UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

JEAN MENDES JANSEN

CRIPTOGRAFIA: Uma Abordagem Para o Ensino Médio

São Luís-MA
2016

JEAN MENDES JANSEN

CRIPTOGRAFIA: Uma Abordagem Para o Ensino Médio

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade Federal do Maranhão, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. João Coelho Silva Filho

São Luís-MA

2016

Jansen, Jean Mendes.

CRIPTOGRAFIA: Uma Abordagem Para o Ensino Médio / Jean Mendes Jansen. - São Luis, 2016.

81 p.

Orientador: João Coelho Silva Filho.

Dissertação (Mestrado) - Universidade Federal do Maranhão, Programa de Mestrado Profissional em Matemática em Rede Nacional, 2016.

1. Criptografia. 2. Funções. 3. Matrizes. 4. Teoria dos Números. I. Filho, João Coelho Silva. II. Título.

CDU

JEAN MENDES JANSEN

CRIPTOGRAFIA: Uma Abordagem Para o Ensino Médio

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade Federal do Maranhão, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Aprovado em 06/10/2016.

BANCA EXAMINADORA

Prof. Dr. João Coelho Silva Filho (Orientador)

Universidade Estadual do Maranhão

Prof. Dr. Félix Silva Costa

Universidade Estadual do Maranhão

Prof.ª Dra. Valeska Martins de Souza

Universidade Federal do Maranhão

À minha família e amigos presentes na minha vida.

AGRADECIMENTOS

À minha família e amigos, por compreender a minha ausência durante o curso.

Ao PROFMAT, um programa de suma importância na qualificação de docentes do nosso País.

Aos professores do PROFMAT, pela dedicação e empenho durante todo o curso.

Ao meu orientador Prof. Dr. João Coelho Silva Filho, pela sugestão do tema e observações durante o trabalho.

Aos meus colegas de turma, pela convivência durante esses dois anos.

"A engenhosidade humana não pode arquitetar uma escrita secreta que a própria engenhosidade humana não possa resolver".

Edgar Allan Poe

RESUMO

O trabalho versa sobre a Criptografia em uma abordagem para o Ensino Médio com finalidade de facilitar e estimular a aprendizagem de conteúdos matemáticos através de aplicações práticas e modernas. É abordado sobre o conceito de criptografia e parte da variedade de métodos de encriptação e desencriptação de mensagens, bem como sua importância nos dias atuais. Além disso, são apresentados conceitos e classificações matemáticas de Funções, Matrizes e noções de Teoria dos Números, que são aplicados aos sistemas criptográficos.

Palavras-chaves: Criptografia. Funções. Matrizes. Teoria dos Números

ABSTRACT

It is about Cryptography for High School students and the primary purpose of this study is to facilitate and to encourage teenagers to learn Mathematics topics using practical and modern applications. In this thesis, it will be showed the concept of Cryptography, part of a variety of message encryption and decryption methods as well as its importance today. Then it will be presented some valuable Mathematical contents, such as Functions, Matrices, and some notions in Number Theory applied to cryptographic systems.

Keywords: Cryptography. Functions. Matrices. Number Theory.

SUMÁRIO

Lista de Figuras

Lista de Tabelas

CAPÍTULO 1

INTRODUÇÃO

A presente dissertação tem como objetivo despertar o interesse dos alunos do Ensino Médio para o aprendizado de Matemática, através da utilização de conceitos básicos deste componente curricular, em situações cotidianas que envolvam a segurança no envio e recebimento de dados e informações.

A opção por esta relevante temática surgiu da necessidade, evidenciada também pelos alunos, de estudar conceitos e definições da disciplina que pudessem de alguma forma aprimorar para as gerações futuras, sem, contudo necessitar de equipamentos tecnológicos de última geração ou que demandassem custos extras.

Tem-se verificado um enorme preconceito em relação ao aprendizado de Matemática, passado de geração para geração, por simplesmente enxergá-la somente dentro da sala de aula, como uma disciplina hermética em si mesma, desprezando suas importantes aplicações na vida real e o seu amplo poder de revolucionar o mundo.

Alia-se a isso o importante momento em que se está vivendo, em que a comunicação e a tecnologia têm ganhado especial destaque, principalmente entre os jovens, através das inúmeras redes sociais, com a utilização em demasia da internet e a não menos importante exposição a que estão sendo submetidos.

A proteção da informação na atualidade tem sido matéria de destaque em vários estudos pelo mundo. Pois desde os primórdios, o homem já sentia a necessidade de guardar segredo para lograr êxito em suas empreitadas. A História mostra que pessoas importantes, como reis, imperadores, entre outros conseguiram aumentar seu domínio, ou mesmo diminuí-lo, durante o processo de transmissão e recebimento de suas mensagens.

De lá para cá, são muitos os códigos utilizados tanto para encriptar quanto para desencriptar informações. Máquinas foram criadas com o objetivo de dificultar a interceptação de mensagens e, outras, justamente para interceptá-las. O fato é que nenhum dado está integralmente seguro, pois a qualquer momento pode surgir um algoritmo mais moderno capaz de superá-lo.

Então, sabendo-se que na atualidade a rede de computadores mundial interliga pessoas de qualquer parte do globo, e é capaz de fazê-lo em poucos segundos, e ainda que governos e empresas se utilizam desse meio para guardar e compartilhar informações preciosas, fica ainda mais evidente que a proteção desses códigos é ferramenta crucial para evitar fraudes e furtos, uma vez que o vazamento dessas informações e dados, que são estratégicos, podem destruir um país, um governo ou mesmo inúmeras pessoas físicas.

Além disso, o artigo 3º, inciso II, da Lei 12.965/14, a Lei 12.737/12, também conhecida como lei Carolina Dieckmann, e também o artigo 5º, inciso X, da Constituição Federal de 1988, garantem, expressamente, a proteção da privacidade e denotam a importância que o Governo Brasileiro tem dado às questões relacionadas à violação e ao compartilhamento de informações privadas.

Para tal, a Ciência da Matemática vem sendo amplamente utilizada, não só para tornar esse processo de decodificação extremamente impossível, pelo máximo de tempo possível, como também para fazer o efeito inverso que é, no mais curto espaço de tempo, ter acesso ao conteúdo ocultado.

Logo, objetiva-se com esse trabalho, através de simples aplicações matemáticas e em consonância com o que se pretende nos Parâmetros Curriculares Nacionais, fazer com que o aluno compreenda conceitos, procedimentos e estratégias matemáticas que permita o desenvolvimento de estudos posteriores, como a criptografia, por exemplo, e a obtenção de uma formação científica geral, além da aplicação de tais conhecimentos na vida cotidiana, na interpretação da ciência e da atividade tecnológica.

> No ensino da Matemática, destacam-se dois aspectos básicos: um consiste em relacionar observações do mundo real com representações (esquemas, tabelas, figuras); outro consiste em relacionar essas representações com princípios e conceitos matemáticos. Nesse processo, a comunicação tem grande importância e deve ser estimulada, levando-se o aluno a falar e a escrever sobre Matemática, a trabalhar com representações gráficas, desenhos, construções, a aprender como organizar e tratar dados. [...] O significado da Matemática para o aluno resulta das conexões que ele estabelece entre ela e as demais disciplinas, entre ela e seu cotidiano e das conexões que ele estabelece entre os diferentes temas matemáticos. (BRASIL, 2007, p.19).

A união entre um tema moderno, que está constantemente na mídia e que envolve softwares diversificados utilizados pelos adolescentes e jovens, diuturnamente, como o *Whatsapp, Facebook, Instagram*, e a utilização de cálculos matemáticos que possibilitem de alguma forma entender e até mesmo aprimorar os métodos de codificação e decodificação existentes, é a receita ideal para que se consiga êxito dentro e fora da sala de aula.

Afinal, o objetivo de todo professor não é tão somente fazer com que o aluno compreenda aquilo que está sendo repassado, mas, principalmente, despertar nele o desejo de transformar o mundo à sua volta, através do entendimento e elaboração de conceitos, do seu desenvolvimento e, por que não, de sua mudança.

Não se quer, como alguns pensam, reproduzir o *status quo*, nem tampouco ensinar verdades aos alunos. O professor só quer que os alunos consigam pensar e raciocinar por si sós. Na verdade, não cabe ao professor ensinar, mas incentivar a pesquisa, o questionamento e a busca pelo conhecimento real que, aliás, são as melhores e mais eficazes ferramentas para o saber.

Para isso, serão apresentados no decorrer deste trabalho, assuntos pertinentes à Criptografia com uma abordagem para o Ensino Médio. No segundo capítulo, falar-se-á sobre a Criptografia ao longo do tempo, enfatizando conceitos básicos de criptografia, sua evolução, as cifras de substituição, o Código de César, a cifra de Vigenère, a cifra de Hill, o disco de cifras e o sistema RSA, [1], [3], [5] e [16].

No terceiro capítulo, a ênfase será para os Fundamentos Matemáticos que serão utilizados no desenvolvimento deste trabalho, a saber: função afim, função quadrática, função exponencial, função logarítmica, função inversa, matrizes e alguns tópicos da Teoria dos Números, [8], [9], [10], [11] e [15].

No quarto capítulo , serão apresentados exemplos de codificações e decodificações de mensagens usando as funções e as matrizes estudadas no capítulo anterior, dando ênfase aos cálculos, propriamente ditos, de funções codificadoras e de suas inversas, decodificadoras.

No quinto capítulo, serão propostas algumas atividades para os alunos do Ensino Médio desenvolverem, em sala de aula ou mesmo em casa, de posse do conhecimento dos capítulos anteriores, contemplando a aplicação de todos os assuntos que foram aqui abordados.

E, por fim, será apresentado um compêndio das soluções das atividades propostas que

servirá de apoio para o esclarecimento de dúvidas que porventura possam surgir ao longo de sua feitura, visando uma aprendizagem contextualizada e significativa.

CAPÍTULO 2

CRIPTOGRAFIA AO LONGO DO TEMPO

A palavra criptografia vem do grego *kryptós* que significa escondido, oculto e *graphé*, escrita. Logo, nada mais é do que uma escrita oculta, ou seja, qualquer mensagem que exija um processo de decifração para ser compreendida.

Ao contrário do que a maioria pensa, a criptografia não é um recurso moderno, pois há registros bem antigos de sua utilização, como os hieróglifos, que exigiam uma profunda interpretação dos interlocutores.

Os hebreus, no ano 600 a.C., foram os primeiros a utilizarem a criptografia por meio de substituição monoalfabética, em que um determinado símbolo do alfabeto é substituído por outro cifrado, como a cifra Atbash em que a primeira letra é substituída pela última, a segunda pela penúltima, a terceira pela antepenúltima, e assim por diante.

Entretanto, por volta de 800 d.C., o matemático árabe (Ibrahim Al-Kadi- 1992), desenvolveu uma técnica capaz de quebrar tais cifras, além de expor diferentes métodos de cifragem, dentre elas, a criptoanálise e a análise de letras e combinações árabes.

Alexander Weekly escreveu, após o início da I Guerra Mundial, um ensaio sobre métodos de criptografia que auxiliaram os britânicos na quebra dos códigos e cifras alemães e escreveu também o famoso conto O Escaravelho de Ouro(Século XIX), baseado na criptoanálise.

Alguns exemplos importantes de decodificação de mensagens daquela época foi o telegrama de Zimmermann que acelerou a entrada dos Estados Unidos na I Guerra Mundial. Já na II Guerra Mundial, os alemães utilizaram uma máquina eletromecânica para criptografar e descriptografar mensagens, ENIGMA, porém matemáticos e mestres de xadrez

britânicos conseguiram quebrar as cifras e decifrar as mensagens dos nazistas.

Outros mecanismos foram criados na chamada Guerra Fria, como a chave simétrica, chave assimétrica, hash, criptografia quântica, entre outros. Sabe-se que o objetivo de tal recurso é notadamente a preservação da segurança do conteúdo da mensagem e, hoje, é bem utilizado na internet, em especial, no que tange às transações financeiras.Uma leitura precisa desse conteúdo são encontrados em, [1], [3] e [16].

2.1 Cifras de substituição

Como o próprio nome sugere, cifras de substituição nada mais são do que substituições de letras do texto original, podendo aparecer de forma individual ou em grupos de comprimento constante, por outras letras, símbolos ou uma combinação de letras e símbolos, anteriormente acordados entre os verdadeiros interlocutores da mensagem, e uma chave. Elas podem ser: monoalfabéticas, polialfabéticas, poligrâmicas, monogrâmicas ou simples, homofônicas e tomográficas.

O sistema monoalfabético, mais antigo, substitui cada um dos caracteres de um texto por outros caracteres, satisfazendo uma tabela previamente acordada, também chamada de cifrantes ou alfabetos cifrantes. O sistema polialfabético, por sua vez, utiliza dois ou mais cifrantes.

Diz-se substituição poligrâmica ou multilaterais, aquela em que grupos de letras são substituídos por outro grupo de letras, não necessariamente do mesmo tamanho da mensagem original, sendo também chamadas de digrâmicas ou bilaterais (grupos de duas letras ou símbolos), trigâmicas ou trilaterais, etc. As monogrâmicas ou unilaterais são aquelas em que cada um dos caracteres é substituído por um outro, ficando o comprimento da mensagem original igual ao da cifrada e a frequência de ocorrência das letras também. Como exemplo desta última, podemos citar Atbash e o Código de César (caso específico que será estudado na subseção 2.1.1).

Dentre as substituições monoalfabéticas poligrâmicas, tem-se a homofônicas, que têm o mesmo som, ou seja, sequências diferentes pronunciadas de forma semelhante e, apesar de ter vários substitutos para cada um dos caracteres, o comprimento de ambas as mensagens é o mesmo. A citar como exemplo a cifra de Babou, [16].

Os sistemas tomográficos ou tomogrâmicos são aqueles em que cada caractere é subs-

tituído por um grupo de duas ou mais letras e números e, obviamente, o comprimento do criptograma é maior do que o original. Como exemplo, tem-se: Código Políbio e a cifra de Bacon, [16].

2.1.1 Código de César

O Código de César, nome dado em homenagem à Júlio César (militar e importante governante romano) por utilizar tal código no envio de mensagens a seus generais, era um código de substituição simples, conforme já dito anteriormente, que consistia na troca de cada letra da mensagem original por outra correspondente a três posições à sua frente.

Na verdade, também se chamava Código de César, qualquer outra substituição de letra por outra a uma determinada distância fixa. Logo, como o alfabeto brasileiro possui 26 (vinte e seis) letras, há 26 (vinte e seis) maneiras distintas de cifrar a mesma mensagem, lembrando que apenas a de deslocamento zero deixará a mensagem cifrada igual à original.

Vale lembrar que naquela época a maioria dos inimigos de César eram analfabetos ou não conheciam a sua língua, o que conferia certo grau de segurança a essas mensagens. Entretanto, sabendo-se que o código de César era o utilizado, conseguia-se facilmente, mesmo utilizando a força bruta, decifrar a mensagem. Veja [16] e [17], para maiores detalhes.

2.1.2 Cifra de Vigenère

Blaise de Vigenère foi um diplomata francês que viveu entre 1523 e 1596 e que abandonou sua carreira para dedicar-se exclusivamente aos estudos relacionados à criptografia.

Para desenvolver sua cifra, utilizou a cifra de substituição polialfabética com palavra-chave, apresentando as Carreiras de Vigenère, uma tabela de alfabetos cifrantes. Em outras palavras, ele aperfeiçoou métodos já propostos como o Código de César, por exemplo, e, em seguida, publicou sua nova cifra em seu livro O *Traité dês chiffres* ou *secretes manières d'escrire* (1586), explicando-a detalhadamente.

A imagem das Carreiras de Vigenère, Figura 2.1, é similar ao Código de César. A diferença consiste numa espécie de codificação envolvendo uma palavra-chave, que pode ser uma letra, uma palavra ou uma frase, que, por sua vez, poderá ter o mesmo tamanho da mensagem original ou, sendo menor, deverá ter cada símbolo acrescentado respectivamente

até que se alcance tal tamanho. A posição de cada símbolo da chave designará a linha e a coluna será representada pelo correspondente símbolo da mensagem original, ou seja, uma espécie de jogo de batalha-naval.

ALFABETO	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
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	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

Figura 2.1: O Quadro de Vigenère.

Como exemplo, a seguinte mensagem: **EU AMO CIFRAS** e uma palavra-chave: **PAZ**, encontrada na Tabela 2.1.

Mensagem original	E	U	A	M	O	C	I	F	R	A	S
Palavra-chave	P	A	Z	P	A	Z	P	A	Z	P	A
Mensagem cifrada	T	U	Z	B	O	B	X	F	Q	P	S

Tabela 2.1: Quadrado de Vigenère.

Para Simon Singh, em seu livro "O livro dos Códigos" [16]: A Ciência do Sigilo - do Antigo Egito à Criptografia Quântica, o Código de Vigenére é uma forma final desenvolvida a partir dos trabalhos do italiano Leone Battista Alberti, criador da primeira máquina criptográfica.

A cifra de Vigenère, como se viu, é fundamentada no uso periódico da chave. Conhecendo-se o tamanho da chave, é possível dividi-la em blocos e analisar a frequência das letras, posição por posição. Logo, a cifra em análise era mais segura na utilização de mensagens pequenas e chaves de tamanho igual ao da mensagem original e, quando geradas ao acaso, tornavam a decodificação praticamente impossível.

2.1.3 Cifras de Hill

A cifra de Hill é um sistema criptográfico que utiliza a transformação matricial para a substituição e aplica alguns conceitos de álgebra e álgebra linear. Foi introduzida por Lester S. Hill(1929), daí o seu nome, e é caracterizado como um cripto-sistema de substituição polialfabética. Não apresentou muita segurança, já que um método para desvendá-la foi rapidamente desenvolvido.

″N-Cifra de Hill″ é o nome que se dá à mensagem codificada utilizando este método. Portanto, caso a matriz utilizada seja 3×3, dar-se-á o nome de ″3-cifra de Hill″. Quanto ao procedimento, consiste em fazer ″m″ combinações lineares dos ″n″ caracteres do texto plano, produzindo ″m″ caracteres do texto criptografado.

Em outras palavras, excetuando-se o caractere ″Z″, cada letra dos textos, original e cifrado, tem o valor que especifica sua posição no alfabeto padrão. À letra ″Z″, dá-se o valor de zero (0), apresentado na Tabela 2.2.

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	0

Tabela 2.2: Cifras de Hill.

2.2 Disco de cifras

O disco de cifras nada mais é do que um misturador que transforma a letra do texto original em letra do texto cifrado. Seu inventor sugeriu que a disposição do disco fosse alterada durante uma mensagem, gerando uma cifra polialfabética, dificultando ainda

mais a sua decodificação ao mudar o modo de mistura durante o processo de cifragem.

Sua concepção básica consiste de dois discos com diâmetros diferentes que são montados de forma concêntrica, onde as escalas com o alfabeto são gravados e, ao movê-los em torno do eixo comum, relacionam-se entre si, permitindo a mudança de cifras de uma forma prática e fácil.

Figura 2.2: Disco de cifras de Cesar.

O disco de cifras de Leone Battista Alberti influenciou algumas outras pessoas a empregar o seu conceito de codificação assistida, como o inventado pelo então Secretário de Estado Americano, Thomas Jefferson, em 1795. Tal máquina consistia em vinte e cinco (25) discos de madeira que giravam em torno de um eixo comum, sendo cada uma delas gravada com as vinte e seis (26) letras do alfabeto, de forma aleatória.

Figura 2.3: Disco de cifras de Thomas Jefferson.

2.3 Sistema RSA

O sistema RSA foi inventado por Ron L. Rivest, Adi Shamir e Len Adleman, em 1978, quando trabalhavam no Massachussets Institute of Technology (M.I.T.) e se baseia em algoritmos computacionais utilizando a chave pública. As letras RSA correspondem às iniciais dos inventores deste código. Dentre os diversos métodos criptográficos, o RSA é um dos mais conhecidos e mais utilizados, em especial, na internet, através do comércio eletrônico, das mensagens de e-mail, entre outros.

O método criptográfico de chave pública permite que qualquer usuário codifique mensagens. Entretanto, somente o destinatário legítimo poderá decodificá-las através da chave secreta de decodificação. Também chamado de assimétrico, pois uma chave é secreta ou privada e a outra, pública. O Netscape é o exemplo mais comum de software de navegação que utilizava tal sistema. Hoje, o Netscape sobrevive no código-fonte do Mozilla Firefox.

O RSA foi desenvolvido tomando por base um antigo problema matemático que era o de obter os fatores primos de um determinado número. Ele explora essa situação ao utilizar um número, que atualmente supera os 1024 e mesmo os 2048 bits, e que é o produto de dois números primos muito grandes. A dificuldade de quebra do código reside na impossibilidade, computacionalmente impraticável de, a partir de uma chave pública, determinar-se a chave privada correspondente.

Em outras palavras, o sistema RSA consiste na multiplicação de dois números primos para se obter um terceiro número, tarefa relativamente fácil. Entretanto, a dificuldade está em se recuperar os dois números primos a partir deste terceiro número, em especial, quando este for grande o bastante, o que ensejará em uma quantidade de tempo considerável para recuperá-lo. Eis o antigo problema de fatoração de números grandes.

Logo, não há o que se temer em publicar a chave pública, pois esta não comprometerá a segurança da mensagem original. Entretanto, há de se proteger, obviamente, a chave privada secreta. Resta então reafirmar que o método RSA, entre vários outros códigos, é o mais utilizado em aplicações comerciais e que tem como vantagem, por ser de chave pública, acabar com o sistema de distribuição de chaves.

É evidente que não se pode afirmar que, como qualquer outro método criptográfico, este código seja inquebrável em curto espaço de tempo. Apesar de ser um dos mais seguros atualmente, nada impede de que alguém crie um novo algoritmo capaz de fatorar estes

números primos em um tempo relativamente pequeno. Até lá, continuar-se-á utilizando tal método. Uma descrição detalhada do RSA é encontrada em [5] e [16].

CAPÍTULO 3

FUNDAMENTOS MATEMÁTICOS

Neste capítulo será abordado fundamentos matemáticos necessários para uma melhor compreensão deste trabalho.

3.1 Função afim

Definição 3.1. Uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ chama-se *função afim* quando existem constantes a e b reais, com $a \neq 0$, tal que

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

para todo x real, onde a constante a é chamada de coeficiente de x, e a constante b é chamada de termo independente da função.

No caso de $b = 0$, a função afim $y = ax + b$ se transforma na função linear $y = ax$. Assim, pode-se dizer que a função linear é um caso particular da função afim.

3.1.1 Gráfico da função afim

Teorema 3.1. O gráfico cartesiano da função $f(x) = ax + b$, com $a \neq 0$, é uma reta.
Demonstração: sejam A, B e C três pontos quaisquer, distintos dois a dois, do gráfico cartesiano da função $y = ax + b$, com $a \neq 0$, cujas coordenadas cartersianas são (x_1, y_1), (x_2, y_2) e (x_3, y_3), repectivamente.

Para provar que o gráfico da função é uma reta, basta mostrar que os pontos A, B e C pertencem a mesma reta.

Note que,

$$A = (x_1, y_1) \in f \Rightarrow y_1 = ax_1 + b \quad \text{(I)};$$

$$B = (x_2, y_2) \in f \Rightarrow y_2 = ax_2 + b \quad \text{(II)};$$

$$C = (x_3, y_3) \in f \Rightarrow y_3 = ax_3 + b \quad \text{(III)}.$$

Subtraindo a igualdade (II) da igualdade (I), resulta

$$y_2 - y_1 = a(x_2 - x_1) \Longrightarrow a = \frac{y_2 - y_1}{x_2 - x_1}.$$

Subtraindo a igualdade (III) da igualdade (II), resulta

$$y_3 - y_2 = a(x_3 - x_2) \Longrightarrow a = \frac{y_3 - y_2}{x_3 - x_2}.$$

Assim,

$$\frac{y_2 - y_1}{x_2 - x_1} = \frac{y_3 - y_2}{x_3 - x_2}.$$

Graficamente, tem-se:

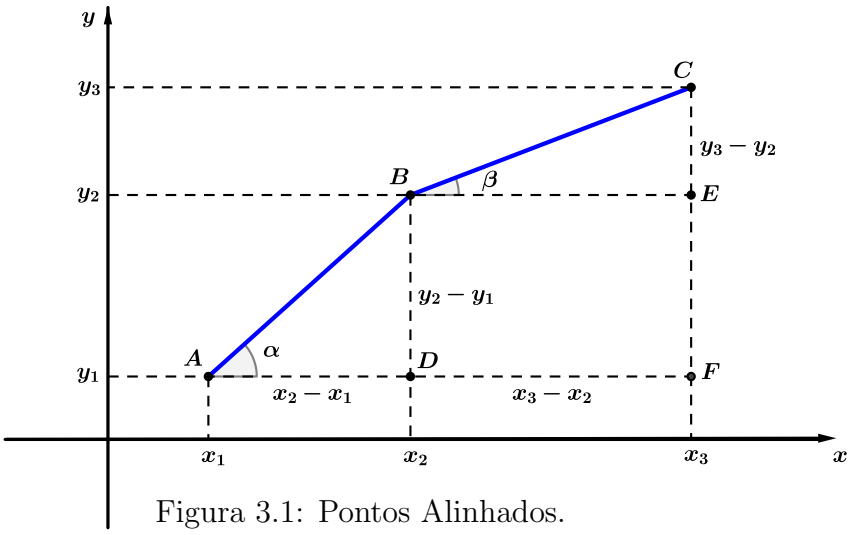

Figura 3.1: Pontos Alinhados.

Os triângulos ABD e BCE são retângulos e têm lados proporcionais, logo são semelhantes. Portanto, os ângulos α e β são iguais. Segue, então que os pontos A, B e C estão alinhados.

3.1.2 Imagem da função afim

Teorema 3.2. O conjunto imagem da função afim $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = ax + b$, com $a \neq 0$, é o conjunto $\mathbb{R}$.

Demonstração: qualquer que seja $y \in \mathbb{R}$, existe $x = \dfrac{y-b}{a} \in \mathbb{R}$ tal que

$$f(x) = f\left(\frac{y-b}{a}\right) = \cancel{a} \cdot \frac{y-b}{\cancel{a}} + b \Longrightarrow f(x) = y - \cancel{b} + \cancel{b} \Longrightarrow f(x) = y.$$

3.1.3 Coeficientes da função afim

O coeficiente a da função afim $f(x) = ax + b$ é denominado coeficiente angular ou declividade da reta representado no plano cartesiano.

O coeficiente b da função $f(x) = ax + b$ é denominado coeficiente linear.

3.1.4 Crescimento e decréscimo da função afim

Teorema 3.3. A função afim $f(x) = ax + b$ é crescente se, e somente se, o coeficiente angular a for positivo.

Demonstração: $f(x) = ax + b$ é crescente, se para dois valores quaisquer x_1 e x_2 do domínio, com $x_1 < x_2$, obtem-se $f(x_1) < f(x_2)$, isto é, para quaisquer que sejam x_1 e x_2, tem-se

$$x_1 < x_2 \Longrightarrow f(x_1) < f(x_2),$$

que pode ser reescrita da seguinte forma

$$\frac{f(x_1) - f(x_2)}{x_1 - x_2} > 0, \quad \text{com} \quad x_1 \neq x_2.$$

Assim,

$$\begin{aligned} \frac{ax_1 + b - (ax_2 + b)}{x_1 - x_2} > 0 \quad &\Rightarrow \quad \frac{ax_1 + \cancel{b} - ax_2 - \cancel{b}}{x_1 - x_2} > 0 \Rightarrow \frac{ax_1 - ax_2}{x_1 - x_2} > 0 \\ &\Rightarrow \quad \frac{a\cancel{(x_1 - x_2)}}{\cancel{x_1 - x_2}} > 0 \Rightarrow a > 0. \end{aligned}$$

Teorema 3.4. A função afim $f(x) = ax + b$ é decrescente se, e somente se, o coeficiente angular a for negativo.

Demonstração: a função afim $f(x) = ax+b$ é decrescente, se para dois valores quaisquer

x_1 e x_2 do domínio, com $x_1 < x_2$, obtem-se $f(x_1) > f(x_2)$, isto é, para quaisquer que sejam x_1 e x_2, tem-se

$$x_1 < x_2 \Longrightarrow f(x_1) > f(x_2),$$

que pode ser reescrita da seguinte forma

$$\frac{f(x_1) - f(x_2)}{x_1 - x_2} < 0, \quad \text{com} \quad x_1 \neq x_2.$$

Assim,

$$\begin{aligned} \frac{ax_1 + b - (ax_2 + b)}{x_1 - x_2} < 0 \quad &\Rightarrow \quad \frac{ax_1 + \cancel{b} - ax_2 - \cancel{b}}{x_1 - x_2} < 0 \Rightarrow \frac{ax_1 - ax_2}{x_1 - x_2} < 0 \\ &\Rightarrow \quad \frac{a\cancel{(x_1 - x_2)}}{\cancel{x_1 - x_2}} < 0 \Rightarrow a < 0. \end{aligned}$$

3.1.5 Função inversa

Teorema 3.5. Seja $f : A \to B$. A relação f^{-1} é uma função de B em A se, e somente se, f é bijetora, [9].

Demonstração : primeiro deve-se mostrar que, se f^{-1} é uma função de B em A, então f é bijetora .

i) Para todo $y \in B$ existe um $x \in A$ tal que $f^{-1}(y) = x$, isto é, $(x, y) \in f^{-1}$, ou ainda, $(x, y) \in f$. Assim f é sobrejetora.

ii) Dados $x_1, x_2, \in A$, com $x_1 \neq x_2$, se tiver $f(x_1) = f(x_2) = y$ resultará $f^{-1}(y) = x_1$ e $f^{-1}(y) = x_2$, o que é absurdo pois y só tem uma imagem em f^{-1}. Assim, $f(x_1) \neq f(x_2)$ e f é injetora.

Como a função f é sobrejetora e injetora, então f é bijetora.

Agora basta mostrar que, se f é bijetora, então f^{-1} é uma função de B em A.

i) Como f é sobrejetora, para todo $y \in B$ existe um $x \in A$ tal que $(x, y) \in f$. Portanto, $(x, y) \in f^{-1}$.

ii) Se $y \in B$, para duas imagens x_1 e x_2 em f^{-1}, vem

$$(y, x_1) \in f^{-1} \quad \text{e} \quad (y, x_2) \in f^{-1}.$$

Logo, $(x_1, y) \in f$ e $(x_2, y) \in f$. Como f é injetora, tem-se que $x_1 = x_2$.

Definição 3.2. Se f é uma função bijetora de A em B, a relação inversa de f é uma função de B em A que denomina-se função inversa de f e indicada por f^{-1}.

Dada a função bijetora f de A em B, definida pela sentença $y = f(x)$, para obter a sentença aberta que define f^{-1}, procede-se do seguinte modo.

1º) Na sentença $y = f(x)$ faz-se uma mudança de variável, isto é, troca-se x por y e y por x, obtendo $x = f(y)$;

2º) Escreva algebricamente a espressão $x = f(y)$, expressando y em função de x para obter $y = f^{-1}(x)$.

Exemplo 3.1. Qual a função inversa da função f bijetora em $\mathbb{R}$ definida por $f(x) = 4x + 1$?

Solução: Se $y = f(x)$, então $y = 4x + 1$. Permutando as variáveis y por x, na equação $y = 4x + 1$, obtem-se $x = 4y + 1$.

Expressando y em função de x, na equação $x = 4y + 1$, resulta

$$4y = x - 1 \Longrightarrow y = \frac{x-1}{4}\cdot$$

Fazendo a mudança de variável y por x na igualdade $y = f(x)$, tem-se $x = f(y)$. Donde, $f^{-1}(x) = y$.

Como $y = \dfrac{x-1}{4}$, então $f^{-1}(x) = \dfrac{x-1}{4}\cdot$

Graficamente, tem-se:

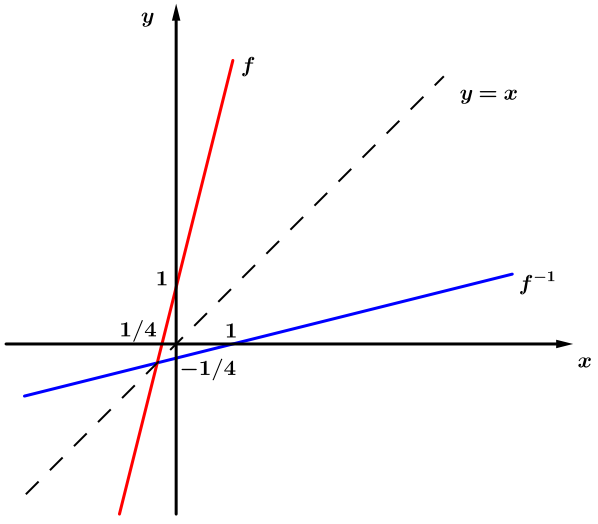

Figura 3.2: Gráfico da função f e da função inversa f^{-1}.

3.2 Função quadrática

Definição 3.3. Uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ chama-se *função quadrática* quando existem constantes a, b e c reais, com $a \neq 0$, tais que

$$f(x) = ax^2 + bx + c$$

para todo x real, onde as constantes a e b são chamadas de coeficientes dos termos x^2 e x, respectivamente, enquanto que a constante c é chamada de termo independente da função.

3.2.1 Gráfico da função quadrática

O gráfico da função quadrática é uma parábola.

Considere d uma reta e F um ponto fora dela, o plano determinado por d e F, chama-se parábola de foco F e diretriz d ao conjunto dos pontos equidistantes de d e F, [11].

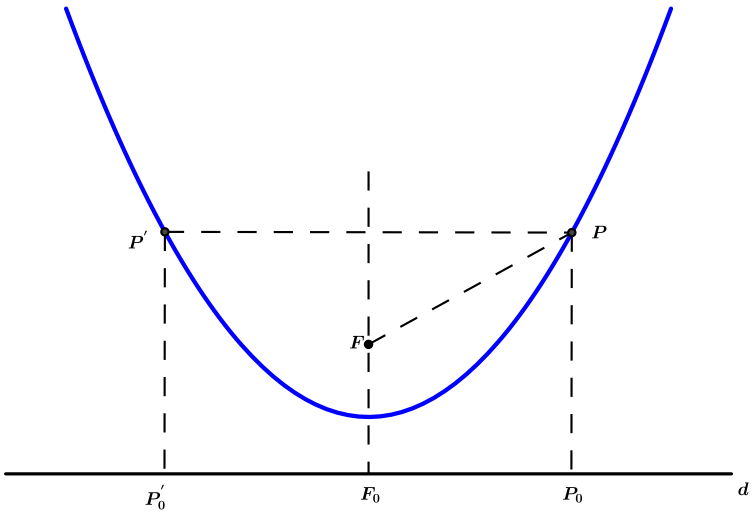

Figura 3.3: Parábola.

P pertence a parábola de foco F e diretriz d, pois $d(P, F) = d(P, P_0)$, com PP_0 perpendicular a d. A perpendicular FF_0, baixada do foco sobre a diretriz, é um eixo de simetria. Se P está sobre a parábola e P' é seu simétrico em relação a reta FF_0 então P' também pertence a parábola, como mostra a Figura 3.3.

3.2.2 Concavidade da parábola

A função quadrática $y = ax^2 + bx + c$, cujo gráfico é uma parábola, tem a concavidade voltada para ″cima″ ou voltada para ″baixo″.

i) Se $a > 0$, a concavidade da parábola está voltada para cima.

ii) Se $a < 0$, a concavidade da parábola está voltada para baixo.

3.2.3 Forma canônica da função quadrática

A construção do gráfico da função quadrática $y = ax^2 + bx + c$, com auxílio de uma tabela, ou seja, atribuindo valores a x e obtendo valores para y nem sempre é conveniente, pois às vezes o ponto de abscissa x pode não ser um número inteiro. Uma das formas de estudar a função quadrática detalhadamente é usando a forma canônica.

De $f(x) = ax^2 + bx + c$, tem-se:

$$\begin{aligned} f(x) = ax^2 + bx + c &= a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = a\left[x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} - \frac{b^2}{4a^2} + \frac{c}{a}\right] \\ &= a\left[\left(x^2 + \frac{b}{a}x + \frac{b^2}{4a^2}\right) - \left(\frac{b^2}{4a^2} - \frac{c}{a}\right)\right] \\ &= a\left[\left(x + \frac{b}{2a}\right)^2 - \left(\frac{b^2 - 4ac}{4a^2}\right)\right]. \end{aligned}$$

Representando $b^2 - 4ac$ por $\triangle$ (discriminante do trinômio do segundo grau), obtem-se:

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

3.2.4 Máximo e mínimo da função quadrática

i) Se $a < 0$, a função quadrática $y = ax^2 + bx + c$ admite o valor máximo $Y_m = -\dfrac{\triangle}{4a}$ para $X_m = -\dfrac{b}{2a}$.
Demonstração: considere a função quadrática na forma canônica

$$Y_m = a\left[\left(X_m + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a^2}\right].$$

Como $a < 0$, o valor de Y_m depende da diferença $\left(X_m + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a^2}$.

Perceba que $-\frac{\triangle}{4a^2}$ é constante por não depender de X_m, apenas dos valores de a, b e c, e $\left(x + \frac{b}{2a}\right)^2 \geqslant 0, \forall\ X_m \in \mathbb{R}$. Assim, a diferença assume o menor valor possível quando $\left(X_m + \frac{b}{2a}\right)^2 = 0 \quad e \quad X_m = -\frac{b}{2a}$.

Substituindo $X_m = -\frac{b}{2a}$ na expressão da forma canônica, obtem-se:

$$\mathrm{Y}_m = a\left[\left(-\frac{b}{2a} + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a^2}\right] = a\left[0^2 - \frac{\triangle}{4a^2}\right] = -\frac{\triangle}{4a}.$$

ii) Se $a > 0$, a função quadrática $y = ax^2 + bx + c$ admite valor mínimo $Y_m = -\frac{\triangle}{4a}$ para $X_m = -\frac{b}{2a}$.

Demonstração: análoga à demonstração do item i).

Observação 3.1. O ponto $V = (X_m, Y_m) = \left(-\frac{b}{2a}, -\frac{\triangle}{4a}\right)$ é chamado vértice da parábola da função quadrática.

Pode-se ainda, obter os zeros da função quadrática $f(x) = ax^2 + bx + c$, isto é, os valores de x reais tais que $f(x) = 0$. Assim, substituindo a forma canônica da função quadrática na equação $ax^2 + bx + c = 0$, obtem-se:

$$\mathrm{a}\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a^2}\right] = 0 \Rightarrow \left(x + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a^2} = 0 \Rightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{\triangle}{4a^2}$$

$$\Rightarrow x + \frac{b}{2a} = \frac{+}{-}\frac{\sqrt{\triangle}}{2a} \Rightarrow x = \frac{-b \overset{+}{-} \sqrt{\triangle}}{2a}.$$

3.2.5 Imagem da função quadrática

Utilizando a forma canônica para estudar a imagem da função quadrática.

Seja $f(x) = a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a^2}\right]$, donde $f(x) = a\left(x + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a}$. Como $\left(x + \frac{b}{2a}\right)^2 \geqslant 0$, para todo x real, existem dois casos, a saber :

1º caso: $a > 0 \Rightarrow a\left(x + \frac{b}{2a}\right)^2 \geqslant 0$. Logo,

$$y = a\left(x + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a} \geqslant -\frac{\triangle}{4a}.$$

2º caso: $a < 0 \Rightarrow a\left(x + \frac{b}{2a}\right)^2 \leqslant 0$. Logo,

$$y = a\left(x + \frac{b}{2a}\right)^2 - \frac{\triangle}{4a} \leqslant -\frac{\triangle}{4a}.$$

Portanto, pelos 1º e 2º casos, conclui-se que:

$$a > 0 \Longrightarrow Im(f) = \left\{y \in \mathbb{R};\ y \geqslant -\frac{\triangle}{4a}\right\};$$

$$a < 0 \Longrightarrow Im(f) = \left\{y \in \mathbb{R};\ y \leqslant -\frac{\triangle}{4a}\right\}.$$

3.2.6 Função quadrática inversa

Seja $f : A \to B$, uma função quadrática tal que $f(x) = ax^2 + bx + c$. Para que f admita a função inversa f^{-1}, é necessário que a função $f : A \to B$ seja bijetora, ou seja, $f^{-1} : B \to A$ é tal que,

$$f(x) = y \Longrightarrow f^{-1}(y) = x.$$

Para que uma função quadrática seja bijetora, deve-se limitar o domínio A da função, para que ele seja um subconjunto de $]-\infty, X_v[$ ou $[X_v, +\infty[$.

Existem algumas técnicas para determinar a função inversa da função quadrática. Uma das técnicas consiste no uso da fórmula de Bháskara, substituindo $f(x)$ por y na função $f(x) = ax^2 + bx + c$, obtem-se $y = ax^2 + bx + c$. Assim, $ax^2 + bx + c - y = 0$.

Isolando x de y, usando a fórmula de Bháskara, tem-se que:

$$\triangle = b^2 - 4a(c - y).$$

Logo,

$$x = \frac{-b \pm \sqrt{b^2 - 4a(c-y)}}{2a}.$$

Deve-se escolher o x_1 ou x_2 de acordo com o domínio da função f, isto é, o que for mais conveniente e depois troca-se os respectivos x_1 ou x_2 por $f^{-1}(x)$ e y por x. Assim,

i) Se $x_1 = \frac{-b + \sqrt{b^2 - 4a(c-y)}}{2a}$ for mais conveniente, então

$$f^{-1}(x) = \frac{-b + \sqrt{b^2 - 4a(c-x)}}{2a}.$$

ii) Se $x_2 = \dfrac{-b - \sqrt{b^2 - 4a(c-y)}}{2a}$ for mais conveniente, então

$$f^{-1}(x) = \frac{-b - \sqrt{b^2 - 4a(c-x)}}{2a}.$$

Uma outra técnica que pode ser aplicada é trocando o x pelo y, em seguida completando os quadrados e isolar o y em um dos membros da igualdade, depois é só trocar o y por $f^{-1}(x)$.

Exemplo 3.2. Defina o domínio e o contradomínio da função $f(x) = 3x^2 + 2x - 5$, de modo que f seja inversível e determine sua inversa.

Solução: Como $a = 3$, $b = 2$ e $c = -5$, com $a > 0$, então a função admite valor mínimo em $Y_v = -\dfrac{\triangle}{4a}$, donde

$$Y_v = -\frac{b^2 - 4ac}{4a} = -\frac{4 + 60}{12} = -\frac{64}{12} = -\frac{16}{3}.$$

Logo, $Im(f) = \left[-\dfrac{16}{3}, +\infty\right)$.

Seja $X_v = -\dfrac{b}{2a} \Longrightarrow X_v = -\dfrac{2}{6} = -\dfrac{1}{3}$. Então,

$$D(f) = \left[-\frac{1}{3}, +\infty\right) \text{ e } CD(f) = Im(f) = \left[-\frac{16}{3}, +\infty\right),$$

isto é,

$$f : \left[-\frac{1}{3}, +\infty\right) \to \left[-\frac{16}{3}, +\infty\right).$$

Agora, já definidos o domínio e o contradomínio da função $f(x) = 3x^2 + 2x - 5$, pode-se determinar a sua inversa.

Aplicando a fórmula $x = \dfrac{-b \pm \sqrt{b^2 - 4a(c-y)}}{2a}$, tem-se:

$$\text{x} = \frac{-2 \pm \sqrt{4 - 12(-5-y)}}{6} = \frac{-2 \pm \sqrt{64 + 12y}}{6} = \frac{-2 \pm 2\sqrt{16 + 3y}}{6} = \frac{-1 \pm \sqrt{16 + 3y}}{3}.$$

Logo,

$$x = \frac{-1 + \sqrt{16 + 3y}}{3} \quad \text{ou} \quad x = \frac{-1 - \sqrt{16 + 3y}}{3}.$$

Como definido o domínio de f, sendo o intervalo $\left[-\dfrac{1}{3}, +\infty\right)$, obtem-se $x = \dfrac{-1 + \sqrt{16 + 3y}}{3}$.

Portanto, $f^{-1}(x) = \dfrac{-1+\sqrt{16+3x}}{3}$, onde $f^{-1} : \left[-\dfrac{16}{3}, +\infty\right) \to \left[-\dfrac{1}{3}, +\infty\right)$.

Em que, $Im(f) = D(f^{-1})$ e $D(f) = Im(f^{-1})$.

Observação 3.2. Poder-se-ia ter definido o domínio da função como sendo o intervalo $\left(\infty-, -\dfrac{1}{3}\right]$ e teria-se a inversa como sendo $f^{-1}(x) = \dfrac{-1-\sqrt{16+3x}}{3}$.

3.3 Função exponencial

É toda função na qual tem-se a variável x como expoente.

A função $f : \mathbb{R} \to \mathbb{R}^+$ definida por $f(x) = a^x$, com $a \in \mathbb{R}^+$ e $a \neq 1$, é chamada de função exponencial de base a, onde $D(f) = \mathbb{R}$ e $CD(f) = \mathbb{R}^+$.

As condições $a > 0$ e $a \neq 1$ são importantes. Isso, porque, se caso $a \leqslant 0$, existem números reais x, tais que a potência a^x não é definida (por exemplo, $(-3)^{1/2}$ não existe em $\mathbb{R}$), e, se $a = 1$, teria-se uma função constante ($f(x) = 1^x = 1, \forall\ x \in \mathbb{R}$).

3.3.1 Gráfico cartesiano da função exponencial

Representando graficamente a função exponencial $f(x) = a^x$, há dois casos a considerar:
Caso I: $a > 1$

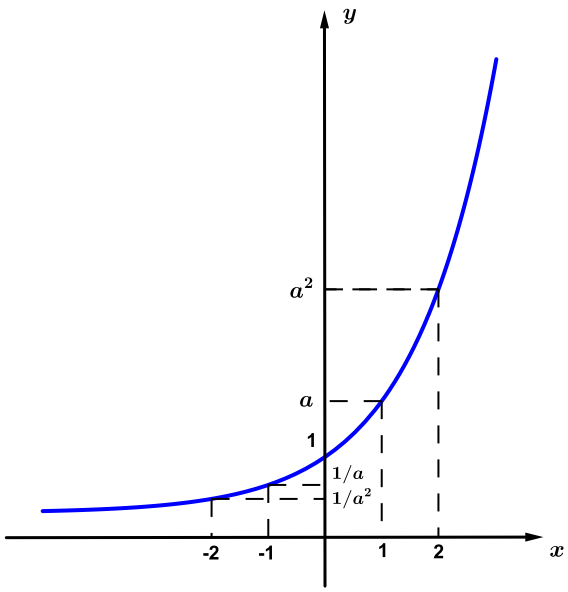

Figura 3.4: Gráfico Cartesiano da Função Exponencial $a > 1$.

Neste caso, a função é crescente(quanto maior o expoente x, maior é a potência a^x).

Caso II: $0 < a < 1$

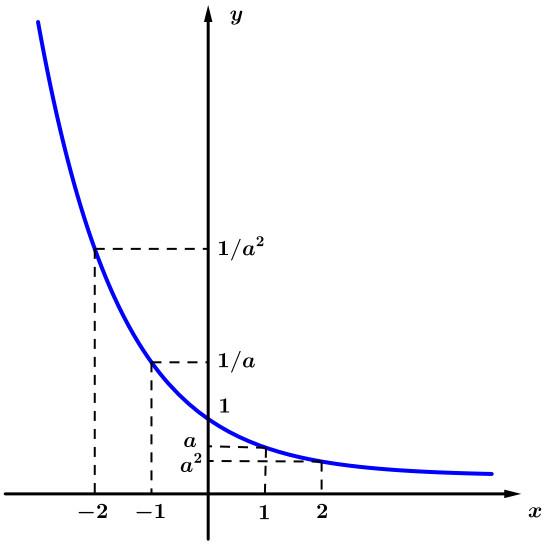

Figura 3.5: Gráfico Cartesiano da Função Exponencial $0 < a < 1$.

Neste caso, a função é decrescente(quanto maior o expoente x, menor é a potência a^x).

3.4 Função logarítmica

Visto anteriormente que a função exponencial $f(x) = a^x$, com $a > 0$ e $a \neq 1$, é uma função $f : \mathbb{R} \to \mathbb{R}^*$. O conjunto imagem dessa função é formado pelos números reais positivos, isto é,

$$Im(f) = \{y \in \mathbb{R} | y > 0\} = \mathbb{R}^*_+.$$

Um número real b está na imagem de f, se existir x tal que $a^x = b$.

Se $b \leqslant 0$, a equação $a^x = b$ não tem solução, visto que $a > 0$, tem-se que $a^x > 0, \forall\, x \in \mathbb{R}$. Se $b > 0$, sempre se pode situar b entre duas potências de base a e expoentes inteiros consecutivos: $a^k \leqslant b \leqslant a^{k+1}, k \in \mathbb{Z}$. Então, a equação $a^x = b$ tem uma solução x, que é um número situado entre os dois expoentes ($k \leqslant x < k+1$). Esta solução é única, devido ao fato de a função ser crescente (Se $a > 1$) ou decrescente (Se $0 < a < 1$).

Seja a um número real positivo e diferente de 1 ($a > 0$ e $a \neq 1$). Se $b > 0$, o número x que é solução da equação $a^x = b$ é denominado logaritmo de b na base a, em símbolos

$$\log_a b = x \iff a^x = b.$$

Em $\log_a b$, diz-se que o número a é base e b é o logaritmando (ou antilogaritmo).

Se considerar um número $a > 0$ e $a \neq 1$, o número $\log_a x$ existe para todo $x > 0$. Assim, numa função f que a cada $x > 0$, faz corresponder o número $\log_a x$. Essa função é denominada função logarítmica na base a.

Portanto, dado um número $a > 0$ e $a \neq 1$, chama-se função logarítmica de base a à função

$$f(x) = \log_a x$$

definida para todo $x > 0$.

A função logarítmica $y = \log_a x$ é a inversa da função exponencial $y = a^x$ e vice-versa. De fato, seja $f(x) = a^x$ uma função exponencial com $a > 0$ e $a \neq 1$, então segue que

$$f(x) = a^x \Longrightarrow y = a^x \Longrightarrow \log_a y = \log_a a^x = \log_a y = x.$$

Portanto, $f^{-1}(x) = \log_a x$.

3.4.1 Gráfico cartesiano da função logarítmica

Representando graficamente a função logarítmica $f^{-1}(x) = \log_a x$, há dois casos a considerar: Caso I: $a > 1$

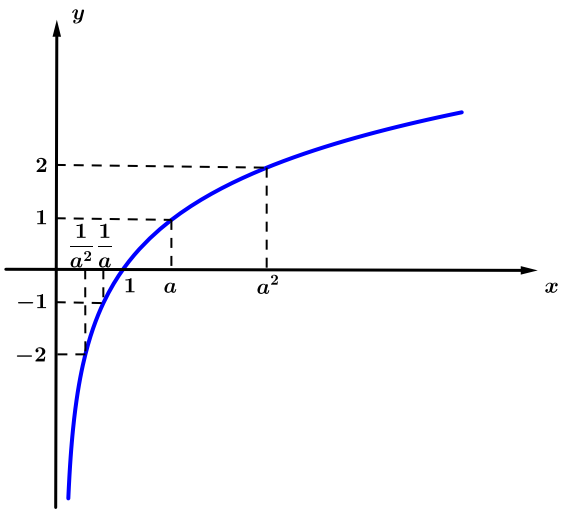

Figura 3.6: Gráfico Cartesiano da Função Logarítmica $a > 1$.

Neste caso, a função é crescente (quanto maior o logaritmando x, maior é o valor de $\log_a x$).

Caso II: $0 < a < 1$

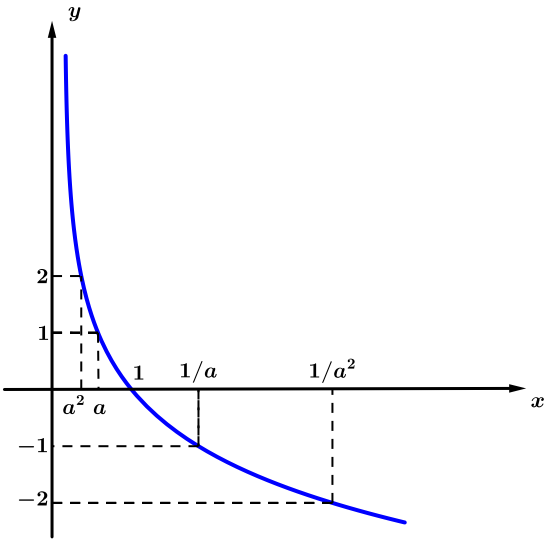

Figura 3.7: Gráfico Cartesiano da Função Logarítmica $0 < a < 1$.

Neste caso, a função é decrescente(quanto maior o logaritmando x, menor é o valor de $\log_a x$).

3.5 Matrizes

Com o avanço computacional, o estudo das matrizes tornou-se muito importante pelas inúmeras aplicações em diversos campos da ciência e tecnologia, como matemática, física, engenharia, computação, ...

Definição 3.4. Denomina-se Matriz a um conjunto de números reais, ou a um conjunto de números complexos dispostos em linhas e colunas, mas colocados entre parênteses ou colchetes. Exemplo:

$$\begin{pmatrix} 1 & 4 & -8 \\ 5 & 0 & 1 \\ 3 & 2 & 7 \end{pmatrix} \quad \text{ou} \quad \begin{bmatrix} 1 & 4 & -8 \\ 5 & 0 & 1 \\ 3 & 2 & 7 \end{bmatrix}.$$

Em tabelas assim dispostas, os números são os elementos. As linhas são enumeradas de cima para baixo e as colunas, da esquerda para direita.

Tabelas com m linhas e n colunas são denominadas matrizes $m \times n$.

3.5.1 Notação geral

Costuma-se representar as matrizes por letras maiúsculas e seus elementos por letras minúsculas acompanhadas de dois índices que indicam, respectivamente, a linha e a coluna que o elemento ocupa na tabela.

Portanto, uma matriz A do tipo $m \times n$ é representada por:

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

ou, abreviadamente, $A = [a_{ij}]_{m \times n}$, onde i e j representam, respectivamente, a linha e a coluna que o elemento ocupa. Por exemplo, a_{13} é o elemento da 1ª linha e da 3ª coluna.

Existem vários tipos de matrizes, como matriz coluna, matriz linha, matriz quadrada, matriz identidade, etc. Com base nesse trabalho e diante de sua grande importância no mundo matemático, estudar-se-á apenas a matriz quadrada.

3.5.2 Matriz quadrada

Seja uma matriz quadrada a_{ij}, $i = 1, 2, \cdots, m$ e $j = 1, 2, \cdots, n$. Se $m = n$, então diz-se que se trata de uma matriz quadrada. Assim, as matrizes

$$A = \begin{bmatrix} 2 & 5 \\ 7 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 8 & 2 \\ 4 & -1 & 5 \\ 9 & 0 & -3 \end{bmatrix},$$

são matrizes quadradas de ordem 2 e 3 respectivamente.

3.5.3 Matriz Identidade

É uma matriz quadrada de ordem n cujos elementos da diagonal principal a_{ij}, com $i = j$, são iguais a 1 e os demais elementos fora da diagonal a_{ij}, com $i \neq j$, são nulos (iguais a zero). A matriz identidade é representada por I_n. Exemplo:

$$I_1 = \begin{bmatrix} 1 \end{bmatrix} \quad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \cdots$$

De modo geral , $I_n = (a_{ij})_{n\times n}$, tal que:

$$a_{ij} = \begin{cases} 1, & \text{se} \quad i = j \\ 0, & \text{se} \quad i \neq j \end{cases} \qquad \forall\ i, j \in \{1, 2, 3, \cdots, n\}.$$

3.5.4 Matriz inversa de uma matriz quadrada

Uma matriz quadrada A, de ordem n,é inversível se, e somente se, existir uma matriz B tal que $AB = BA = I_n$.

A matriz B, quando existe, é chamada matriz inversa de A e é representada por A^{-1}. Assim,

$$AA^{-1} = A^{-1}A = I_n.$$

As matrizes A e I_n sendo do tipo $n \times n$, a matriz A^{-1} , se existe, é também do tipo $n \times n$.

Se não existe A^{-1}, então a matriz A é não inversível. Para verificar se uma matriz é inversível, basta verificar se ela possui uma inversa à direita ou uma inversa à esquerda.

3.5.5 Determinante

É um número real associado a uma matriz quadrada. Existem alguns métodos para calcular o determinante de uma matriz quadrada de ordem $n \geq 2$.

O leitor interessado pode obter essas informações no livro: Fundamentos de matemática elementar v.4 de Iezzi e Hazzan [10].

3.5.6 Existência da matriz inversa

Suponha que A seja uma matriz de ordem n inversível. Tem-se que:

$AA^{-1} = I_n \Longrightarrow det(AA^{-1}) = det(I_n) \Longrightarrow det(A)det(A^{-1}) = 1.$

Como o produto de $det(A)$ por $det(A^{-1})$ é 1, tem-se $det(A) \neq 0$. Reciprocamente, pode-se verificar que $detA^{-1} \neq 0$, então existe A^{-1}.

Portanto, conclui-se que A é inversível se, e somente se, $detA \neq 0$.

3.6 Noções de Teoria dos Números

3.6.1 Divisão Euclidiana

Sejam a e b números naturais não nulos $a > b$. Existem números naturais r (resto) e q (quociente), tais que $a = bq + r$, onde $0 \leq r < b$.

Os naturais r e q são únicos para cada divisão euclidiana, [5] e [15].

Demonstração: Suponha que na divisão de a por b, obtem-se dois restos distintos e também dois quocientes distintos, isto é, $a = bq_1 + r_1$, $0 \leq r_1 < b$ e $a = bq_2 + r_2$, $0 \leq r_2 < b$. Então deve-se mostrar que esses restos são iguais e os quocientes também.

Segue que,

$$bq_1 + r_1 = bq_2 + r_2 \Longrightarrow b(q_1 - q_2) = r_2 - r_1.$$

Logo, b é divisor de $r_2 - r_1$, como $0 \leq r_1 < b$ e $0 \leq r_2 < b$, então $r_2 - r_1 = 0 \Longrightarrow r_2 = r_1$.

Portanto, $q_1 = q_2$.

3.6.2 Algoritmo de Euclides

Suponha que tenha dois inteiros positivos a e b. O máximo divisor comum entre a e b é o maior inteiro positivo d que é divisor de a e também de b. Se d é o máximo divisor comum entre a e b, escreve-se $d = mdc(a, b)$. Se $mdc(a, b) = 1$, fala-se que os números são primos entre si ou coprimos, [5].

Dados dois números a e b inteiros positivos, com $a \geq b$, para calcular o $mdc(a, b)$, o algoritmo de Euclides consiste em dividir a por b, achando resto r_1 . Se $r_1 \neq 0$, dividindo b por r_1, obtendo resto r_2. Se $r_2 \neq 0$, divide-se r_1 por r_2, obtendo o resto r_3. E assim sucessivamente. O último resto diferente de zero dessas divisões sucessivas é o máximo divisor comum entre a e b.

Essas divisões podem ser indicadas, utilizando-se um diagrama, [5].

	q_1	q_2	q_3	$\cdots$		q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	$\cdots$	r_n	0	

Tabela 3.1: Algoritmo de Euclides.

Este processo é conhecido como dispositivo prático em que o $mdc(a, b)$ é o último resto não nulo do processo de divisões, em que se garante:

$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2), \cdots, mdc(r_{n-2}, r_{n-1}) = mdc(r_{n-1}, r_n) = mdc(r_n, 0) = r_n$.

Exemplo 3.3. Calcule o máximo divisor comum de 1340 e 36.

Solução: Pelo dispositivo prático da Tabela 3.2:

	37	4	2
1340	36	8	4
8	4	0	

Tabela 3.2: Dispositivo Prático.

O último resto não nulo é 4, tem-se que $mdc(1340, 36) = 4$.

3.6.3 Algoritmo Euclidiano estendido

Considere o problema de calcular α e β na equação $\alpha a + \beta b = mdc(a, b)$.

Poder-se-ia começar achando $mdc(a, b)$ pelo algoritmo Euclidiano e tendo depois de calcular α e β. Assim, se expressaria α e β usando valores dos quocientes e restos obtidos nas divisões sucessivas, com um pouco de cuidado. Mas, infelizmente esse método muito trabalhoso é ineficiente do ponto de vista computacional se os números forem muito grandes ou até mesmo impossível, [5].

A versão do algoritmo Euclidiano estendido que será apresentado se deve a D. E. KNUTH(2004), autor de uma série de livros chamada ″THE ART OF COMPUTER ″, que é considerada a bíblia da teoria dos algoritmos(Knuth 1991).

O algoritmo de Euclides estendido é utilizado, em especial, para o cálculo de inverso modular. Na equação $\alpha a + \beta b = mdc(a, b)$, se a e b são coprimos, então α é o inverso modular de a módulo b e β é o inverso modular de b módulo a. Esta propriedade é amplamente utilizada no estudo de criptografia, mais precisamente, no processo de quebra de chaves privadas do método de encriptação RSA, [5] e [14].

A implementação inventada pelo KNUTH é muito mais sutil. A idéia consiste em expressar cada um dos restos obtidos nas divisões sucessivas em termos de a e b de forma semelhante à fórmula $\alpha a + \beta b = mdc(a, b)$. Segue então que calculando o $mdc(a, b)$, obtem-se a sequência de divisões em que os restos são reescritos como uma combinação linear de a e b.

Portanto,

$$a = bq_1 + r_1 \text{ e } r_1 = \alpha_1 a + \beta_1 b$$
$$b = r_1 q_2 + r_2 \text{ e } r_2 = \alpha_2 a + \beta_2 b$$
$$r_1 = r_2 q_3 + r_3 \text{ e } r_3 = \alpha_3 a + \beta_3 b$$
$$r_2 = r_3 q_4 + r_4 \text{ e } r_4 = \alpha_4 a + \beta_4 b$$
$$\vdots$$
$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \text{ e } r_{n-1} = \alpha_{n-1} a + \beta_{n-1} b$$
$$r_{n-2} = r_{n-1} q_n + r_4 \text{ e } r_n = 0.$$

Os números $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ e $\beta_1, \beta_2, \cdots, \beta_{n-1}$ são inteiros a serem determinados. Colocando em coluna, os restos, os quocientes e os inteiros a serem determinados, obtem-se:

Resto	Quociente	α	β	
a	*	?	?	
b	*	?	?	
r_1	q_1	α_1	β_1	$r_1 = \alpha_1 a + \beta_1 b$
r_2	q_2	α_2	β_2	$r_2 = \alpha_2 a + \beta_2 b$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-1}	q_{n-1}	α_{n-1}	β_{n-1}	$r_{n-1} = \alpha_{n-1} a + \beta_{n-1} b$
r_n	q_n	α_n	β_n	$r_n = \alpha_n a + \beta_n b$
r_{n+1}	q_{n+1}	α_{n+1}	β_{n+1}	$r_{n+1} = \alpha_{n+1} a + \beta_{n+1} b$

Tabela 3.3: Algoritmo de Euclides Estendido.

Note que as duas primeiras linhas não correspondem a nenhuma divisão, ou seja, nem a e nem b são restos e foram introduzidas para facilitar os cálculos adiante.

O problema agora é descobrir como preencher as colunas α e β. Observe que ao dividir r_{n-1} por r_n, obtem-se quociente q_{n-1} e resto r_{n+1}, logo:

$$r_{n-1} = r_n q_{n+1} + r_{n+1} \Rightarrow r_{n+1} = r_{n-1} - r_n q_{n+1}.$$

Substituindo $r_{n-1} = \alpha_{n-1}a + \beta_{n-1}b$ e $r_n = \alpha_n a + \beta_n b$ em $r_{n+1} = r_{n-1} - r_n q_{n+1}$, obtendo:

$$\begin{aligned} r_{n+1} &= \alpha_{n-1}a + \beta_{n-1}b - q_{n+1}(\alpha_n a + \beta_n b) \\ r_{n+1} &= \alpha_{n-1}a + \beta_{n-1}b - \alpha_n q_{n+1}a - \beta_n q_{n+1}b \\ r_{n+1} &= a(\alpha_{n-1} - \alpha_n q_{n+1}) + b(\beta_{n-1} - \beta_n q_{n+1}). \end{aligned}$$

Assim, pode-se estabelecer uma regra de acordo com a Tabela 3.3, pois tem-se que $\alpha_{n-1} - \alpha_n q_{n+1}$ é o α_{n+1} e $\beta_{n-1} - \beta_n q_{n+1}$ é o β_{n+1}. Para calcular α_{n+1}, deve-se subir duas linhas e fazer $\alpha_{n-1} - \alpha_n q_{n+1}$ e para calcular β_{n+1} é de forma análoga.

O problema agora é achar valores para as duas primeiras linhas para continuar preenchendo a Tabela 3.3. Interpretando estas linhas como as demais, tem-se

$$a = \alpha_{-1}a + \beta_{-1}b \text{ e } b = \alpha_0 a + \beta_0 b,$$

o que nos sugere $\alpha_{-1} = 1$, $\beta_{-1} = 0$, $\alpha_0 = 0$ e $\beta_0 = 1$.

Exemplo 3.4. Encontre o $mdc(1326, 42)$ e determine α e β tais que $1326\alpha + 42\beta = mdc(1326, 42)$.

Solução: Construindo a tabela, tem-se:

Resto	Quociente	α	β
1326	*	1	0
42	*	0	1
24	31	1 - 0 · 31	0 - 1 · 31
18	1	0 - 1 · 1	1 - 1 · (-31)
6	1	1 - 1 · (-1)	-31 - 1 · 32
0	3	*	*

Tabela 3.4: Dispositivo Prático de Euclides Estendido.

Portanto,

$mdc(1326, 42) = 6$ e $\alpha = 2, \beta = -63$, isto é,

$$1326 \cdot 2 + 42 \cdot (-63) = 6$$

.

3.6.4 Congruência

Definição: Se a e b são inteiros, diz-se que a é congruente a b módulo m $(m > 0)$ se $m|(a - b)$, ou seja, m divide $a - b$. Denotar-se isto por $a \equiv b \ (mod\ m)$. Se $m \not|(a - b)$, dize-se que a é incongruente a b módulo m e denotar-se por $a \not\equiv b \ (mod\ m)$.

Exemplo 3.5. $13 \equiv 3 \ (mod\ 5)$, pois $5|13 - 3$
$8 \not\equiv 1 \ (mod\ 2)$, pois $2 \not|8 - 1$.

Dado um módulo m, pode-se provar que qualquer inteiro a é equivalente, módulo m, a exatamente um dos inteiros: $0, 1, 2, 3, \cdots, m - 1$. Este inteiro é chamado o resíduo de a módulo m e denotando por $\mathbb{Z}_m = \{[0], [1], [2], [3], \cdots, [m - 1]\}$ o conjunto dos resíduos de a módulo m.

Se a é um inteiro não-negativo, então seu resíduo módulo m é simplesmente o resto da divisão de a por m. A noção de congruência é uma ferramenta poderosa e útil pelo fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros.

Por se tratar de um assunto bastante extenso, recomenda-se a leitura das referências [5] e [14].

3.6.5 Função ϕ Euler

Definição: O número $\phi(m)$ é o número de inteiros positivos menores que, ou iguais a m, que são relativamentes primos com m.

Nota-se com isso que a partir da definição, tem-se que $\phi(p) = p - 1$, se p é primo, já que ele é coprimo com os demais menores que ele próprio.

O estudo da função ϕ de Euler é de fundamental importância na criptografia, sistema

RSA. A seguir, serão apresentadas propriedades da função ϕ de Euler que serão extremamente úteis:

Teorema 3.6. A função ϕ de Euler é uma função aritmética multiplicativa, ou seja, sendo m e n dois inteiros positivos tais que o $mdc(m,n) = 1$, então $\phi(m,n) = \phi(m) \cdot \phi(n)$, [5].

Demonstração:

Note que, se m ou n vale 1, a proposição é diretamente verdadeira.

Agora, suponha que $m > 1$ e $n > 1$. Será construída uma tabela com m colunas e n linhas, contendo todos os inteiros positivos de 1 até $m \cdot n$.

1	2	...	h	...	m
m + 1	m + 2	...	m + h	...	2m
2m + 1	2m + 2	...	2m + h	...	3m
⋮	⋮	⋮	⋮	⋮	⋮
(n - 1) m + 1	(n - 1) m + 2	...	(n - 1) m + h	...	mn

Tabela 3.5: Função ϕ de Euler.

Na primeira linha o número de inteiros menores que m e primos com m é igual a $\phi(m)$, então existem apenas $\phi(m)$ colunas em que os primeiros termos destas colunas são primos com m. Desde que $mdc(q.m.h, m) = mdc(h, m)$, os inteiros da h-ésima coluna são primos com m se, e somente se, h é primo com m. Daí, concluí-se que quando o primeiro elemento de cada coluna, que são os elementos da primeira linha, é primo com m, então todos os elementos destas colunas são primos com m. Assim, existem exatamente $\phi(m)$ colunas formada com inteiros que são todos primos com m.

Analisar-se-ão somente estas colunas em que todos inteiros são primos com m. Nestas colunas tem-se que $mdc(h, m) = 1$, então o número de elementos de cada coluna $[h, m + h, 2m + h, \cdots, (n-1)m + h]$ que são primos com n é igual a $\phi(n)$, pois para isto ocorrer basta que o $mdc(h, n)$ seja igual a 1. Portanto, o número de inteiros menores que mn e que são primos com mn é igual a $\phi(m) \cdot \phi(n)$, isto é, $\phi(mn) = \phi(m) \cdot \phi(n)$, em destaque, [5] e [14].

Teorema 3.7. Para P primos e α um número inteiro positivo, tem-se $\phi(P^\alpha) = P^\alpha - P^{\alpha-1}$.

Demonstração: Pela definição da função ϕ de Euler, sabe-se que $\phi(P^\alpha)$ é o número de inteiros positivos não superiores a $\phi(P^\alpha)$ e primos com $\phi(P^\alpha)$. Mas, os únicos números primos não primos com $\phi(P^\alpha)$ e menores do que ou iguais $\phi(P^\alpha)$ são aqueles divisíveis por P. Como os múltiplos de P não superiores a $\phi(P^\alpha)$ são em número, $\phi(P^{\alpha-1})$ o resultado segue.

Teorema 3.8. Se $n = P^{k_1}P^{k_2}\cdots P_r^{k_r}$ é a decomposição canônica do inteiro positivo $n > 1$, então

$$\phi(n) = (P_1^{k_1} - P_1^{k_1-1})(P_2^{k_2} - P_2^{k_2-1})...(P_r^{k_r} - P_r^{k_r-1}) = n(1-\tfrac{1}{P_1})(1-\tfrac{1}{P_2})(1-\tfrac{1}{P_3})\cdots(1-\tfrac{1}{P_r}).$$

Demonstração: Como $P_1, P_2, \cdots, P_r$ são todos primos, então o máximo comum de qualquer par desses primos é igual a 1.

Portanto, como $\phi(n)$ é uma função aritmética multiplicativa:

$\phi(n) = \phi(P_1^{k_1}P_2^{k_2}\cdots P_r^{k_r}) = \phi(P_1^{k_1})\phi(P_2^{k_2})\cdots\phi(P_r^{k_r}) = (P_1^{k_1} - P_1^{k_1-1})(P_2^{k_2} - P_2^{k_2-1})\cdots(P_r^{k_r} - P_r^{k_r-1}) = n(1-\frac{1}{P_1})(1-\frac{1}{P_2})\cdots(1-\frac{1}{P_r})$.

Exemplo 3.6. Calcular $\phi(7865)$.

Como $7865 = 5 \cdot 11^2 \cdot 13$, tem-se:

$$\phi(7865) = (5-1)(11^2-11)(13-1) = 4 \cdot 110 \cdot 12 = 5280.$$

Teorema 3.9. Um número inteiro a é inversível módulo m quando existe um b tal que $ab \equiv 1\ (mod\ m)$, isto é, todos os números inversíveis módulo m são os coprimos com m, ou seja, $mdc(a, b) = 1$.

Demonstração : Suponha que $mdc(a, m) \neq 1, a < m$, então $ab \equiv 1\ (mod\ m) \Leftrightarrow ab = mk + 1 \Leftrightarrow ab - mk = 1$, k é um inteiro. Isso significa que uma combinação linear de a, m tem que dar 1. Absurdo, pois a menor combinação linear que pode ocorrer entre dois números é seu mdc, que neste caso, é diferente de 1.

Teorema 3.10 (Teorema de Euler)**.** Seja a um inteiro positivo e m outro inteiro positivo com $mdc(a, m) = 1$. Então, sempre vale que $a^{\phi(m)} \equiv 1\ (mod\ m)$.

Demonstração: Note que $b_1, b_2, \cdots, b_{\phi(m)}$ são os números primos com m menores que m, eles são todos inversíveis e representam todos os inversíveis módulo m. Logo, se ao selecionar a tal que $mdc(a, m) = 1$, então $ab_1, ab_2, \cdots, ab_{\phi(m)}$ também representará todos

os inversíveis módulo m. Assim, se ao multiplicar todos os números deste conjunto e analisar o produto módulo m, ter-se-á $a^{\phi(m)}b_1b_2\cdots b_{\phi(m)} \equiv a^{\phi(m)} \equiv 1\ (mod\ m)$.

Exemplo 3.7. Calcule o inverso de 3 módulo 7 usando o algoritmo de Euclides.

Solução: Tem-se que $mdc(3,7) = 1$, logo o inverso b existe.

$b \times 3 \equiv 1\ (mod\ 7)$, pelo algoritmo de Euclides, tem-se:

$7 = 2 \times 3 + 1 \Rightarrow -2 \times 3 + 1 \times 7 = 1$. Assim, -2 é um inverso de 3 módulo 7. Logo, todo inteiro congruente com -2 módulo 7 é também inverso de 3.

Portanto, b pode ser $-2, 5, 12, 19, \cdots$

CAPÍTULO 4

CODIFICAÇÃO E DECODIFICAÇÃO DE MENSAGENS UTILIZANDO FUNÇÕES E MATRIZES

Neste capítulo, serão apresentados os métodos de codificação e decodificação utilizando funções e matrizes. Tais métodos são interessantes do ponto de vista prático, tornando assim uma ferramenta no ensino e aprendizagem das funções e matrizes.

Exemplo 4.1. Inicialmente, associa-se cada letra do alfabeto aos números, segundo a Tabela 4.1.

A	B	C	D	E	F	G	H	I	J	K	L	M
2	1	3	5	4	7	8	9	11	26	12	13	30

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	#
10	14	17	21	25	6	19	20	24	16	15	18	28	31

Tabela 4.1: Tabela para codificação da função afim.

Função cifradora: $f(x) = 5x - 4$.

Mensagem a ser cifrada: "DIGA NÃO ÀS DROGAS".

Tem-se a Tabela 4.2, em que o símbolo #, será usado como espaço entre as palavras durante todo o trabalho.

Letra	Sequência numérica	Cálculo da imagem da função f(x) = 5x - 4
A	2	f(2) = 6
D	5	f(5) = 21
G	8	f(8) = 36
I	11	f(11) = 51
N	10	f(10) = 46
O	14	f(14) = 66
R	25	f(25) = 121
S	6	f(6) = 26
#	31	f(31) = 151

Tabela 4.2: Codificadora da função afim.

Para enviar a mensagem cifrada em uma sequência alfabética, faz-se necessário o uso de aritmética modular, pois nem sempre há um correspondente alfabético, como visto na Tabela 4.1. Sempre que ocorrer um inteiro maior que 26, ele será substituído pelo resto da divisão deste inteiro por 26, tal que o resto é um dos inteiros $0, 1, 2, 3, ..., 25$. Este procedimento será realizado durante todo o restante do trabalho e fornecerá um inteiro com equivalente alfabético. Pelo fato da congruência ser uma relação de equivalência, o processo é reversível. Para maiores esclarecimentos, veja a solução da atividade 1 do capítulo 5.

Assim,

A mensagem cifrada é :

QRNSQUSOQSJQQPONSJ

Cálculo da função inversa, decodificadora da imagem.

Seja $f(x) = y = 5x - 4$, permutando as variáveis e expressando y em função de x, tem-se:

$$x = 5y - 4 \Longrightarrow 5y = x + 4 \Longrightarrow y = \frac{x+4}{5}$$

Isto é, $f^{-1}(x) = \frac{x+4}{5}$.

Cálculo das imagens de $f^{-1}(x) = \frac{x+4}{5}$.

Sequência numérica	$f^{-1}(x) = \frac{x+4}{5}$	Letra
6	$f^{-1}(6) = \frac{6+4}{5} = 2$	A
21	$f^{-1}(21) = \frac{21+4}{5} = 5$	D
36	$f^{-1}(36) = \frac{36+4}{5} = 8$	G
51	$f^{-1}(51) = \frac{51+4}{5} = 11$	I
46	$f^{-1}(46) = \frac{46+4}{5} = 10$	N
66	$f^{-1}(66) = \frac{66+4}{5} = 14$	O
121	$f^{-1}(121) = \frac{121+4}{5} = 25$	R
26	$f^{-1}(26) = \frac{26+4}{5} = 6$	S
151	$f^{-1}(151) = \frac{151+4}{5} = 31$	#

Tabela 4.3: Decodificadora da função afim.

A mensagem decifrada é: "DIGA NÃO ÀS DRODAS".

Exemplo 4.2.

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	27	28

Tabela 4.4: Tabela para codificação da função quadrática I.

Função cifradora: $f(x) = 2x^2 - 3x + 1$.

Mensagem a ser cifrada(Célebre frase de René Descartes): "PENSO, LOGO EXISTO".

Organizando as letras por ordem, tem-se a Tabela 4.5:

Letra	Sequência numérica	Cálculo da imagem da função $f(x) = 2x^2 - 3x + 1$
E	5	$f(5) = 2{\cdot}5^2 - 3 \cdot 5 + 1 = 36$
G	7	$f(7) = 2{\cdot}7^2 - 3 \cdot 7 + 1 = 78$
I	9	$f(9) = 2{\cdot}9^2 - 3 \cdot 9 + 1 = 136$
L	12	$f(12) = 2{\cdot}12^2 - 3 \cdot 12 + 1 = 253$
N	14	$f(14) = 2{\cdot}14^2 - 3 \cdot 14 + 1 = 351$
O	15	$f(15) = 2{\cdot}15^2 - 3 \cdot 15 + 1 = 406$
P	16	$f(16) = 2{\cdot}16^2 - 3 \cdot 16 + 1 = 465$
S	19	$f(19) = 2{\cdot}19^2 - 3 \cdot 19 + 1 = 666$
T	20	$f(20) = 2{\cdot}20^2 - 3 \cdot 20 + 1 = 741$
X	24	$f(24) = 2{\cdot}24^2 - 3 \cdot 24 + 1 = 1081$
,	27	$f(27) = 2{\cdot}27^2 - 3 \cdot 27 + 1 = 1378$
#	28	$f(28) = 2{\cdot}28^2 - 3 \cdot 28 + 1 = 1485$

Tabela 4.5: Codificadora da função quadrática I.

A mensagem cifrada é :

WJMPPZSPCPCJOFPMP

Cálculo da função inversa, decodificadora da imagem.

A parábola tem a concavidade voltada para cima, pois $a > 0$, admitindo assim um valor mínimo dado por $Y_v = -\dfrac{\Delta}{4a} = -\dfrac{b^2 - 4ac}{4a} = -\dfrac{(-3)^2 - 4 \cdot 2 \cdot 1}{4 \cdot 2} = -\dfrac{1}{8}$.
Portanto,

$Im(f) = \left[-\dfrac{1}{8}, +\infty\right)$ e $X_v = -\dfrac{b}{2a} = -\dfrac{(-3)}{2 \cdot 2} = \dfrac{3}{4}$, assim $D(f) = \left(-\infty, \dfrac{3}{4}\right]$ ou $D(f) = \left[\dfrac{3}{4}, +\infty\right)$, para que f seja inversível.

Aplicando a fórmula $x = \dfrac{-b \pm \sqrt{b^2 - 4a(c-y)}}{2a}$, tem-se:

$$x = \frac{-(-3) \pm \sqrt{(-3)^2 - 4 \cdot 2(1-y)}}{2 \cdot 2} = \frac{3 \pm \sqrt{9 - 8 + 8y}}{4} = \frac{3 \pm^{+}_{-} \sqrt{1 + 8y}}{4}.$$

Assim,

$$x = \frac{3+\sqrt{1+8y}}{4} \quad ou \quad x = \frac{3-\sqrt{1+8y}}{4}.$$

Logo, $f^{-1}(x) = \dfrac{3+\sqrt{1+8x}}{4}$ ou $f^{-1}(x) = \dfrac{3-\sqrt{1+8x}}{4}$.

i) Se $D(f) = \left[\dfrac{3}{4}, +\infty\right)$, a função conveniente é $f^{-1}(x) = \dfrac{3+\sqrt{1+8x}}{4}$;

ii) Se $D(f) = \left(-\infty, \dfrac{3}{4}\right]$ a função conveniente é $f^{-1}(x) = \dfrac{3-\sqrt{1+8x}}{4}$.

De acordo com Tabela 4.4, a função decodificadora conveniente é $f^{-1}(x) = \dfrac{3+\sqrt{1+8x}}{4}$.

Cálculo das imagens de $f^{-1}(x) = \dfrac{3+\sqrt{1+8x}}{4}$.

Sequência numérica	$f^{-1}(x) = \dfrac{3+\sqrt{1+8x}}{4}$	Letra
465	$f^{-1}(465) = \dfrac{3+\sqrt{1+8\cdot 465}}{4} = 16$	P
36	$f^{-1}(36) = \dfrac{3+\sqrt{1+8\cdot 36}}{4} = 5$	E
351	$f^{-1}(351) = \dfrac{3+\sqrt{1+8\cdot 351}}{4} = 14$	N
666	$f^{-1}(666) = \dfrac{3+\sqrt{1+8\cdot 666}}{4} = 19$	S
406	$f^{-1}(406) = \dfrac{3+\sqrt{1+8\cdot 406}}{4} = 15$	O
1378	$f^{-1}(1378) = \dfrac{3+\sqrt{1+8\cdot 1378}}{4} = 27$	,
253	$f^{-1}(253) = \dfrac{3+\sqrt{1+8\cdot 253}}{4} = 12$	L
78	$f^{-1}(78) = \dfrac{3+\sqrt{1+8\cdot 78}}{4} = 7$	G
1485	$f^{-1}(1485) = \dfrac{3+\sqrt{1+8\cdot 1485}}{4} = 28$	#
1081	$f^{-1}(1081) = \dfrac{3+\sqrt{1+8\cdot 1081}}{4} = 24$	X
136	$f^{-1}(136) = \dfrac{3+\sqrt{1+8\cdot 136}}{4} = 9$	I
741	$f^{-1}(741) = \dfrac{3+\sqrt{1+8\cdot 741}}{4} = 20$	T

Tabela 4.6: Decodificadora da função quadrática I.

A mensagem decifrada é: "PENSO, LOGO EXISTO".

Observe que a ordem das letras do nosso alfabeto, quando associadas aos números, não são levadas em conta. No Exemplo 4.3, associar-se-ão as letras do alfabeto com números inteiros negativos e positivos e utilizar-se-á uma função quadrática cifradora.

Exemplo 4.3.

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

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	#
3	4	5	6	7	8	9	10	11	12	13	14	15	16

Tabela 4.7: Tabela para codificação da função quadrática II.

Função cifradora: $f(x) = -3x^2 - x + 5$.

Mensagem a ser cifrada: "NÚMEROS INTEIROS E CRIPTOGRAFIA RSA".

Cálculos das imagens de $f(x) = -3x^2 - x + 5$.

Letra	Sequência numérica	Cálculo da imagem da função
A	-10	f(-10) = -3(-10)^2 − (−10) + 5 = −285
C	-8	f(-8) = -3(-8)^2 − (−8) + 5 = −179
E	-6	f(-6) = -3(-6)^2 − (−6) + 5 = −97
F	-5	f(-5) = -3(-5)^2 − (−5) + 5 = −65
G	-4	f(-4) = -3(-4)^2 − (−4) + 5 = −39
I	-2	f(-2) = -3(-2)^2 − (−2) + 5 = −5
M	2	f(2) = -3·2^2 − 2 + 5 = −9
N	3	f(3) = -3·3^2 − 3 + 5 = −25
O	4	f(4) = -3·4^2 − 4 + 5 = −47
P	5	f(5) = -3·5^2 − 5 + 5 = −75
R	7	f(7) = -3·7^2 − 7 + 5 = −149
S	8	f(8) = -3·8^2 − 8 + 5 = −195
T	9	f(9) = -3·9^2 − 9 + 5 = −247
U	10	f(10) = -3·10^2 − 10 + 5 = −305
#	16	f(16) = -3·16^2 − 16 + 5 = −779

Tabela 4.8: Codificadora da função quadrática II.

A mensagem cifrada é :

LRBORPXLFLXOFRPXLOLNRFNXPXRLXFLLRXL

Cálculo da função inversa, decodificadora da imagem.

A parábola tem a concavidade voltada para baixo, pois $a = -3 < 0$, admitindo assim, um valor máximo no ponto de abscissa

$$X_v = -\frac{b}{2a} = -\frac{(-1)}{2(-3)} = -\frac{1}{6}.$$

Assim,

$$Y_v = -\frac{\Delta}{4a} = -\frac{(-1)^2 - 4(-3)5}{4(-3)} = -\frac{61}{-12} = \frac{61}{12}.$$

Desse modo, tem-se que:

$$Im(f) = \left(-\infty, \frac{61}{12}\right] \quad e \quad D(f) = \left(-\infty, \frac{1}{6}\right] \quad ou \quad D(f) = \left[-\frac{1}{6}, +\infty\right)$$

para que f seja inversível, isto é , uma função bijetora.

Aplicando a fórmula $x = \dfrac{-b \pm \sqrt{b^2 - 4a(c-y)}}{2a}$, tem-se:

$$\begin{aligned} x &= \frac{-(-1) \pm \sqrt{(-1)^2 - 4(-3)(5-y)}}{2(-3)} = \frac{1 \pm \sqrt{1 + 60 - 12y}}{-6} \\ &= \frac{-1 \pm \sqrt{61 - 12y}}{6}. \end{aligned}$$

Portanto,

$$x = \frac{-1 + \sqrt{61 - 12y}}{6} \quad ou \quad x = \frac{-1 - \sqrt{61 - 12y}}{6}.$$

Logo,

$$f^{-1}(x) = \frac{-1 + \sqrt{61 - 12x}}{6} \quad ou \quad f^{-1}(x) = \frac{-1 - \sqrt{61 - 12x}}{6}.$$

i) Se $D(f) = \left(-\infty, -\dfrac{1}{6}\right]$, então a função inversa conveniente é

$$f^{-1}(x) = \frac{-1 - \sqrt{61 - 12x}}{6};$$

ii) Se $D(f) = \left[-\frac{1}{6}, +\infty\right)$, então a função inversa conveniente é

$$f^{-1}(x) = \frac{-1+\sqrt{61-12x}}{6}.$$

Cálculo das imagens de $f^{-1}(x) = \frac{-1 \pm \sqrt{61-12x}}{6}$.

Sequência numérica	Cálculo das imagens da função inversa	Letra
-285	$f^{-1}(-285) = \frac{-1-\sqrt{61-12(-285)}}{6} = -10$	A
-179	$f^{-1}(-179) = \frac{-1-\sqrt{61-12(-179)}}{6} = -8$	C
-97	$f^{-1}(-97) = \frac{-1-\sqrt{61-12(-97)}}{6} = -6$	E
-65	$f^{-1}(-65) = \frac{-1-\sqrt{61-12(-65)}}{6} = -5$	F
-39	$f^{-1}(-39) = \frac{-1-\sqrt{61-12(-39)}}{6} = -4$	G
-5	$f^{-1}(-5) = \frac{-1-\sqrt{61-12(-5)}}{6} = -2$	I
-9	$f^{-1}(-9) = \frac{-1+\sqrt{61-12(-9)}}{6} = 2$	M
-25	$f^{-1}(-25) = \frac{-1+\sqrt{61-12(-25)}}{6} = 3$	N
-47	$f^{-1}(-47) = \frac{-1+\sqrt{61-12(-47)}}{6} = 4$	O
-75	$f^{-1}(-75) = \frac{-1+\sqrt{61-12(-75)}}{6} = 5$	P
-149	$f^{-1}(-149) = \frac{-1+\sqrt{61-12(-149)}}{6} = 7$	R
-195	$f^{-1}(-195) = \frac{-1+\sqrt{61-12(-195)}}{6} = 8$	S
-247	$f^{-1}(-247) = \frac{-1+\sqrt{61-12(-247)}}{6} = 9$	T
-305	$f^{-1}(-305) = \frac{-1+\sqrt{61-12(-305)}}{6} = 10$	U
-779	$f^{-1}(-779) = \frac{-1+\sqrt{61-12(-779)}}{6} = 16$	#

Tabela 4.9: Decodificadora da função quadrática II.

A mensagem decifrada é: "NÚMEROS INTEIROS E CRIPTOGRAFIA RSA".

Exemplo 4.4.

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	27

Tabela 4.10: Tabela para codificação da função exponencial.

Função cifradora: $f(x) = 2^x$.

Mensagem a ser cifrada: "TENHA CORAGEM".

Cálculos das imagens de $f(x) = 2^x$.

Letra	Sequência numérica	Cálculo da imagem da função $f(x) = 2^x$
A	1	$f(1) = 2^1 = 2$
C	3	$f(3) = 2^3 = 8$
E	5	$f(5) = 2^5 = 32$
G	7	$f(7) = 2^7 = 128$
H	8	$f(8) = 2^8 = 256$
M	13	$f(13) = 2^{13} = 8192$
N	14	$f(14) = 2^{14} = 16384$
O	15	$f(15) = 2^{15} = 32768$
R	18	$f(18) = 2^{18} = 262144$
T	20	$f(20) = 2^{20} = 1048576$
#	27	$f(27) = 2^{27} = 134217728$

Tabela 4.11: Codificadora da função exponencial.

A mensagem cifrada é :

VFDVBHHHLBXFB

Cálculo da função inversa, decodificadora da imagem.

$f(x) = 2^x \Rightarrow y = 2^x \Rightarrow \log_2 y = \log_2 2^x \Rightarrow \log_2 y = x$, trocando x por y, tem-se

$$f^{-1}(x) = \log_2 x.$$

Cálculo das imagens de $f^{-1}(x) = \log_2 x$.

Mensagem recebida	Imagem da função inversa	Letra
2	$f^{-1}(2) = \log_2 2 = 1$	A
8	$f^{-1}(8) = \log_2 8 = 3$	C
32	$f^{-1}(32) = \log_2 32 = 5$	E
128	$f^{-1}(128) = \log_2 128 = 7$	G
256	$f^{-1}(256) = \log_2 256 = 8$	H
8192	$f^{-1}(8192) = \log_2 8192 = 13$	M
16384	$f^{-1}(16384) = \log_2 16384 = 14$	N
32768	$f^{-1}(32768) = \log_2 32768 = 15$	O
262144	$f^{-1}(262144) = \log_2 262144 = 18$	R
1048576	$f^{-1}(1048576) = \log_2 1048576 = 9$	T
134217728	$f^{-1}(134217728) = \log_2 134217728 = 27$	#

Tabela 4.12: Decodificadora da função exponencial.

A mensagem decifrada é: "TENHA CORAGEM".

Exemplo 4.5. Neste método de criptografia, o remetente vai usar uma matriz A para criptografar a mensagem e o destinatário uma matriz B de mesma ordem para decodificar.

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	27

Tabela 4.13: Tabela para codificação da matriz cifradora.

Matriz cifradora: $A = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$

Mensagem a ser cifrada: "TEORIA DOS NÚMEROS".

Tabela 4.14, com suas respectivas associações :

T	E	O	R	I	A	#	D	O	S	#	N	U	M	E	R	O	S
20	5	15	18	9	1	27	4	15	19	27	14	21	13	5	18	15	19

Tabela 4.14: Codificadora da matriz.

Como a matriz cifradora tem duas linhas e duas colunas, deve-se arranjar a sequência de números em uma matriz com duas linhas. Assim, a matriz mensagem será a matriz

$$M = \begin{bmatrix} 20 & 5 & 15 & 18 & 9 & 1 & 27 & 4 & 15 \\ 19 & 27 & 14 & 21 & 13 & 5 & 18 & 15 & 19 \end{bmatrix}$$

Se a mensagem tivesse uma quantidade ímpar de símbolos, poder-se-á completar a matriz com zeros ou qualquer outro número inteiro maior que 26.

Agora, para codificar a mensagem, multiplica-se a matriz M pela matriz cifradora A obtendo uma matriz N, isto é, $N = A \cdot M$ como segue:

$$N = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 20 & 5 & 15 & 18 & 9 & 1 & 27 & 4 & 15 \\ 19 & 27 & 14 & 21 & 13 & 5 & 18 & 15 & 19 \end{bmatrix}$$

Efetuando a multiplicação das matrizes, tem-se:

$$N = \begin{bmatrix} 155 & 150 & 115 & 159 & 92 & 28 & 171 & 87 & 140 \\ 58 & 59 & 43 & 60 & 35 & 11 & 63 & 34 & 53 \end{bmatrix}$$

Em seguida, alinha-se os elementos da matriz N para obter a mensagem cifrada.

A Mensagem cifrada é :

YTKCNBOIJFGQHIKKHA

Uma característica importante deste tipo de criptografia, é que enquanto havia repetições de números representando as letras repetidas na mensagem original, essas repetições não se preservam na mensagem cifrada.

Para decifrar a mensagem, faz-se os passos contrários, o primeiro passo a fazer é colocar a sequência numérica em uma matriz N de duas linhas :

$$N = \begin{bmatrix} 155 & 150 & 115 & 159 & 92 & 28 & 171 & 87 & 140 \\ 58 & 59 & 43 & 60 & 35 & 11 & 63 & 34 & 53 \end{bmatrix}$$

Em seguida, o destinatário de posse da matriz B decifradora, tal que, $A \cdot B = B \cdot A = I$, aplica a propriedade da multiplicação de matrizes $B \cdot N = B \cdot A \cdot M = I \cdot M = M$.

Sabendo que $B = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$, segue que:

$$M = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 155 & 150 & 115 & 159 & 92 & 28 & 171 & 87 & 140 \\ 58 & 59 & 43 & 60 & 35 & 11 & 63 & 34 & 53 \end{bmatrix}$$

Efetuando a multiplicação das matrizes tem-se:

$$M = \begin{bmatrix} 20 & 5 & 15 & 18 & 9 & 1 & 27 & 4 & 15 \\ 19 & 27 & 14 & 21 & 13 & 5 & 18 & 15 & 19 \end{bmatrix}$$

Colocando os números em uma sequência numérica e associando cada um a sua respectiva letra, conforme Tabela 4.15:

20	5	15	18	9	1	27	4	15	19	27	14	21	13	5	18	15	19
T	E	O	R	I	A	#	D	O	S	#	N	U	M	E	R	O	S

Tabela 4.15: Decodificadora da matriz.

A mensagem decifrada é: "TEORIA DOS NÚMEROS".

CAPÍTULO 5

APLICAÇÕES: ATIVIDADES LÚDICAS NO PROCESSO ENSINO-APRENDIZAGEM DA CRIPTOGRAFIA PARA O ENSINO MÉDIO

O presente capítulo tem como objetivo proporcionar ao leitor um aprimoramento do conteúdo até então apresentado, através de questões contextualizadas, cujas resoluções envolvam o conhecimento algébrico e a realidade que os cercam.

5.1 Atividades

Atividade 1. Considere a Tabela 5.1:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5

O	P	Q	R	S	T	U	V	W	X	Y	Z	#	?
6	7	8	9	10	11	12	13	14	15	16	17	18	19

Tabela 5.1: Tabela para codificação da atividade 1.

Suponha que Marcos e Antônio estejam trocando mensagens cifradas através de uma função afim. Marcos enviou a seguinte mensagem para Antônio:

GPQRXOREXXQPBPXMPXJXFUXLPC

e a informação de que $f(1) = 8$ e $f(-2) = -7$. Qual a mensagem enviada para Antônio?

Atividade 2. André, aluno do segundo ano do ensino médio e apaixonado por Luciana de sua turma, resolve mandar uma mensagem criptografada para ela sem que a turma saiba. André monta a seguinte Tabela 5.2, relacionando letras e números.

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	27

Tabela 5.2: Tabela para codificação da atividade 2.

Adotando $f(x) = 3x - 4$, como função cifradora, ou seja, a função que vai ocultar a mensagem, André manda a seguinte mensagem para Luciana:

YIOYJOEK

e envia também a Tabela 5.2, e a função cifradora $f(x) = 3x - 4$. Pergunta-se:

a) O que Luciana deve fazer para decodificar a mensagem?

b) Um grupo de alunos se apodera da tabela e da sequência numérica e ouviu André falar que usou a função afim para cifrar sua mensagem. Com base nessas informações, é possível descobrir a função e decifrar a mensagem enviada à Luciana?

Atividade 3. Usando a Tabela 5.2, da atividade 2, decodifique a frase criptografada:

PBNPSBRBLPBBRZYERSB

sendo que a função usada para cifrar a frase foi $f(x) = x^2 - 2x + 3$.

Atividade 4. Conforme a Tabela 5.3, e utilizando a função $f(x) = 2x^2 - 3x + 1$, como função cifradora, faça o que se pede:

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

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	#
3	4	5	6	7	8	9	10	11	12	13	14	15	16

Tabela 5.3: Tabela para codificação da atividade 4.

a) Cifre a frase **"É IMPORTANTE ESTUDAR MATEMÁTICA"**;

b) Ache a inversa da função cifradora $f(x) = 2x^2 - 3x + 1$;

c) Decodifique a frase cifrada:

BXHAZKZDZKHUHFHSXSH

Atividade 5. A seguinte palavra **PLHLBBV**, foi cifrada usando a função $f(x) = 2^x$ e a Tabela 5.4. Decodifique-a.

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	27

Tabela 5.4: Tabela para codificação da atividade 5.

Atividade 6. Uma das célebres frases de Isaac Newton foi criptografada usando a seguinte matriz

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{bmatrix}$$ e a Tabela 5.5:

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	27

Tabela 5.5: Tabela para codificação da atividade 6.

Obtendo a frase cifrada:

CONSTRUIMOSAMUXSUMROCSIWMGAFHKVLIMOHFRLADJ

Descubra a frase cifrada ?

Atividade 7. A chave de codificação do sistema RSA é (n, e), em que, $(n = pq)$ onde p e q são primos e $e \in \mathbb{N}$, tal que $mdc(e, \phi(n)) = 1$. Daí, tem-se que:

i) e é inversível módulo $\phi(n)$;

ii) $e \neq 1$ por motivo de segurança;

iii) $e \neq 2$, pelo fato que $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$ que é par.

Portanto, $e > 2$ e deve ser ímpar. Com essas informações, para codificar uma letra associada a um número inteiro, basta usar a seguite fórmula $C \equiv l^e(mod n)$. Em que l representa o valor numérico da letra que será codificada e C o valor numérico da letra codificada.

Adotando os primos $p = 5$ e $q = 11$, faça o que se pede:

a) Codifique a palavra **"CRIPTOGRAFIA"**. Usando a Tabela 5.6:

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

Tabela 5.6: Tabela para codificação da atividade 7.

b) como $mdc(e, \phi(n)) = 1$, então e possui um inverso multiplicativo. Assim, pode-se afirmar que existem inteiros a e b tal que $ae + b\phi(n) = 1$, onde a é o inverso modular de e. Para decifrar a palavra cifrada, basta aplicar a fórmula $l \equiv C^a(mod n)$.

Com base nessas informações, decodifique a palavra do item anterior.

Atividade 8. A mensagem $6355 - 5075$ foi codificada pelo método RSA usando a senha $n = 7597$ e $e = 4947$. Além disso, sabe-se que $\phi(n) = 7420$. Decodifique a mensagem. (Atividade retirada do livro Números Inteiros e Criptografia RSA, 2011, página 191).

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 5.7: Tabela para codificação da atividade 8.

5.2 Soluções das atividades

Atividade 1

Solução: De acordo com o enunciado a função é da forma $f(x) = ax + b$, com $a, b \in \mathbb{R}$, e $a \neq 0$.

Sabendo-se que $f(1) = 8$ e $f(-2) = -7$, pode-se achar a função cifradora por se tratar de uma equação da reta e como bastam dois pontos para determinar uma reta, tem-se:

$$\begin{cases} f(1) = a \cdot 1 + b = a + b = 8 \\ f(-2) = a \cdot (-2) + b = -2a + b = -7 \end{cases} \Longrightarrow \begin{cases} a + b = 8 \\ -2a + b = -7 \end{cases}$$

Resolvendo o sistema obtem-se $a = 5$ e $b = 3$ logo, $f(x) = 5x + 3$.

Agora, para decifrar a mensagem é preciso achar a função inversa de $f(x) = 5x + 3$ pelo fato de f ser bijetiva, para todo $x \in \mathbb{R}$. Então, $f(x) = y \Leftrightarrow f(y) = x$, segue que:

$5x + 3 = y \Leftrightarrow 5y + 3 = x$, isolando y tem-se:

$$y = \frac{x-3}{5}.$$

Portanto, $f^{-1}(x) = \frac{x-3}{5}$.

Cada letra da frase cifrada corresponde a um dos restos: 0, 1, 2, 3, ... ,25. Obtidos pela divisão das imagens de f maiores que 26 por 26. Tem-se que, para todo x pertencente a Tabela 5.1, implica que, $f(x) = y \equiv a \ (mod\ 26)$, onde a pertence a Tabela 5.1.

Assim,

$f(-8) = -37 \equiv -11 \equiv 15 \ (mod\ 26); f(-7) = -32 \equiv -6 \equiv 20 \ (mod\ 26);$

$f(-6) = -27 \equiv -1 \ (mod\ 26); f(-5) = -22 \equiv 4 \ (mod\ 26); f(-4) = -17 \equiv 9 \ (mod\ 26);$

$f(-3) = -12 \equiv 14 \ (mod\ 26); f(-2) = -7 \equiv 19 \ (mod\ 26); f(-1) = -2 \equiv -2 \ (mod\ 26);$

$f(0) = 3 \equiv 3 \ (mod\ 26); f(1) = 8 \equiv 8 \ (mod\ 26); f(2) = 13 \equiv 13 \ (mod\ 26);$

$f(4) = 23 \equiv -3 \ (mod\ 26); f(5) = 28 \equiv 2 \ (mod\ 26); f(6) = 33 \equiv 7 \ (mod\ 26);$

$f(7) = 38 \equiv 12 \ (mod\ 26); f(8) = 43 \equiv 17 \ (mod\ 26); f(9) = 48 \equiv -4 \ (mod\ 26);$

$f(10) = 53 \equiv 1 \ (mod\ 26); f(11) = 58 \equiv 6 \ (mod\ 26); f(12) = 63 \equiv 11 \ (mod\ 26);$

$f(13) = 68 \equiv 16 \ (mod\ 26); f(14) = 73 \equiv -5 \ (mod\ 26); f(15) = 78 \equiv 0 \ (mod\ 26);$

$f(16) = 83 \equiv 5 \ (mod\ 26); f(17) = 88 \equiv 10 \ (mod\ 26); f(18) = 93 \equiv 15 \ (mod\ 26);$

$f(19) = 98 \equiv -6 \ (mod\ 26).$

Outra alternativa de achar as imagens de f através dos inteiros, é usando a definição de congruência, isto é, sendo $f(x) = y \equiv a \ (mod\ 26)$, tem-se que:

$$26|(y - a).$$

Logo, existe um $k \in \mathbb{Z}$, tal que $y - a = 26k$.

Segue que,

$$y = 26k + a,$$

com $k \in \mathbb{Z}$ e a pertence a Tabela 5.1. Para achar o valor de y, usa-se a função inversa de f.

Assim,

$$f^{-1}(y) = \frac{26k + a - 3}{5}, \text{ com } -8 \leq f^{-1}(y) \leq 19.$$

Para $a = -2$, segue que:

$$f^{-1}(y) = \frac{26k - 5}{5} \Rightarrow -8 \leq \frac{26k - 5}{5} \leq 19 \Rightarrow -40 \leq 26k - 5 \leq 95 \Rightarrow -35 \leq 26k \leq 100.$$

Consequentemente, os possíveis valores para k, são -1, 0, 1, 2, 3. Por inspeção segundo a Tabela 5.1, $k = 0$.

Portanto, $y = -2 \Rightarrow f^{-1}(-2) = -1 \rightarrow \mathbf{H}$.

Para $a = 7$, segue que:

$$f^{-1}(y) = \frac{26k + 4}{5} \Rightarrow -8 \leq \frac{26k + 4}{5} \leq 19 \Rightarrow -40 \leq 26k - 5 \leq 95 \Rightarrow -40 \leq 26k \leq 91.$$

Consequentemente, os possíveis valores para k, são -1, 0, 1, 2, 3. Por inspeção segundo a Tabela 5.1, $k = 1$.

Portanto, $y = 33 \Rightarrow f^{-1}(33) = 6 \rightarrow \mathbf{O}$.

Para $a = 8$, segue que:

$$f^{-1}(y) = \frac{26k + 5}{5} \Rightarrow -8 \leq \frac{26k + 5}{5} \leq 19 \Rightarrow -40 \leq 26k + 5 \leq 95 \Rightarrow -45 \leq 26k \leq 90.$$

Consequentemente, os possíveis valores para k, são -1, 0, 1, 2, 3. Por inspeção segundo a Tabela 5.1, $k = 0$.

Portanto, $y = 8 \Rightarrow f^{-1}(8) = 1 \rightarrow \mathbf{J}$.

Para $a = 9$, segue que:

$$f^{-1}(y) = \frac{26k + 6}{5} \Rightarrow -8 \leq \frac{26k + 9}{5} \leq 19 \Rightarrow -40 \leq 26k + 9 \leq 95 \Rightarrow -49 \leq 26k \leq 86.$$

Consequentemente, os possíveis valores para k, são -1, 0, 1, 2, 3. Por inspeção segundo a Tabela 5.1, $k = -1$.

Portanto, $y = -17 \Rightarrow f^{-1}(-17) = -4 \rightarrow \mathbf{E}$.

E assim por diante, segue o resultado. Pode haver casos de ambiguidades. Nestes casos, é só verificar que letra se encaixa melhor na palavra, ou seja que tenha sentido.

As estratégias apresentadas até aqui serão aplicadas nas demais atividades, cujos cálculos serão omitidos. É aconselhável o uso da primeira pela praticidade e agilidade.

O processo de decifragem, está na Tabela 5.8:

Mensagem recebida	Imagem da função inversa	Letra
-2	$f^{-1}(-2) = (-2-3)/5 = -1$	H
33	$f^{-1}(33) = (33-3)/5 = 6$	O
8	$f^{-1}(8) = (8-3)/5 = 1$	J
-17	$f^{-1}(-17) = (-17-3)/5 = -4$	E
93	$f^{-1}(93) = (93-3)/5 = 18$	#
58	$f^{-1}(58) = (58-3)/5 = 11$	T
48	$f^{-1}(48) = (48-3)/5 = 9$	R
-37	$f^{-1}(-37) = (-37-3)/5 = -8$	A
-7	$f^{-1}(-7) = (-7-3)/5 = -2$	G
-22	$f^{-1}(-22) = (-22-3)/5 = -5$	D
53	$f^{-1}(53) = (53-3)/5 = 10$	S
23	$f^{-1}(23) = (23-3)/5 = 4$	M
38	$f^{-1}(38) = (38-3)/5 = 7$	P
3	$f^{-1}(3) = (3-3)/5 = 0$	I
98	$f^{-1}(98) = (98-3)/5 = 19$	?

Tabela 5.8: Decodificadora da atividade 1.

Obtendo, **"HOJE TERÁ JOGO DO SAMPAIO ?"**

Atividade 2

a) **solução:** Para decodificar a mensagem, primeiramente Luciana deve achar a inversa da função $f(x) = 3x - 4$, como segue:

$f(x) = y \Leftrightarrow f(y) = x \Rightarrow 3x - 4 = y \Leftrightarrow 3y - 4 = x$, isolando y tem-se:

$$y = \frac{x+4}{3}.$$

Portanto, $f^{-1}(x) = \frac{x+4}{3}$.

Segue o processo de decifragem, conforme Tabela 5.9:

Mensagem recebida	Imagem da função inversa	Letra
-1	$f^{-1}(-1) = \frac{-1+4}{3} = 1$	A
35	$f^{-1}(35) = \frac{35+4}{3} = 13$	M
41	$f^{-1}(41) = \frac{41+4}{3} = 15$	O
77	$f^{-1}(77) = \frac{77+4}{3} = 27$	#
62	$f^{-1}(62) = \frac{62+4}{3} = 22$	V
41	$f^{-1}(41) = \frac{41+4}{3} = 15$	O
5	$f^{-1}(5) = \frac{5+4}{3} = 3$	C
11	$f^{-1}(11) = \frac{11+4}{3} = 5$	E

Tabela 5.9: Decodificadora da atividade 2.

Obtendo, **"AMO VOCÊ".**

b) **Solução:** sim, pois como se trata de uma função afim que representa uma reta, basta que os alunos achem duas associações corretas entre números da sequência original e codificada.

Atividade 3

Solução: Para decodificar a frase é preciso achar a inversa da função $f(x) = x^2 - 2x + 3$.

Já é sabido que deve-se limitar o domínio da função para que exista a inversa.

Como $a = 1 > 0$, a parábola tem a concavidade voltada para cima admitindo assim, um valor mínimo dado por

$$Y_v = -\frac{b^2 - 4ac}{4a} = -\frac{(-2)^2 - 4 \cdot 1 \cdot 3}{4 \cdot 1} = 2.$$

Logo, $Im(f) = [2, +\infty)$.

$X_v = -\frac{b}{2a} = -\frac{(-2)}{2 \cdot 1} = 1$, portanto $D(f) = (-\infty, 1]$ ou $D(f) = [1, +\infty)$ para que f seja inversível.

Pode-se obter a função inversa usando a fórmula $x = \frac{-b \pm \sqrt{b^2 - 4a(c-y)}}{2a}$.

Assim,

$$x = \frac{-(-2) \pm \sqrt{(-2)^2 - 4 \cdot 1(3-y)}}{2 \cdot 1} = \frac{2 \pm \sqrt{-8 + 4y}}{2} = 1 \pm \sqrt{-2 + y}.$$

Portanto,

$$f^{-1}(x) = 1 + \sqrt{-2 + x} \quad \text{ou} \quad f^{-1}(x) = 1 - \sqrt{-2 + x}.$$

Como nessa tabela só possui inteiros positivos, a função conveniente é $f^{-1}(x) = 1 + \sqrt{-2 + x}$.

Segue o processo de decifragem, conforme Tabela 5.10:

Mensagem recebida	Imagem da função inversa	Letra
198	$f^{-1}(198) = 1 + \sqrt{-2 + 198} = 15$	O
678	$f^{-1}(678) = 1 + \sqrt{-2 + 678} = 27$	#
326	$f^{-1}(326) = 1 + \sqrt{-2 + 326} = 19$	S
123	$f^{-1}(123) = 1 + \sqrt{-2 + 123} = 12$	L
18	$f^{-1}(18) = 1 + \sqrt{-2 + 18} = 5$	E
402	$f^{-1}(402) = 1 + \sqrt{-2 + 402} = 21$	U
146	$f^{-1}(146) = 1 + \sqrt{-2 + 146} = 13$	M
2	$f^{-1}(2) = 1 + \sqrt{-2 + 2} = 1$	A
363	$f^{-1}(363) = 1 + \sqrt{-2 + 363} = 20$	T
291	$f^{-1}(291) = 1 + \sqrt{-2 + 291} = 18$	R

Tabela 5.10: Decodificadora da atividade 3.

Obtendo, **"O SOL É UMA ESTRELA".**

Atividade 4

Solução:

a) Numerando as letras da frase de acordo com a tabela e calculando o valor das imagens através da função $f(x) = 2x^2 - 3x + 1$, obtem-se:

Letra	Sequência númérica	Cálculo da imagem da função
A	-10	$f(-10) = 231$
C	-8	$f(-8) = 153$
D	-7	$f(-7) = 120$
E	-6	$f(-6) = 91$
I	-2	$f(-2) = 15$
M	2	$f(2) = 3$
N	3	$f(3) = 10$
O	4	$f(4) = 21$
P	5	$f(5) = 36$
R	7	$f(7) = 78$
S	8	$f(8) = 105$
T	9	$f(9) = 136$
U	10	$f(10) = 171$
#	16	$f(16) = 465$

Tabela 5.11: Codificadora da atividade 4.

Assim, a frase cifrada fica:

XHZNWFKQHUQXHXLQZAHKHNHQXNHQZHH.

b) Como $a = 2 > 0$, a parábola tem a concavidade voltada para cima, admitindo assim, um valor mínimo dado por

$$Y_v = -\frac{b^2 - 4ac}{4a} = -\frac{(-3)^2 - 4 \cdot 2 \cdot 1}{4 \cdot 2} = \frac{-1}{8}.$$

Então, $Im(f) = \left[\frac{-1}{8}, +\infty\right)$.

$X_v = -\frac{b}{2a} = -\frac{(-3)}{2 \cdot 2} = \frac{3}{4}$, portanto $D(f) = (-\infty, \frac{3}{4}]$ ou $D(f) = [\frac{3}{4}, +\infty)$ para que f seja inversível.

Pode-se obter a função inversa usando a fórmula $x = \dfrac{-b \pm \sqrt{b^2 - 4a(c-y)}}{2a}$.

Assim,

$$x = \frac{-(-3) \pm \sqrt{(-3)^2 - 4 \cdot 2(1-y)}}{2 \cdot 2} = \frac{3 \pm \sqrt{1+8y}}{4}.$$

Portanto, $f^{-1}(x) = \dfrac{3+\sqrt{1+8x}}{4}$ ou $f^{-1}(x) = \dfrac{3-\sqrt{1+8x}}{4}$.

i) Se $D(f) = \left(-\infty, \dfrac{3}{4}\right]$, a função conveniente é $f^{-1}(x) = \dfrac{3-\sqrt{1+8x}}{4}$;

ii) Se $D(f) = \left[\dfrac{3}{4}, +\infty\right)$, a função conveniente é $f^{-1}(x) = \dfrac{3+\sqrt{1+8x}}{4}$.

c) Usando a função inversa conveniente do item b, obtem-se:

Mensagem recebida	Imagem da função inversa	Letra
105	$f^{-1}(105) = \dfrac{3+\sqrt{1+8\cdot 105}}{4} = 8$	S
91	$f^{-1}(91) = \dfrac{3-\sqrt{1+8\cdot 91}}{4} = -6$	E
465	$f^{-1}(465) = \dfrac{3+\sqrt{1+8\cdot 465}}{4} = 16$	#
120	$f^{-1}(120) = \dfrac{3-\sqrt{1+8\cdot 120}}{4} = -7$	D
15	$f^{-1}(15) = \dfrac{3-\sqrt{1+8\cdot 15}}{4} = -2$	I
78	$f^{-1}(78) = \dfrac{3+\sqrt{1+8\cdot 78}}{4} = 7$	R
45	$f^{-1}(45) = \dfrac{3-\sqrt{1+8\cdot 45}}{4} = -4$	G
10	$f^{-1}(10) = \dfrac{3+\sqrt{1+8\cdot 10}}{4} = 3$	N
231	$f^{-1}(231) = \dfrac{3-\sqrt{1+8\cdot 231}}{4} = -10$	A
21	$f^{-1}(21) = \dfrac{3+\sqrt{1+8\cdot 21}}{4} = 4$	O
190	$f^{-1}(190) = \dfrac{3-\sqrt{1+8\cdot 190}}{4} = -9$	B

Tabela 5.12: Decodificadora da atividade 4.

Obtendo, **"SE DIRIGIR NÃO BEBA".**

Atividade 5

Solução: para decifrar a mensagem, é preciso achar a função inversa da exponencial $f(x) = 2^x$.

Como a inversa da função exponencial é a função logarítmica, segue os cálculos:

$f(x) = 2^x \Rightarrow y = 2^x \Rightarrow \log_2 y = \log_2 2^x \Rightarrow \log_2 y = x$, trocando x por y, tem-se:

$$f^{-1}(x) = \log_2 x.$$

Segue o processo de decifragem, conforme tabela 5.13:

Mensagem recebida	Imagem da função inversa	Letra
65536	$f^{-1}(65536) = \log_2 65536 = 16$	P
262144	$f^{-1}(262144) = \log_2 262144 = 18$	R
32768	$f^{-1}(32768) = \log_2 32768 = 15$	O
64	$f^{-1}(64) = \log_2 64 = 6$	F
8192	$f^{-1}(8192) = \log_2 8192 = 13$	M
2	$f^{-1}(2) = \log_2 2 = 1$	A
1048576	$f^{-1}(1048576) = \log_2 1048576 = 22$	T

Tabela 5.13: Decodificadora da atividade 5.

Obtendo, **"PROFMAT".**

Atividade 6

Solução: Para decifrar a mensagem deve-se achar a matriz inversa de A. Como $det(A) \neq 0$, existe uma matriz B, tal que $AB = BA = I$.

Seja B uma matriz quadrada de mesma ordem de A, tem-se:

$$B = \begin{bmatrix} a & b & c \\ e & f & g \\ h & i & j \end{bmatrix}.$$

Assim,

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Efetuando a multiplicação das matrizes e usando a propriedade da igualdade, obtem-se um sistema de equações. Resolvendo esse sistema, tem-se $a = 1, b = 0, c = 0$, d= -2, e=1, f=0, g=1, h= -2,i=1.

Portanto,

$$B = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & -2 & 1 \end{bmatrix}$$

Como há 42 números codificados, pode-se montar uma matriz M, com 3 linhas e 14 colunas como segue:

$$M = \begin{bmatrix} 3 & 15 & 14 & 19 & 20 & 18 & 21 & 9 & 13 & 15 & 19 & 27 & 13 & 21 \\ 24 & 45 & 47 & 65 & 44 & 41 & 55 & 19 & 35 & 49 & 65 & 59 & 53 & 58 \\ 60 & 89 & 100 & 116 & 87 & 91 & 93 & 34 & 84 & 96 & 116 & 105 & 108 & 114 \end{bmatrix}$$

Seja N a matriz mensagem original, tem-se que $M = AN \Rightarrow BM = BAN = IN = N$.

Assim,

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 & 15 & 14 & 19 & 20 & 18 & 21 & 9 & 13 & 15 & 19 & 27 & 13 & 21 \\ 24 & 45 & 47 & 65 & 44 & 41 & 55 & 19 & 35 & 49 & 65 & 59 & 53 & 58 \\ 60 & 89 & 100 & 116 & 87 & 91 & 93 & 34 & 84 & 96 & 116 & 105 & 108 & 114 \end{bmatrix}$$

Fazendo a multiplicação das matrizes, tem-se:

$$N = \begin{bmatrix} 3 & 15 & 14 & 19 & 20 & 18 & 21 & 9 & 13 & 15 & 19 & 27 & 13 & 21 \\ 18 & 15 & 19 & 27 & 4 & 5 & 13 & 1 & 9 & 19 & 27 & 5 & 27 & 16 \\ 15 & 14 & 20 & 5 & 19 & 27 & 4 & 5 & 27 & 13 & 5 & 14 & 15 & 19 \end{bmatrix}$$

Portanto, consultando a tabela e associando os números da matriz da esquerda para a direita e de cima para baixo, obtem-se:

"CONSTRUÍMOS MUROS DEMAIS E PONTES DE MENOS".

Atividade 7

Solução:

a) Sendo $C \equiv l^e \ (mod\ n)$ a fórmula de codificação, precisa-se achar a chave de codificação (n, e). Tem-se que:

$$\phi(n) = \phi(pq) = (p-1)(q-1), \text{ implica } \phi(55) = 40.$$

Segue que,

$mdc(\phi(n), e) = 1$ implica que $mdc(40, e) = 1$, logo $e = 3$, que é o menor primo, tal que $mdc(40, 3) = 1$. Como l representa a letra com seu valor numérico a ser criptografada, tem-se a Tabela 5.14.

Palavra	Cálculos através $C \equiv l^e \ (mod\ 55)$	Valor da letra criptografada
C	$C \equiv 3^3 \equiv 27 \ (mod\ 55) \equiv 27$	27
R	$C \equiv 18^3 \equiv 5832 \ (mod\ 55) \equiv 2$	2
I	$C \equiv 9^3 \equiv 729 \ (mod\ 55) \equiv 14$	14
P	$C \equiv 16^3 \equiv 4096 \ (mod\ 55) \equiv 26$	26
T	$C \equiv 20^3 \equiv 8000 \ (mod\ 55) \equiv 25$	25
O	$C \equiv 15^3 \equiv 3375 \ (mod\ 55) \equiv 20$	20
G	$C \equiv 7^3 \equiv 343 \ (mod\ 55) \equiv 13$	13
A	$C \equiv 1^3 \equiv 1 \ (mod\ 55) \equiv 56$	56
F	$C \equiv 6^3 \equiv 216 \ (mod\ 55) \equiv 51$	51

Tabela 5.14: Codificadora da atividade 7.

Portanto, a palavra criptografada é **"ABNZYTMBDYND".**

b) Como e é coprimo de $\phi(n)$, ele obrigatoriamente tem um inverso multiplicativo, visto que, $mdc(e, \phi(n)) = 1$. Então existem a e b inteiros, tal que $ae + b\phi(n) = 1$, ou seja $3a + 40b = 1$ onde a é o inverso modular de e.

Para achar a e b, usa-se o algoritmo de Euclides estendido, Tabela 5.15:

Restos	Quocientes	x	y
40	$*$	1	0
3	$*$	0	1
1	13	$1 - 13 \cdot 0 = 1$	$0 - 1 \cdot 13 = -13$
0	3		

Tabela 5.15: Algortimo da atividade 7.

Portanto, tem-se $-13 \cdot 3 + 1 \cdot 40 = 1$, isto é $a = -13$, como a deve ser positivo, toma-se $a = 27$ pois, 27 é o menor inteiro positivo, tal que $27 \equiv -13 \ (mod\ 40)$.

Assim, usando a fórmula $l \equiv C^a \ (mod\ n)$, obtem-se a decodificação:

$$C = 27 \Rightarrow l \equiv 27^{27} \equiv (3^3)^{27} \equiv 3^{81} \ (mod\ 55),$$

como $(3, 55) = 1$, então pela função ϕ de Euler, tem-se:

$3^{\phi(55)} \equiv 1 \ (mod\ 55) \Rightarrow 3^{40} \equiv 1 \ (mod\ 55) \Rightarrow 3^{80} \equiv 1 \ (mod\ 55) \Rightarrow 3^{81} \equiv 3 \ (mod\ 55)$.
Logo, $l \equiv 27^{27} \equiv 3 \ (mod\ 55)$.

$$C = 2 \Rightarrow l \equiv 2^{27} \equiv 134217728 \equiv 18 \ (mod\ 55).$$

$$C = 14 \Rightarrow l \equiv 14^{27} \ (mod\ 55).$$

Perceba que, $14^{27} = 2^{27} \cdot 7^{27}$, tem-se que, $2^{27} \equiv 18 \ (mod\ 55)$.

$7^9 \equiv 40353607 \equiv 52 \ (mod\ 55) \Rightarrow 7^{27} \equiv 52^3 \equiv 28 \ (mod\ 55) \Rightarrow l \equiv 14^{27} \equiv 18 \cdot 28 \equiv$
$504 \equiv 9 \ (mod\ 55)$.

$$C = 26 \Rightarrow l \equiv 26^{27} \ (mod\ 55).$$

Perceba que, $26^{27} = 2^{27} \cdot 13^{27}$, tem-se que, $2^{27} \equiv 18 \ (mod\ 55)$.

$13^3 \equiv 2197 \equiv 52 \ (mod\ 55) \Rightarrow 13^9 \equiv 52^3 \equiv 140608 \equiv 28 \ (mod\ 55) \Rightarrow 13^{27} \equiv 28^3 \equiv$
$21952 \equiv 7 \ (mod\ 55) \Rightarrow l \equiv 26^{27} \equiv 18 \cdot 7 \equiv 126 \equiv 16 \ (mod\ 55)$.

$$C = 25 \Rightarrow l \equiv 25^{27} \equiv 5^{54} \ (mod\ 55).$$

Perceba que, $5^9 \equiv 1953125 \equiv 20\ (mod\ 55) \Rightarrow l \equiv 5^{54} \equiv 20^6 \equiv 20\ (mod\ 55)$.

$$C = 20 \Rightarrow l \equiv 20^{27}\ (mod\ 55).$$

Perceba que, $20^{27} = 2^{27}.2^{27}.5^{27}$ e $5^9 \equiv 20\ (mod\ 55) \Rightarrow 5^{27} \equiv 20^3 \equiv 8000 \equiv 25\ (mod\ 55) \Rightarrow l \equiv 20^{27}\ (mod\ 55) \equiv 18.18.25 \equiv 8100 \equiv 15\ (mod\ 55)$.

$$C = 13 \Rightarrow l \equiv 13^{27}\ (mod\ 55).$$

Esse cálculo foi feito acima, logo $l \equiv 13^{27} \equiv 7\ (mod\ 55)$.

$$C = 56 \Rightarrow l \equiv 56^{27}\ (mod\ 55).$$

Perceba que, $56^{27} = 7^{27}.8^{27} = 7^{27}.2^{27}.2^{27}.2^{27} \Rightarrow l \equiv 56^{27} \equiv 28.18.18.18 \equiv 163296 \equiv 1\ (mod\ 55)$.

$$C = 51 \Rightarrow l \equiv 51^{27}\ (mod\ 55).$$

Perceba que, $51^{27} = 3^{27}.17^{27}$, tem-se $17^3 \equiv 4913 \equiv 18\ (mod\ 55) \Rightarrow 17^9 \equiv 18^3 \equiv 5832 \equiv 2\ (mod\ 55) \Rightarrow 17^{27} \equiv 8\ (mod\ 55)$.

$3^9 \equiv 19683 \equiv 48\ (mod\ 55) \Rightarrow 3^{27} \equiv 48^3 \equiv 110592 \equiv 42\ (mod\ 55)$.

Portanto, $l \equiv 51^{27} \equiv 42.8 \equiv 336 \equiv 6\ (mod\ 55)$.

Assim, tem-se a Tabela 5.16.

3	18	9	16	20	15	7	18	1	6	9	1
C	R	I	P	T	O	G	R	A	F	I	A

Tabela 5.16: Decodificadora da atividade 7.

Atividade 8

Solução: Como $mdc(e, \phi(n)) = 1$. Então existem a e b inteiros, tal que $ae + b\phi(n) = 1$, ou seja $4947a + 7420b = 1$ onde a é o inverso modular de e. Pelo algoritmo de Euclides estendido, tem-se a Tabela 5.17:

Restos	Quocientes	x	y
7420	$*$	1	0
4947	$*$	0	1
2473	1	1	-1
1	2	-2	3
0	2473	$*$	$*$

Tabela 5.17: Algoritmo da atividade 8.

Portanto, $(-2).7420 + 3.4947 = 1$, assim $a = 3$.

Para decodificar, faz-se o uso da fórmula da atividade 7.

$6355^2 = 40386025 \equiv 373$ $(mod\ 7596)$.

$6355^3 \equiv 373.6355 \equiv 2370415 \equiv 151$ $(mod\ 7596)$.

Logo, $l = 151$.

$5075^2 = 25755625 \equiv 1795$ $(mod\ 7596)$.

$5075^3 \equiv 1795.5075 \equiv 9109625 \equiv 822$ $(mod\ 7596)$.

Logo, $l = 822$.

Portanto, tem-se o bloco **151822**. Quebrando o bloco adequadamente, obtem-se a Tabela 5.18.

15	18	22
F	I	M

Tabela 5.18: Decodificando

CAPÍTULO 6

CONSIDERAÇÕES FINAIS

Ao longo deste estudo, meramente instrutivo, verificou-se uma preocupação extremamente contundente em relação à árdua tarefa dos professores de Matemática no que tange à desmistificação de que a disciplina que lecionam seja ″completamente inútil″ e que, por outro lado, deveria ser considerada, inclusive, a musa das Ciências Exatas e Naturais. Isso, porque a Matemática está presente na Física, na Química, na Biologia, entre outras também importantes disciplinas do nosso cotidiano através de situações comuns, como a entrega e o recebimento de um troco no supermercado, o cálculo mental do tempo ao atravessar a rua, a leitura das horas, o cálculo da média escolar, etc.

Por motivos já explicitados, é imprescindível que os alunos percebam a utilidade e a aplicação dos conteúdos trabalhados em sala de aula. Para isso, é tarefa dos professores levarem conteúdos corriqueiros e também modernos para que se sintam do processo ensino-aprendizagem.

A escolha da temática Criptografia com uma abordagem para o Ensino Médio é um perfeito exemplo de como essa metodologia pode e deve dar certo, pois alia a obtenção de conhecimentos matemáticos com a necessidade de comunicar-se, em especial, com segurança e através da tecnologia.

As atividades desenvolvidas mostram que a Criptografia é uma ferramenta poderosa que estimula a criatividade, a curiosidade e a imaginação. À Matemática, por sua vez, deve-se parte do seu avanço, já que esta delineia estratégias com o propósito de tornar as codificações cada vez mais complexas e difíceis.

Com uma combinação tão perfeita, não há o que se temer em relação ao aprendizado

contextualizado. A aprendizagem eficaz é justamente aquela que compreende conhecimento teórico e a visualização, ou mesmo vivência, da prática, o que torna o processo bem mais interessante.

O resultado principal é que os alunos serão despertados para o aprofundamento do assunto aqui tratado para, quem sabe, criarem novos códigos, contribuindo para o sistema de segurança futuro.

Referências Bibliográficas

[1] ALECRIM, E. **História e Aplicações da Criptografia.** Disponível em $< http : //www.infowester.com/criptografia.php. >$. Acesso em 26 JUL 2016.

[2] BRASIL, MEC/SEF.; Parâmetros curriculares nacionanais: Matemática, Brasília,1997.

[3] BUCHMANN, J. **Introdução à criptografia.** São Paulo: Berkeley, 2002.

[4] BROWN, D. **Fortaleza digital.** Tradução de Carlo Irineu da Costa. 2. ed. Rio de Janeiro: Sextante, 2008.

[5] COUTINHO, S.C. **Números inteiros e criptografia RSA**. 2ªed. Rio de Janeiro: IMPA, 2011.

[6] FERRONI, Marcelo. **Quebrando códigos.** Revista Galileu Especial Eureca. Globo: 2003. p. 34-35.

[7] HOHENWARTER, M.**GEOGEBRA**.Disponível em :$< www.geogebra.org >$. Acessado em 20 de Abril de 2016.

[8] HOWARD, A.; RORRES, C. **Álgebra linear com aplicações.** 8. ed. Porto Alegre: Bookmann, 2001.

[9] IEZZI, G.; MURAKAMI, C. **Fundamentos de matemática elementar.** 8. ed. São Paulo: Atual, 2004. v.1.

[10] IEZZI, G.; HAZZAN, S. **Fundamentos de matemática elementar.** 8. ed. São Paulo: Atual, 2004. v.4.

[11] LIMA,E.L.;**Geometria analítica e Álgebra linear**.Rio de Janeiro, IMPA,2001.

[12] LIMA,E.L.;CARVALHO, P.C.P.;WAGNER, E.;MORGADO, A.C.**A matemática do ensino médio**. 10. ed.Rio de Janeiro: SBM ,2012. v.1.

[13] MENEZES, L.A.; CARVALHO, M.P. **Criptografia na sala de aula.** In X Encontro Nacional de Educação Matemática. 2010, Salvador-Bahia. Anais do X Encontro Nacional de Educação Matemática. Sociedade Brasileira de Educação Matemática. Ilhéus, Bahia: Via Litterarum, 2010.

[14] MUNIZ NETO, A.C. **Tópicos de matemática elementar**: teoria dos números. 2. ed. Rio de Janeiro: SBM, 2013. v. 5.

[15] SANTOS, J.P.O. **Introdução à teoria dos números.** 3. ed. Rio de Janeiro: IMPA, 2012. 2. ed. Rio de Janeiro: SBM, 2013. 5 v.

[16] SINGH, S. **O livro dos códigos.** Tradução de Jorge Calife. Rio de Janeiro: Record, 1999.

[17] TAMAROZZI, A.C. **Codificando e decifrando mensagens.** In Revista do Professor de Matemática 45. SBM, 2001. p. 41-47.

[18] TERADA, R. **Criptografia e a importância das suas aplicações.** In Revista do Professor de Matemática 12. Rio de Janeiro: SBM, 1988.