, e somente se, elementos distintos de **A** têm imagens distintas em **B**. Em símbolos,*

$$(\forall x_1,\ x_2 \in A),\ (x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)).$$

Definição 2.1.11. *Uma função f de A em B é* ***bijetora*** *se, e somente se,* $\boldsymbol{f}$ *é sobrejetora e injetora.*

2.1.8 Função Inversa

Considere os conjuntos $A = \{1,\ 2,\ 3,\ 4\}$, $B = \{2,\ 3,\ 4,\ 5\}$ e as funções f, g e h de A em B definidas por

$$f = \{(1,5),\ (2,2),\ (3,4)\},$$

$$g = \{(1,2),\ (2,3),\ (3,4),\ (4,4)\}\ e$$

$$h = \{(1,2),\ (2,3),\ (3,4),\ (4,5)\}.$$

Como toda função de A em B é uma relação binária podemos considerar suas relações inversas f^{-1}, g^{-1} e h^{-1}, isto é,

$$f^{-1} = \{(5,1),\ (2,2),(4,3)\},$$

$$g^{-1} = \{(2,1),\ (3,2),\ (4,3),\ (4,4)\}\ e$$

$$h^{-1} = \{(2,1),\ (3,2),\ (4,3),(5,4)\}.$$

Note que

- f^{-1} não é uma função de B em A, pois $D(f^{-1}) = \{2,\ 4,\ 5\} \neq B$,
- g^{-1} não é uma função de B em A, pois $D(g^{-1}) = \{2,\ 3,\ 4\} \neq B$, além disso $(4,3) \in g^{-1}$ e $(4,4) \in g^{-1}$ sendo $3 \neq 4$,
- h^{-1} é uma função de B em A.

Conforme se observa, pode ocorrer que a relação inversa não seja uma função de B em A.

Definição 2.1.12. *Seja f uma função de A em B. Dizemos que f é uma função invertível (ou inversível) se a relação inversa $f^{-1} \in B \times A$ é uma função.*

Segue da definição que para f^{-1} ser uma função de B em A, f deve cumprir as seguintes condições:

(i) $D(f^{-1}) = Im(f) = B$, ou seja, f deve ser **sobrejetora**.

(ii) Cada elemento de B deve ser imagem de um único elemento de A pela função f, caso contrário, em f^{-1}, um mesmo elemento teria duas imagens distintas, o que não pode ocorrer. Resumindo, f deve ser **injetora**.

Desta forma, as condições acima são necessárias e suficientes, ou seja, tem-se:

Proposição 2.1.13. *Seja $f : A \to B$ uma função. A relação f^{-1} é uma função de B em A se, e somente se, $\boldsymbol{f}$ for bijetora.*

Demonstração

($\Rightarrow$) Provemos que se f^{-1} é uma função, então f é bijetora.

De fato:

(i) Seja $y \in B$, como $f^{-1} : B \to A$ é uma função, existe $x \in A$, tal que $f^{-1}(y) = x$ e, portanto, $f(x) = y$, ou seja, f é sobrejetora.

(ii) Sejam $x_1,\ x_2 \in A$, tais que $f(x_1) = y = f(x_2)$. Então $(x_1, y) \in f$ e $(x_2, y) \in f$ e, dai, $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$. Como f^{-1} é uma função, segue que $x_1 = x_2$. Portanto, f é injetora.

De (i) e (ii) concluí-se que f é *bijetora.*

($\Leftarrow$) Provemos que se f é bijetora, então f^{-1} é uma função:

De fato:

(i) Como f é sobrejetora, dado $y \in B$, existe $x \in A$ tal que $f(x) = y$ e, portanto, $f^{-1}(y) = x$. Assim, $D(f^{-1}) = B$.

(ii) Seja $y \in B$ e suponhamos $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$. Então $(x_1, y) \in f$ e $(x_2, y) \in f$, isto é, $f(x_1) = y = f(x_2)$. Como f é injetora segue que $x_1 = x_2$.

De (i) e (ii) concluímos que f^{-1} é uma função de B em A. ■

Proposição 2.1.14. *Seja $f : A \to B$ uma função bijetora. Se f^{-1} é a função inversa de f então $f^{-1} \circ f = I_A$ e $f \circ f^{-1} = I_B$. Aqui $I_A : A \to A$ é a função identidade $I_A(x) = x$ e $I_B : B \to B$ é a função identidade $I_B(y) = y$.*

Demonstração

De fato, como f é bijetora, sabemos que o mesmo ocorre com f^{-1}. Daí

$$\forall x \in A,\ (f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = I_A(x),$$

ou seja, $f^{-1} \circ f = I_A$.

Analogamente,

$$\forall x \in B,\ (f \circ f^{-1})(x) = f(f^{-1}(x)) = x = I_B(x),$$

ou seja, $f \circ f^{-1} = I_B$. ■

2.2 Aritmética das Classes Residuais

Junto com a Teoria de Funções, a Aritmética dos Inteiros (em destaque *Congruências*) complementa o eixo principal do trabalho, que nada mais é do que levar para a sala de aula uma matemática vista de forma prática e agradável, pois, aplicadas na criptografia, tais teorias encontram-se presentes no dia a dia do aluno, mesmo do ensino fundamental, dado o grande número de aparelhos celulares por estes utilizados.

2.2.1 Congruência - Definição e propriedades

Definição 2.2.1. *Sejam a, b, $m \in \mathbb{Z}$, com $m > 1$ dizemos que a é congruente a b módulo m se m divide $a - b$ e escrevemos $a \equiv b\ (mod\ m)$.*

Em símbolos

$$a \equiv b\ (mod\ m) \iff m|(a - b)$$

Proposição 2.2.2. *Sejam a e b dois inteiros, tem-se que $a \equiv b\ (mod\ m)$ se, e somente se, a e b possuem o mesmo resto quando divididos por m.*

Demonstração

($\Leftarrow$) Suponha que a e b possuem o mesmo resto quando divididos por m, então existem inteiros r, q_1 *e* q_2 tais que

$$a = mq_1 + r \quad e \quad b = mq_2 + r.$$

Logo

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

e, consequentemente,

$$m|(a - b),$$

ou seja, $a \equiv b\ (mod\ m)$. ($\Rightarrow$) Suponha, agora que $a \equiv b\ (mod\ m)$, ou seja, $m|(a-b)$. Pela divisão euclidiana, temos que

$$a = mq_1 + r_1, \quad com\ 0 \leqslant r_1 < m,$$

$$b = mq_2 + r_2, \quad com\ 0 \leqslant r_2 < m.$$

Dai,

$$a - b = m(q_1 - q_2) + (r_1 - r_2)$$

Como $m|m(q_1 - q_2)$, e, $0 \leqslant |r_1 - r_2| < m$ segue que $m|(r_1 - r_2)$, se, e somente se, $r_1 - r_2 = 0$.

Portanto, $a \equiv b\ mod\ m$ se, e somente se, $r_1 = r_2$ o que é equivalente a dizer que $m|(a - b)$. ■

Proposição 2.2.3. *(Propriedades fundamentais das congruências)*
Sejam os inteiros a, b, c, d, m *e* n *com* $m > 1$ *e* $n \geqslant 1$. *Valem as seguintes propriedades:*

(i) $a \equiv a\ (mod\ m)$ (reflexividade);

(ii) *Se* $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$ (simetria);

(iii) *Se* $a \equiv b\ (mod\ m)$ *e* $b \equiv c\ (mod\ m)$ então $a \equiv c\ (mod\ m)$ (transitividade);

(iv) *Se* $a + c \equiv b + c \ (mod\ m)$ então $a \equiv b \ (mod\ m)$;

(v) *Se* $a \equiv b \ (mod\ m)$ *e* $c \equiv d \ (mod\ m)$, então $a + c \equiv b + d \ (mod\ m)$;

(vi) *Se* $a \equiv b \ (mod\ m)$ *e* $c \equiv d \ (mod\ m)$, então $a \cdot c \equiv b \cdot d \ (mod\ m)$;

(vii) *Se* $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$;

(viii) *Se* $a \equiv b \ (mod\ m)$, então $ac \equiv bc \ (mod\ m)$.

Demonstração

(i) e (ii) são imediatas.

(iii) Temos, por hipótese, $m|(a-b)$ e $m|(b-c)$, logo $m|(a-b)+(b-c)$, ou seja, $m|(a-c)$ e, portanto, $a \equiv c \ (mod\ m)$;

(iv) Como, por hipótese, $a + c \equiv b + c \ (mod\ m)$, temos que $m|(a+c)-(b+c)$, logo $m|(a-b)$, isto é, $a \equiv b \ (mod\ m)$;

(v) Por hipótese, $m|(a-b)$ e $m|(c-d)$, logo $m|(a-b)+(c-d) = (a+c)-(b+d)$ e, portanto, $a + c \equiv b + d \ (mod\ m)$;

(vi) Note que $ac - bd = ac - ad + ad - bd = a(c-d) + d(a-b)$ pela propriedade (v), segue que $m|(ac-bd)$ e, consequentemente, $ac \equiv bd \ (mod\ m)$;

(vii) Isto segue de (vi) tomando $c = a$ e $d = b$ e usando indução sobre n;

(viii) Por hipótese, $a - b = mq$ para algum $q \in Z$. Daí, multiplicando-se ambos os membros da igualdade por c obtemos: $ac - bc = m(qc)$. De onde se conclui que $ac \equiv bc \ (mod\ m)$.

■

Proposição 2.2.4. *Sejam* $a,\ b,\ c$ *e* $m \in \mathbb{Z}$ *com* $m > 1$. *Se* $mdc(c, m) = 1$ *então* $ac \equiv bc \ (mod\ m)$ *implica* $a \equiv b \ (mod\ m)$.

Demonstração

Se $ac \equiv bc \ (mod\ m)$, então $m|ac - bc = (a-b)c$ e como $mdc(c, m) = 1$, segue que $m|(a-b)$ e portanto $a \equiv b \ (mod\ m)$. ■

2.2.2 Sistema completo de restos

Definição 2.2.5. *Seja $m > 0$ um inteiro fixo. Chamamos de sistema completo de resíduos módulo m todo conjunto de m inteiros $S = \{r_1,\ r_2,\ \ldots,\ r_m\}$ que satisfaz:*

1. $r_i \not\equiv r_j\ (mod\ m)$ *para* $i \neq j$
2. $\forall n \in \mathbb{Z},\ \exists\ r_i |\ n \equiv r_i\ (mod\ m)$

Proposição 2.2.6. *O conjunto $S = \{0,\ 1,\ 2,\ \ldots, m-1\}$ é um sistema completo de resíduos módulo m.*

Demonstração

Devemos mostrar que todo inteiro a é congruente módulo m a apenas um dos elementos de S. De fato, seja $a \in \mathbb{Z}$. Pelo algoritmo da divisão euclidiana de a por m, existem inteiros q e r tais que

$$a = qm + r,\ com\ 0 \leqslant r \leqslant m-1.$$

Logo, $a - r = mq$, isto é, $a \equiv r\ (mod\ m)$. Pela unicidade do resto o resultado segue.

■

Proposição 2.2.7. *Se $\{r_1,\ r_2,\ \ldots,\ r_m\}$ é um sistema completo de resíduos módulo m e a e b são inteiros com $mdc(a,m) = 1$, então*

$$\{ar_1 + b,\ ar_2 + b,\ \ldots,\ ar_m + b\}$$

também é um sistema completo de resíduo.

Demonstração

Como, por hipótese, $mdc(a,m) = 1$, considerando-se a propriedade (iv) de congruência e a proposição 2.2.4, temos que

$$ar_i + b \equiv\ ar_j + b\ (mod\ m) \Longleftrightarrow ar_i \equiv ar_j\ (mod\ m) \Longleftrightarrow r_i \equiv r_j\ (mod\ m) \Longleftrightarrow i = j,$$

Isto mostra que $ar_1 + b,\ ar_2 + b,\ \ldots,\ ar_m + b$ são dois a dois incongruentes módulo m e, portanto, formam um sistema completo de resíduos. ■

Exemplo 2.2.1. *$S = \{15,\ 16,\ 17,\ 18,\ 19\}$ é um sistema completo de resíduos (mod 5) uma vez que:*
$15 \equiv 0\ (mod\ 5)$, $16 \equiv 1\ (mod\ 5)$, $17 \equiv 2\ (mod\ 5)$, $18 \equiv 3\ (mod\ 5)$ *e* $19 \equiv 4\ (mod\ 5)$.

2.2.3 Classes Residuais

Definição 2.2.8. *Seja $m \in \mathbb{Z}$ tal que $m > 1$. O conjunto $[a] = \{x \in \mathbb{Z} |\ x \equiv a\ (mod\ m)\}$ é chamado classe residual módulo m do elemento $a \in \mathbb{Z}$.*

Denotaremos por $\mathbb{Z}_m$ o conjunto de todas as classes residuais módulo m.

Proposição 2.2.9. *Seja m um inteiro maior do que 1. Valem as seguintes propriedades:*

(i) $[a] = [b]$ *se, e somente se,* $a \equiv b\ (mod\ m)$;

(ii) Se $[a] \cap [b] \neq \varnothing$, *então* $[a] = [b]$.

Demonstração

(i) Suponha $[a] = [b]$, como $a \in [a]$, segue $a \in [b]$, logo $a \equiv b\ (mod\ m)$.
Reciprocamente, suponha $a \equiv b\ mod\ m$, então, pela propriedade (iii) temos $x \equiv a\ (mod\ m)$ *e* $a \equiv b\ (mod\ m) \Longrightarrow x \equiv b\ (mod\ m)$ logo, $x \in [a]$ se, e somente se, $x \in [b]$, de onde $[a] = [b]$.

(ii) Se $[a] \cap [b] \neq \varnothing$, existe $c \in [a] \cap [b]$. Então $c \in [a]$ e $c \in [b]$. Daí, pela propriedade (ii), segue que $c \equiv a\ (mod\ m) \Longrightarrow a \equiv c\ (mod\ m)$ e $c \equiv b (mod\ m) \Longrightarrow b \equiv c\ (mod\ m)$ logo, pela propriedade (iii) tem-se $a \equiv b\ mod\ m)$ e, pelo item *(i)* acima, segue que $[a] = [b]$ ■

Observação: Sejam $[a] \in \mathbb{Z}_m$ e $x \in \mathbb{Z}$. Se $[x] = [a]$ então x é dito representante da classe residual $[a]$.

Exemplos 2.2.1.

1. *Seja* $m = 2$, *então:*

$$[0] = \{x \in \mathbb{Z} |\ x \equiv 0\ (mod\ 2)\} \ = \ \{x \in \mathbb{Z} |\ x\ \acute{e}\ par\}$$

$$[1] = \{x \in \mathbb{Z} |\ x \equiv 1\ (mod\ 2)\} \ = \ \{x \in \mathbb{Z} |\ x\ \acute{e}\ \acute{i}mpar\}$$

Ou seja, $[a] = [0]$, *se a é par e* $[a] = [1]$, *se a é ímpar.*

2. *Seja* $m = 3$. *Então*

$$[0] = \{3k |\ k \in \mathbb{Z}\}$$

$$[1] = \{3k + 1 |\ k \in \mathbb{Z}\}$$

$$[2] = \{3k + 2 |\ k \in \mathbb{Z}\}$$

e

$$[a] = \begin{cases} [0]\,, & \textit{se a é múltiplo de 3} \\ [1]\,, & \textit{se a tem resto 1 quando dividido por 3} \\ [2]\,, & \textit{se a tem resto 2 quando dividido por 3} \end{cases}$$

3. *Se* $m = 4$, *qualquer múltiplo de 4 é representante da classe residual* $[0]$. *Temos que -7, -3, 1, 5, 9, etc, são representantes da classe residual* $[1]$, *-6, -2, 2, 6, etc, são representantes da classe residual* $[2]$ *e -5, -1, 3, 7, etc, são representantes da classe residual* $[3]$.

Proposição 2.2.10. *Para cada* $a \in \mathbb{Z}$ *existe um, e somente um* $r \in \mathbb{Z}$ *com* $0 \leqslant r \leqslant m - 1$, *tal que* $[a] = [r]$.

Demonstração

Seja $a \in \mathbb{Z}$. Pela divisão euclidiana existem inteiros q e r, com $0 \leqslant r \leqslant m - 1$, tais que $a = mq + r$. Logo, é único o inteiro r tal que $0 \leqslant r \leqslant m-1$ e $a \equiv r\ (mod\ m)$. Decorre, portanto, que é único o inteiro r tal que $0 \leqslant r \leqslant m - 1$ e $[a] = [r]$. ■

Corolário 2.2.11. *Existem exatamente m classes residuais mdulo m distintas, a saber* $[0]$, $[1]$, ..., $[m - 1]$.

Do corolário acima podemos concluir que, apesar de $\mathbb{Z}$ ser um conjunto infinito, $\mathbb{Z}_m$ é um conjunto finito e reparte $\mathbb{Z}$ em m subconjuntos onde cada um deles

é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m. Logo, obtemos a seguinte partição de $\mathbb{Z}$:

$$[0] = \{x \in \mathbb{Z} |\ x \equiv 0\ (mod\ m)\}$$

$$[1] = \{x \in \mathbb{Z} |\ x \equiv 1\ (mod\ m)\}$$

$$\vdots$$

$$[m-1] = \{x\mathbb{Z} |\ x \equiv (m-1)\ (mod\ m)\}$$

Note que

$$[m] = [0],\ [m+1] = [1], \ldots$$

Portanto, podemos parar em $[m-1]$. Assim

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

Observação: Uma das vantagens das classes residuais módulo m é transformar a congruência $a \equiv b\ (mod\ m)$ na igualdade $[a] = [b]$.

Podemos definir as seguintes operações em $\mathbb{Z}_m$:

Adição:

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \mapsto \mathbb{Z}_m$$

$$([a], [b]) \mapsto [a] + [b] := [a + b]$$

Multiplicação:

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \mapsto \mathbb{Z}_m$$

$$([a], [b]) \mapsto [a] \cdot [b] := [a \cdot b]$$

Uma vez definidas tais operações usando os representantes a e b para as classes residuais $[a]$ e $[b]$, respectivamente, devemos verificar que ao mudarmos estes representantes, não mudam os valores de $[a + b]$ e $[a \cdot b]$.

De fato, considere $a \equiv a'\ (mod\ m)$ e $b \equiv b'\ (mod\ m)$, então os itens *(v)* e *(vi)* da Proposição 2.2.3 nos garante que $[a + b] = [a' + b']$ e $[a \cdot b] = [a' \cdot b']$.

Propriedades da adição:

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

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

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

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

A_4: **Existência do simétrico:** $[a] + [m - a] = [0]$, para todo $a < m$

Propriedades da multiplicação:

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

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

M_2: **Comutatividade:** $[a] \cdot [b] = [b] \cdot [a]$;

M_3: **Existência da unidade:** $([a] \cdot [1]) = [a]$;

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

Demonstração

As demonstrações não apresentam grandes dificuldades e tomam como bases os axiomas referentes as operações com números inteiros. Demonstremos A_4 e AM.

A_4 : Lembrando que $[m] = [0]$ e que $m - a$ é o oposto de a temos

$$[a] + [m - a] = [a + m - a] = [m] = [0].$$

AM : Temos que

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

$$= [a \cdot b] + [a \cdot c] = [a] \cdot [b] + [a] \cdot [c].$$

■

Definição 2.2.12. *Dados* $[a]$ *e* $[b]$ *pertencentes a* $\mathbb{Z}_m$*, se* $[a] \cdot [b] = 1$*, então* $[a]$ *será dito invertível e* $[b]$ *será o inverso de* $[a]$*.*

Exemplos 2.2.2.

1. As tabelas da adição e multiplicação em $\mathbb{Z}_5 = \{[0],\ [1],\ [2],\ [3],\ [4]\}$ *são*

+	[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]

.	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

2. As tabelas da adição e multiplicação de $\mathbb{Z}_6 = \{[0],\ [1],\ [2],\ [3],\ [4],\ [5]\}$ *são*

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

.	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Observação: $\mathbb{Z}_m$ com as operações definidas acima é um anel. A seguir damos a caracterização dos elementos invertíveis em $\mathbb{Z}_m$.

Proposição 2.2.13. *Seja* $[a] \in \mathbb{Z}_m$. $[a]$ *é invertível se, e somente se,* $mdc(a,\ m) = 1$.

Demonstração

($\Rightarrow$) Suponha que $[a]$ é invertível, então existe $[b] \in \mathbb{Z}$ tal que $[1] = [a] \cdot [b] = [a \cdot b]$, logo $a \cdot b \equiv 1\ (mod\ m)$, isto é, existe $k \in \mathbb{Z}$ tal que $a \cdot b + k \cdot m = 1$, e, portanto, $mdc(a, m) = 1$.

($\Leftarrow$) Suponha agora que $mdc(a, m) = 1$, então existem inteiros b e k tais que $a \cdot b + m \cdot k = 1$ e consequentemente, $[1 - m \cdot k] = [a \cdot b]$. Dai

$$[1] = [1] + [0] = [1] + [-(m \cdot k)] = [1 + (-m \cdot k)] = [1 - m \cdot k] = [a \cdot b] = [a] \cdot [b]$$

Portanto, $[a]$ é invertível. ■

Proposição 2.2.14. $\mathbb{Z}_m$ *é um corpo se, e somente se,* m *é primo.*

Demonstração

($\Rightarrow$) Suponha por absurdo que $\mathbb{Z}_m$ seja um corpo e que m não seja primo, então $m = m_1 \cdot m_2$ com $1 < m_1 < m$ e $1 < m_2 < m$. Logo, $[0] = [m] = [m_1 \cdot m_2] = [m_1] \cdot [m_2]$ com $[m_1] \neq 0$ e $m_2 \neq 0$, contradição.

($\Leftarrow$) Suponha agora m primo. Como $mdc\ (i,\ m) = 1$ para $i = 1,\ 2,\ \ldots,\ m-1$, segue pela proposição anterior que $i = 1,\ 2,\ \ldots,\ m-1$, são invertíveis. Portanto, $\mathbb{Z}_m$ é um corpo. ■

Capítulo 3

Criptografia na sala de aula

Um dos grandes problemas enfrentados pelo professor em sala de aula, principalmente na Educação Básica (Ensino Fundamental II e Ensino Médio), é a falta de interesse dos alunos em relação aos temas que são abordados e da forma como o são. Como, por exemplo, despertar num aluno que não tem muita afinidade com as matérias exatas o interesse por temas como trigonometria, números complexos ou mesmo funções? A resposta para esta questão não é fácil de ser respondida.

Uma possível solução é trazer para a sala de aula possíveis aplicações que façam parte do dia a dia do aluno ou, pelo menos, que este possa vislumbrar alguma utilidade, pois assim o professor pode despertar nele sua curiosidade e/ou o impulso exploratório. Neste contexto podemos citar a criptografia que nos permite desenvolver de forma bem simples grandes temas do Ensino Médio tais como, matrizes e/ou funções e que, ao mesmo tempo, estão presentes a todo instante, dado a sua necessidade exigida no envio e recebimento de informações no mundo virtual, uma realidade compartilhada pela grande maioria dos estudantes.

Outra coisa que deve ser levada em conta é a diversidade encontrada em sala de aula, uma vez que, nem todos os alunos aprendem da mesma maneira. A criptografia se enquadra perfeitamente no contexto, pois as resoluções dos problemas, conforme veremos adiante, podem ser realizadas de formas diferentes permitindo que os alunos em nível mais avançados trabalhem soluções mais teóricas, ao passo que, os alunos que apresentem dificuldades com o tema, trabalhem usando procedimentos mais simples.

Para isso utilizaremos a criptografia de substituição associada às funções na codificação (cifragem) e às funções inversas na decodificação. Logo, há aqui a possibilidade de trabalhar com os seguintes conceitos:

(a) funções;

(b) propriedades de funções, mais especificamente injetora, sobrejetora e bijetora;

(c) função inversa;

(d) aritmética dos inteiros.

3.0.4 Cifrário por função afim

Neste processo criptográfico utiliza-se funções da forma $f(x) = ax + b$ ou $f(x) = ax + b \ (mod \ m)$, em que os valores de x são fornecidos pelos números correspondentes às posições das letras no alfabeto. Nota-se que este modelo de cifragem nada mais é que uma extensão da Cifra de Caesar.

Uma vez cifrada a mensagem usando a função $f(x) = ax + b$, esta poderá ser enviada ao destinatário como uma sequência de letras ou de números. Para enviar a mensagem como uma sequência numérica basta calcular $f(x)$ segundo a posição correspondente de cada letra da mensagem e enviá-la. Já para mandar a mensagem como uma sequência de letras, o emissor deverá, após a conversão correspondente à cada letra da mensagem por $f(x)$, fazer uso de uma tabela obtida a partir das classes residuais módulo m, ou seja, $\mathbb{Z}_m$.

Na decodificação da mensagem, o destinatário deverá fazer o processo inverso do método utilizado na codificação e, para isso, terá as seguintes opções:

(i) recebendo a sequência de números codificados, resolver a equação $f(x) = y$;

(ii) recebendo a sequência de números codificados, determinar a função inversa de $f(x)$, isto é, $f^{-1}(x)$ e com a sequência recebida, usando $f^{-1}(x)$, fazer a transcrição da mensagem. Note que a função utilizada na codificação da mensagem deve ser bijetora, pois,

- o fato de ser injetora nos garante que letras diferentes sejam enviadas a letras diferentes;

- o fato de ser sobrejetora garante que toda letra seja imagem de outra letra;
- o fato de ser bijetora, pela proposição 2.1.13 garante que $f^{-1}(x)$ seja uma função.

(iii) caso receba a mensagem através de uma sequência de letras, consultar a mesma tabela $\mathbb{Z}_m$ utilizada pelo emissor da mensagem que, juntamente com a função inversa de $f(x)$, será a chave de decodificação da mensagem.

O item (i) é o mais simples dos três, ao passo que o item (iii) faz uso dos dois primeiros, cobrando do aluno maior domínio na teoria das funções, além de servir como fundamento teórico para o estudo de congruência módulo m.

As mensagens cifradas usando funções da forma $f(x) = ax + b \ (mod\ m)$ só poderão ser decodificadas através de sua função inversa, pois este método torna impossível deciframos a mensagem resolvendo a equação $f(x) = y$. Isso exige um certo cuidado na escolha do coeficiente a como pode ser observado a seguir no exemplo a seguir.

Exemplo 3.0.2. *Considere o conjunto* $\mathbb{Z}_{26} = \{1,\ 2,\ 3,\ \ldots,\ 26\}$ *e a função* $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ *definida por* $f(x) = 2x + 5 \ (mod\ 26)$. *Temos que*

$$f(1) = 2 \cdot 1 + 5 = 7 \ (mod\ 26)$$

e

$$f(14) = 2 \cdot 14 + 5 = 33 \equiv 7 \ (mod\ 26)$$

Isto é, f *não é bijetora.*

Lema 3.0.15. *Sejam* $a,\ b \in \mathbb{Z}$ *com* $a \neq 0$. *A função de* $\mathbb{Z}$ *em* $\mathbb{Z}$ *definida por* $f(x) = ax + b$ *é injetora.*

Demonstração

De fato, como $a \neq 0$, dados $x_1,\ x_2 \in \mathbb{Z}$ temos que, $f(x_1) = f(x_2) \iff ax_1 + b = ax_2 + b \iff ax_1 = ax_2 \iff x_1 = x_2$. Logo f é injetora. ■

Lema 3.0.16. *Sejam* $a,\ b,\ m \in \mathbb{Z}$, *com* $a \neq 0$ *e* $m > 1$ *e, ainda,* $\mathbb{Z}_m = \{[1],\ [2],\ [3],\ \ldots,\ [m]\}$. *A função* $f : \mathbb{Z}_m \to \mathbb{Z}_m$ *definida por* $f(x) = ax+b\ (mod\ m)$ *é bijetora se, e somente se,* $mdc(a, m) = 1$.

Demonstração

Sejam $[x],\ [y] \in \mathbb{Z}_m$, tais que $ax + b \equiv ay + b\ (mod\ m)$. Como, por hipótese, $mdc(a, m) = 1$, das proposições 2.2.3 item (iv) e 2.2.4 tem-se

$$ax + b \equiv ay + b\ (mod\ m) \Rightarrow ax \equiv ay\ (mod\ m) \Rightarrow x \equiv y\ (mod\ m) \Rightarrow$$
$$\text{x - y} \equiv 0\ (mod\ m).$$

Como $[x],\ [y] \in \mathbb{Z}_m$ vem que $|x - y| < m$. Logo, $|x - y| = 0 \Leftrightarrow [x] = [y]$ e então f é injetora. Como $\mathbb{Z}_m$ é um conjunto finito, segue-se que f é bijetora.

Reciprocamente, suponha f bijetora e seja $b = mq + r$ para algum $q \in \mathbb{Z}$ e $0 \leqslant r \leqslant m - 1$. Então $[r + 1] \in \mathbb{Z}_m$ e portanto existe $[x_0] \in \mathbb{Z}_m$, tal que $ax_0 \equiv r + 1\ (mod\ m)$ Da proposição 2.2.6 tem-se que $\mathbb{Z}_m$ é um sistema completo de resíduo módulo m. Daí $f(x_0) = ax_0 + b \equiv r + 1\ (mod\ m)$. Substituindo b e fazendo as reduções módulo m obtém-se, $ax_0 \equiv 1\ (mod\ m)$. Logo, existe $s \in \mathbb{Z}$, tal que $ms+ax_0 = 1$. Seja $d = mdc\ (a, m)$. Como d divide m e d divide a, concluímos que d divide $ms + ax_0 = 1$. Portanto, $d = 1$.

■

Exemplos 3.0.3. *1. Sejam* $A = \{1,\ 2,\ \ldots,\ 28,\ 29\}$, $B \subset \mathbb{Z}$ *e* f *a função de* A *em* B *definida por* $f(x) = 3x + 5$. *Usando* f *codifique a mensagem "FALO NADA, APENAS OBSERVO."*

(i) Inicialmente associa-se cada letra a um número em $\mathbb{Z}_{29}$, *conforme sua posição no alfabeto incluindo mais três símbolos, quais sejam, o ponto final, a vírgula e o espaço, pois assim, ao trabalhar com congruências módulo 29 que, sendo primo, facilita o trabalho na escolha do coeficiente a da função. Uma vez feitas as associações embaralha-se as letras usando* $f(x)$.

(ii) Inicia-se o procedimento trocando as letras pelos números correspondes às suas posições e obtém-se:

6 1 12 15 29 14 1 4 1 28 29 1 16 5 14 1 19 29 15 2 19 5 18 22 15 27

...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
-57	-56	-55	-54	-53	-52	-51	-50	-49	-48	-47	-46	-45	-44	-43	-42	-41	-40	-39	-38	-37	-36	-35	-34	-33	-32	-31	-30	-29
-28	-27	-26	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	,	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Tabela 3.1: Posicionamento de letras e símbolos em $\mathbb{Z}_{29}$

(iii) Agora, cifra-se a mensagem usando $f(x)$*:*

$f(6) = 3\cdot 6+5 = 18+5 = 23$*;* $f(1) = 3\cdot 1+5 = 3+5 = 8$; $f(12) = 3\cdot 12+5 = 36+5 = 41$, *e assim, sucessivamente e obtemos:* $f(15) = 50$, $f(29) = 92$; $f(14) = 47$, $f(4) = 17$, $f(28) = 89$, $f(16) = 53$, $f(19) = 62$, $f(2) = 11$, $f(18) = 59$, $f(22) = 71$, $f(27) = 86$.

Gerando assim a seguinte sequência numérica.

23 8 41 50 92 47 8 17 8 89 92 8 53 20 47 8 62 92 50 11 62 20 59 71 50 86

O emissário da mensagem pode enviar a sequência acima ao destinatário ou convertê-la numa nova sequência numérica consultando a tabela 3.1. A conversão na nova sequência é mostrada abaixo.

23	8	41	50	92	47	8	17	8	89	92	8	53	20	47	62	92	50	11	62	20	59	71	50	86
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
23	8	12	21	5	18	8	17	2	5	8	24	20	18	8	4	5	21	11	4	20	1	13	21	28

Após conversão pode enviá-la como uma sequência numérica, ou então, usando novamente a tabela 3.1, transformar a sequência de números numa sequência de letras (mostrada abaixo) para então enviá-la.

WHLUERHQHBEHXTRHDEUKDTAMU,

2. *Decodificando a mensagem do exercício 1: A decodificação, nesse caso pode ser feita de uma das três maneiras:*

(a) *Se o receptor da mensagem receber a sequência abaixo,*

23 8 41 50 92 47 8 17 8 89 92 8 53 20 47 8 62 92 50 11 62 20 59 71 50 86

usará como chave de decodificação $f(x) = 3x + 5$*, e resolverá a equação* $f(x) = y$*, onde* y *são os valores dados pela mensagem recebida.*
Então, calculando-se $f(x) = 23$, $f(x) = 8$, $f(x) = 41$, ..., $f(x) = 86$. *obtemos*
$f(x) = 23 \Rightarrow 23 = 3x + 5 \Rightarrow 18 = 3x \Rightarrow x = 6$,
$f(x) = 8 \Rightarrow 8 = 3x + 5 \Rightarrow 3 = 3x \Rightarrow x = 1$,
$f(x) = 41 \Rightarrow 41 = 3x + 5 \Rightarrow 36 = 3x \Rightarrow x = 12$. *e assim, sucessivamente, obtendo* $f(50) = 15$, $f(92) = 29$, ..., $f(86) = 27$, *que, após consultada a tabela 3.1 gera a mensagem "FALO NADA, APENAS OBSERVO."*

(b) *Recebendo a sequência de números abaixo, a chave de decodificação é a função inversa de* $f(x)$ *juntamente com a tabela 3.1.*

23 8 12 21 5 18 8 17 2 5 8 24 20 18 8 4 5 21 11 4 20 1 13 21 28

(i) *Neste caso, procede-se da seguinte maneira: obtém-se* $f^{-1}(x)$*, definida por* $f^{-1} : B \to A$*, tal que* $f^{-1}(x) = 10x + 8$. *Para obter* $f^{-1}(x)$ *faz-se:*

$$[3]x + [5] = y \Longleftrightarrow [3]x = y - [5] \Longleftrightarrow [3]x = y + [24] \ (*)$$

onde

$$[3x] = [1] \Longleftrightarrow [3] \cdot [x] = [1]$$

Para determinar o inverso de $[3]$ *em* $\mathbb{Z}_{29}$ *fazemos*

$$3x = 29q + 1$$

Por inspeção obtemos $q = 1$ *e* $x = 10$. *Daí, multiplicando* $(*)$ *por 10 obtemos*

$$x = 10y + 240 \Longleftrightarrow x = 10y + 8$$

Uma vez que $[240] = [8]$ *em* $\mathbb{Z}_{29}$. *Daí* $f^{-1}(x) = 10x + 8$.
A partir daí, basta calcular $f^{-1}(x)$ *para a sequência dada e após, con-*

sultarmos a tabela 3.1. Então,

$f^{-1}(23) = 10 \cdot 23 + 8 = 238$. *Letra* ***F*** *de acordo com a tabela;*

$f^{-1}(8) = 10 \cdot 8 + 8 = 88$. *Letra* ***A*** *de acordo com a tabela, e assim, sucessivamente, até a decodificação da mensagem.*

(ii) Caso receba a mensagem como uma sequência de letras, receberá a sequência abaixo.

$$WHLUERHQHBEHXTRHDEUKDTAMU,$$

associará cada letra à sua posição correspondente de acordo com a tabela 3.1, para, em seguida, usar a chave de decodificação, que é $f^{-1}(x)$ *(obtida no item (b), isto é,* $f^{-1}(x) = 10x + 8$. *Logo,*

23 8 12 21 5 18 8 17 2 5 8 24 20 18 8 4 5 21 11 4 20 1 13 21 28

Substituindo cada valor da sequência acima em $f^{-1}(x)$*, decodifica-se a mensagem.*

3. *Considere* $A = \{1,\ 2, \ldots,\ 29\}$*, e a função definida por*

$$f : A \to A \text{ definida por } f(x) = \begin{cases} x + 8, & \text{se } 1 \leq x \leq 21; \\ x - 21, & \text{se } 21 \leq x \leq 29. \end{cases}$$

para codificar a frase "A MATEMÁTICA É A RAINHA E A SERVA DE TODAS AS CIÊNCIAS.".

(i) Da tabela 3.1 obtém-se a seguinte sequência numérica:

1 29 13 1 20 5 13 1 20 9 3 1 29 5 29 1 29 18 1 9 14 8 1 29 5 29 1 29 19 5 18

22 1 29 4 5 29 20 15 4 1 19 29 1 19 29 3 9 5 14 3 9 1 19 27

(ii) A codificação é obtida pela f *calculando-se* $f(1)$, $f(29)$, ..., $f(27)$*, isto é,* $f(1) = 1 + 8 = 9$, $f(29) = 29 - 21 = 8$, $f(13) = 13 + 8 = 21$*, e assim, sucessivamente obtendo:*

$f(20) = 28$, $f(5) = 13$, $f(9) = 17$, $f(3) = 11$, $f(18) = 26$, $f(14) = 22$, $f(8) = 16$, $f(19) = 27$, $f(22) = 1$, $f(4) = 12$, $f(15) = 21$ *e* $f(27) = 6$.

Usando a tabela 3.1 obtém-se as seguintes sequências

9 8 21 9 28 13 21 9 28 17 11 9 8 13 8 9 8 26 9 17 22 16 9 8 13 8 9 8 27 13 26 1 9 8 12 13 8 28 23 12 9 27 8 9 27 8 11 17 13 22 11 17 9 27 6

ou,

IHUI,MUI,QKIHMHIHZIQVPIHMHIH.MZAIHLMH,WLI.HI.HKQMVKQI.F

4. *Decodificando a mensagem do exercício 3: O receptor, para decodificar a mensagem deverá proceder de uma das seguintes maneiras:*

   (a) *Recebendo a mensagem*

   9 8 21 9 28 13 21 9 28 17 11 9 8 13 8 9 8 26 9 17 22 16 9 8 13 8 9 8 27 13 26 1 9 8 12 13 8 28 23 12 9 27 8 9 27 8 11 17 13 22 11 17 9 27 6

   a chave de decodificação é a função inversa de f seguida da tabela 3.1. Inicialmente obtém-se função inversa de f, isto é, para $A = \{1,\ 2, \ldots,\ 29\}$, tem-se

$$f^{-1} : A \to A \ definida\ por\ f^{-1}(x) = \begin{cases} x + 21, & se\ 1 \leq x \leq 8; \\ x - 8, & se\ 9 \leq x \leq 29. \end{cases}$$

   Uma vez obtida f^{-1}, calcula-se $f^{-1}(9)$, $f^{-1}(8)$, $f^{-1}(21)$, ..., $f^{-1}(6)$, que são os valores recebidos na mensagem, ou seja, $f^{-1}(9) = 9 - 8 = 1$, $f^{-1}(8) = 8 + 21 = 29$, $f^{-1}(21) = 21 - 8 = 13$, e assim, sucessivamente obtendo $f^{-1}(28) = 20$, $f^{-1}(13) = 5$, $f^{-1}(17) = 9$, $f^{-1}(11) = 3$, $f^{-1}(26) = 18$, $f^{-1}(22) = 14$, $f^{-1}(16) = 8$, $f^{-1}(27) = 19$, $f^{-1}(1) = 22$, $f^{-1}(12) = 4$, $f^{-1}(23) = 15$ e $f^{-1}(6) = 27$.

   que, após consultada a tabela 3.1, retorna a mensagem original, isto é,

   "A MATEMÁTICA É A RAINHA E A SERVA DE TODAS AS CIÊNCIAS"

   (b) *Recebendo a mensagem*

   IHUI,MUI,QKIHMHIHZIQVPIHMHIH.MZAIHLMH,VLI.HI.HKILVKQI.F

a chave de decodificação é, na sequência a tabela 3.1 para transformar a sequência de letras em uma sequência numérica, segundo sua posição em $\mathbb{Z}_{29}$ *e, após, a função inversa de* f *(obtida em (a)). Efetuados tais procedimentos, calcula-se o valor correspondente de cada símbolo e transcreve-se a mensagem.*

Observação: *Os métodos apresentados acima são interessantes como introdução do conceito de* ***congruência módulo m*** *que será visto no próximo exemplo. A vantagem desses modelos criptográficos é que podemos trabalhar a decodificação da mensagem de duas formas diferentes, porém, a desvantagem está na necessidade da construção de uma tabela muito grande na maioria das vezes. Isto pode ser resolvido utilizando funções da forma* $f(x) = ax+b \ (mod\, m)$ *conforme veremos a seguir.*

5. *Considere o conjunto* $A = \{1, 2, \ldots, 28, 29\}$ *e a função* f *de* A *em* A *definida por* $f(x) = 5x + 4 \ (mod\ 29)$. *Como* $mdc\ (5, 29) = 1$ *podemos utilizá-la para codificarmos a mensagem "Penso, logo existo". Então tem-se:*

   (i) Relacionando as letras com os números correspondentes às suas posições tem-se:

   16 5 14 19 15 28 - 29 - 12 15 7 15 - 29 - 5 24 9 19 20 15 27

   (ii) Codifica-se a mensagem pela $f(x)$ *calculando* $f(16),\ f(5),\ \ldots,\ f(20),\ f(15)$ *e obtém-se* $f(16) = 5 \cdot 16 + 4 = 84 \equiv 26\ (mod\ 29),\ f(5) = 5 \cdot 5 + 4 = 29\ (mod\ 29),\ f(14) = 5 \cdot 14 + 4 = 74 \equiv 16\ (mod\ 29),\ f(19) = 5 \cdot 19 + 4 = 99 \equiv 12\ (mod\ 29),$ *segue que,* $f(15) = 79 \equiv 21\ (mod\ 29),\ f(28) = 144 \equiv 28\ (mod\ 29),\ f(29) = 149 \equiv 4\ (mod\ 29),\ f(12) = 64 \equiv 6\ (mod\ 29),\ f(7) = 39 \equiv 10\ (mod\ 29),\ f(24) = 124 \equiv 8\ (mod\ 29),\ f(9) = 49 \equiv 20\ (mod\ 29),\ f(20) = 104 \equiv 17\ (mod\ 29),\ f(27) = 139 \equiv 23\ (mod\ 29).$

   O que resulta em

   26 29 16 12 21 28 4 6 21 10 21 4 29 8 20 12 17 21 23

   Associando, agora, cada número a sua letra correspondente na tabela 3.1 gera-se a seguinte mensagem a ser enviada ao destinatário.

Z PLU,DFUJUD HTLQUW

(iii) Tal como o emissor, o destinatário terá que substituir a sequência de letras recebidas para obter o número correspondente às suas posições no alfabeto a fim de decodificar a mensagem. A sequência recebida é

26 29 16 12 21 28 4 6 21 10 21 4 29 8 20 12 17 21 23

A decodificação da mensagem é feita usando a "chave de decodificação", que nada mais é do que a função inversa de $f(x) = 5x + 4 \ (mod\ 29)$. *Ela é dada forma* $f^{-1}(x) = a'x + b' \ (mod\ m)$. *Logo:*

- *Como mdc* $(5, 29) = 1$, *pela proposição 2.2.13 existem* a', $s \in \mathbb{Z}$ *tal que* $5a' + 29s = 1$;
- *Aplicando o método das divisões sucessivas*

	5	1	4
29	5	4	1
4	1	0	

e usando algoritmo de Euclides de trás para frente tem-se

$$1 = 5 - 1 \cdot 4,$$
$$4 = 29 - 5 \cdot 5.$$

Segue que

$$1 = 5 - 1 \cdot 4 = 5 - 1 \cdot (29 - 5 \cdot 5) = 6 \cdot 3 - 1.29.$$

Portanto, uma solução de $5a' + 29s = 1$ *é* $(6, -1)$ *o que fornece* $a' = 6$. *Para determinar* b' *basta resolver a equação* $5 \cdot a + b' = 29$ *com* $a = 5$ *o que resulta em* $b' = 5$. *Daí*

$$f^{-1}(x) = 6x + 5.$$

De fato,

$(f \circ f^{-1})(x) = 5 \cdot (6x+5)+4 \ (mod\ 29) = 30x+29 \ (mod\ 29) = x \ (mod\ 29)$

$(f^{-1}\circ f)(x) = 6\cdot(5x+4)+5\ (mod\ 29) = 30x+29\ (mod\ 29) = x\ (mod\ 29)$

isto é, $f \circ f^{-1} = f^{-1} \circ f = I$

- *Aplicando* f^{-1} *na sequência acima obtém-se* $f^{-1}(26) = 6 \cdot 26 + 5 = 156+5 = 161 \equiv 16\ (mod\ 29)$, $f^{-1}(29) = 6\cdot 29+5 = 174+5 = 179 \equiv 5\ (mod\ 29)$, $f^{-1}(16) = 6 \cdot 16 + 5 = 96 + 5 = 101 \equiv 14\ (mod\ 29)$. *Segue que,* $f^{-1}(12) = 19$, $f^{-1}(21) = 15$, $f^{-1}(28) = 28$, $f^{-1}(4) = 29$. $f^{-1}(6) = 12$, $f^{-1}(10) = 10$, $f^{-1}(8) = 24$, $f^{-1}(20) = 9$, $f^{-1}(17) = 20$, $f^{-1}(23) = 27$.

  Após os cálculos substitui-se os números pelas letras correspondentes e obtém-se a mensagem.

3.0.5 Cifrário por função quadrática

Neste modelo de codificação utiliza-se funções da forma $f(x) = x^2 + bx + c$, porém deve-se estabelecer algumas condições em seu domínio, uma vez que as funções de segundo grau não são injetoras.

Lema 3.0.17. *Sejam* $a,\ b,\ c \subset \mathbb{Z}$ *com* $a > 0$. *A função* $f : \left[\frac{-b}{2a},\ \infty\right) \to \left[\frac{-\Delta}{4a},\ \infty\right)$, *definida por* $f(x) = ax^2 + bx + c$ *é bijetora.*

Demonstração

(i) Provemos que f é injetora. Note que

$$f(x) = ax^2 + bx + c = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = a\left(x^2 + \frac{b}{a}x + \frac{c}{a} + \frac{b^2}{4a^2} - \frac{b^2}{4a^2}\right) =$$

$$= a\left[\left(x + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2}\right] = a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a} = a\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a}.$$

Daí, para $x_1,\ x_2 \in [\frac{-b}{2a}, \infty)$, tem-se

$$f(x_1) = f(x_2) \iff a\left(x_1 + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a} = a\left(x_2 + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a} \iff$$

$$a\left(x_1 + \frac{b}{2a}\right)^2 = a\left(x_2 + \frac{b}{2a}\right)^2 \iff \left(x_1 + \frac{b}{2a}\right)^2 = \left(x_2 + \frac{b}{2a}\right)^2.$$

Como $x_1,\ x_2 \geq \dfrac{-b}{2a}$ então $x_1 + \dfrac{b}{2a} \geq 0$ e $x_2 + \dfrac{b}{2a} \geq 0$. Logo, pode-se escrever

$$f(x_1) = f(x_2) \iff \left(x_1 + \frac{b}{2a}\right)^2 = \left(x_2 + \frac{b}{2a}\right)^2 \iff x_1 + \frac{b}{2a} = x_2 + \frac{b}{2a} \iff x_1 = x_2.$$

De onde conclui-se que f é injetora.

(ii) Provemos agora que f é sobrejetora. De fato, dado $y \in [\frac{-\Delta}{4a}, \infty)$ existe

$$x = \sqrt{\frac{1}{a}\left(y + \frac{\Delta}{4a}\right)} \ - \ \frac{b}{2a} \mid f(x) = a\left(\sqrt{\frac{1}{a}\left(y + \frac{\Delta}{4a}\right)} \ - \ \frac{b}{2a} + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a}$$

$$= a\left(\sqrt{\frac{1}{a}\left(y + \frac{\Delta}{4a}\right)}\ \right)^2 - \frac{\Delta}{4a} = a\left(\frac{1}{a}\left(y + \frac{\Delta}{4a}\right)\right) - \frac{\Delta}{4a} = y.$$

Logo, f é sobrejetora. De *(i)* e *(ii)* conclui-se que f é bijetora. ■

Exemplos 3.0.4. *Sejam $A = \{1,\ 2,\ 3,\ \ldots,\ 29\}$ e B, convenientemente escolhido, e a função $f : A \to B$ definida por $f(x) = x^2 + 6x + 8$. Usando $f(x)$, codificamos a mensagem "FALO NADA, APENAS OBSERVO.".*

(i) Como $A \subset [-3, \infty)$, e $B \subset [-1, \infty)$ segue do lema 3.0.17 que f é bijetora. Logo, podemos relacionar cada letra com o número de sua respectiva posição e obtemos a sequência a seguir:

6 1 12 15 29 14 1 4 1 28 29 1 16 5 14 1 19 29 15 2 19 5 18 22 15 27

(ii) Aplicando $f(x) = x^2 + 6x + 8$ na sequência acima obtemos:
$f(6) = 6^2 + 6\cdot 6 + 8 = 36 + 36 + 8 = 80$, $f(1) = 1^2 + 6\cdot 1 + 8 = 1 + 6 + 8 = 15$, $f(12) = 12^2 + 6\cdot 12 + 8 = 144 + 72 + 8 = 224$, *continuando os cálculos de f temos* $f(15) = 325$, $f(29) = 1023$, $f(14) = 288$, $f(4) = 48$, $f(28) = 960$, $f(16) = 360$, $f(5) = 63$, $f(19) = 483$, $f(2) = 24$, $f(18) = 440$, $f(22) = 624$, $f(27) = 899$, *que gera a seguinte sequência:*

63 15 224 325 1023 288 15 48 15 960 1023 15 360 63 288 15 483 1023 325 24 483 63 440 624 325 899.

Agora é só enviar a mensagem ao destinatário que poderá escolher uma das duas chaves para decifrar a mensagem, quais sejam, ele conhece $f(x)$ e, a partir daí, resolve as equações $f(x) = y$, ou usa a função inversa de $f(x)$.

(iii) Resolvendo as equações $f(x) = y$. Neste caso, $f(x) = 80$, $f(x) = 15$, ..., $f(x) = 899$. Calculando temos:

$f(x) = 80 \Rightarrow x^2 + 6x + 8 = 80 \Rightarrow x^2 + 6x - 72 = 0$,

$\Delta = 6^2 - 4 \cdot 1 \cdot (-72) = 36 + 288 = 324$,

$x = \dfrac{-6 \pm 18}{2}$ *o que fornece $x_1 = 6$ e $x_2 = -12$. Como $-12 \notin B$ considera-se apenas $x_1 = 6$. Procedendo desta forma, decifra-se a mensagem recebida.*

(iv) Utilizando a função inversa de $f(x)$, isto é, $f^{-1} : B \to A$ em que

$y = x^2 + 6x + 8 = x^2 + 6x + 9 - 1 = (x + 3)^2 - 1 \Rightarrow y + 1 = (x + 3)^2 \Rightarrow x + 3 = \sqrt{y + 1} \Rightarrow x = \sqrt{y + 1} - 3$, *ou ainda,*

$$f^{-1}(x) = \sqrt{x + 1} - 3.$$

Portanto, a sequência

63 15 224 325 1023 288 15 48 15 960 1023 15 360 63 288 15 483 1023 325 24 483 63 440 624 325 899

é levada em

6 1 12 15 29 14 1 4 1 28 29 1 16 5 14 1 19 29 15 2 19 5 18 22 15 27

que corresponde à frase "FALO NADA, APENAS OBSERVO."

Os exemplos acima ilustram como a criptografia pode ser um bom exemplo de adaptação entre teoria e prática, pois faz parte da vivência do aluno enquanto usuário da internet. Deve ser ressaltado o problema que surge ao se tentar trabalhar as funções quadráticas juntamente com as classes residuais, uma vez que, congruências do tipo

$$x^2 \equiv a \ (mod\ m) \ com\ a,\ m \in \mathbb{N}\ e\ m > 1$$

nem sempre tem solução. Por exemplo, $6^2 = 36 \equiv 7 \equiv 529 = 23^2$ $(mod\ 29)$ o que retorna, na decodificação em duas letras diferentes, isto é, pela tabela utilizada o número 6 corresponde à letra F enquanto que o número 23 à letra W o que pode causar um erro de leitura.

Capítulo 4

Conclusão

Saber enfrentar os desafios diários de uma sala de aula é papel fundamental do professor. Encontrar meios que ultrapassem a barreira do desinteresse e que motivem os alunos a participarem de forma mais produtiva durante a aula, de forma a melhorar a aprendizagem da sala como um todo e não simplesmente da minoria mais capaz, é uma arte considerável.

Buscar novos métodos de ensino, de tal forma a aproximar o conteúdo da aula à vivência do aluno, talvez seja uma das soluções para minimizar o problema.

O que torna a criptografia interessante como elemento de estudo é que, além de sua história, que pode ser usada para ilustrar a aula, está repleta de conceitos matemáticos, alguns mais simples, outros mais complexos. Cabe ao professor enquadrar, de acordo com o tema a ser abordado na aula, qual modelo criptográfico vai usar. Conforme visto, ao cifrar uma mensagem pra enviá-la a um destinatário, de tal forma que somente este possa lê-la, usamos um procedimento e cabe ao destinatário fazer o processo inverso. Desta forma, fica evidente a necessidade das operações inversas.

A cítala espartana, apesar de não ter recebido maior atenção no trabalho, é uma boa opção para trabalharmos com o aluno o conceito de matrizes e até mesmo geometria, pois usa um bastão para criptografar a mensagem.

Usada por Júlio Caesar nas campanas militares do exército romano, a cifragem de mensagens através do deslocamento das letras no alfabeto acabou ganhando o nome de Código Caesar e pode ser usada para explorar temas como função (em

destaque para as polinomiais) na codificação e função inversa na decodificação. Avançando um pouco mais, é possível explorar temas como congruência e classe residual. Isto pôde ser observado no decorrer do presente trabalho.

Os exemplos mostrados nos dá uma ideia de como codificar uma função de 1º grau e de como o professor pode desenvolver com o aluno a resolução de equações do tipo "$f(x) = y$" ou, no caso de uma turma mais avançada, resolver a função inversa de "$f(x)$", que é a chave de decodificação, para depois decodificar a mensagem.

Também pudemos perceber, que, ao usarmos funções do tipo "$f(x) = ax + b\ (mod\ m)$" na codificação de uma mensagem, a decodificação só é possível após a determinação da função inversa de "$f(x)$". Funções da forma $f(x) = ax^2 + bx + c$ podem ser usadas, mas tomando-se o cuidado na determinação dos coeficientes $a,\ b,\ c$ da função, uma vez que a mesma, deve ser bijetora. Já, funções da forma $f(x) = ax^2 + bx + c\ (mod\ m)$ devem ser evitas pois não são injetoras.

Conforme se observa, a criptografia é um tema fascinante que permite ao professor desenvolver assuntos, muitas vezes de difícil compreensão pelos alunos, além do que, desperta a curiosidade dos mesmos, pelo fato de estarem o tempo todo ligados na internet a qual, depende de maneira fundamental da criptografia para garantir a segurança de mensagens que trafegam pela rede.

Referências Bibliográficas

[1] HEFEZ, Abramo. Elementos de aritmética.2.ed. Rio de Janeiro: *SBM*, 2011. 176p. (Coleção do Professor de Matemática)

[2] HEFEZ, Abramo. Curso de álgebra v.1. Rio de Janeiro: *IMPA*, 1993. 226p. (Coleção Universitária)

[3] DOMINGUES, Hugino H; IEZZI, Gelson. Álgebra moderna.4.ed. São Paulo: *ATUAL*, 2003. 368p.

[4] IEZZI, Gelson et al. Fundamentos de matemática elementar.Conjuntos e funções.ed. São Paulo: *ATUAL*, 1993. 317p.

[5] SILVA, Aparecida F. da; SANTOS, Clotilzio M. dos. Aspectos formais da computação. São Paulo: *UNESP*, 2009. Campus de São José do Rio Preto.

[6] SILVA, Eduardo Gomes da. Explorando vertentes matemáticas nos códigos de barras. 2013. 55 f. Dissertação (mestrado) - Universidade Estadual Paulista Julio de Mesquita Filho. Instituto de Biociências, Letras e Ciências Exatas, 2013. Disponível em: <http://hdl.handle.net/11449/88591>. (Acesso em 25 jan. 2016)

[7] COUTINHO, Severino C. Criptografia (Distribuição IMPA/OBMEP). Disponível em:<http://www.obmep.org.br/docs/apostila7.pdf> (Acesso em 01 de fev. 2017)

[8] SÔNEGO, Dubes. A admirável aritmética do relógio e do calendário. **Cálculo** São Paulo: *SEGMENTO*, ano 5, edição 53, p.20-33, jun.2015.

[9] COSTA JUNIOR, Edson M., VIEIRA, Marcelo L., CAETANO, Natália G. A criptografia em sala de aula. **RPM** Rio de Janeiro: *SBM*, ano 34, edição 89, p.32-34, 1º quadrimestre de 2016.

[10] SANTOS, José P. de O. Introdução à Teoria dos Números.3.ed. Rio de Janeiro: *IMPA*, 2015. 196p.

[11] WIKIPÉDIA. (A enciclopédia livre). Disponível em:<https://pt.wikipedia.org/> (Acesso em 15 de fev. 2016)

[12] BIASE, Adrile G., AGUSTINI, Edson. Criptografias ElGamal, Rabin e algumas técnicas de ciframento. **FAMAT em Revista** Uberlândia-MG: *UFU*, ano 6, edição 13.dez. 2009. Disponível em: <http://www.portal.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/FAMAT_Revista_13_1.pdf>. (Acesso em jul. 2017)