UNIVERSIDADE LUTERANA DO BRASIL

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM ENSINO DE CIÊNCIAS E MATEMÁTICA

CLARISSA DE ASSIS OLGIN

CURRÍCULO NO ENSINO MÉDIO: UMA EXPERIÊNCIA COM O TEMA CRIPTOGRAFIA

Dissertação apresentada ao Programa de Pós - Graduação em Ensino de Ciências e Matemática da Universidade Luterana do Brasil para obtenção do título de mestre em Ensino de Ciências e Matemática.

Orientadora: Profª Drª Claudia Lisete Oliveira Groenwald

Canoas, 2011

CLARISSA DE ASSIS OLGIN

CURRÍCULO NO ENSINO MÉDIO: UMA EXPERIÊNCIA COM O TEMA CRIPTOGRAFIA

Orientadora: Profª Drª Claudia Lisete Oliveira Groenwald

Dissertação de Mestrado apresentada ao Programa de Pós - Graduação em Ensino de Ciências e Matemática da Universidade Luterana do Brasil para obtenção do título de Mestre em Ensino de Ciências e Matemática.

Área de concentração: Ensino e Aprendizagem em Ensino de Ciências e Matemática.

BANCA EXAMINADORA

Profª Drª Carmen Teresa Kaiber – ULBRA

Prof. Dr. Arno Bayer – ULBRA

Prof. Dr. Marcio Antonio da Silva – UFMS

Dedico este trabalho à minha família, em especial à minha mãe e minha irmã, que muito me ajudaram durante o percurso acadêmico.

AGRADECIMENTO

Agradeço a Deus, pois Ele colocou ao meu lado pessoas tão especiais como a minha família.

À minha mãe, Maria de Lourdes Nunes de Assis, um especial agradecimento, pelo amor, carinho e incondicional auxílio durante o percurso acadêmico.

À minha irmã, Larissa Olgin da Silva, pela amizade e constante presença, auxiliando-me nos momentos de necessidade.

À Professora Doutora Claudia Lisete Oliveira Groenwald pelo trabalho de orientação desenvolvido com competência, dedicação e amizade.

Aos Professores Doutores Arno Bayer, Carmen Teresa Kaiber e Marcio Antonio da Silva pelas sugestões que ajudaram a enriquecer este trabalho.

Aos professores do Programa de Pós-Graduação em Ensino de Ciências e Matemática da Universidade Luterana do Brasil, pelos conhecimentos necessários à minha formação.

Também, à equipe diretiva da Escola Técnica Estadual 31 de Janeiro que, permitiram o desenvolvimento da pesquisa e aos alunos da turma 231, 3º ano do Ensino Médio, do ano de 2010, os quais participaram desta investigação.

Educar é semear com sabedoria e colher com paciência.

Augusto Cury

RESUMO

O trabalho apresenta a Criptografia para o desenvolvimento de atividades didáticas que aliem os conteúdos matemáticos do Ensino Médio a esse tema e, que incentivem o manuseio de calculadoras científicas no Ensino de Matemática. Hoje, a Criptografia é utilizada em auditorias eletrônicas, na autenticação de ordens eletrônicas de pagamento, no código de verificação do ISBN, nos navegadores de Internet, entre outras situações do dia a dia. O problema desta pesquisa foi como desenvolver uma Engenharia Didática que envolva os conteúdos matemáticos do Ensino Médio com o tema Criptografia. Este trabalho teve por objetivo geral investigar a possibilidade de implementar uma Engenharia Didática para o desenvolvimento do tema Criptografia, aliado aos conteúdos de Matemática do Ensino Médio. Para alcançar o objetivo geral foram traçados os seguintes objetivos específicos: investigar a relação entre a Criptografia e os conteúdos matemáticos do Ensino Médio; pesquisar atividades didáticas com o tema Criptografia para o Ensino Médio; implementar um experimento com alunos do Ensino Médio com a sequência didática desenvolvida; investigar se o aluno estabelece relações com o tema Criptografia através das atividades didáticas aplicadas. Para isso, foi elaborada uma sequência didática dirigida ao 3º ano do Ensino Médio, utilizando criptogramas, Cifra de César, Cifra do Chiqueiro, Cifra de Playfair e os conteúdos de função linear, função quadrática, função exponencial, função logarítmica e matrizes. A Engenharia Didática foi a metodologia utilizada nessa investigação, pois preocupa-se com aspectos relacionados à realidade da sala de aula. Foram desenvolvidas as quatro fases da engenharia didática, que são: as análises preliminares, a concepção e análise *a priori*, a experimentação e a análise *a posteriori* e validação. A Engenharia Didática, como metodologia de investigação, é um esquema experimental que se caracteriza pelas realizações didáticas em sala de aula, as quais apresentam as seguintes características: concepção, realização, observação e análise de sequências de ensino. Neste trabalho, as variáveis microdidáticas foram: o tema Criptografia envolvendo códigos e senhas e os conteúdos de Matemática do Ensino Médio. As hipóteses foram: existe relação entre o tema Criptografia e os conteúdos do Ensino Médio; o aluno é capaz de chegar aos conceitos de Criptografia, partindo de atividades didáticas com os conteúdos matemáticos, desenvolvidas em sala de aula, no Ensino Médio. A fase da experimentação foi desenvolvida em uma escola estadual de ensino, no município de Campo Bom, no estado do Rio Grande do Sul, nos meses de agosto e setembro, durante 14 h/a. Os resultados apontam que a Criptografia é um tema adequado ao desenvolvimento de atividades didáticas utilizando os conteúdos matemáticos que são trabalhados no Ensino Médio. Essas atividades, utilizando códigos e senhas, oportunizam aos alunos reforçar os conteúdos já estudados e utilizar a calculadora como um recurso facilitador para cálculos longos.

Palavras-chave: Educação Matemática. Currículo no Ensino Médio. Criptografia. Calculadoras.

ABSTRACT

The study presents Cryptography as a tool to develop didactic activities that blend it to high school mathematics contents and that promote the use of scientific calculators in the teaching of mathematics. Today, Cryptography is used in electronic audits, in the authentication of electronic standing orders, in ISBN code verification, in Internet browsers, among other everyday applications. The problem proposed in this research was to develop a Didactic Engineering that links high school mathematics contents to Cryptography. The general aim of this study was to investigate the possibility to implement a Didactic Engineering to develop the theme Cryptography, as associated to high school mathematics contents. The specific aims were: to investigate the relationship between Cryptography and high school mathematics contents; to research into didactic activities on the theme Cryptography applied to high school; to conduct an experiment with high school pupils using the didactic sequence developed; to investigate whether the pupil develops a relationship with the theme Cryptography through the didactic activities applied. With this in mind, a didactic sequence was developed directed to high school 11th grade pupils, using cryptograms, Ceaser cipher, Pigpen cipher, Playfair cipher, linear function, quadratic function, exponential function, logarithmic function and matrices. Didactic Engineering was the methodology used in this investigation, since it addresses the aspects related to the reality of the classroom. Four phases of Didactic Engineering were developed: preliminary analyses; *a priori* conception and analyses; experiment; and *a posteriori* analysis and validation. Didactic Engineering, as an investigation methodology, is an experimental device characterized by the didactic achievements in the classroom, which present the following characteristics: conception, conduction, observation and analysis of teaching sequences. In this study, the microdicactic variables were: the theme Cryptography of codes and passwords and high school mathematics contents. The hypotheses were: is there a relationship between the theme Cryptography and high school contents? Is the pupil able to understand the concepts in Cryptography based on the didactic activities addressing mathematics contents developed in the high school classroom. The experimental stage was conducted in a state school in the city of Campo Bom, Rio Grande do Sul, Brazil, between August and September, covering 14 teaching hours. The results indicate that Crytpography is an appropriate theme considering the development of didactic activities that utilize high school mathematics contents. These activities, which utilize codes and passwords, afford pupils to consolidate the contents previously studied and to use a calculator as a facilitation resource for long calculations.

Keywords: Mathematics Education. High school Curriculum. Cryptography. Calculators.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Este trabalho apresenta a Criptografia para o desenvolvimento de atividades didáticas no Currículo de Matemática do Ensino Médio. Esse tema, segundo Tamarozzi (2001), permite ao professor de Matemática desenvolver atividades didáticas de codificação e decodificação, para revisar, reforçar e aprofundar os conteúdos matemáticos do Ensino Médio. Nesse sentido, buscou-se verificar, nesta investigação, se o referido estudo vai ao encontro dos critérios estabelecidos por Silva (2009) para escolha e organização de temas que possam compor o Currículo de Matemática do Ensino Médio. A Criptografia é conhecida como a arte de escrever em códigos, de forma a permitir que somente o destinatário conheça o conteúdo da mensagem. Atualmente, está sendo utilizada na autenticação de ordens eletrônicas de pagamento, nos navegadores de internet, na transmissão digital, entre outras situações da vida cotidiana.

Esta investigação justifica-se porque é importante que o professor trabalhe com temas atuais. Além disso, cabe a ele proporcionar ao educando o contato com as tecnologias, entre elas a calculadora. As calculadoras possibilitam que o estudante dedique maior concentração às estratégias para resolução de problemas, não desperdiçando tempo com cálculos longos e repetitivos, pois esse não é o objetivo das atividades propostas pelo professor. Assim, o tema em estudo possibilita ao professor de Matemática do Ensino Médio pesquisar e desenvolver atividades didáticas para exercitar e revisar conteúdos desenvolvidos em sala de aula, através de atividades de codificação e decodificação, envolvendo os conteúdos matemáticos do Ensino Médio.

A metodologia da pesquisa, utilizada nesta investigação, foi a Engenharia Didática que, segundo Pais (2005, p. 108), “reforça a confiabilidade da pesquisa e sua potencialidade se deve à defesa do vínculo com a realidade da sala de aula”.

O trabalho está organizado em três capítulos. O primeiro apresenta os pressupostos teóricos, o histórico da Criptografia e uma reflexão sobre a importância do tema escolhido para o Currículo de Matemática do Ensino Médio.

No segundo capítulo, estão os pressupostos metodológicos da investigação, o problema, as hipóteses, os objetivos e a metodologia utilizada. Apresenta, também, os sujeitos investigados e os instrumentos de coleta de dados.

O terceiro capítulo traz a Engenharia Didática como metodologia de investigação e o desenvolvimento de suas fases. Na primeira, a das análises preliminares, apresentam-se as análises dos artigos de congressos, seminários e periódicos de Matemática. Na segunda fase, da Concepção e Análise *a priori*, estão o planejamento e a organização da sequência didática e a análise das possíveis resoluções dos alunos às atividades didáticas presentes na sequência elaborada. A terceira fase é a experimentação, que apresenta a turma em que foi realizado o experimento e as aulas da sequência. Na última fase, a Análise *a posteriori* e validação, encontram-se os resultados coletados na pesquisa, bem como uma reflexão sobre os dados coletados com as conclusões da investigação.

1 REFERENCIAL TEÓRICO

Este capítulo apresenta o embasamento teórico da pesquisa e a importância do tema Criptografia para o desenvolvimento de atividades didáticas para o Currículo de Matemática do Ensino Médio, procurando ressaltar a importância do uso da calculadora em sala de aula.

1.1 O HISTÓRICO DO TEMA CRIPTOGRAFIA

A Criptografia é bastante antiga, pois já havia indícios, no sistema de escrita hieroglífica dos egípcios e dos romanos, da utilização de códigos secretos para transmitir seus planos de batalha (TAMAROZZI, 2001).

A palavra Criptografia vem das palavras gregas *kriptós,* que significa escondido, oculto e *graphein,* que significa escrita (SINGH, 2003), e é conhecida como arte ou ciência de escrever em códigos (TAMAROZZI, 2001). Segundo Shokranian (2005), enviar uma mensagem em código pode apresentar dois objetivos: o primeiro é enviar uma mensagem secreta e o segundo é proteger o conteúdo da mensagem.

O *Citale* espartano foi o primeiro aparelho criptográfico militar, utilizado durante o século V a.C. O *Citale* (figura 1) consistia em um bastão de madeira, em que se enrolava uma tira de couro e escrevia-se a mensagem ao longo do comprimento desse bastão. Para enviar a mensagem, de forma segura, a tira de couro era retirada do bastão de madeira e utilizada como um cinto, onde a mensagem ficava voltada para dentro. Utilizando a tira de couro como cinto, a mensagem ficava sem sentido. Para decifrá-la, era necessário que o receptor tivesse um bastão de mesmo diâmetro.

Figura 1: exemplo de *Citale* Espartano.

Uma das formas de criptografar é utilizando a substituição de uma letra por outra ou por um símbolo que é denominado de cifra. Um exemplo de cifra é Cifra de

César, que a utilizava para fins militares. Existem registros em que César descreve como enviou uma mensagem para Cícero, que estava cercado e prestes a se render. Nessa mensagem, Júlio César substituiu as letras do alfabeto romano por letras gregas (SINGH, 2003). Outro exemplo de cifra utilizada por Júlio César consistia em substituir cada letra da mensagem original por outra que estivesse três casas à frente no mesmo alfabeto (figura 2). César utilizava o alfabeto normal para escrever a mensagem e o alfabeto cifrado era utilizado para codificar a mensagem que mais tarde seria enviada.

Alfabeto Normal	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
Alfabeto Cifrado	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

Figura 2: quadro do método de substituição utilizado por Júlio César.

Fonte: adaptado de Singh(2003, p. 27)

Utilizando a figura 2 e considerando como texto original a palavra “MATEMÁTICA”, tem-se o seguinte texto cifrado: “PDWHPDWLFD”. Na Cifra de César, para dificultar a decodificação, removem-se os espaços entre as palavras no texto cifrado. Essa não é uma Cifra segura, pois possui 25 chaves em potencial. Logo, ao ser interceptada, se desconfiarem que o método utilizado foi a Cifra de César é necessário verificar 25 possibilidades para decifrar a mensagem, o que a torna uma cifra simples de decodificar (SINGH, 2003).

Como as cifras de substituição monoalfabéticas[1] eram muito simples e facilmente decifradas por criptoanalistas (pessoas que tentam descobrir o método de codificação), através da análise de frequência de cada letra, no texto cifrado, surge a necessidade de criar cifras mais complexas. Assim, no século XVI, surgiu a cifra de substituição polialfabética[2], criada pelo diplomata francês Blaise Vigenère (SINGH, 2003). Essa cifra foi denominada Cifra de Vigenère (figura 3) e utiliza 26 alfabetos cifrados diferentes para cifrar uma mensagem.

[1] A cifra monoalfabética utiliza um alfabeto para cifrar uma mensagem (SINGH, 2003).
[2] A cifra polialfabética utiliza mais de um alfabeto para cifrar uma mensagem (SINGH, 2003).

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

Figura 3: quadro de Vigenère.

Fonte: Singh(2003, p. 66)

No Quadrado de Vigenère, há o alfabeto normal, seguido de 26 alfabetos cifrados. Cada alfabeto tem um deslocamento de uma casa à frente no mesmo alfabeto, seguindo o princípio do Código de César. De acordo com Singh (2003), para escrever uma mensagem codificada pelo Quadrado de Vigenère, combina-se uma palavra-chave, por exemplo: **VIDA**. Para cifrar a palavra ÁLGEBRA, é preciso escrever a palavra-chave quantas vezes for necessário, pois cada letra da palavra **VIDA** equivale a uma letra da palavra álgebra (figura 4).

V	I	D	A	V	I	D
A	L	G	E	B	R	A

Figura 4: exemplo do uso da Cifra de Vigenère.

Para codificar as letras da frase é necessário usar a linha correspondente à letra da palavra-chave relacionada. Para V, por exemplo, utiliza-se o alfabeto da linha 26 e a coluna da letra A. Assim, a primeira letra “A” será traduzida como U, que é intersecção entre “V e A”. Para I, usaremos a linha 8 e o “L” será traduzido como “S” e continua-se a cifragem, conforme a figura 5.

Palavra-chave	V	I	D	A	V	I	D
Texto Normal	A	L	G	E	B	R	A
Texto Cifrado	U	S	I	D	V	Y	C

Figura 5: cifragem utilizando a Cifra de Vigenère.

Outro exemplo de Cifra de substituição monoalfabética, é a Cifra do Chiqueiro, utilizada pelos maçons livres, para guardar seus segredos (SINGH, 2003). A cifra consiste em substituir uma letra por um símbolo, seguindo o padrão apresentado na figura 6.

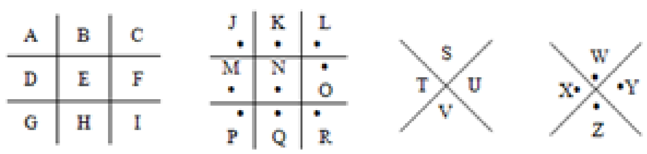


Figura 6: exemplo do padrão utilizado pela Cifra do Chiqueiro.

A codificação da Cifra do Chiqueiro é realizada encontrando a posição da letra em uma das quatro grades da figura 6 e desenhando a porção da grade que representa a letra a ser codificada. A letra **E**, por exemplo, corresponde ao símbolo □.

Outro tipo de cifra é a de Playfair, utilizada pelos jovens apaixonados da Inglaterra vitoriana. Como não podiam expressar seu amor publicamente, eles começaram a trocar mensagens codificadas através dos jornais, em colunas dedicadas às mensagens dos leitores. Essas colunas ficaram conhecidas como “colunas de óbito” (SINGH, 2003). Charles Babbage e seus amigos Sir Wheatstone e o barão Lyon Playfair foram os criadores da Cifra de Playfair, que substitui cada par de letras da mensagem a ser codificada por outro par de letras. Para codificar, primeiramente, escolhe-se uma palavra-chave, por exemplo, ULBRA. Antes da cifragem, as letras do alfabeto são escritas em um quadrado 5X5, começando com a palavra-chave e combinando as letras I e J em um único elemento, conforme a figura 7.

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

Figura 7: quadro da Cifra de Playfair.

A mensagem original é escrita em pares de letras, ou dígrafos. As duas letras, em qualquer dígrafo, devem ser diferentes, o que se consegue inserindo, por exemplo, uma letra *x,* caso apareçam letras iguais ou se o número de letras for ímpar. A cifragem começa da seguinte forma: se as duas letras estiverem na mesma linha, elas são substituídas pela letra imediatamente à direita de cada uma delas, se uma delas estiver no final da linha, é substituída pela letra que está no começo da linha. Se ambas as letras estiverem na mesma coluna, serão substituídas pela letra que está imediatamente abaixo de cada uma e, neste caso, se uma das letras for a última letra da coluna, será substituída pela que está no topo da coluna.

Se as letras, no dígrafo, não estiverem nem na mesma linha, nem na mesma coluna, usa-se a seguinte regra: para cifrar a primeira letra, olha-se ao longo de sua linha até chegar à coluna em que está a segunda letra; a letra que estiver nessa intersecção irá substituir a primeira letra. Para cifrar a segunda letra, utilize o mesmo raciocínio.

A figura 8 apresenta um exemplo de codificação utilizando a cifra referida.

Texto original	A vida é bela.
Texto original em pares	AV – ID – AE – BE – LA
Texto Codificado	UZ – PI – BG – EK – BU

Figura 8: exemplo de cifragem utilizado pela Cifra de Playfair.

Para codificar o par AV, como não estão na mesma linha e nem na mesma coluna, utiliza-se a regra de olhar primeiro ao longo da linha até chegar à coluna onde está a segunda letra. A letra que estiver na intersecção irá substituir a primeira letra. Para cifrar a segunda letra, utiliza-se o mesmo raciocínio, conforme figura 9.

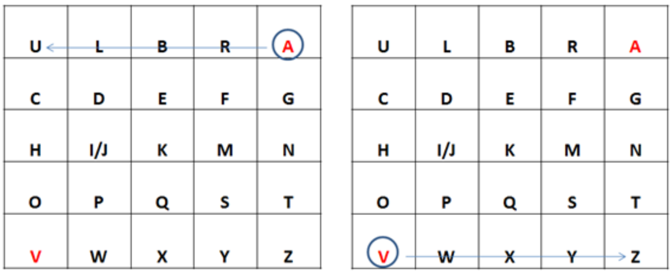


Figura 9: exemplo da cifragem do par AD utilizando a Cifra de Playfair.

Outro exemplo de Cifra é a Cifra ADFGVX, uma cifra de guerra que se acreditava dar maior segurança às mensagens a serem enviadas, pois era de substituição e transposição[3]. Foi utilizada pelos alemães, que acreditavam fosse imbatível, mas o criptoanalista Georges Painvin quebrou a Cifra ADFGVX e descobriu onde os alemães atacariam (SINGH, 2003). As letras ADFGVX foram escolhidas porque, quando traduzidas para os pontos e traços do código Morse, diminuem a possibilidade de erros durante a transmissão.

Segundo Singh (2003), a Cifra ADFGVX, para codificar utiliza uma grade 6x6, preenchida com 36 quadrados, onde se colocam as 26 letras do alfabeto e 10 algarismos. Na primeira linha e coluna, colocam-se as letras A, D, F, G, V e X, conforme figura 10.

	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	O	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	0	F	Q

Figura 10: quadro da Cifra ADFGVX.

Inicia-se a codificação, pegando-se cada letra da mensagem a ser enviada, localizando a sua posição na grade e substituindo-se pelas letras da linha e da

[3] A Cifra de transposição consiste em rearranjar as letras da mensagem, gerando um anagrama (SINGH, 2003).

coluna. Por exemplo, **d** será substituído por **AG**. Uma mensagem codificada por essa cifra ficará conforme a figura 11.

Palavra original	Lógica
Palavra codificada	DADGGVVGFGDV

Figura 11: exemplo de codificação da Cifra ADFGVX.

Para cifrar a letra L, localiza-se sua posição na grade e se substitui pelas letras que estão na sua linha e coluna, como mostra a figura 12.

	A	D	F	G	V	X
A	8	p	3	d	1	N
D	l	t	4	o	A	H
F	7	k	b	c	5	Z
G	j	u	6	w	G	M
V	x	s	v	i	R	2
X	9	e	y	0	F	Q

l = DA

Figura 12: exemplo de codificação da Cifra ADFGVX.

De acordo com o Singh (2003), o italiano Leon Battista Alberti foi o criador da primeira máquina criptográfica, o Disco de Cifras, que é composta por dois discos de cobre, um maior que o outro, onde fixaram-se as letras do alfabeto ao longo dos discos, colocando o disco menor em cima do maior e fixando um pino para agir como eixo. Os discos podiam ser girados independentemente, fazendo com que os dois alfabetos mudassem suas posições. Para criptografar uma mensagem com a Cifra de César, posiciona-se o A do disco maior ao lado do N do disco menor (figura 13).

Figura 13: exemplo de Disco de Cifras.

O Disco de Cifras é um misturador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado, porém seu inventor sugeriu que fosse mudada a disposição do disco durante uma mensagem, o que geraria uma cifra polialfabética. Isso dificultaria a sua decodificação pois, desse modo, ele estaria mudando o modo de mistura durante a cifragem e isso tornaria a cifra difícil de ser quebrada.

No ano de 1918, o inventor Artur Scherbius e seu amigo Richard Ritter fundaram uma empresa. Um dos projetos de Artur Scherbius era substituir os sistemas criptográficos, usados na primeira guerra mundial. Então, utilizando a tecnologia do século XX, ele desenvolveu uma máquina criptográfica, a qual era uma versão elétrica do Disco de Cifras (SINGH, 2003). Essa máquina denominou-se Enigma (figura 14) e ficou conhecida como o mais terrível sistema de criptografia já conhecido.

Figura 14: ilustração da máquina enigma.

Singh (2003) afirma que, para decifrar uma mensagem da Enigma, o destinatário precisaria ter outra Enigma e uma cópia do livro de códigos, contendo o ajuste inicial dos misturadores para cada dia. A Enigma ficou conhecida como o mais terrível sistema criptográfico da história, pois foi utilizada pelos alemães durante a Segunda Guerra Mundial, possibilitando que eles tivessem o mais seguro sistema de criptografia do mundo. Durante anos, os alemães acreditaram que a Enigma era indecifrável, até Hans-Thilo Schmitdt vender informações sobre a Enigma para as potências estrangeiras, prejudicando, assim, a segurança da Alemanha, pois a partir das informações dadas por ele, era possível criar uma réplica da Enigma. Essas informações, porém, não eram suficientes para decodificar as mensagens da Enigma, pois era necessário saber o ajuste inicial da máquina.

Em 1943, foi projetado o Colossus, um computador inglês o qual possuía uma dimensão enorme e funcionava por meio de válvulas, que chegava a processar cerca de 5 mil caracteres por segundo. Esse computador foi utilizado durante a Segunda Guerra Mundial para decodificar os códigos criados pela máquina Enigma. O Colossus (figura 15) deu início a uma era moderna da criptografia, na qual os computadores eram programados com chaves de codificação muito mais complexas do que as utilizadas pela Enigma. Essa nova técnica de criptografia era de uso exclusivo do governo e de militares, para guardar informações (SINGH, 2003).

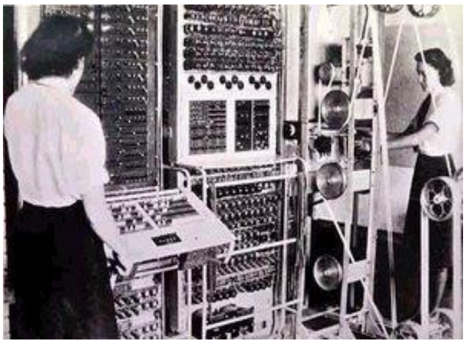


Figura 15: ilustração do Colossus.

Contudo, os criptonalistas continuavam decifrando os textos, analisando a frequência com que cada letra aparece no texto cifrado. Uma maneira de superar esse problema foi dividir o texto em grupos de letras e criptografar o texto comum por grupos, em vez de uma letra de cada vez. Um dos métodos de criptografar que utiliza essa ideia é a chamada Cifra de Hill, que se utiliza de transformações matriciais e de um sistema poligráfico, o qual é um sistema de criptografia em que o texto comum é dividido em conjuntos de n letras. Cada um é substituído por um conjunto de n letras cifradas. Essa cifra recebeu esse nome, pois faz referência a Lester S. Hill, que introduziu esse sistema em dois artigos escritos em 1929 e 1931: "Cryptography in the Algebraic Alphabet", e "Concerning Certain Linear Transformation Apparatus of Cryptography" (ANTON; RORRES, 2001).

As criptografias complexas utilizadas nos computadores não apresentavam muita segurança, então foram criados dois algoritmos de codificação, o DES (sistema de chave secreta) e RSA (sistema de chave pública).

De acordo com Singh (2003), um dos algoritmos de cifragem mais usados era um produto da IBM, conhecido como Lucifer, desenvolvido por Horst Feistel em 1970. O sistema Lucifer era considerado um dos mais poderosos sistemas de cifragem disponíveis comercialmente e foi utilizado por várias organizações. Era tão poderoso que oferecia a possibilidade de um padrão de cifragem, além das capacidades de quebra de códigos da NSA[4]. Como a NSA não queria um padrão de cifragem que ela não poderia quebrar, então limitou o número de chaves do sistema Lucifer, de modo que ele oferecesse segurança à comunidade civil e que a NSA fosse capaz de decodificar. A versão desse sistema com a chave limitada foi oficialmente adotada em 23 de novembro de 1976 e batizada como Padrão de Cifragem de Dados (DES – Data Encryption Standard). A DES é um algoritmo de criptografia em blocos, composto da substituição de caracteres em blocos de 64 bits, utilizando uma chave de 56 bits. Sua estrutura é composta de 16 estágios de criptografia, executando, durante todo o processo, séries de transposições e substituições de caracteres, bem como, a recombinação de blocos. A adoção da DES resolveu um problema de padronização, encorajando as empresas a utilizarem a criptografia para sua segurança. A DES era suficientemente forte para garantir a segurança contra ataques de rivais comerciais, pois era impossível para uma empresa com um computador civil quebrar uma mensagem cifrada com a DES, porque o número de chaves possíveis era suficientemente grande. O problema do algoritmo DES é a distribuição de chaves, pois a chave de codificação é a mesma de decodificação. O DES não busca manter o segredo do seu algoritmo de codificação, mas o segredo da chave usada para codificar uma mensagem específica. A tecnologia DES tem sido utilizada em vários produtos comerciais e é o algoritmo de

[4] NSA – Agência de Segurança Nacional do Estados Unidos da América

criptografia escolhido pelos usuários comerciais. Várias companhias utilizam o DES, dentre elas a General Eletric, a IBM e a Motorola.

Porém, o mais conhecido dos métodos de criptografia é o RSA, código inventado em 1978, por R. L Rivest, A. Shamir e L. Adleman. As letras RSA correspondem às iniciais dos inventores do algoritmo (SINGH, 2003). O RSA é, atualmente, o mais usado em aplicações comerciais. É utilizado, por exemplo, no netscape, um dos mais populares softwares de navegação da internet. O RSA é o primeiro algoritmo de chave pública completo, que funciona para criptografia e assinaturas digitais. O algoritmo RSA é de fácil compreensão, pois usa como base o fato de que é extremamente difícil fatorar um número que é o resultado da multiplicação de dois números primos com muitos algarismos. Segundo Singh (2003), o único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém encontre um método rápido para fatorar esses números primos, mas a grande vantagem desse sistema de chave pública é que ela acaba com os problemas da distribuição de chaves.

Um dos códigos, utilizados nos dias atuais, que trabalha o conteúdo matemático de aritmética modular, é o “Código de verificação ISBN” (*International Standard Book Number*), o qual possibilita ao professor de Matemática explorar esse conteúdo no Ensino Médio. É escrito como quatro blocos de dígitos separados por hífens ou por espaços em branco. Lendo-se da esquerda para a direita, o primeiro bloco identifica o país ou a área da língua entre os participantes; o segundo bloco identifica as editoras daquele grupo e o terceiro é o número atribuído pela editora para a obra (ANTON; BUSBY, 2006). O último bloco consiste em um único dígito, de 0 a 9 ou um X, que representa a_{10}, sendo os 9 primeiros dígitos do ISBN: a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9. Para calcularmos o dígito verificador do código ISBN, utilizamos a seguinte fórmula: $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$. Para encontrar o dígito verificador do código ISBN 852440124-X, procede-se da seguinte forma:

$$X= \left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$$

$$X= [1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9] \bmod 11$$

$$X= [1.8 + 2.5 + 3.2 + 4.4 + 5.4 + 6.0 + 7.1 + 8.2 + 9.4] \bmod 11$$

$$X= [8 + 10 + 6 + 16 + 20 + 0 + 7 + 16 + 36] \bmod 11$$

$$X= 119 \bmod 11$$

X= 9

Assim, o dígito verificador é 9.

Constata-se, através dos exemplos mostrados ao longo deste capítulo, que a Criptografia, no decorrer da história, vem sendo utilizada para fins militares, pessoais e sociais. Outras abordagens desse tema são as aplicações em auditoria eletrônica, na autenticação de ordens eletrônicas de pagamento, nos navegadores de Internet, entre outras situações da vida cotidiana.

No Brasil e em outros países, a Criptografia está sendo aplicada em diversas áreas, tais como:

> Recursos humanos: auditoria eletrônica e lacre de arquivos de pessoal e pagamentos; compras e vendas: autenticação de ordens eletrônicas de pagamento; recursos jurídicos: transmissão digital e custódia de contratos; automação de escritórios: autenticação e privacidade de informação. (TERADA, 1988, p. 4)

Além disso, para Tamarozzi (2001), a Criptografia possibilita o desenvolvimento de atividades didáticas envolvendo o conteúdo de funções e matrizes, os quais se constituem em material útil para exercícios, atividades e jogos de codificação, em que o professor pode utilizá-los para fixação de conteúdos. Nesse contexto, pode-se perceber que a Criptografia possibilita o desenvolvimento de atividades didáticas, que podem ser desenvolvidas no Ensino Médio, levando os alunos a aprimorarem seus conhecimentos. Segundo Groenwald e Franke (2008), o tema Criptografia permite interligar os conteúdos matemáticos às situações do mundo real e ajuda a desenvolver habilidades e competências na resolução de problemas, a criar estratégias de resolução, a ter autonomia durante o processo de aprendizagem, com isso, tornando-os mais autoconfiantes e concentrados na realização das atividades. De acordo com Cantoral et al (2000), esse tema pode ser um recurso o qual permitirá ao professor desenvolver atividades didáticas que proporcionem aulas as quais despertem a atenção e o interesse dos alunos para os conteúdos trabalhados em sala de aula.

O professor de Matemática pode trabalhar com o aluno a utilização do tema Criptografia através do planejamento de uma sequência didática de atividades com códigos e senhas para aplicação no Ensino Básico. Neste trabalho, foi desenvolvida uma sequência didática para o 3º ano do Ensino Médio, aliando as aplicações já citadas aos conteúdos de Matemática do Ensino Médio.

1.2 A IMPORTÂNCIA DO TEMA CRIPTOGRAFIA NO CURRÍCULO DE MATEMÁTICA DO ENSINO MÉDIO

Segundo a Lei de Diretrizes e Bases da Educação Nacional (BRASIL, Lei 9394, 1996), o Ensino Médio apresenta as seguintes finalidades:

> - a consolidação e o aprofundamento dos conhecimentos adquiridos no ensino fundamental, possibilitando o prosseguimento de estudos;
> - a preparação básica para o trabalho e a cidadania do educando, para continuar aprendendo, de modo a ser capaz de se adaptar com flexibilidade a novas condições de ocupação ou aperfeiçoamento posteriores;
> - o aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico;
> - a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina.

Na etapa final da Educação Básica, espera-se que o estudante esteja preparado para atuar na sociedade, na qual está inserido, de forma efetiva, sabendo se comunicar claramente, resolver problemas do dia-a-dia e do trabalho, tomar decisões, trabalhar com eficiência e em cooperação.

Encontra-se, nas Orientações Curriculares para o Ensino Médio (2006), que o aluno deve ser capaz de utilizar a Matemática: na resolução de problemas do cotidiano; para modelar fenômenos das distintas áreas do conhecimento; para compreender a Matemática como conhecimento social e construído ao longo da história; para entender a importância da Matemática no desenvolvimento científico e tecnológico.

Nesse sentido, para poder alcançar as finalidades do ensino, é necessário um currículo que atenda aos princípios referidos. Neste trabalho, o conceito de currículo está fundamentado em Coll (1999):

> Currículo é o projeto que preside as atividades educativas escolares, define suas intenções e proporciona guias de ação adequadas e úteis para os professores, que são diretamente responsáveis pela sua execução. Para isso, o currículo proporciona informações concretas sobre o que ensinar, quando ensinar, como ensinar e que, como e quando avaliar (1999, p. 45).

Ainda, conforme o autor, o currículo é a realização do planejamento curricular, tomada de decisão dos objetivos que se deseja alcançar, organização dos conteúdos, elaboração das estratégias didáticas, definição da metodologia de ensino. Portanto, é “a estratégia para a ação educativa” (D’AMBROSIO, 1997, p. 68).

Outro ponto chave para a realização de uma aprendizagem significativa, para Coll (1999), é a funcionalidade:

> A educação escolar deve sempre ocupar-se de que os conhecimentos adquiridos – conceitos, habilidades, valores, normas etc – sejam funcionais, isto é, possam ser efetivamente utilizados quando as circunstâncias nas quais o aluno se encontrar assim exigirem (1999, p. 55).

O currículo deve sempre levar em consideração os aspectos de funcionalidade dos conteúdos para os alunos, em que se proponham atividades didáticas que levem os alunos a visualizarem a aplicabilidade dos mesmos, seja em situações dentro ou fora do ambiente escolar, no cotidiano ou na história (COLL, 1999).

A escolha de temas para o Ensino Médio deve possibilitar o uso de conteúdos de Matemática, permitindo que o aluno aprofunde e exercite os conteúdos já trabalhados em séries anteriores, crie estratégias de resolução de problemas, tenha autonomia na resolução das atividades didáticas e trabalhe em grupo, buscando aprimorar a sua formação acadêmica e social. Buscando, nesse sentido, alcançar as indicações citadas anteriormente.

Nesse contexto, através do tema Criptografia, é possível trabalhar os conteúdos procedimentais, pois esse é um dos três tipos de conteúdos explorados por Coll et al (2000). Os conteúdos podem ser conceituais, procedimentais e atitudinais. Os conceituais são os que devem ser compreendidos, os que os alunos devem ser capazes de dotar de significado, de forma a estabelecer relações significativas que os levem a compreendê-los (COLL et al, 2000). Os conteúdos procedimentais são um conjunto de ações ordenadas, que permitem chegar a um determinado objetivo, referem-se ao saber fazer, ao saber agir de forma eficaz frente a um problema (ZABALA, 1998). Os conteúdos atitudinais referem-se aos valores, atitudes e normas.

Neste trabalho, buscou-se usar esses três tipos de conteúdos. Os conceituais estão explorados na investigação dos conceitos de Criptografia em relação aos conteúdos de Matemática desenvolvidos no Ensino Médio, como os conceitos de aritmética modular, funções e matrizes. Os conteúdos procedimentais utilizados nas atividades didáticas de codificação e decodificação, que necessitam que o aluno articule um processo de resolução. Nesse sentido, o aluno deve pensar nas estratégias, técnicas e regras para solucionar o problema, formulando e comprovando hipóteses.

Também foram utilizados os conteúdos atitudinais, pois durante a aplicação das atividades didáticas objetivou-se que os alunos desenvolvessem o respeito à estratégia de resolução do colega, participação nas atividades didáticas, cooperação no trabalho em grupo, respeito ao material didático, interesse e autonomia nas resoluções. Isso vai ao encontro do que é proposto no Plano Nacional de Educação (2001), o qual coloca que o Ensino Médio deve preparar os estudantes para os desafios da vida moderna, na qual deverá:

> Permitir a aquisição de competências relacionadas ao pleno exercício da cidadania e da inserção produtiva: auto-aprendizagem; percepção da dinâmica social e capacidade para nela intervir; compreensão dos processos produtivos; capacidade de observar, interpretar e tomar decisões; domínio de aptidões básicas de linguagens, comunicação, abstração; habilidades para incorporar valores éticos de solidariedade, cooperação e respeito às individualidades (BRASIL, 2001).

Trabalhar com o tema proposto pode permitir que o estudante desenvolva habilidades que podem ser utilizadas no ambiente de trabalho e no convívio em sociedade, pois é um tema atual, de grande utilização, aplicado a várias situações da vida moderna e adapta-se aos conteúdos do Currículo de Matemática do Ensino Médio.

Outro aspecto importante que também faz parte dos desafios da vida moderna para os jovens do Ensino Médio são as exigências referentes à disciplina de Matemática para os futuros trabalhadores que, de acordo com Pollak apud Pires (2000), são:

> Ser capaz de propor problemas com as operações adequadas; conhecer técnicas diversas para propor e resolver problemas; compreender as implicações matemáticas de um problema; poder trabalhar em grupo sobre um problema; ver a possibilidade de aplicar idéias matemáticas tanto a problemas comuns como a complexos; estar preparado para enfrentar-se com problemas abertos, já que a maioria dos problemas reais não estão bem formulados; acreditar na utilidade e na validade da Matemática (2000, p. 155).

É preciso preparar os jovens do Ensino Médio para o mundo do trabalho, desenvolver habilidades e competências que possibilitem a inserção dos mesmos na sociedade de forma igualitária. Para inseri-los no mundo das relações sociais, a escola deverá ser um ambiente que propicie relações sociais de igualdade, de trabalho em grupo, de reconhecimento das individualidades do grupo, de respeito às diferenças, etc. Uma forma de estimular o desenvolvimento dessas habilidades é “propondo aulas de Matemática que estimulem a participação, valorizem a iniciativa, os avanços individuais, o crescimento coletivo, o respeito mútuo” (PIRES, 2000, p.156).

Raths apud Coll (1999) propõe doze princípios para ajudar o professor a justificar a necessidade de se incluir ou não uma atividade no Currículo, afirmando que uma atividade é preferível a outra se:

> 1. permite ao aluno tomar decisões razoáveis quanto ao modo de desenvolvê-la e verificar as consequências da sua escolha;
> 2. atribuir ao aluno um papel ativo em sua realização;
> 3. exigir do aluno uma pesquisa de ideias, processos intelectuais, acontecimentos ou fenômenos de ordem pessoal ou social e estimulá-lo a comprometer-se com a mesma;
> 4. obrigar o aluno a interagir com sua realidade;
> 5. puder ser realizada por alunos de diversos níveis de capacidade e com interesses diferentes;
> 6. obrigar o aluno a examinar num novo contexto uma ideia, conceito, lei, que já conhece;
> 7. obrigar o aluno a examinar ideias ou acontecimentos que normalmente são aceitos sem discussão pela sociedade;
> 8. colocar o aluno e o educador numa posição de sucesso, fracasso ou crítica;
> 9. obrigar o aluno a reconsiderar e revisar seus esforços iniciais;
> 10. obrigar a aplicar e dominar regras significativas, normas ou disciplinas;
> 11. oferecer ao aluno a possibilidade de planejá-la com outros, participar do seu desenvolvimento e comparar os resultados obtidos;
> 12. for relevante para os propósitos e interesses explícitos dos alunos.
>
> (1999, p. 80-81)

Observando o exposto acima, entende-se que o tema Criptografia está fortemente ligado aos princípios 1, 2, 3, 4, 6 e 11. Ao primeiro princípio, devido à possibilidade que oferece de elaborar atividades didáticas em que o aluno pode criar estratégias de resolução de problemas e verificar a sua validade. O segundo princípio refere-se ao fato das atividades didáticas aliarem o tema aos conteúdos matemáticos do Ensino Médio, possibilitando aos alunos autonomia para verificar o melhor caminho para encontrar a solução, permitindo que eles mobilizem seus conhecimentos e se tornem mais ativos no processo de ensino. O princípio três também pode ser percebido nas atividades didáticas com o tema Criptografica, pois exigem que os alunos se concentrem na resolução, criem estratégias e as verifiquem. A Criptografia oportuniza atividades didáticas que estão presentes na vida cotidiana e que envolvem conteúdos matemáticos como, por exemplo, atividade de criptogramas e Código ISBN, o que corresponde ao princípio quatro. O princípio seis pode ser percebido no fato da Criptografia proporcionar o desenvolvimento de atividades didáticas que possibilitam revisar e reforçar os conteúdos já trabalhados, tais como, princípios fundamentais da aritmética, funções e matrizes, além de explorar novos conteúdos, no Currículo de Matemática do Ensino Médio como, por exemplo, a atividade envolvendo o Código de verificação ISBN, que explora o conteúdo de aritmética modular. O trabalho em grupo é essencial, porque permite a discussão dos caminhos para a resolução.

Segundo Groenwald e Ruiz (2006, p. 21):

> As pessoas que trabalham em grupo possuem mais idéias, mais energia e mais criatividade para enfrentar obstáculos do que uma pessoa só, além de reforçar as competências individuais. Logo, o resultado de um trabalho em grupo é mais produtivo que a soma das competências individuais.

As atividades presentes na pesquisa fazem com que o aluno tenha que compreender os processos de resolução do colega e vice-versa, para entender a lógica de resolução do outro, princípio onze, além de possibilitar o trabalho em grupo.

Pensando em um Currículo que leve em consideração as finalidades do Ensino Médio propostas pela Lei de Diretrizes e Bases e pelas Orientações Curriculares para o Ensino Médio, surge uma questão importante, que são os critérios para escolha e organização de temas para o Currículo de Matemática do Ensino Médio, aliando temas da atualidade e conteúdos de Matemática. Para Silva (2009), os temas para o Ensino Médio podem ser selecionados de acordo com quatro critérios: riqueza, reflexão, realidade e responsabilidade. A riqueza refere-se à escolha de temas que mostrem o quão rico um Currículo pode ser. Esse critério também se refere à prática do professor, que deve planejar suas aulas para mostrar o quanto pode ser explorado um tema em sala de aula se esse for bem planejado. A reflexão, de acordo com Silva (2009), propõe que o Currículo de Matemática abra espaço para discussão de conteúdos específicos de uma comunidade, levando em consideração aspectos relativos ao papel social da Matemática, ou seja:

> A reflexão, portanto, seria um componente necessário para que cada comunidade pudesse debater, a partir de problemas locais, quais os conteúdos necessários para uma investigação profunda, que possa implicar soluções ou a determinação de caminhos para políticas públicas voltadas ao respeito ao direito do próximo (SILVA, p.190).

O critério realidade está ligado à escolha de temas que possibilitem trabalhar com problemas reais. Um exemplo exposto pelo autor é o trabalho com Modelagem Matemática, que traz uma situação do cotidiano e é modelado, utilizando os recursos matemáticos fórmulas, deduções, etc. O critério responsabilidade refere-se à utilização dos conteúdos, que podem ser para fins militares, tecnológicos, sociais, mostrando qual a implicação do seu uso na sociedade. Por exemplo, no conteúdo de Estatística, em que se podem explorar aspectos como o crescimento populacional e o que pode ocorrer se houver mais natalidade do que mortalidade no país, pois pode ocasionar o aumento no tempo de serviço para aposentadorias, a falência de institutos de previdências, etc.

Os critérios para organização dos temas, segundo Silva (2009), são: recursão, relações, rigor e ressignificação. O critério recursão, dentro da organização dos conteúdos, significa proporcionar aos estudantes a possibilidade de recorrer a conteúdos já estudados em novos contextos. O critério relações refere-se à organização dos conteúdos quanto ao tempo para passar os conteúdos propostos para as três séries do Ensino Médio. Além disso, existem as questões referentes à sociedade e comunidade na qual a escola está inserida, que devem fazer parte do currículo, com o professor trabalhando essas questões em sala de aula. Conforme o autor, o critério rigor é caracterizado por uma proposta curricular que represente uma necessidade, por parte dos professores, de tomar decisões, replanejar, traçar novos objetivos e repensar as estratégias metodológicas em conjunto com alunos e equipe diretiva. O critério ressignificação está relacionado à importância que o autor dá à História da Matemática como um campo de estudo que pode fornecer subsídios à organização curricular da Matemática, com a ressignificação possibilitando recontextualizar um conteúdo dentro de outro tema, produzindo novos significados e relações enriquecedoras entre vários temas.

O tema Criptografia vai ao encontro de quatro critérios propostos por Silva (2009): riqueza, relação, recursão e resignificação. O primeiro deles, riqueza é percebido na possibilidade de desenvolver atividades didáticas que possibilitam usar padrões e regras de codificação e decodificação. O critério relação apresenta-se nas atividades didáticas que são possíveis com o tema, pois permite que o professor explore diversos conteúdos matemáticos como, por exemplo, funções, matrizes e aritmética modular, em atividades de codificação e decodificação, que podem envolver o aluno na resolução das atividades e motivá-los ao estudo dos conteúdos abordados. A Criptografia pode ser um recurso didático para trabalhar conteúdos matemáticos, desenvolvidos em sala de aula, anteriormente, pelos professores, dentro de um contexto que envolve segurança de dados, o que se refere ao critério recursão. O critério ressignificação pode ser percebido na possibilidade de recontextualizar um conteúdo dentro de outro tema, produzindo novos significados e relações enriquecedoras entre vários temas.

Trabalhar com esse tema, aliado aos conteúdos matemáticos do Ensino Médio, pode ser uma estratégia para o professor de Matemática revisar e reforçar alguns conteúdos, possibilitando ao estudante dessa etapa do Ensino Básico conhecer um pouco da história da Criptografia e ampliar seus conhecimentos referentes aos conteúdos desenvolvidos nas atividades didáticas propostas.

2 PRESSUPOSTOS METODOLÓGICOS DA INVESTIGAÇÃO

Este capítulo trata do problema da pesquisa, das hipóteses, dos objetivos e da metodologia de pesquisa, que foi uma Engenharia Didática, a qual seguiu suas quatro fases: as análises preliminares, a concepção e análise a *priori* das situações didáticas, a experimentação e a análise a *posteriori* e validação.

2.1 PROBLEMA

Como desenvolver uma Engenharia Didática que envolva os conteúdos matemáticos do Ensino Médio com o tema Criptografia?

2.2 HIPÓTESES

O presente projeto tem as seguintes hipóteses:

- existe relação entre o tema Criptografia e os conteúdos do Ensino Médio;
- através das atividades didáticas com o tema Criptografia aluno é capaz de aprofundar e revisar os conteúdos matemáticos do Ensino Médio e conhecer o tema.

2.3 OBJETIVOS

Este trabalho tem como objetivo geral investigar a possibilidade de implementar uma Engenharia Didática para o desenvolvimento do tema Criptografia aliado aos conteúdos de Matemática do Ensino Médio.

Os objetivos específicos da pesquisa foram:

- investigar a relação entre a Criptografia e os conteúdos matemáticos do Ensino Médio;
- pesquisar e selecionar atividades didáticas com o tema Criptografia para o Ensino Médio;
- desenvolver atividades aliando o tema Criptografia aos conteúdos matemáticos do Ensino Médio;
- implementar (desenvolver, aplicar e avaliar) um experimento com alunos do Ensino Médio com a sequência didática desenvolvida.

2.4 METODOLOGIA

A metodologia de pesquisa adotada foi a Engenharia Didática, a qual apresenta dois níveis de pesquisa, a microengenharia e a macroengenharia (MACHADO, 2008). A pesquisa, em microengenharia, estuda um determinado assunto, preocupando-se com os fenômenos que ocorrem em sala de aula. A macroengenharia compõe a complexidade da microengenharia com os fenômenos do processo de ensino e aprendizagem (ARTIGUE, 1995). Este projeto se baseia em uma microengenharia, pois busca desenvolver uma Engenharia Didática que envolva os conteúdos matemáticos do Ensino Médio com o tema Criptografia.

Também é importante ressaltar que a metodologia de Engenharia Didática possui uma validação essencialmente interna, que possibilita a confrontação da análise a *priori* com a *posteriori* (ARTIGUE, 1995).

Essa engenharia exige que o educador realize um projeto que desafie a sua criatividade. Nesse sentido, apresenta-se o tema Criptografia como motivador e desencadeador de situações-problema. Dessa forma, a Engenharia Didática relaciona os conceitos matemáticos e as situações didáticas propostas pelo educador.

Segundo Pais (2005, p.101), uma Engenharia Didática é composta por quatro fases consecutivas, que se dividem em: análises preliminares; concepção e análise *a priori*; aplicação de uma sequência didática e a análise *a posteriori* e validação.

Dentro da pesquisa em Engenharia Didática, na fase das análises preliminares, é realizada a análise do objeto em estudo, ou seja, é feito um referencial teórico que irá fundamentar o projeto. Nessa fase, o educador deve levar em consideração as constatações empíricas, concepções do aprendiz e compreender as condições nas quais será exposta a experiência. Dessa forma, este trabalho procura destacar as principais descrições do tema Criptografia, relacionando-o com o Currículo de Matemática. Nessa fase da pesquisa, também se deve levar em consideração:

> A análise epistemológica dos conteúdos contemplados pelo ensino; a análise do ensino atual e de seus efeitos; a análise da concepção dos alunos, das dificuldades e dos obstáculos que determinam sua evolução; a análise do campo dos entraves no qual vai se situar a efetiva realização didática (MACHADO, 2008, p. 238).

O levantamento dessas questões deve considerar o objetivo da pesquisa, pois o pesquisador deve ter clareza sobre o que realmente deseja pesquisar (MACHADO, 2008).

Com relação à pesquisa, na fase das análises preliminares, foi realizada pesquisa bibliográfica, com o propósito de investigar o tema Criptografia, sua história e aplicações. Essa fase foi um estudo exploratório, buscando aliar a Criptografia e os conteúdos matemáticos do Ensino Médio, desenvolvendo atividades didáticas, para que o estudante consiga reforçar conteúdos e agir em atividades didáticas com aplicações do tema.

Segundo Artigue (1995), na fase da concepção e análise *a priori,* busca-se delimitar as variáveis didáticas, que podem ser, variáveis macro-didáticas ou globais, as quais se referem à organização geral da engenharia, ou variáveis micro-didáticas ou locais, que se referem à organização de uma fase da engenharia. Nessa fase, buscou-se delimitar e compreender as variáveis didáticas, as quais foram analisadas durante o desenvolvimento da sequência didática, procurando determinar quais são as variáveis relevantes para a pesquisa, buscando uma relação do conteúdo de Matemática do Ensino Médio com as atividades propostas que levem o aluno a adquirir conceitos relevantes sobre o tema. As variáveis macro-didáticas foram o tema Criptografia e o Currículo de Matemática do Ensino Médio, pois possibilitam o desenvolvimento de atividades didáticas que levem o estudante a reforçar conteúdos abordados anteriormente. As variáveis micro-didáticas são os conteúdos de Matemática envolvidos nas atividades propostas.

De acordo com Artigue (1995), as análises *a priori* apresentam uma parte descritiva e uma parte de previsão, referente à situação adidática que se pretende aplicar. Isso é reforçado por Machado (2008), o qual afirma que análise *a priori*:

> Comporta uma parte de descrição e outra de previsão e está centrada nas características de uma situação adidática que se quis criar e que se quer aplicar aos alunos visados pela experimentação (MACHADO, 2008, pg. 243).

O pesquisador deve se preocupar em descrever as características da situação didática, verificar as possibilidades de ação dos alunos e analisar qual seria o comportamento do aluno frente à situação aplicada. Para Machado (2008):

> A análise a priori objetiva a consideração do aluno sob dois aspectos: o descritivo e o previsivo. Não há nela, tradicionalmente, lugar para o papel do professor, que, quando aparece, é simplesmente no aspecto descritivo. O aluno é considerado o ator principal (MACHADO, 2008, pg.244).

Nas análises *a priori*, foram descritas as características da situação adidática que se pretendia aplicar e procurou-se prever as ações possíveis do estudante durante a situação proposta.

Na fase de experimentação, realizou-se a aplicação da sequência didática, na qual se conseguiu aproximar os resultados práticos da análise teórica. A Engenharia Didática se utiliza das sequências didáticas para construção de um conhecimento significativo pelo aluno, onde o educador busca novas intervenções com a finalidade de articular diferentes atividades no decorrer de uma unidade didática (PAIS, 2005). Na experimentação, foram explicados aos alunos os objetivos e as condições necessárias para a realização do experimento. Também aplicaram-se os instrumentos da pesquisa e foram realizados registros das observações.

Segundo Pannuti (2004):

> A sequência didática é uma outra modalidade organizativa que se constitui numa série de ações planejadas e orientadas com o objetivo de promover uma aprendizagem específica e definida. Essas ações são seqüenciais, de forma a oferecer desafios com o grau de complexidade crescente, para que as crianças possam colocar em movimento suas habilidades, superando-as e atingindo novos níveis de aprendizagem (2004, p. 4).

Zabala (1998) diz que uma sequência didática é formada por aulas planejadas e analisadas previamente, com o objetivo de verificar situações de aprendizagem envolvendo os conceitos previstos no projeto elaborado pelo educador. A Criptografia é um tema que proporciona ao professor a liberdade de realizar diversas atividades, com graus de complexidade distintos, que busquem desencadear, no aluno, habilidades e competências que o tornem mais autônomo durante o seu processo de ensino e aprendizagem (GROENWALD; FRANKE, 2007). No decorrer do trabalho, a fase da aplicação da sequência didática constituiu-se da realização de um experimento para o qual se fez uso das atividades didáticas desenvolvidas em uma turma da 3ª série do Ensino Médio.

Na fase das análises *a posteriori,* foram analisados os dados da aplicação da sequência didática, obtidos através de diversos recursos: a observação direta do pesquisador, questionários aplicados nos alunos participantes do experimento, a análise dos registros desses alunos. Através da análise, conseguiu-se identificar e mostrar a realidade da produção dos alunos no desenvolvimento da sequência didática.

A validação foi o processo de verificação dos objetivos pré-estabelecidos no projeto, comparados com a confrontação dos resultados obtidos nas análises *a priori* e *a posteriori* que, segundo Machado (2008), possibilita ao professor/pesquisador avaliar a sua proposta metodológica.

A escolha dessa metodologia se deve ao fato da validação da pesquisa ser realizada, sobretudo, internamente, confrontando os dados da análise *a priori* e da análise *a posteriori* (MACHADO, 2008).

2.4.1 Sujeitos da pesquisa

O experimento foi realizado em uma turma de 3º ano do Ensino Médio, de uma escola pública da rede estadual do município de Campo Bom, no Rio Grande do Sul. Teve a duração de 14 horas aula, possibilitando 7 encontros de 2 horas aula cada, nos meses de agosto e setembro de 2010. A turma que participou da fase da experimentação era composta por 44 alunos. Cabe, ainda, salientar que a professora/pesquisadora não era a professora titular da turma que participou da fase de experimentação da pesquisa.

2.4.2 Instrumentos de coleta de dados

Para coleta de dados foi aplicado um questionário prévio (apêndice A) no primeiro dia de aula do experimento, com o qual se pretendeu conhecer a turma na qual seria realizado o experimento e, na última aula, após a realização de todas as atividades propostas, também foi aplicado um questionário pós-experimento (apêndice B), para verificar a opinião dos alunos sobre as atividades didáticas propostas, se encontraram dificuldades na resolução das atividades, com relação aos conteúdos abordados, se a calculadora foi um recurso que facilitou a resolução das atividades. A análise dos resultados foi baseada nas produções escritas dos alunos, através do material recolhido pela professora/pesquisadora, nas observações diretas de atividades realizadas pelos alunos em sala de aula e nos questionários aplicados.

3 ENGENHARIA DIDÁTICA COM O TEMA CRIPTOGRAFIA NO 3º ANO DO ENSINO MÉDIO

Neste capítulo, apresentam-se as fases da Engenharia Didática, que deram suporte ao trabalho desenvolvido, no 3º ano do Ensino Médio, com atividades didáticas envolvendo o tema Criptografia.

3.1 FASE DAS ANÁLISES PRELIMINARES

Segundo Pais (2005), para as análises preliminares, é necessária a referência de um quadro teórico, sobre o qual o pesquisador fundamenta suas principais categorias, tais como, constatações empíricas, concepções dos sujeitos envolvidos e as condições da realidade sobre a qual a experiência será realizada. Considera, também, que, para melhor organizar a análise preliminar, é recomendável proceder a uma descrição das principais dimensões que definem o fenômeno a ser estudado e que se relacionam com o sistema de ensino.

As análises preliminares foram realizadas através de pesquisa em livros didáticos, artigos de congressos, revistas da área de Matemática, buscando aplicações e atividades didáticas do tema em estudo para o Ensino Médio. Nessa fase, também foi realizada a análise de artigos: Revista do Professor de Matemática (RPM), Educação Matemática em Revista – RS, Revista Latinoamericana de Investigación en Matemática Educativa (RELIME), livros didáticos, Banco de Questões das Olimpíadas Brasileiras de Matemática, dissertações de mestrado, artigos de congresso e seminários.

3.1.1 Codificando e decifrando mensagens

O artigo “Codificando e decifrando mensagens”, do autor Antonio Carlos Tamarozzi, publicado na Revista do Professor de Matemática, número 45, do ano de 2001, nas páginas 41 a 43, apresenta duas atividades didáticas envolvendo os conteúdos matemáticos do Ensino Médio, aliados ao tema Criptografia, no qual a primeira atividade didática explora o tema com o conteúdo de função linear. É possível verificar que, para resolução da atividade, o aluno trabalha os conteúdos matemáticos de imagem da função e função inversa. A segunda atividade didática alia o tema ao conteúdo de matrizes de ordem 2. Essa atividade permite que o aluno trabalhe os conteúdos de multiplicação de matrizes e matriz inversa. A atividade didática do autor que será apresentada é a que envolve o conteúdo de função linear, figura 16.

Inicialmente, relacionamos números ao alfabeto (o símbolo # representa um espaço em branco) que vamos utilizar nos modelos. Assim:

#	A	B	...	J	K	L	...	V	W	X	Y	Z
0	1	2	...	10	11	12	...	22	23	24	25	26

Portanto, cifrar uma mensagem recai no problema de permutar números por meio de uma regra *f*. Pode-se fazer isso, de forma muito prática, por exemplo, através das funções afins $f(x) = ax + b$, com *a*, *b* inteiros, $a \neq 0$, definidas no conjunto {0, 1,..., 26}. Suponhamos que Ana e Ivo desejem trocar mensagens sigilosas utilizando o alfabeto escolhido. O primeiro passo a tomarem é definirem a função cifradora, digamos $f(x) = 2x - 3$.

Assim, por exemplo, à mensagem: R E V I S T A R P M

Ana associa a sequência numérica: 18 5 22 9 19 20 1 0 18 16 13

E transmite a sequência numérica obtida pelas imagens de *f*, isto é, 33 7 41 15 35 37 −1 −3 33 29 23.

Ao recebê-la, Ivo, calculando a imagem de $f^{-1}(x) = \frac{x+3}{2}$ nessa sequência e utilizando a correspondência alfabeto-numérica, obtém a mensagem original.

Depois de os alunos dominarem o processo, seria oportuno que o professor propusesse situações em que um intruso tente decifrar mensagens, apoderando-se das sequências numéricas codificadas. Como estamos utilizando funções afins, para tanto, é suficiente apenas duas associações corretas entre números das sequências original e codificada. Admitindo que sejam conhecidas essas associações, é um exercício interessante para os alunos determinarem *f*.

(TAMAROZZI, 2001, p.41-42)

Figura 16: exemplo de atividades de Criptografia com função linear.

A atividade didática apresentada pelo autor pode ser um recurso para trabalhar em sala de aula de forma a exercitar e revisar o conteúdo matemático de função linear, onde o professor pode explorar a idéia de função e função inversa em uma mesma atividade.

3.1.2 Criptografia: uma aplicação de álgebra linear

O artigo “Criptografia: uma aplicação de álgebra linear”, dos autores Solange dos Santos Nieto, Célia Mendes Carvalho Lopes e Alcides Ferreira da Silva, presente no X Internacional Conference on Engineering and Technology Education, em 2008, mostra uma possibilidade de trabalhar com o tema Criptografia envolvendo a sua história e os conteúdos matemáticos do Ensino Médio. O conteúdo explorado neste artigo é o de Matrizes de ordem 3, em que o aluno recebe uma matriz A codificadora, que possui inversa, constrói uma matriz mensagem, denominada matriz M, realiza o cálculo de multiplicação de matrizes para codificar. Para decodificar, o aluno deverá multiplicar a matriz resultante da multiplicação da matriz A pela matriz M, pela matriz inversa da matriz A. Uma forma do professor explorar essa atividade está presente na figura 17.

O primeiro passo é codificar a mensagem. Vamos passar da forma alfabética para a forma numérica, utilizando a seguinte correspondência indicada na tabela a seguir.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
2	1	4	3	6	5	8	7	10	9	12	11	14	13
O	P	Q	R	S	T	U	V	W	X	Y	Z	#	.
16	15	18	17	20	19	22	21	24	23	26	25	28	27

Essa correspondência pode ser alterada e poderia, inclusive, servir como um novo exercício a ser sugerido ao aluno, para que ele verificasse que esta é uma escolha qualquer. Escolhemos uma matriz quadrada qualquer, que tenha inversa. Escolhemos, por exemplo, a matriz A (chamada codificadora) $A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 0 \\ 1 & 1 & 3 \end{bmatrix}$.

Trabalhamos, com o aluno, o cálculo da inversa. Chamaremos de B a matriz inversa de A.

No exemplo, $A^{-1} = B = \begin{bmatrix} 3 & -2 & -2 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{bmatrix}$.

A matriz onde escrevemos a mensagem será denominada M.

$$M = \begin{bmatrix} 6 & 3 & 22 & 4 & 2 & 4 & 2 & 16 & 28 & 6 & 14 & 28 \\ 6 & 13 & 8 & 6 & 13 & 7 & 2 & 17 & 10 & 2 & 28 & 6 \\ 28 & 19 & 6 & 4 & 13 & 16 & 11 & 16 & 8 & 10 & 2 & 27 \end{bmatrix}$$

Assim, a mensagem codificada será encontrada pelo produto M. A e chamaremos essa matriz de N.

$$N = A.M =$$
$$\begin{bmatrix} 62 & 41 & 34 & 12 & 28 & 36 & 24 & 48 & 44 & 26 & 18 & 82 \\ -6 & -13 & -8 & -6 & -13 & -7 & -2 & -17 & -10 & -2 & -28 & -6 \\ 96 & 73 & 48 & 22 & 54 & 59 & 37 & 81 & 62 & 38 & 48 & 115 \end{bmatrix}$$

Desse modo, N é a matriz que chega ao seu destinatário, que deverá utilizar a matriz B(matriz decodificadora) para decifrar a mensagem, já que B.N = B.AM = I.M = M(mensagem). No exemplo, temos que

$$B.N = \begin{bmatrix} 6 & 3 & 22 & 4 & 2 & 4 & 2 & 16 & 28 & 6 & 14 & 28 \\ 6 & 13 & 8 & 6 & 13 & 7 & 2 & 17 & 10 & 2 & 28 & 6 \\ 28 & 19 & 6 & 4 & 13 & 16 & 11 & 16 & 8 & 10 & 2 & 27 \end{bmatrix}$$

Observe que esse produto é a matriz enviada pelo remetente, portanto, a mensagem codificada é: 6, 3, 22, 4, 2, 4, 2, 16, 28, 6, 14, 28, 6, 13, 8, 6, 13, 7, 2, 17, 10, 2, 28, 6, 28, 19, 6, 4, 13, 16, 11, 16, 8, 10, 2, 27

Portanto,a mensagem é “EDUCAÇÃO EM ENGENHARIA E TECNOLOGIA.”

(NIETO, LOPES e SILVA, 2008).

Figura 17: exemplo de atividades de codificação envolvendo matrizes.

Essa atividade é uma forma do professor explorar o conteúdo de matrizes de ordem 3, em sala de aula, onde o aluno poderá exercitar os conteúdos de multiplicação de matrizes de ordem 3 e os procedimentos para encontrar a matriz inversa de ordem 3.

3.1.3 Códigos e senhas no Ensino Básico

O artigo “Código e senhas no Ensino Básico”, das autoras Claudia Lisete Oliveira Groenwald, Rosvita Fuelber Franke e Clarissa de Assis Olgin, presente na revista Educação Matemática em Revista, do Rio Grande do Sul, publicado em 2009, páginas 41 a 50. Apresenta aplicações do tema Criptografia ao longo da história, com atividades envolvendo a Cifra de César, a Cifra de Vigenère, a Cifra Chiqueiro e o Código ISBN, que trabalha com aritmética modular, um conteúdo pouco explorado no Ensino Médio.

Após as atividades para introduzir o tema, tem-se atividades didáticas que aliam os temas aos conteúdos matemáticos de função quadrática e função exponencial e função logarítmica. A atividade explorada referente a esse artigo é o código com função exponencial e logaritmo (figura 18), por ser um conteúdo que apresenta poucas atividades didáticas envolvendo aplicabilidades. Na atividade, as autoras mostram como o professor pode explorar esse conteúdo, trabalhando com imagem da função para codificar, com o cálculo da função inversa exponencial e logarítmica, onde se pretende que o aluno compreenda que as funções exponenciais e logarítmicas são funções inversas.

Primeiro, relaciona-se cada letra do alfabeto a um número, conforme observa-se a seguir.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Crie uma mensagem a ser enviada: **MATEMÁTICA**

Cifre esta mensagem, utilizando a função escolhida.

Entregue a mensagem cifrada para que seu colega a decifre.

Seja a função $f(x) = 2^x$, calcula-se a imagem da função para cada algarismo da sequência numérica:

Letra	**Sequência Numérica**	**Imagem da função** $f(x) = 2^x$
M	13	$f(x) = 2^x = 2^{13} = 8192$
A	1	$f(x) = 2^x = 2^1 = 2$
T	20	$f(x) = 2^x = 2^{20} = 1048576$
E	5	$f(x) = 2^x = 2^5 = 32$
I	9	$f(x) = 2^x = 2^9 = 512$
C	3	$f(x) = 2^x = 2^3 = 8$

Seja a função inversa $x = log_2 y$, calcula-se a imagem da função para cada algarismo da sequência numérica:

Sequência Numérica Recebida	**Imagem da inversa da função codificadora** $x = log_2 y$	**Letra encontrada no alfabeto inicial**
8192	$2^x = 8192 \rightarrow x = 13$	M
2	$2^x = 2 \rightarrow x = 1$	A
1048576	$2^x = 1048576 \rightarrow x = 20$	T
32	$2^x = 32 \rightarrow x = 5$	E
8192	$2^x = 8192 \rightarrow x = 13$	M
2	$2^x = 2 \rightarrow x = 1$	A
1048576	$2^x = 1048576 \rightarrow x = 20$	T
512	$2^x = 512 \rightarrow x = 9$	I
8	$2^x = 8 \rightarrow x = 3$	C
2	$2^x = 2 \rightarrow x = 1$	A

(FRANKE; GROENWALD; OLGIN, 2009, p. 47).

Figura 18: exemplo de atividades de Criptografia envolvendo função exponencial e logarítmica.

3.1.4 Currículo de Matemática no Ensino Básico: a importância do desenvolvimento e pensamentos de alto nível

O artigo “Currículo de matemática no Ensino Básico: a importância do desenvolvimento dos pensamentos de alto nível”, dos autores Claudia Lisete Oliveira Groenwald e Giovanni da Silva Nunes, está presente na Revista Latinoamericana de Investigación en Matemática Educativa, publicada em 2007, páginas 97 a 116. Esse artigo trata da importância de desenvolver, no Currículo de Matemática, os três tipos de conteúdos, os conceitos e fatos, os procedimentais e os atitudinais para o desenvolvimento do pensamento de alto nível e apresenta um exemplo de atividade didática que envolve Criptograma (figura 19), a qual proporciona ao aluno do Ensino Médio trabalhar com questões relativas a planejamento de estratégias de resolução de problemas, o que é pertinente a essa etapa do Ensino Básico, em que os alunos devem sair preparados também para o mundo do trabalho e esse, por sua vez, pode precisar que o profissional seja capaz de tomar decisões e verificar a implicação da mesma.

Sabendo que cada letra representa um algarismo distinto e que existe apenas uma resposta, que adição é essa? AMOR + AMOR + AMOR = ÓDIO.

Para a realização dessa atividade, é necessário que o aluno procure sistematizar as informações relevantes, formular hipóteses, prever os resultados e elaborar estratégias de enfrentamento das questões.

Informação relevante: $3A \leq 9 \Rightarrow A \leq 3$.

Hipóteses: A=1 ou A=2 ou A=3.

Prevendo resultados: i) se A = 1, então, O = 3 ou O = 4 ou O = 5;
ii) se A = 2, então, O = 6 ou O = 7 ou O = 8;
iii) se A = 3, então, O = 9.

Verificação das hipóteses (enfrentamento das questões):

O raciocínio lógico leva a testar “iii” primeiramente, porque, dado A=3, só há uma possibilidade para O, a saber, O = 9.

Verificamos que essa possibilidade é falsa: se A = 3, então, 3R = 9 ou 3R = 19.

$3R = 9 \Rightarrow R = 3$: é falso, porque R deve ser um valor diferente de A;

3R = 19 é falso, porque R é um valor inteiro.

Além disso, é importante que o aluno se dê conta de que 3R > 27 não ocorre; logo, não é possível 29, 39 etc.

Todas as hipóteses devem ser verificadas com esse tipo de raciocínio. Por exemplo, a hipótese de que A=1 e O = 3 é facilmente descartada, porque leva a concluir que 3R = 3 implicando R = 1, o que é impossível, porque A não é igual a R.

Passemos, então, para a verificação da hipótese verdadeira: se A = 2 e O = 8, então 3R = 18, pois é o único múltiplo de 3 entre 0 e 27 que termina em 8; logo, R = 6. Sabemos que 3O = 24, então I = 5 e M = 7 e D = 3.

Logo, a conta esperada é: $3 \times 2\,786 = 8\,358$ ou 2 786 + 2 786 + 2 786 = 8 358.

(GROENWALD; NUNES, 2007, p.105-108).

Figura 19: exemplo de atividades de Criptogramas.

3.1.5 Livro didático: Tudo é Matemática

O livro didático, da 5ª série do Ensino Fundamental, do autor Luiz Roberto Dante, editado no ano de 2004 e publicado pela editora Ática, na página 33, apresenta atividades didáticas envolvendo Criptogramas. A atividade apresenta o conceito de Criptografia, um breve histórico da mesma e atividades didáticas envolvendo o conteúdo de operações com Números Naturais, conforme a figura 20.

Criptografia é a arte de escrever usando números ou códigos. No século XVI, o francês François Viète destacou-se pela extrema habilidade em decifrar mensagens secretas, quando seu país estava em guerra contra a Espanha. Atualmente, a criptografia é bastante usada, por exemplo, na internet, para garantir a segurança na transmissão de dados.

Vamos tentar decifrar os criptogramas abaixo? Cada letra indica um algarismo. Letras iguais representam algarismos iguais e letras diferentes representam algarismos diferentes. Use o raciocínio lógico e descubra o valor de cada letra em cada criptograma. Depois, refaça as operações para conferi-las.

a) $\begin{array}{r} A\ B \\ +\,C\ A \\ \hline A\ B\ A \end{array}$ b) $\begin{array}{r} N\ O\ V\ E \\ +\,T\ R\ \hat{E}\ S \\ \hline D\ O\ Z\ E \end{array}$ c) $\begin{array}{r} X\ Y \\ +\ Y\ X \\ \hline X\,X\,Z \end{array}$

(DANTE, 2004, p.33).

Figura 20: exemplo de atividades de Criptogramas.

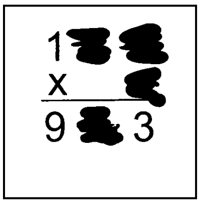
Acredita-se que essa atividade possibilita ao aluno desenvolver estratégias de resolução de problemas, na qual ele deve levantar hipóteses, testá-las e verificar se a resposta dada ao problema é verdadeira.

3.1.6 Atividades didáticas de Criptografia no banco de questões da Olimpíada Brasileira de Matemática

O banco de questões da Olimpíada Brasileira de Matemática, editado no ano de 2009, pela OBMEP, apresenta atividades didáticas de criptogramas envolvendo operações com Números Naturais. Desse banco foram analisadas e aplicadas na sequência quatro atividades didáticas, em que a primeira, a terceira e a quarta atividade envolvem o conteúdo de multiplicação de Números Naturais e a segunda atividade envolve o conteúdo de adição de Números Naturais, conforme se observa na figura 21.

1) (Olímpiada Brasileira de Matemática – 2009) Davi estava fazendo uma conta no caderno quando sua caneta estragou e borrou quatro algarismos, como na figura. Ele se lembra que só havia algarismos ímpares na conta. Qual é a soma dos algarismos manchados?

a) 14
b) 18
c) 20
d) 26
e) 28



2) (Banco de questões: Olímpiada Brasileira de Matemática – 2009) Qual é o número? - Na adição apresentada na figura, letras iguais representam o mesmo algarismo e letras diferentes, algarismos diferentes. Encontre o número ABCDE.

$$\begin{array}{r} ABCDE \\ BCDE \\ CDE \\ DE \\ E \\ \hline AAAAA \end{array}$$

3) (Banco de questões: Olímpiada Brasileira de Matemática – 2009) Multiplicação com letras - Na operação abaixo, as letras a, b e c são algarismos distintos e diferentes de
1. Determine os valores de a, b e c.

$$\begin{array}{r} abb \\ \times\quad c \\ \hline bcb1 \end{array}$$

4) (Banco de questões: Olímpiada Brasileira de Matemática – 2009) Qual é o **número?** – Um número de 6 algarismos começa por 1. Se deslocamos esse algarismo 1 da primeira posição para última à direita, obtemos um novo número de 6 algarismos que é o triplo do número de partida. Qual é esse número?

(BANCO DE QUESTÕES, 2009).

Figura 21: exemplo de atividades envolvendo o tema de Criptografia.

3.1.7 Contribuições da neurociência cognitiva para a formação de professores e pedagogos

O autor Tabacow, no ano de 2006, em sua dissertação de mestrado, com o título “Contribuições da neurociência cognitiva para a formação de professores e pedagogos”, apresenta uma atividade didática envolvendo a descoberta de algarismos, na qual cada letra representa um algarismo distinto e sabe-se que a letra D representa o algarismo 5. Esta atividade é denominada Criptograma e está presente na figura 22.

Quanto vale a soma de DONALD + GERALD =ROBERT, sendo dado D = 5 e sabendo que cada letra tem um valor único, variando de zero a nove?

$$\begin{array}{ccccccc} & D & O & N & A & L & D \\ + & G & E & R & A & L & D \\ \hline & R & O & B & E & R & T \end{array}$$

(HUFFMAN e COLS apud TABACOW, 2006).

Figura 22: exemplo de atividades envolvendo o tema de Criptografia.

Entende-se que esse tipo de atividade possibilita ao aluno revisar e ampliar sua compreensão sobre os conceitos de aritmética, já estudados no Ensino Fundamental. Permite, também, que utilize as habilidades de: levantar hipóteses e comprovar essas hipóteses; resolver problemas.

3. 2 FASE DA CONCEPÇÃO E ANÁLISES *A PRIORI*

A fase da concepção e análise *a priori* deu-se em dois momentos. O primeiro foi o planejamento e organização da sequência didática e o segundo foi a análise das possíveis resoluções dos alunos às atividades didáticas presentes na sequência elaborada, pois, de acordo com Artigue (1995), na análise *a priori,* descrevem-se as características da situação que se pretende aplicar, procurando prever as ações dos alunos.

Nas análises a priori, foram descritas as características da situação adidática que se pretendia aplicar e procurou-se prever as ações possíveis do estudante durante a situação proposta.

3.2.1 Planejamento da sequência didática que foi desenvolvida na fase da experimentação da Engenharia Didática

As atividades didáticas apresentadas na fase da experimentação foram elaboradas de forma a propiciar o trabalho em grupo e a discussão, em sala de aula, de assuntos relevantes à disciplina, oportunizando o uso da calculadora em sala de aula, como um instrumento facilitador. A sequência didática elaborada com o tema Criptografia para o Ensino Médio, que foi utilizada na fase de experimentação, seguiu as seguintes etapas:

1º) introdução do tema Criptografia através de uma abordagem histórica, realizada pela professora/pesquisadora;

2º) resolução de atividades didáticas que aliam o tema em estudo aos conteúdos matemáticos do Ensino Médio.

A sequência didática proposta, nesta investigação, procurou trabalhar com as aplicações do tema Criptografia, através de atividades envolvendo Cifra de César, Cifras do Chiqueiro e a Cifra de Playfair. Também apresenta atividades envolvendo criptogramas, para introduzir o tema e revisar o conteúdo de Aritmética, já trabalhado no Ensino Fundamental, atividades envolvendo o Dígito Verificador do Código ISBN, em que se pretendeu introduzir o conteúdo de Aritmética Modular, que não é trabalhado no Ensino Médio, através de uma aplicação. Os conteúdos de funções e matrizes foram escolhidos, pois dentre os abordados no Ensino Médio acredita-se que o tema em estudo permite explorar esses conteúdos e suas propriedades, de forma a revisar e ampliar os conhecimentos dos alunos para os mesmos, possibilitando-lhes aplicar o conteúdo de função inversa e matriz inversa em atividades didáticas de decodificação.

3.2.2 Análise das possíveis resoluções dos alunos

Este sub-capítulo apresenta a análise de todas as questões presentes nas atividades didáticas propostas aos alunos na fase da experimentação.

Etapa 1

As atividades didáticas envolvendo Criptogramas objetivam que os alunos apliquem seus conhecimentos de Aritmética em uma situação nova. As atividades envolvem uma situação de descoberta de números representados por letras, introduzindo, assim, o conceito de Criptografia.

Atividade 1 – Criptogramas

a) Descubra o valor de cada letra, no Criptograma a seguir, sabendo que cada uma representa um algarismo distinto de zero a nove.

$$\begin{array}{r} A\ B \\ +\ C\ A \\ \hline A\ B\ A \end{array}$$

Possíveis soluções dos alunos

a) O aluno pode tentar resolver a atividade por tentativa e erro, atribuindo para cada letra valores aleatórios.

b) O aluno pode resolver a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Informação relevante: B = 0 e A $\neq$ 0

Hipóteses: A = 1

Prevendo resultados: i) se A = 1, B = 0, então, C = 9.

Verificação das hipóteses: verifica-se que as possibilidades são verdadeiras, pois $\begin{array}{r} 1\ 0 \\ +\ 9\ 1 \\ \hline 1\ 0\ 1 \end{array}$.

b) Descubra o valor de cada letra, no Criptograma a seguir, sabendo que cada uma representa um algarismo distinto de zero a nove.

$$\begin{array}{r} X\ Y \\ +\ Y\ X \\ \hline X\ X\ Z \end{array}$$

Possíveis soluções dos alunos

a) O aluno pode tentar resolver a atividade por tentativa e erro, atribuindo para cada letra valores aleatórios.

b) O aluno pode resolver a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Informação relevante: Y + X = Z e X + Y = XX[5]

Hipóteses: X = 1

Prevendo resultados: i) se X = 1, então, Y = 9 e Z = 0.

Verificação das hipóteses: verifica-se que as possibilidades são verdadeiras, pois $\begin{array}{r} 1^{1}\ \ 9 \\ +\ \ 9\ \ 1 \\ \hline 1 1\ \ 0 \end{array}$.

c) Descubra o valor de cada letra, no Criptograma a seguir, sabendo que cada uma representa um algarismo distinto de zero a nove.

$$\begin{array}{r} N\ O\ V\ E \\ +T\ R\ \hat{E}\ S \\ \hline D\ O\ Z\ E \end{array}$$

Possíveis soluções dos alunos

a) O aluno pode tentar resolver a atividade por tentativa e erro, atribuindo para cada letra valores aleatórios.

b) O aluno pode resolver a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Informação relevante: S = 0

Hipóteses: O + R =O, temos O + R > 10

Prevendo resultados: i) se S = 0, O = 8, R = 9, então, E = 5, V = 6, Z = 1, N = 2, T = 4 e D = 7.

Verificação das hipóteses: verifica-se que as possibilidades são verdadeiras.

d) Descubra o valor de cada letra, no Criptograma a seguir, sabendo que cada uma representa um algarismo distinto de zero a nove.

$$\begin{array}{r} L\ \ U\ \ A \\ +\ T\ \ U\ \ A \\ \hline S\ A\ L\ \ A \end{array}$$

Possíveis soluções dos alunos

[5] No Criptograma Y + X = Z e X + Y = XX o termo XX é um número de dois algarismos, onde um x é o algarismo das unidades e o outro x o algarismo das dezenas.

a) O aluno pode tentar resolver a atividade por tentativa e erro, atribuindo para cada letra valores aleatórios.

b) O aluno pode resolver a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Informação relevante: A = 0

Hipóteses: L + T $\geq$ 10

Prevendo resultados: i) se A = 0, U = 2, então, L = 4, T = 6, S = 1;

ii) se A = 0, U = 4, então, L = 8 , T = 2, S = 1.

Verificação das hipóteses: verifica-se que as possibilidades são verdadeiras e que há várias possibilidades de valores para as letras L, U, T.

e) Descubra o valor de cada letra, no Criptograma a seguir, sabendo que cada uma representa um algarismo distinto de zero a nove.

$$D\ O\ C\ E \div D\ O = T\ I\ O$$

Possíveis soluções dos alunos

a) O aluno pode tentar resolver a atividade por tentativa e erro, atribuindo para cada letra valores aleatórios.

b) O aluno pode resolver a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Informação relevante: DO ÷ DO = T, T = 1

Hipóteses: D $\geq$ 2

Prevendo resultados: i) se D = 2, O = 3, então, C = 6, E = 9, I = 0.

Verificação das hipóteses: verifica-se que a possibilidade é verdadeira.

f) Quanto vale a soma de DONALD + GERALD =ROBERT, sendo dado D = 5 e sabendo que cada letra tem um valor único variando de zero a nove?

$$\begin{array}{r} D\ O\ N\ A\ L\ D \\ +\,G\ E\ R\ A\ L\ D \\ \hline R\ O\ B\ E\ R\ T \end{array}$$

Possíveis soluções dos alunos

a) O aluno pode tentar resolver a atividade por tentativa e erro, atribuindo para cada letra valores aleatórios.

b) O aluno pode resolver a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Informação relevante: D = 5, T = 0, L $\neq$ 2, L $\neq$ 7, D + G < 10, L + L > 10, R > 6, E = 9, A = 4

Hipóteses: O = 2

Prevendo resultados: i) L = 8, então, R = 7, N = 6, G = 1, B = 3.

Verificação das hipóteses: verifica-se que a possibilidade é verdadeira.

g) Qual é o número? Na adição apresentada a seguir, letras iguais representam o mesmo algarismo e letras diferentes, algarismos diferentes. Encontre o número ABCDE.

$$\begin{array}{rccccc} & A & B & C & D & E \\ & & B & C & D & E \\ + & & & C & D & E \\ & & & & D & E \\ & & & & & E \\ \hline & A & A & A & A & A \end{array}$$

Possíveis soluções dos alunos

a) O aluno pode tentar resolver a atividade por tentativa e erro, atribuindo para cada letra valores aleatórios.

b) O aluno pode resolver a questão sistematizando as informações relevantes, formulando hipóteses e elaborando estratégias para resolução.

Informação relevante: letras iguais representam o mesmo algarismo, letras distintas representam algarismos diferentes.

Hipóteses: A = 5

Prevendo resultados: i) E = 7, então, D = 8, C = 4, B = 2.

Verificação das hipóteses: verifica-se que a possibilidade é verdadeira.

Etapa 2

As atividades didáticas envolvendo a Cifra de César objetivam que os alunos conheçam e aprendam a utilizar cifras de substituição monoalfabética, conhecendo e aplicando conceitos do tema em estudo.

Atividade 2 – Cifra de César

a) Cifre a frase “MATEMÁTICA É PARA VIDA”, utilizando a Cifra de César, utilizando a figura 23.

Alfabeto Normal	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
Alfabeto Cifrado	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

Figura 23: quadro do método de substituição utilizado por Júlio César.

Fonte: Adaptado de Singh (2003, p.27)

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com a codificação utilizada por Júlio César, na qual ele visualizará na figura 23, o quadro do método de substituição de Júlio César e substituirá a letra do alfabeto normal pela letra do alfabeto cifrado. Assim, espera-se que o aluno encontre, como mensagem cifrada, “PDWHPDWLFDHSDUDYLGD”.

b) Decodifique a frase “d-y-l-g-h-x-p-d-s-h-f-d-g-h-w-h-d-w-u-r-t-x-h-q-d-r-s-h-u-p-l-w-h-q-v-d-l-r-v-s-r-u-l-v-v-r-f-d-q-w-h-f-k-r-u-h-g-d-q-f-h-u-l-d-h-y-l-y-d-l-q-w-h-q-v-d-p-h-q-w-h-d-q-w-h-v-t-x-h-d-f-r-u-w-l-q-d-v-h-i-h-f-k-h-h-d-s-h-f-d-w-h-u-p-l-q-h-v-h-p-d-s-o-d-x-v-r-v”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com a codificação utilizada por Júlio César, decodificando, substituindo a letra do alfabeto cifrado pela letra do alfabeto normal, encontrando como texto decodificado a mensagem “A vida é uma peça de teatro que não permite ensaios. Por isso, cante, chore, dance, ria e viva intensamente, antes que a cortina se feche e a peça termine sem aplausos.”.

c) Codifique a frase “Não pense nos momentos difíceis como o fim do mundo, e sim como mais um obstáculo a ser superado.”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com a codificação utilizada por Júlio César, onde ele visualizará na figura 23, o quadro do método de substituição de Júlio César e substituirá a letra do alfabeto normal pela letra do alfabeto cifrado. Assim, espera-se que o aluno encontre, como mensagem cifrada, “QDRSHQVHQRVPRPHQWVGLILFHLVFRPRRILPGRPXQGR HVLPFRPRPDLVXPREVWDFXORDVHUVXSHUDGR”.

d) Decodifique a frase “v-h-q-d-r-s-x-g-h-u-v-h-g-h-v-w-d-f-d-u-s-h-o-r-w-d-o-h-q-w-r-y-h-q-f-d-s-h-o-r-h-v-i-r-u-f-r”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, conforme a codificação utilizada por Júlio César, decodificando, substituindo a letra do alfabeto cifrado pela letra do alfabeto normal, encontrando como texto decodificado a mensagem “Se não puder se destacar pelo talento, vença pelo esforço.”.

e) Codifique a frase “É melhor estar preparado para uma oportunidade e não ter nenhuma, do que ter uma oportunidade e não estar preparado”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, conforme a codificação utilizada por Júlio César, onde ele visualizará na figura 23, o quadro do método de substituição de Júlio César e substituirá a letra do alfabeto normal pela letra do alfabeto cifrado. Assim, espera-se que o aluno encontre, como mensagem cifrada, “HPHOKUHVWDUSUHSDUDGRSDUDXPDRSRUWXQLGDGH HQRDWHRQHQKXPDGRTXHWHUXPDRSRUWXQLGDGHHQDRHVWDUSUHSD UDGR”.

f) Decodifique a frase “y-r-o-w-d-u-d-w-u-d-v-h-p-h-o-k-r-u-t-x-h-v-h-s-h-u”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com a codificação utilizada por Júlio César, decodificando, substituindo a letra do alfabeto cifrado pela letra do alfabeto normal, encontrando como texto decodificado a mensagem “Voltar atrás é melhor que perder-se no caminho.”.

g) Codifique a frase “Há pessoas que transformam o sol numa simples mancha amarela, mas há também aquelas que fazem de uma simples mancha amarela o próprio sol”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com a codificação utilizada por Júlio César, onde ele visualizará na figura 23, o quadro do método de substituição de Júlio César e substituirá a letra do alfabeto normal pela letra do alfabeto cifrado. Assim, espera-se que o aluno encontre, como mensagem cifrada, “HDSHVVRDVTXHWUDQVIRUPDPRVROQXPDVLPOHVPDQ FKDDPDUHODPDVKDWDPEHPDTXHODVTXHIDCHPGHXPDVLPOHVPDQFKDD PDUHODRSURSULRVRO”.

h) Decodifique a frase “d-p-h-d-y-l-g-d-h-r-v-e-r-v-d-p-l-j-r-v-v-h-p-s-u-h”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que o aluno encontre o valor de cada letra, conforme a codificação utilizada por Júlio César, decodificando, substituindo a letra do alfabeto cifrado pela letra do alfabeto normal, encontrando como texto decodificado a mensagem “Ame a vida e os bons amigos sempre.”.

i) Codifique a frase “As pessoas mais felizes não têm as melhores coisas. Elas sabem fazer o melhor das oportunidades que aparecem em seus caminhos.”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com a codificação utilizada por Júlio César, onde ele visualizará na figura 23, o quadro do método de substituição de Júlio César e substituirá a letra do alfabeto normal pela letra do alfabeto cifrado. Assim, espera-se que o aluno encontre, como mensagem cifrada, “DVSHVVRDVPDLVIHOLCHVQDRWHPDVPHOKRUHVFRLVD VHODVVDEPIDCHURPHOKRUGDVRSRUWXQLGDGHVTXHDSAUHFHPHPVHXV FDPLQKRV”.

j) Decodifique a frase “r-f-d-p-l-q-k-r-s-d-u-d-d-i-h-o-l-f-l-g-d-g-h-h-v-w-d-h-p-y-l-y-h-u-p-r-v-r-s-u-h-v-h-q-w-h”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que o aluno encontre o valor de cada letra, conforme a codificação utilizada por Júlio César, decodificando, substituindo a letra do alfabeto cifrado pela letra do alfabeto normal, encontrando como texto decodificado a mensagem “O caminho para a felicidade está em vivermos o presente.”.

k) Codifique a frase “Lembrar é fácil para quem tem memória, esquecer é difícil para quem tem coração.”, utilizando a Cifra de César.

Possível solução dos alunos

Espera-se que o aluno encontre o valor de cada letra, de acordo com a codificação utilizada por Júlio César, onde ele visualizará na figura 23, o quadro do método de substituição de Júlio César e substituirá a letra do alfabeto normal pela letra do alfabeto cifrado. Assim, espera-se que o aluno encontre, como mensagem cifrada, “OHPEUDUHIDFLOSDUATXHPWHPPHPRULDHVTXHFHUHGLILFLOSDU DTXHPWHPFRUDFRD”.

Etapa 3

As atividades didáticas envolvendo a Cifra do Chiqueiro têm por objetivo que os alunos conheçam e aprendam a utilizar cifras de substituição de letras por posições as quais ocupam.

Atividade 3 – Cifra do Chiqueiro

a) Considerando a figura 24, codifique a frase "A felicidade não está no fim da jornada, e sim em cada curva do caminho que percorremos para encontrá-la.", utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

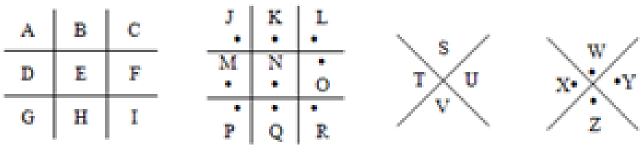
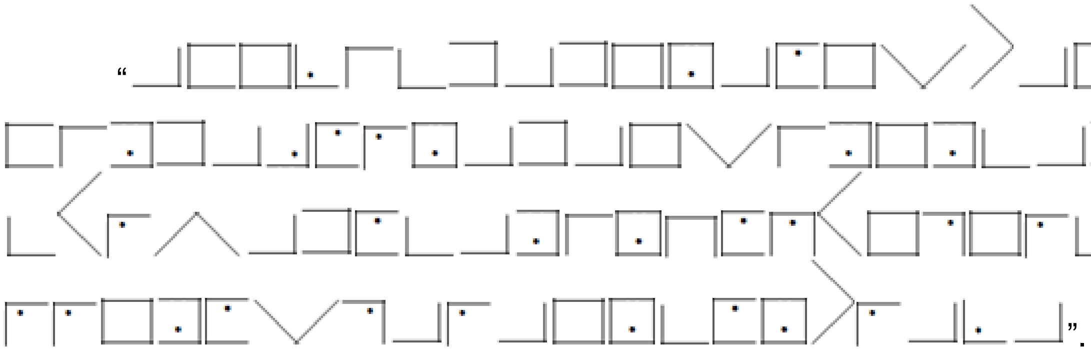


Figura 24: exemplo do padrão utilizado pela Cifra do Chiqueiro.

Possível solução dos alunos

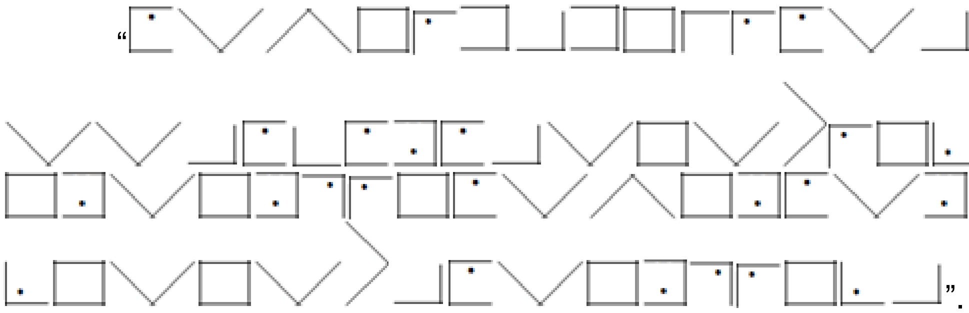
Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, conforme o padrão utilizado pela Cifra de Chiqueiro, onde ele substituirá a letra do alfabeto normal pela sua posição, de acordo com a figura 24. Assim, espera-se que o aluno encontre, como mensagem cifrada:



b) Considerando a figura 24, codifique a frase "Os verdadeiros amigos são como as estrelas. Nem sempre os vês, mas eles estão sempre lá.", utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

Possível solução dos alunos

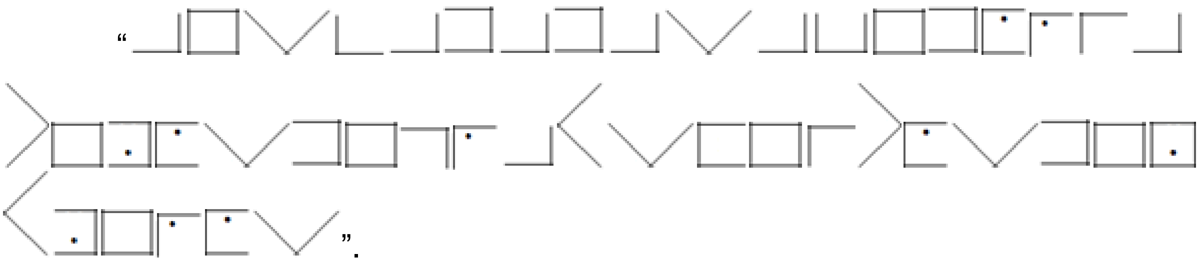
Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com o padrão utilizado pela Cifra de Chiqueiro, onde ele substituirá a letra do alfabeto normal pela sua posição, conforme a figura 24. Assim, espera-se que o aluno encontre, como mensagem cifrada:



c) Considerando a figura 24, codifique a frase "A escada da sabedoria tem os degraus feitos de números.", utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

Possível solução dos alunos

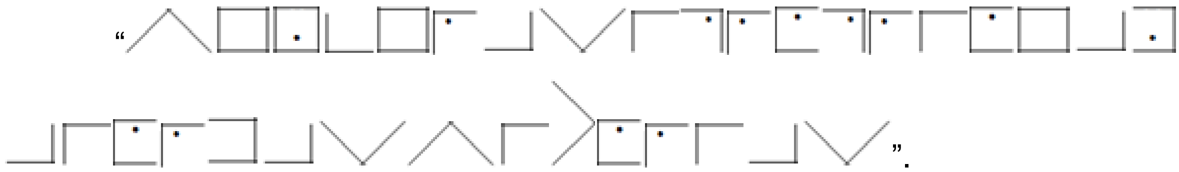
Espera-se que o aluno encontre o valor de cada letra, conforme o padrão utilizado pela Cifra de Chiqueiro, onde ele substituirá a letra do alfabeto normal pela sua posição, de acordo com a figura 24. Assim, espera-se que o aluno encontre, como mensagem cifrada:

“”.

d) Considerando a figura 24, codifique a frase "Vencer a si próprio é a maior das vitórias.", utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

Possível solução dos alunos

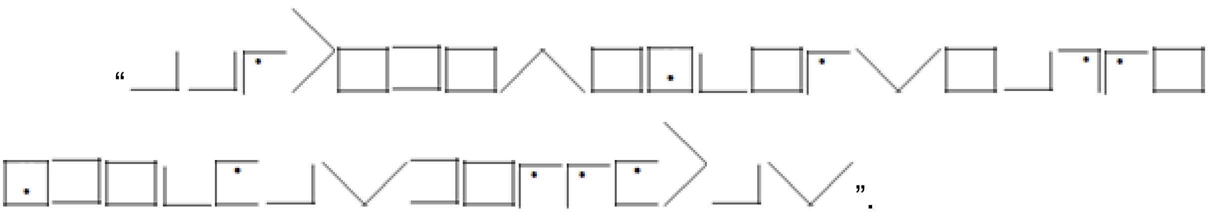
Espera-se que o aluno encontre o valor de cada letra, de acordo com o padrão utilizado pela Cifra de Chiqueiro, onde ele substituirá a letra do alfabeto normal pela sua posição, conforme a figura 24. Assim, espera-se que o aluno encontre, como mensagem cifrada:

“”.

e) Considerando a figura 24, codifique a frase "A arte de vencer se aprende com as derrotas.", utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

Possível solução dos alunos

Espera-se que, nessa atividade, o aluno encontre o valor de cada letra, de acordo com o padrão utilizado pela Cifra de Chiqueiro, onde ele substituirá a letra do alfabeto normal pela sua posição, de acordo com a figura 24. Assim, espera-se que o aluno encontre, como mensagem cifrada:

“”.

Etapa 4

As atividades didáticas envolvendo a Cifra de Playfair têm por objetivo trabalhar com os alunos uma forma de Criptografar que envolve agrupamento de letras.

Atividade 4 – Cifra de Playfair

a) Codifique a mensagem “Podemos escolher o que semear, mas somos obrigados a colher aquilo que plantamos.”, de acordo com a Cifra de Playfair, utilizando o quadro da figura 25.

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

Figura 25: quadro da Cifra de Playfair.

Possível solução dos alunos

Nessa atividade, espera-se que o aluno codifique a mensagem, utilizando corretamente o método utilizado por Playfair, onde ele escreverá a mensagem em dígrafos: Po-de-mo-se-sc-ol-he-ro-qu-es-em-ea-rm-as-so-mo-so-br-ig-ad-os-ac-ol-he-ra-qu-il-oq-eu-pl-an-ta-mo-sx. Como o número de letras é ímpar, coloca-se, ao final, a letra “x”. Agora, utilizando o procedimento de cifragem, tem-se a mensagem codificada “pq-ef-hs-qf-of-pu-kc-us-ob-fq-fk-gb-fs-rt-tr-hs-tp-ra-nd-lg-pt-vg-vp-ck-au-ob-pd-os-bc-wd-gt-zg-hs-qy”.

b) Codifique a mensagem “A escola da experiência é a mais educativa.”, utilizando a Cifra de Playfair.

Possível solução dos alunos

Espera-se que o aluno codifique a mensagem, utilizando corretamente o método utilizado por Playfair, onde ele escreverá a mensagem em dígrafos: Ae-sc-ol-ad-ae-xp-er-iê-nc-ia-éa-ma-is-ed-uc-at-iv-ax. Como o número de letras é ímpar, coloca-se, ao final, a letra “x”. Agora, utilizando o procedimento de cifragem, tem-se a mensagem codificada “bg-oe-pv-lg-bg-wq-fb-kd-hg-nl-gb-nr-pm-fe-ch-gz-wh-zb”.

c) Codifique a mensagem “A amizade é o ingrediente mais importante na receita da vida.”, utilizando a Cifra de Playfair.

Possível solução dos alunos

Espera-se que o aluno codifique a mensagem, utilizando corretamente o método utilizado por Playfair, onde ele escreverá a mensagem em dígrafos: Ax-am-iz-ad-ex-éo-in-gr-ed-ie-nt-em-ai-si-mp-or-ta-nt-em-ar-ec-ei-ta-da-vi-da.

Como aparecem letras repetidas, coloca-se a letra “x”. Agora, utilizando o procedimento de cifragem, tem-se a mensagem codificada “bz-rn-nw-lg-kb-cq-kh-fa-fe-kd-tz-fk-ln-pm-i/js-su-zg-tz-fk-ua-fd-dk-zg-gl-wh-gl”.

d) Codifique a mensagem “Não basta conquistar a sabedoria, é preciso usá-la.”, utilizando a Cifra de Playfair.

Possível solução dos alunos

Espera-se que o aluno codifique a mensagem, utilizando corretamente o método utilizado por Playfair, onde ele escreverá a mensagem em dígrafos: Nã-ob-as-ta-co-nq-ui-st-ar-as-ab-ed-or-ia-ép-re-ci-so-us-ál-ax, como o número de letras é ímpar coloca-se ao final a letra “x”. Agora, utilizando o procedimento de cifragem, tem-se a mensagem codificada “tg-qu-rt-zg-hv-kt-lh-to-ua-rt-ur-fe-su-nl-dq-bf-dh-tp-ro-ub-bz”.

e) Codifique a mensagem “Viver significa lutar.”, utilizando a Cifra de Playfair.

Possível solução dos alunos

Nessa atividade, espera-se que o aluno codifique a mensagem, utilizando corretamente o método de Playfair, onde ele escreverá a mensagem em dígrafos: Vi-ve-rs-ig-ni-fi-ca-lu-ta-rx. Como o número de letras é ímpar, coloca-se, ao final, a letra “x”. Agora, utilizando o procedimento de cifragem, tem-se a mensagem codificada “wh-xc-fy-nd-hk-dm-gu-bl-zg-by”.

Etapa 5

As atividades didáticas envolvendo o Código ISBN têm por objetivo que o estudante resolva atividades envolvendo o conteúdo de aritmética modular e utilize corretamente a fórmula X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$. Esse é um exemplo comum do uso desse tema na vida moderna.

Atividade 5 – Código ISBN

a) Encontre o dígito verificador do código ISBN 852440124-X.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando uma estratégia para resolução.

Informação relevante: ISBN 852440124-X e X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$

Prevendo resultados: espera-se que o aluno aplique corretamente a fórmula e encontre o valor desejado.

X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$

X= [1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9] mod11

X= [1.8 + 2.5 + 3.2 + 4.4 + 5.4 + 6.0 + 7.1 + 8.2 + 9.4] mod11

X= [8 + 10 + 6 + 16 + 20 + 0 + 7 + 16 + 36] mod11

X= 119 mod 11

X= 9

Assim, o dígito verificador é 9.

b) Encontre o dígito verificador do código ISBN 852130206-X.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando uma estratégia para resolução.

Informação relevante: 852130206-X e X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$

Prevendo resultados: espera-se que o aluno aplique corretamente a fórmula e encontre o valor desejado.

X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$

X= $[1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9]$ mod11

X= [1.8 + 2.5 + 3.2 + 4.1 + 5.3 + 6.0 + 7.2 + 8.0 + 9.6] mod11

X= [8 + 10 + 6 + 4 + 15 + 0 + 14 + 0 + 54] mod11

X= 111 mod 11

X= 1

Assim, o dígito verificador é 1.

c) Encontre o dígito verificador do código ISBN 852130399-X.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando uma estratégia para resolução.

Informação relevante: ISBN 852130399-X e X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$

Prevendo resultados: espera-se que o aluno aplique corretamente a fórmula e encontre o valor desejado.

X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$

X= $[1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9]$ mod11

X= [1.8 + 2.5 + 3.2 + 4.1 + 5.3 + 6.0 + 7.3 + 8.9 + 9.9] mod11

X= [8 + 10 + 6 + 4 + 15 + 0 + 21 + 72 + 81] mod11

X= 217 mod 11

X= 8

Assim, o dígito verificador é 8.

d) Encontre o dígito verificador do código ISBN 852790248-X.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando uma estratégia para resolução.

Informação relevante: ISBN 852790248-X e X= $\left[\sum_{i=1}^{9} i(a_i)\right] \bmod 11$

Prevendo resultados: espera-se que o aluno aplique corretamente a fórmula e encontre o valor desejado.

X= $\left[\sum_{i=1}^{9} i(a_i)\right] \mod 11$

X= [1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9] mod11

X= [1.8 + 2.5 + 3.2 + 4.7 + 5.9 + 6.0 + 7.2 + 8.4 + 9.8] mod11

X= [8 + 10 + 6 + 28 + 45 + 0 + 14 + 32 + 72] mod11

X= 215 mod 11

X= 6

Assim, o dígito verificador é 6.

e) Encontre o dígito verificador do código ISBN 852410553-X.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando uma estratégia para resolução.

Informação relevante: ISBN 852410553-X e X= $\left[\sum_{i=1}^{9} i(a_i)\right] \mod 11$

Prevendo resultados: espera-se que o aluno aplique corretamente a fórmula e encontre o valor desejado.

X= $\left[\sum_{i=1}^{9} i(a_i)\right] \mod 11$

X= [1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9] mod11

X= [1.8 + 2.5 + 3.2 + 4.4 + 5.1 + 6.0 + 7.5 + 8.5 + 9.3] mod11

X= [8 + 10 + 6 + 16 + 5 + 0 + 35 + 40 + 27] mod11

X= 147 mod 11

X= 4

Assim, o dígito verificador é 4.

f) Encontre o dígito verificador do código ISBN 858756413-X.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando uma estratégia para resolução.

Informação relevante: ISBN 858756413-X e X= $\left[\sum_{i=1}^{9} i(a_i)\right] \mod 11$

Prevendo resultados: espera-se que o aluno aplique corretamente a fórmula e encontre o valor desejado.

X= $\left[\sum_{i=1}^{9} i(a_i)\right] \text{mod} 11$

X= [$1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9$] mod11

X= [1.8 + 2.5 + 3.8 + 4.7 + 5.5 + 6.6 + 7.4 + 8.1 + 9.3] mod11

X= [8 + 10 + 24 + 28 + 25 + 36 + 28 + 8 + 27] mod11

X= 194 mod 11

X= 7

Assim, o dígito verificador é 7.

Etapa 6

As atividades didáticas envolvendo Código com Função Linear têm por objetivo revisar e reforçar o conceito de função, imagem da função, cálculo de função inversa, permitindo que o aluno amplie seus conhecimentos referentes a esses conteúdos já estudados no Ensino Médio.

Atividade 6 – Código com função linear

a) Considere a figura 26 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26 e codifique a mensagem “A vida é bela.”, utilizando o Código com Função Linear, sabendo que a função codificadora é *f(x)* = 5x + 1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figura 26: quadro do valor numérico de cada letra.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f*(x) = 5x + 1

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 1 – 22 – 9 – 4 – 1 – 5 – 2 – 5 – 12 – 1.

Cálculo da imagem de cada algarismo da sequência:

f(1) = 5.1 + 1 = 6 *f(22)* = 5.22 + 1 = 111 *f(9)* = 5.9 + 1 = 46 *f(4)* = 5.4 + 1 = 21 *f(5)* = 5.5 + 1 = 26 *f(2)* = 5.2 + 1= 11

f(12) = 5.12 + 1 = 61

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 5 x 1 + 1 e tecle *enter*, obtendo 6. Para os demais algarismos, espera-se que eles utilizem as teclas de cursor , para se mover pelo visor e a tecla "*clear*" , para apagar o algarismo que desejam modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 6 – 111 – 46 – 21 – 6 – 26 – 11 – 26 – 61 – 6

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de *f(x)* = 5x + 1 é:

f(x) = 5x + 1

f(x) -1 = 5x

$$\frac{f(x)-1}{5} = x$$

Logo, a função inversa corresponde a $f^{-1}(x) = \frac{x-1}{5}$.

b) Considere a figura 26 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26 e codifique a mensagem "O segredo não é correr atrás das borboletas. E sim cuidar do jardim para que elas venham até você.", utilizando o Código com Função Linear, sabendo que a função codificadora é *f(x)* = 6x + 5.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = 6x + 5

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra.

A sequência numérica do texto é: 15 – 19 – 5 – 7 – 18 – 5 – 4 – 15 – 14 – 1 – 15 – 5 – 3 – 15 – 18 – 18 – 5 – 18 – 1 – 20 – 18 – 1 – 19 – 4 – 1 – 19 – 2 – 15 – 18

– 2 – 15 – 12 – 5 – 20 – 1 – 19 – 5 – 19 – 9 – 13 – 3 – 21 – 9 -4 – 1 – 18 – 4 – 15 – 10 – 1 – 18 – 9 – 13 – 16 – 1 – 18 – 1 – 17 – 21 – 5 – 5 – 12 – 1 – 19 – 22 – 5 – 14 – 8 – 1 – 13 – 1 – 20 – 5 – 22 – 15 – 3 – 5

Cálculo da imagem de cada algarismo da sequência:

f(15) = 6.15 + 5 = 95	*f(19)* = 6.19 + 5 = 119	*f(5)* = 6.5 + 5 = 35
f(7) = 6.7 + 5 = 47	*f(18)* = 6.18 + 5 = 113	*f(4)* = 6.4 + 5 = 29
f(14) = 6.14 + 5 = 89	*f(1)* = 6.1 + 5 = 11	*f(3)* = 6.3 + 5 = 23
f(20) = 6.20 + 5 =125	*f(2)* = 6.2 + 5 = 17	*f(12)* = 6.12 + 5 = 77
f(9) = 6.9 + 5 = 59	*f(13)* = 6.13 + 5 = 83	*f(21)* = 6.21 + 5 = 131
f(10) = 6.10 + 5 = 65	*f(16)* = 6.16 + 5 = 101	*f(17)* = 6.17 + 5 = 107
f(22) = 6.22 + 5 = 137	*f(8)* = 6.8 + 5 = 53	

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 95 – 119 – 35 – 47 – 113 – 35 – 29 – 95 – 89 – 11 – 95 – 35 – 23 – 95 – 113 – 113 – 35 – 113 – 11 – 125 – 113 – 11 – 119 – 29 – 11 – 119 – 17 – 95 – 113 – 17 – 95 – 77 – 35 – 125 – 11 – 119 – 35 – 119 – 59 – 83 – 23 – 131 – 59 – 29 – 11 – 113 – 29 – 95 – 65 – 11 – 113 – 59 – 83 – 101 – 11 – 113 – 11 – 107 – 131 – 35 – 35 – 77 – 11 – 119 – 137 – 35 – 89 – 53 – 11 – 83 – 11 – 125 – 35 – 137 – 95 – 23 – 35.

Verificação das hipóteses: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de *f(x)* = 6x + 5 é:

f(x) = 6x + 5

f(x) - 5 = 6x

$$\frac{f(x)-5}{6} = x$$

Logo, a função inversa corresponde a $f^{-1}(x) = \frac{x-5}{6}$.

c) Considere a tabela da figura 26 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26 e, sabendo que a função cifradora é f(x) = - 3x + 7, decodifique a mensagem “-38 / 1/ -38 /-32 /-2 /-38 /-32 / 1 / 4/ -53/ -8/ -8 /4/ -44/ -56/

-8/ -29/ -8/ -44/ -56/ -8/ -8/ -53/ -47/ -5/ -59/ 4/ -5/ -38/ -8/ -32/ -35/ -38/ -32/ -8/ -5/ -38/ -50/ -35/ -38/ -50/ -50/ -38/ -50/ -50/ -38/ -35/ -17/ -38/ -50.”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = - 3x + 7

Prevendo resultados: espera-se que o aluno realize o cálculo da função inversa e calcule a imagem para cada valor da mensagem cifrada.

A função inversa de *f(x)* = - 3x + 7 é:

f(x) = - 3x + 7

f(x) – 7 = - 3x

$$\frac{f(x)-7}{-3}=x$$

A função inversa corresponde a $f^{-1}(x)=\frac{-x+7}{3}$.

Cálculo da imagem de cada algarismo da sequência:

$f(-38)^{-1}=\frac{38+7}{3}=15$ $f(-8)^{-1}=\frac{8+7}{3}=5$ $f(-5)^{-1}=\frac{5+7}{3}=4$

$f(1)^{-1}=\frac{-1+7}{3}=2$ $f(-44)^{-1}=\frac{44+7}{3}=17$ $f(-59)^{-1}=\frac{59+7}{3}=22$

$f(-32)^{-1}=\frac{32+7}{3}=13$ $f(-56)^{-1}=\frac{56+7}{3}=21$ $f(-35)^{-1}=\frac{35+7}{3}=14$

$f(-2)^{-1}=\frac{2+7}{3}=3$ $f(-29)^{-1}=\frac{29+7}{3}=12$ $f(-50)^{-1}=\frac{50+7}{3}=19$

$f(4)^{-1}=\frac{-4+7}{3}=1$ $f(-47)^{-1}=\frac{47+7}{3}=18$ $f(-17)^{-1}=\frac{17+7}{3}=8$

$f(-53)^{-1}=\frac{53+7}{3}=20$

Assim, o aluno encontrará como sequência numérica decodificada: 15 – 2 – 15 – 13 – 3 – 15 – 13 – 2 – 1 – 20 – 5 – 5 – 1 – 17 – 21 – 5 – 12 – 5 – 17 – 21 – 5 – 5 20 – 18 – 1 – 22 – 1 – 4 – 15 – 5 – 13 – 14 – 15 – 13 – 5 – 4 – 15 – 19 – 14 – 15 – 19 – 19 – 15 – 19 – 19 – 15 – 14 – 8 – 15 – 19.

Substituindo os algarismos pelas letras correspondentes, de acordo com a figura 26, tem-se que a mensagem é “O bom combate é aquele que é travado em nome dos nossos sonhos.”.

d) Considere a tabela da figura 26 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26 e, utilizando a função cifradora $f(x)=\frac{5x+28}{4}$. Codifique a mensagem “Se você não pode controlar o vento, ajuste as velas.”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x)=\frac{5x+28}{4}$

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 19 – 5 – 22 – 15 – 3 – 5 – 14 – 1 – 15 – 16 –1 5 – 4 – 5 – 3 – 15 – 14 – 20 – 18 – 15 – 12 – 1 – 18 – 15 – 22 – 5 – 14 – 20 – 15 – 1 – 10 – 21 – 19 – 20 – 5 – 1 – 19 – 22 – 5 – 12 – 1 – 19.

Cálculo da imagem de cada algarismo da sequência:

$f(19)=\frac{5.19+28}{4}=30{,}75$ $f(20)=\frac{5.20+28}{4}=32$ $f(21)=\frac{5.21+28}{4}=33{,}25$

$f(5)=\frac{5.5+28}{4}=13{,}25$ $f(18)=\frac{5.18+28}{4}=29{,}50$ $f(4)=\frac{5.4+28}{4}=12$

$f(15)=\frac{5.15+28}{4}=25{,}75$ $f(12)=\frac{5.12+28}{4}=22$ $f(10)=\frac{5.10+28}{4}=19{,}5$

$f(3)=\frac{5.3+28}{4}=10{,}75$ $f(1)=\frac{5.1+28}{4}=8{,}25$ $f(22)=\frac{5.22+28}{4}=34{,}50$

$f(14)=\frac{5.14+28}{4}=24{,}50$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite (5 x 19 + 28) ÷ 4 e tecle *enter*, obtendo 30,75. Para os demais algarismos, espera-se que eles utilizem a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que desejam modificar, com isso, modificando apenas a variável *x*. Nessa atividade, é importante que o professor saliente a importância da utilização dos parênteses, pois pode alterar o resultado.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 30,75 – 13,25 – 34,5 – 25,75 – 10,75 – 13,25 – 24,5 – 8,25 – 25,75 – 27 – 25,75 – 12– 13,25 – 10,75 – 25,75 – 24,5 – 32 – 29,5 – 25,75 – 22 – 8,25 – 29,5 – 25,75 – 34,5 – 13,25 – 24,5 – 32 – 25,75 – 8,25 – 19,5 – 33,25 – 30,75 – 32 – 13,25 – 8,25 – 30,75 – 34,5 – 13,25 – 22 – 8,25 – 30,75.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = \frac{5x+28}{4}$ é:

$$f(x) = \frac{5x+28}{4}$$

$$4f(x) = 5x+28$$

$$4f(x) - 28 = 5x$$

$$\frac{4f(x)-28}{5} = x$$

A função inversa corresponde a $f^{-1}(x) = \frac{4x-28}{5}$.

e) Considere a tabela da figura 26 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26. Utilizando a função cifradora f(x) = 2x - 7, codifique a mensagem “Sonhe com a vida, mas não perca a vida por um sonho.”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f*(x) = 2x – 7

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 19 – 15 – 14 – 8 – 5 – 3 – 15 – 13 – 1 – 22 – 9 – 4 – 1 – 13 – 1 – 19 – 14 – 1 – 15 – 16 – 5 – 18 – 3 – 1 – 1 – 22 – 9 – 4 – 1 – 16 – 15 – 18 – 21 – 13 – 19 – 15 – 14 – 8 – 15.

Cálculo da imagem de cada algarismo da sequência:

f(19) = 2.19 – 7 = 31　　*f(8)* = 2.8 – 7 = 9　　*f(13)* = 2.13 – 7 = 19 *f(15)* = 2.15 – 7 = 23 *f(5)* = 2.5 – 7 = 3 *f(1)* = 2.1 – 7 = -5

f(14) = 2.14 – 7 = 21 *f(3)* = 2.3 – 7 = -1 *f(22)* = 2.22 – 7 = 37

f(9) = 2.9 – 7 = 11 *f(18)* = 2.18 – 7 = 29 *f(4)* = 2.4 – 7 = 1

f(16) = 2.16 – 7 = 25 *f(21)* = 2.21 – 7 = 35

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 2 x 19 – 7 e tecle *enter*, obtendo 31. Para os demais algarismos, espera-se que ele utilize a tecla cursor , para se mover pelo visor e a tecla *clear* , para apagar o algarismo que desejam modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 31/ 23/ 21/ 9/ 3/ -1/ 23/ 19/ -5/ 37/ 11/ 1/ -5/ 19/ -5/ 31/ 21/ -5/ 23/ 25/ 3/ 29/ -1/ -5/ -5/ 37/ 11/ 1/ -5/ 25/ 23/ 29/ 35/ 19/ 31/ 23/ 21/ 9/ 23.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de *f(x)* = 2x – 7 é:

f(x) = 2x – 7

f(x) + 7 = 2x

$$\frac{f(x)+7}{2} = x$$

Logo, a função inversa corresponde a $f^{-1}(x) = \frac{x+7}{2}$.

f) Considere a tabela da figura 26 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26 e, sabendo que a função cifradora f(x) = 3x + 4, decodifique a mensagem “ 61/ 19/ 46/ 7/ 49/ 52/ 67/ 16/ 19/ 58/ 61/ 19/ 16/ 19/ 61/ 64/ 7/ 13/ 7/ 58/ 52/ 19/ 40/ 49/ 64/ 7/ 40/ 19/ 46/ 64/ 49/ 70/ 19/ 46/ 13/ 7/ 52/ 19/ 40/ 49/ 19/ 61/ 22/ 49/ 58/ 13/ 49 ”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = 3x + 4

Prevendo resultados: espera-se que o estudante realize o cálculo da função inversa e calcule a imagem para cada valor da mensagem cifrada.

A função inversa de *f(x)* = 3x + 4 é:

f(x) = 3x + 4

f(x) – 4 = 3x

$$\frac{f(x)-4}{3}=x$$

A função inversa corresponde a $f^{-1}(x)=\frac{x-4}{3}$.

Cálculo da imagem de cada algarismo da sequência:

$$f^{-1}(61)=\frac{61-4}{3}=19 \qquad f^{-1}(19)=\frac{19-4}{3}=5 \qquad f^{-1}(46)=\frac{46-4}{3}=14$$

$$f^{-1}(7)=\frac{7-4}{3}=1 \qquad f^{-1}(49)=\frac{49-4}{3}=15 \qquad f^{-1}(52)=\frac{52-4}{3}=16$$

$$f^{-1}(67)=\frac{67-4}{3}=21 \qquad f^{-1}(16)=\frac{16-4}{3}=4 \qquad f^{-1}(58)=\frac{58-4}{3}=18$$

$$f^{-1}(64)=\frac{64-4}{3}=20 \qquad f^{-1}(40)=\frac{40-4}{3}=12 \qquad f^{-1}(70)=\frac{70-4}{3}=22$$

$$f^{-1}(13)=\frac{13-4}{3}=3 \qquad f^{-1}(22)=\frac{22-4}{3}=6$$

Assim, o aluno encontrará como sequência numérica descriptografada: 19 – 5 – 14 – 1 – 15 – 16 – 21 – 4 – 5 – 18 – 19 – 5 – 4 – 5 – 19 – 20 – 1 – 3 – 1 – 18 – 16 – 5 – 12 – 15 – 20 – 1 – 12 – 5 – 14 – 20 – 15 – 22 – 5 – 14 – 3 – 1 – 16 – 5 – 12 – 15 – 5 – 19 – 6 – 15 – 18 – 3 – 15.

Substituindo os algarismos pelas letras correspondentes, de acordo com a figura 26, tem-se que a mensagem é “Senão puder se destacar pelo talento, vença pelo esforço.”.

Etapa 7

As atividades didáticas envolvendo Código com Função Quadrática têm por objetivo revisar e reforçar o conceito de função, imagem da função, cálculo de função inversa, permitindo que o aluno amplie seus conhecimentos referentes a esses conteúdos já estudados no Ensino Médio.

Atividade 7 – Código com Função Quadrática

a) Considere a figura 27 e codifique a palavra “O livro é uma caixa mágica.”, utilizando o Código com Função Quadrática, sabendo que a função codificadora é $f(x) = x^2 + 2x + 6$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figura 27: quadro do valor numérico de cada letra.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x) = x^2 + 2x + 6$.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 15 – 12 – 9 – 22 – 18 – 15 – 5 – 21 – 13 – 1 – 3 – 1 – 9 – 24 – 1 – 13 – 1 – 7 – 9 – 3 – 1.

Cálculo da imagem de cada algarismo da sequência:

$f(15) = 15^2 + 2.15 + 6 = 261$ $\quad$ $f(18) = 18^2 + 2.18 + 6 = 366$

$f(12) = 12^2 + 2.12 + 6 = 174$ $\quad$ $f(9) = 9^2 + 2.9 + 6 = 105$

$f(5) = 5^2 + 2.5 + 6 = 41$ $\quad$ $f(1) = 1^2 + 2.1 + 6 = 9$

$f(3) = 3^2 + 2.3 + 6 = 21$ $\quad$ $f(21) = 21^2 + 2.21 + 6 = 489$

$f(24) = 24^2 + 2.24 + 6 = 630$ $\quad$ $f(13) = 13^2 + 2.13 + 6 = 201$

$f(22) = 22^2 + 2.22 + 6 = 534$ $\quad$ $f(7) = 7^2 + 2.7 + 6 = 69$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 15 ^ 2 + 30 + 6 e tecle enter, obtendo 261. Para os demais algarismos, espera-se que ele utilize a tecla cursor 

para se mover pelo visor e a tecla

clear , para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 261 – 174 – 105 – 534 – 366 – 261 – 41 – 489 – 201 – 9 – 21 – 9 – 105 – 630 – 9 – 201 – 9 – 69 – 105 – 21 – 9.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = x^2 + 2x + 6$ é:

$x^2 + 2x + 6 - y = 0$

$\Delta = b^2 - 4ac$

$\Delta = 2^2 - 4.1.(6 - y)$

$\Delta = 4 - 24 + 4y$

$\Delta = -20 + 4y$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-2 \pm \sqrt{-20 + 4y}}{2.1}$$

$$x = \frac{-2 \pm 2\sqrt{-5 + y}}{2}$$

$$x = -1 \pm \sqrt{-5 + y}$$

Logo, a função inversa corresponde a $f^{-1}(x) = -1 + \sqrt{-5 + x}$.

b) Codifique a mensagem "O maravilhoso da fantasia é nossa capacidade de torná-la realidade.", utilizando a função chave: $f(x) = x^2 + x + 1$.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x) = x^2 + x + 1$.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 15 – 13 – 1 – 18 – 1 – 22 – 9 – 12 – 8 – 15 – 19 – 15 – 4 – 1 – 6 – 1 – 14 – 20 – 1 – 19 – 9 – 1 – 5 – 14 – 15 – 19 – 19 – 1 – 3 – 1 – 16 – 1 – 3 – 9 – 4 – 1 – 4 – 5 – 4 – 5 – 20 – 15 – 18 – 14 – 1 – 12 – 1 – 18 – 5 – 1 – 12 – 9 – 4 – 1 – 4 – 5.

Cálculo da imagem de cada algarismo da sequência:

f(15) $=15^2 + 15 + 1 = 241$ *f(18)* $=18^2 + 18 + 1 = 343$ *f(12)* $=12^2 + 12 + 1 = 157$

f(13) $=13^2 + 13 + 1 = 183$ *f(22)* $=22^2 + 22 + 1 = 507$ *f(8)* $=8^2 + 8 + 1 = 73$

f(1) $=1^2 + 1 + 1 = 3$ *f(9)* $=9^2 + 9 + 1 = 91$ *f(19)* $=19^2 + 19 + 1 = 381$

f(14) $=14^2 + 14 + 1 = 211$ *f(6)* $=6^2 + 6 + 1 = 43$ *f(4)* $= 4^2 + 4 + 1 = 21$

f(20) $=20^2 + 20 + 1 = 421$ *f(5)* $=5^2 + 5 + 1 = 31$ *f(3)* $=3^2 + 3 + 1 = 13$

f(16) $= 16^2 + 16 + 1 = 273$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 15 ^ 2 + 15 + 1 e tecle *enter*, obtendo 241. Para os demais algarismos, espera-se que eles utilizem a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que desejam modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 241 – 183 – 3 – 343 – 3 – 507 – 91 – 157 – 73 – 241 – 381 – 241 – 21 – 3 – 43 – 3 – 211 – 421 – 3 – 381 – 91 – 3 – 31 – 211 – 241 – 381 – 381 – 3 – 13 – 3 – 273 – 3 – 13 – 91 – 21 – 3 – 21 – 31 – 21 – 31 – 421 – 241 – 343 – 211 – 3 – 157 – 3 – 343 – 31 – 3 – 157 – 91 – 21 – 3 – 21 – 31.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = x^2 + x + 1$ é:

$x^2 + x + 1 – y = 0$

$\Delta = b^2 – 4ac$

$\Delta = 1^2 – 4.1. (1 – y)$

$\Delta = 1 – 4 + 4y$

$\Delta = – 3 + 4y$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-1 \pm \sqrt{-3 + 4y}}{2.1}$$

$$x = \frac{-1 \pm \sqrt{-3 + 4y}}{2}$$

Logo, a função inversa corresponde a $f^{-1}(x) = \dfrac{-1 \pm \sqrt{-3 + 4y}}{2}$.

c) Codifique a mensagem "Cultivar alegria custa menos que a tristeza e traz melhores resultados!.", utilizando a função chave: f(x) = x^2 + 4x + 4.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = x^2 + 4x + 4.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 3 – 21 – 12 – 20 – 9 – 22 – 1 – 18 – 1 – 12 – 5 – 7 – 18 – 9 – 1 – 3 – 21 – 19 – 20 – 1 – 13 – 5 – 14 – 15 – 19 – 17 – 21 – 5 – 1 – 20 – 18 – 9 – 1 – 3 – 21 – 19 – 20 – 1 – 13 – 5 – 14 – 15 – 19 – 17 – 21 – 5 – 1 – 20 – 18 – 9 – 19 – 20 – 5 – 26 – 1 – 5 – 20 – 18 – 1 – 26 – 13 – 5 – 12 – 8 – 15 – 18 – 5 – 19 – 18 – 5 – 19 – 21 – 12 – 20 – 1 – 4 – 15 – 19.

Cálculo da imagem de cada algarismo da sequência:

f(3) =3^2 + 4.3 + 4 = 25	*f(1)* =1^2 + 4.1 + 4 = 9
f(14) =14^2 + 4.14 + 4 = 256	*f(21)* =21^2 + 4.21 + 4 = 529
f(18) =18^2 + 4.18 + 4 = 400	*f(15)* =15^2 + 4.15 + 4 = 289
f(12) =12^2 + 4.12 + 4 = 196	*f(5)* =5^2 + 4.5 + 4 = 49
f(17) =17^2 + 4.17 + 4 = 361	*f(20)* =20^2 + 4.20 + 4 = 484
f(7) =7^2 + 4.7 + 4 = 81	*f(26)* =26^2 + 4.26 + 4 = 784
f(9) =9^2 + 4.9 + 4 = 121	*f(19)* =19^2 + 4.19 + 4 = 441

f(22) $=22^2 + 4.22 + 4 = 576$ *f(8)* $=8^2 + 4.8 + 4 = 100$

f(13) $=13^2 + 4.13 + 4 = 225$ *f(4)* $=4^2 + 4.4 + 4 = 36$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 3 ^ 2 + 12 + 4 e tecle *enter*, obtendo 25. Para os demais algarismos, espera-se que ele utilize a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que desejam modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 25 – 529 – 196 – 484 – 121 – 576 – 9 – 400 – 9 – 196 – 49 – 81 – 400 – 121 – 9 – 25– 529 – 441 – 484 – 9 – 225 – 49 – 256 – 289 – 441 – 361 – 529 – 49 – 9 – 484 – 400 – 121 – 9 – 25 – 529 – 441 – 484 – 9 – 225 – 49 – 256 – 289 – 441 – 361 – 529 – 49 – 9 – 484 – 400 – 121 – 441 – 484 – 49 – 784 – 9 – 49 – 484 – 400 – 9 – 784 – 225 – 49 – 196 – 100 – 289 – 400 – 49 – 441 – 400 – 49 – 441 – 529 – 196 – 484 – 9 – 36 – 289 – 441.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de *f(x)* $= x^2 + 4x + 4$ é:

$x^2 + 4x + 4 - y = 0$

$\Delta = b^2 - 4ac$

$\Delta = 4^2 - 4.1.\ (4 - y)$

$\Delta = 16 - 16 + 4y$

$\Delta = 4y$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-4 \pm \sqrt{4y}}{2.1}$$

$$x = \frac{-4 \pm 2\sqrt{y}}{2}$$

$$x = -2 \pm \sqrt{y}$$

Logo, a função inversa corresponde a $f^{-1}(x) = -2 + \sqrt{x}$.

d) Codifique a mensagem "O mundo mágico dos números.", sabendo que a função codificadora é $f(x) = x^2 + 14x + 49$.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x) = x^2 + 14x + 49$.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo, que corresponde a uma letra, e utilize corretamente a calculadora.

A sequência numérica do texto é: 15 – 13 – 21 – 14 – 4 – 13 – 1 – 7 – 9 – 3 – 15 – 4 – 15 – 19 – 14 – 21 – 13 – 5 – 18 – 15 – 19.

Cálculo da imagem de cada algarismo da sequência:

$f(7) = 7^2 + 14.7 + 49 = 196$

$f(14) = 14^2 + 14.14 + 49 = 441$

$f(21) = 21^2 + 14.21 + 49 = 784$

$f(9) = 9^2 + 14.9 + 49 = 256$

$f(13) = 13^2 + 14.13 + 49 = 400$

$f(15) = 15^2 + 14.15 + 49 = 484$

$f(5) = 5^2 + 14.5 + 49 = 144$

$f(19) = 19^2 + 14.19 + 49 = 676$

$f(1) = 1^2 + 14.1 + 49 = 64$

$f(3) = 3^2 + 14.3 + 49 = 100$

$f(18) = 18^2 + 14.18 + 49 = 625$

$f(4) = 4^2 + 14.4 + 49 = 121$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 15 ^ 2 + 210 + 49 e tecle *enter*, obtendo 484. Para os demais algarismos, espera-se que eles utilizem a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 484 – 400 – 784 – 441 – 121 – 400 – 64 – 196 – 256 – 100 – 484 – 121 – 484 – 676 – 441 – 784 – 400 – 144 – 625 – 484 – 676.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de *f(x)* = x^2 + 14x + 49 é:

x^2 + 14x + 49 – y = 0

$\Delta = b^2 - 4ac$

$\Delta = 14^2 - 4.1.(49 - y)$

$\Delta = 196 - 196 + 4y$

$\Delta = 4y$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-14 \pm \sqrt{4y}}{2.1}$$

$$x = \frac{-14 \pm 2\sqrt{y}}{2}$$

$$x = -7 \pm \sqrt{y}$$

Logo, a função inversa corresponde a $f^{-1}(x) = -7 + \sqrt{x}$.

e) Decodifique a mensagem “211/ 343/ 183/ 421/ 157/ 21/ 307/ 211/ 343/ 13/ 211/ 157/ 73/ 183/ 1/ 157/ 211/ 157/ 421/ 183/ 13/ 211”, sabendo que a função cifradora é *f(x)* = x^2 - x + 1.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = x^2 – x + 1

Prevendo resultados: espera-se que o aluno realize o cálculo da função inversa e calcule a imagem para cada valor da mensagem cifrada.

A função inversa de *f(x)* = x^2 – x + 1 é:

f(x) = x^2 – x + 1

x^2 – x + 1 – y = 0

$\Delta = b^2 - 4ac$

$\Delta = (-1)^2 - 4.1.(1 - y)$

$\Delta = 1 - 4 + 4y$

$\Delta = -3 + 4y$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{1 \pm \sqrt{-3+4y}}{2.1}$$

$$x = \frac{1 \pm \sqrt{-3+4y}}{2}$$

A função inversa corresponde a $f^{-1}(x) = \dfrac{1+\sqrt{-3+4x}}{2}$.

Cálculo da imagem de cada algarismo da sequência:

$$f^{-1}(211) = \frac{1+\sqrt{-3+4.211}}{2} = 15 \qquad f^{-1}(183) = \frac{1+\sqrt{-3+4.183} = 14}{2}$$

$$f^{-1}(343) = \frac{1+\sqrt{-3+4.343}}{2} = 19 \qquad f^{-1}(421) = \frac{1+\sqrt{-3+4.421}}{2} = 21$$

$$f^{-1}(307) = \frac{1+\sqrt{-3+4.307}}{2} = 18 \qquad f^{-1}(13) = \frac{1+\sqrt{-3+4.13}}{2} = 4$$

$$f^{-1}(1) = \frac{1+\sqrt{-3+4.1}}{2} = 1 \qquad f^{-1}(157) = \frac{1+\sqrt{-3+4.157}}{2} = 13$$

$$f^{-1}(21) = \frac{1+\sqrt{-3+4.21}}{2} = 5 \qquad f^{-1}(73) = \frac{1+\sqrt{-3+4.73}}{2} = 9$$

Assim, o aluno encontrará como sequência numérica decodificada: 15 – 19 – 14 – 21 – 13 – 5 – 18 – 15 – 19 – 4 – 15 – 13- 9 -14 – 1 – 13 – 15 – 13 – 21 – 14 – 4 – 15.

Substituindo os algarismos pelas letras correspondentes, de acordo com a figura 27, tem-se que a mensagem é “Os números dominam o mundo.”.

f) Decodifique a mensagem “5, 509, 93, 23, 5, 33, 9, 33, 159, 5”, sabendo que a função codificadora é *f*(x) = x^2 + x + 3.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = x^2 + x + 3

Prevendo resultados: espera-se que o aluno realize o cálculo da função inversa e calcule a imagem para cada valor da mensagem cifrada.

A função inversa de *f(x)* = x^2 + x + 3 é:

f(x) = x^2 + x + 3

$x^2 + x + 3 – y = 0$

$\Delta = b^2 – 4ac$

$\Delta = (-1)^2 – 4.1. (3 – y)$

$\Delta = 1 – 12 + 4y$

$\Delta = - 11 + 4y$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-1 \pm \sqrt{-11 + 4y}}{2.1}$$

$$x = \frac{-1 \pm \sqrt{-11 + 4y}}{2}$$

A função inversa corresponde a $f^{-1}(x) = \dfrac{-1 + \sqrt{-11 + 4x}}{2}$.

Cálculo da imagem de cada algarismo da sequência:

$$f^{-1}(5) = \frac{-1 + \sqrt{-11 + 4.5}}{2} = 1$$

$$f^{-1}(93) = \frac{-1 + \sqrt{-11 + 4.93} = 9}{2}$$

$$f^{-1}(509) = \frac{-1 + \sqrt{-11 + 4.509}}{2} = 22$$

$$f^{-1}(33) = \frac{-1 + \sqrt{-11 + 4.33}}{2} = 5$$

$$f^{-1}(9) = \frac{-1 + \sqrt{-11 + 4.9}}{2} = 2$$

$$f^{-1}(159) = \frac{-1 + \sqrt{-11 + 4.159}}{2} = 12$$

$$f^{-1}(23) = \frac{-1 + \sqrt{-11 + 4.23}}{2} = 4$$

Assim, o aluno encontrará como sequência numérica decodificada: 1 – 22 – 9 – 4 – 1 – 5 – 2 – 5 – 12 – 1.

Substituindo os algarismos pelas letras correspondentes, de acordo com a figura 27, tem-se que a mensagem é “A vida é bela.”.

Etapa 8

As atividades didáticas envolvendo Código com Função Exponencial e Logarítmica têm por objetivo revisar as propriedades da potenciação, equações exponenciais, cálculo da imagem de uma função, logaritmo mudança de base e utilizar as funções da calculadora, por exemplo, potenciação, fração, dízima periódica, desta forma, procurando revisar os conteúdos já trabalhados e ampliar os conhecimentos dos alunos referentes ao mesmo.

Atividade 8 – Código com função exponencial e logarítmica

a) Codifique e decodifique a palavra "MATEMÁTICA", utilizando a figura 28, sabendo que a função codificadora é $f(x) = 2^x$.

A	B	C/Ç	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figura 28: quadro do valor numérico de cada letra.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x) = f(x) = 2^x$

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 13 – 1 – 20 – 5 – 13 – 1 – 20 – 9 – 3 – 1.

Cálculo da imagem de cada algarismo da sequência:

$f(5) = 2^5 = 32$ $\qquad$ $f(13) = 2^{13} = 8192$

$f(9) = 2^9 = 512$ $\qquad$ $f(1) = 2^1 = 2$

$f(3) = 2^3 = 8$ $\qquad$ $f(20) = 2^{20} = 1048576$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 2 ^ 13 e tecle *enter*, obtendo 8192. Para os demais algarismos, espera-se que ele utilize a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*. Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 8192 – 2 – 1048576 – 32 – 8192 – 2 – 1048576 – 512 – 8 – 2.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = 2^x$ é:

$f(x) = 2^x$

$\log_2 y = x$

A função inversa corresponde a $\log_2 y = x$.

b) Considere a figura 28 e a função cifradora *f(x)* = $2^x.2^1$. Utilize a propriedade ($a^x \,.\, a^y = a^{x+y}$) na função dada e codifique o texto “O Bom combate é aquele que é travado em nome dos nossos Sonhos.”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = $2^x.2^1$.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 15 – 2 – 15 – 13 – 3 – 15 – 13 – 2 – 1 – 20 – 5 – 5 – 1 – 17 – 21 – 5 – 12 – 5 – 17 – 21 – 5 – 5 – 20 – 18 – 1 – 22 – 1 – 4 – 15 – 5 – 13 – 14 – 15 – 13 – 5 – 4 – 15 – 19 – 14 – 15 – 19 – 19 – 15 – 19 – 19 – 15 – 14 – 8 – 15 – 19.

Cálculo da imagem de cada algarismo da sequência:

$f(15) = 2^{15}.2^1 = 2^{15+1} = 65536$	$f(1) = 2^1.2^1 = 2^{2+1} = 4$
$f(21) = 2^{21}.2^1 = 2^{21+1} = 4194304$	$f(2) = 2^2.2^1 = 2^{2+1} = 8$
$f(20) = 2^{20}.2^1 = 2^{20+1} = 2097152$	$f(12) = 2^{12}.2^1 = 2^{12+1} =8192$
$f(13) = 2^{13}.2^1 = 2^{13+1} = 16384$	$f(5) = 2^5.2^1 = 2^{5+1} = 64$
$f(18) = 2^{18}.2^1 = 2^{18+1} =524288$	$f(17) = 2^{17}.2^1 = 2^{17+1} = 262144$
$f(3) = 2^3.2^1 = 2^{3+1} = 16$	$f(22) = 2^{22}.2^1 = 2^{22+1} =8388608$
$f(4) = 2^4.2^1 = 2^{4+1} = 32$	$f(14) = 2^{14}.2^1 = 2^{14+1} = 32768$
$f(19) = 2^{19}.2^1 = 2^{19+1} =1048576$	$f(8) = 2^8.2^1 = 2^{8+1} = 512$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 2 ^ (15 + 1) e tecle *enter*, obtendo 65536. Para os demais algarismos, espera-se que ele utilize a tecla cursor 

, para se mover pelo visor e a tecla

clear , para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 65536 – 8 – 65536 – 16384 – 16 – 65536 – 16384 – 8 – 4 – 2097152 – 64 – 64 – 4 – 262144 – 4194304 – 64 – 8192 – 64 – 262144 – 4194304 – 64 – 64 – 2097152 – 524288 – 4 – 8388608 – 4 – 32 – 65536 – 64 – 16384 – 32768 – 65536 – 16384 – 64 – 32 – 65536 – 1048576 – 32768 – 65536 – 1048576 – 1048576 – 65536 – 1048576 – 1048576 – 65536 – 32768 – 512 – 65536 – 1048576.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = 2^x.2^1$ é:

$f(x) = 2^x.2^1$

$\log_2 y = x + 1$

A função inversa corresponde a $\log_2 y = x + 1$.

c) Considere a figura 28 e a função cifradora $f(x) = \log_2 x$ e codifique a mensagem “Por mais longa que seja a caminhada, o mais importante é dar o primeiro passo.”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x) = \log_2 x$.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 16 – 15 – 18 – 13 – 1 – 9 – 19 – 12 – 15 – 14 – 7 – 1 – 17 – 21 – 5 – 19 – 5 – 10 – 1 – 1 – 3 – 1 – 13 – 9 – 14 – 8 – 1- 4 – 1 – 15 – 13 – 1 – 9 – 19 -9 – 13 – 16 – 15 – 18 – 20 – 1- 14 – 20 – 5 – 5 – 4 – 1 – 18 – 15 – 16 – 18 – 9 – 13 – 5 – 9 – 18 – 15 – 16 – 1 – 19 – 19 – 15.

Cálculo da imagem de cada algarismo da sequência:

$y = \log_2 16 \rightarrow 2^y = 16 \rightarrow y = 4$

$y = \log_2 19 \rightarrow y = \frac{\log 19}{\log 2} \rightarrow y = 4{,}248$

$y = \log_2 15 \rightarrow y = \frac{\log 15}{\log 2} \rightarrow y = 3{,}907$

$y = \log_2 12 \rightarrow y = \frac{\log 12}{\log 2} \rightarrow y = 3{,}585$

$y = \log_2 18 \rightarrow y = \frac{\log 18}{\log 2} \rightarrow y = 4{,}170$

$y = \log_2 14 \rightarrow y = \frac{\log 14}{\log 2} \rightarrow y = 3{,}807$

$y = \log_2 13 \rightarrow y = \frac{\log 13}{\log 2} \rightarrow y = 3{,}700$

$y = \log_2 7 \rightarrow y = \frac{\log 7}{\log 2} \rightarrow y = 2{,}807$

$y = \log_2 1 \rightarrow 2^y = 1 \rightarrow y = 0$

$y = \log_2 17 \rightarrow y = \frac{\log 17}{\log 2} \rightarrow y = 4{,}087$

$y = \log_2 9 \rightarrow y = \frac{\log 9}{\log 2} \rightarrow y = 3{,}170$

$y = \log_2 20 \rightarrow y = \frac{\log 20}{\log 2} \rightarrow y = 4{,}322$

$y = \log_2 5 \rightarrow y = \frac{\log 5}{\log 2} \rightarrow y = 2{,}322$

$y = \log_2 4 \rightarrow 2^y = 4 \rightarrow y = 2$

$y = \log_2 8 \rightarrow 2^y = 8 \rightarrow y = 3$

$y = \log_2 3 \rightarrow y = \frac{\log 3}{\log 2} \rightarrow y = 1{,}585$

$y = \log_2 10 \rightarrow y = \frac{\log 10}{\log 2} \rightarrow y = 3{,}322$

$y = \log_2 21 \rightarrow y = \frac{\log 21}{\log 2} \rightarrow y = 4{,}392$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite log(9) ÷ log(2) e tecle *enter*; arredondando obtém 3,17. Para os demais algarismos, espera-se que ele utilize a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 4 – 3,907 – 4,170 – 3,700 – 0 – 3,170 – 4,248 – 3,585 – 3,907 – 3,807 – 2,807 – 0 – 4,087 – 4,392 – 2,322 – 4,248 – 2,322 – 3,322 – 0 – 0 – 1,585 – 0 – 3,700 – 3,170 – 3,807 – 3 – 0 – 2 – 0 – 3,907 – 3,700 – 0 – 3,170 – 4,248 – 3,170 – 3,700 – 4 – 3,907 – 4,170 – 4,322 – 0 – 3,807 – 4,322 – 2,322 – 2,322 – 2 – 0 – 4,170 – 3,907 – 4 – 4,170 – 3,170 – 3,700 – 2,322 – 3,170 – 4,170 – 3,907 – 4 – 0 – 4,248 – 4,248 – 3,907.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = \log_2 x$ é:

$f(x) = \log_2 x$

$2^y = x$

A função inversa corresponde a $x = 2^y$.

d) Considere a figura 28 e a função cifradora *f(x)* = $2^x{:}2^2$. Utilize a propriedade ($a^x : a^y = a^{x-y}$) na função dada e codifique o texto “1048576/ 8192/ 1024/ 262144/ 0,5/ 65536/ 0,5/ 262144/ 65536/ 0,5/ 131072/ 8/ 2048/ 8/ 1024/ 64/ 8192/ 65536/ 32768/ 524288/ 8/ 16384/ 8/ 65536/ 4/ 8/ 65536/ 131072/ 8/ 4096/ 8192/ 2/ 0,5/ 2048/ 128/ 4096/ 64/ 8192”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = $2^x{:}2^2$

Prevendo resultados: espera-se que o aluno realize o cálculo da função inversa e calcule a imagem para cada valor da mensagem cifrada.

A função inversa de *f(x)* = $2^x{:}2^2$ é:

$f(x) = 2^x{:}2^2$

$f(x) = 2^{x-2}$

$\log_2 y = x - 2$

A função inversa corresponde a $\log_2 y = x - 2$.

Cálculo da imagem de cada algarismo da sequência:

$2^{x-2} = 1048576 \rightarrow x = 22$	$2^{x-2} = 131072 \rightarrow x = 19$
$2^{x-2} = 8192 \rightarrow x = 15$	$2^{x-2} = 8 \rightarrow x = 5$
$2^{x-2} = 1024 \rightarrow x = 12$	$2^{x-2} = 2048 \rightarrow x = 13$
$2^{x-2} = 262144 \rightarrow x = 20$	$2^{x-2} = 32768 \rightarrow x = 17$
$2^{x-2} = 0{,}5 \rightarrow x = 1$	$2^{x-2} = 524288 \rightarrow x = 21$
$2^{x-2} = 65536 \rightarrow x = 18$	

Assim, o aluno encontrará como sequência numérica descriptografada: 22 – 15 – 12 – 20 – 1- 18 – 1 – 20 – 18 – 1 – 19 – 5 – 13 – 5 – 12 – 8 – 15 – 18 – 17 – 21 – 5 – 16 – 5 – 18 – 4 – 5 – 18 – 19 – 5 – 14 – 15 – 3 – 1 – 13 – 9 – 14 – 8 – 15.

Substituindo os algarismos pelas letras correspondentes, de acordo com a figura 28, tem-se que a mensagem é "Voltar atrás é melhor que perder-se no caminho.".

e) Considere a figura 28 e a função cifradora $f(x) = \left(2^x\right)^{\frac{1}{2}}$. Utilize a propriedade $((a^x)^y = a^{xy})$ na função dada e codifique o texto "A morte do homem começa no instante que ele desiste de aprender.".

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x) = \left(2^x\right)^{\frac{1}{2}}$.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 1 – 13 – 15 – 18 – 20 – 5- 4 – 15 – 8 – 15 – 13 – 5- 13 – 3 – 15 – 13 – 5 – 3 – 1 – 14 – 15 – 9 – 14 – 19 – 20 – 1 – 14 – 20 – 5- 17 – 21 – 5 – 5 – 12 – 5- 4 – 5 – 19 – 9- 19 – 20 – 5 – 4 – 5 – 1 – 16 – 18 – 5 – 14 – 4 – 5 – 18.

Cálculo da imagem de cada algarismo da sequência:

$f(1) = 2^{\frac{1}{2}} = 1{,}41$ $\qquad$ $f(3) = 2^{\frac{3}{2}} = 2{,}83$

$f(13) = 2^{\frac{13}{2}} = 90{,}51$ $\qquad$ $f(14) = 2^{\frac{14}{2}} = 128$

$f(15) = 2^{\frac{15}{2}} = 181{,}02$ $\qquad$ $f(9) = 2^{\frac{9}{2}} = 22{,}63$

$f(18) = 2^{\frac{18}{2}} = 512$ $\qquad$ $f(19) = 2^{\frac{19}{2}} = 724{,}08$

$f(20) = 2^{\frac{20}{2}} = 1024$ $\qquad$ $f(17) = 2^{\frac{17}{2}} = 362{,}04$

$f(5) = 2^{\frac{5}{2}} = 5{,}66$ $\qquad$ $f(21) = 2^{\frac{21}{2}} = 1448{,}15$

$f(4) = 2^{\frac{4}{2}} = 4$ $\qquad$ $f(12) = 2^{\frac{12}{2}} = 64$

$f(8) = 2^{\frac{8}{2}} = 16$ $\qquad$ $f(16) = 2^{\frac{16}{2}} = 256$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 2 ^ (1 ÷ 2) e tecle *enter*, obtendo 1,41. Para os demais algarismos, espera-se que utilize a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 1,41 – 90,51 – 181,02 – 512 – 1024 – 5,66 – 4 – 181,02 – 16 – 181,02 – 90,51 – 5,66 – 90,51 – 2,83 – 181,02 – 90,51 – 5,66 – 2,83 – 1,41 – 128 – 181,02 – 22,63 – 128 – 724,08 – 1024 – 1,41 – 128 – 1024 – 5,66 – 362,04 – 1448,15 – 5,66 – 5,66 – 64 – 5,66 – 4 – 5,66 – 724,08 – 22,63 – 724,08 – 1024 – 5,66 – 4 – 5,66 – 1,41 – 256 – 512 – 5,66 – 128 – 4 – 5,66 – 512.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = \left(2^x\right)^{\frac{1}{2}}$ é:

$$f(x) = \left(2^x\right)^{\frac{1}{2}}$$

$$\log_2 y = \frac{x}{2}$$

A função inversa corresponde a $\log_2 y = \frac{x}{2}$.

f) Considere a figura x e a função cifradora *f(x)* = $3^x.3^1$. Utilize a propriedade ($a^x \cdot a^y = a^{x+y}$) na função dada e codifique o texto “É muito fácil ser pedra, o difícil é ser vidraça.”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e *f(x)* = $3^x.3^1$.

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 5 – 13 – 21 – 9 – 20 – 15 – 6 – 1 – 3 – 9 – 12 – 19 – 5 – 18 – 16 – 5 – 4 – 18 – 1 – 15 – 4 – 9 – 6 – 9 – 3 – 9 – 12 – 5 – 19 – 5 – 18 – 22 – 9 – 4 – 18 – 1 – 3 – 1.

Cálculo da imagem de cada algarismo da sequência:

$f(5) = 3^5.3^1 = 3^{5+1} =81$

$f(20) = 3^{20}.3^1 = 3^{20+1} = 10460353203$

$f(13) = 3^{13}.3^1 = 3^{13+1} = 4782969$

$f(15) = 3^{15}.3^1 = 3^{15+1} = 43046721$

$f(21) = 3^{21}.3^1 = 3^{21+1} = 31381059609$

$f(6) = 3^6.3^1 = 3^{6+1} = 2187$

$f(9) = 3^9.3^1 = 3^{9+1} = 59049$

$f(1) = 3^1.3^1 = 3^{1+1} = 9$

$f(22) = 3^{22}.3^1 = 3^{22+1} = 94143178827$

$f(4) = 3^4.3^1 = 3^{4+1} = 243$

$f(3) = 3^3.3^1 = 3^{3+1} = 81$

$f(12) = 3^{12}.3^1 = 3^{12+1} = 1594323$

$f(19) = 3^{19}.3^1 = 3^{19+1} = 3486784401$

$f(18) = 3^{18}.3^1 = 3^{18+1} = 1162261467$

$f(16) = 3^{16}.3^1 = 3^{16+1} = 129140163$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 3 ^ (5 + 1) e tecle *enter*, obtendo 729. Para os demais algarismos, espera-se que ele utilize a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 729 – 4782969 – 31381059609 – 59049 – 10460353203 – 43046721 – 2187 – 9 – 81 – 59049 – 1594323 – 3486784401 – 729 – 1162261467 – 129140163 – 729 – 243 – 1162261467 – 9 – 43046721 – 243 – 59049 – 2187 – 59049 – 81 – 59049 – 1594323 – 81 – 3486784401 – 729 – 1162261467 – 94143178827 – 59049 – 243 – 1162261467 – 9 – 81 – 9.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = 3^x.3^1$ é:

$f(x) = 3^x.3^1$

$f(x) = 3^{x + 1}$

$\log_3 y = x + 1$

A função inversa corresponde a $\log_3 y = x + 1$.

j) Considere a figura 28 e a função cifradora $f(x) = 2^x.2^3$. Utilize a propriedade ($a^x \,.\, a^y = a^{x+y}$) na função dada e codifique o texto “A mentira é uma verdade que se esqueceu de acontecer.”.

Possível solução dos alunos

a) O aluno pode resolver a questão, sistematizando as informações relevantes e elaborando estratégias para resolução.

Informação relevante: A = 1, B = 2, C = 3, ... e $f(x) = 2^x.2^3$

Prevendo resultados: pretende-se que o aluno seja capaz de realizar o cálculo da imagem da função para cada algarismo que corresponde a uma letra e utilize corretamente a calculadora.

A sequência numérica do texto é: 1 – 13 – 5 – 14 – 20 – 9 – 18 – 1 – 5 – 21 – 13 – 1 – 22 – 5 – 18 – 4 – 1 – 4 – 5 – 17 – 21 – 5 – 19 – 5 – 5 – 19 – 17 – 21 – 5 – 3 – 5 – 21 – 4 – 5 – 1 – 3 – 15 – 14 – 20 – 5 – 3 – 5 – 18.

Cálculo da imagem de cada algarismo da sequência:

$f(1) = 2^1.2^3 = 2^{1+3} = 16$

$f(13) = 2^{13}.2^3 = 2^{13+3} = 65536$

$f(5) = 2^5.2^3 = 2^{5+3} = 256$

$f(14) = 2^{14}.2^3 = 2^{14+3} = 131072$

$f(20) = 2^{20}.2^3 = 2^{20+3} = 8388608$

$f(9) = 2^9.2^3 = 2^{9+3} = 4096$

$f(18) = 2^{18}.2^3 = 2^{18+3} = 2097152$

$f(22) = 2^{22}.2^3 = 2^{22+3} = 33554432$

$f(4) = 2^4.2^3 = 2^{4+3} = 128$

$f(3) = 2^3.2^3 = 2^{3+3} = 64$

$f(17) = 2^{17}.2^3 = 2^{17+3} = 1048576$

$f(15) = 2^{15}.2^3 = 2^{15+3} = 262144$

$f(19) = 2^{19}.2^3 = 2^{19+3} = 4194304$

$f(21) = 2^{21}.2^3 = 2^{21+3} = 16777216$

Nesse caso, espera-se que o estudante utilize a calculadora da seguinte forma: digite 2 ^ (1 + 3) e tecle *enter*, obtendo 16. Para os demais algarismos, espera-se que ele utilize a tecla cursor 

, para se mover pelo visor e a tecla *clear* 

, para apagar o algarismo que deseja modificar, com isso, modificando apenas a variável *x*.

Sendo o texto codificado, a imagem de cada algarismo encontrado na função será: 16 – 65536 – 256 – 131072 – 8388608 – 4096 – 2097152 – 16 – 256 – 16777216 – 65536 – 16 – 33554432 – 256 – 2097152 – 128 – 16 – 128 – 256 – 1048576 – 16777216 – 256 – 4194304 – 256 – 256 – 4194304 – 1048576 – 16777216 – 256 – 64 – 256 – 16777216 – 128 – 256 – 16 – 64 – 262144 – 131072 – 8388608 – 256 – 64 – 256 – 2097152.

Verificação da estratégia: espera-se que o aluno faça o cálculo da função inversa, para verificar se os resultados encontrados estão corretos.

A função inversa de $f(x) = 2^x.2^3$ é:

$f(x) = 2^x.2^3$

$f(x) = 2^{x+3}$

$\log_2 y = x + 3$

A função inversa corresponde a $\log_2 y = x + 3$.

Etapa 9

As atividades didáticas envolvendo Código com Matrizes têm por objetivo revisar o conceito de matriz, multiplicação de matrizes, operações com matrizes, matriz transposta, cálculo de matriz inversa, visando reforçar e ampliar o conhecimento dos alunos.

Atividade 9 – Código com matrizes

a) Considere a tabela da figura 29 e codifique a palavra "FELICIDADE”, sabendo que a matriz codificadora é $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$.

A	B	C/Ç	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figura 29: quadro do valor numérico de cada letra.

Possível solução dos alunos

O aluno deve observar que uma das informações relevantes apresentada na questão é a matriz codificadora $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$.

Tomando por base a figura 29, o aluno deverá montar a sequência numérica da mensagem: “6 – 5 – 12 – 9 – 3 – 9 – 4 – 1 – 4 – 5”.

Em seguida, deve fazer a matriz da mensagem: $M = \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}$.

Para codificar, o aluno deverá realizar multiplicação de matrizes, em que ele multiplicará a matriz A com a matriz M:

$$AM = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}$$

$$AM = \begin{pmatrix} 27 & 51 & 33 & 11 & 23 \\ 26 & 48 & 39 & 8 & 24 \end{pmatrix}$$

Os elementos da matriz AM corresponderão à mensagem codificada:

Verificação das hipóteses: o aluno poderá verificar se realizou o procedimento corretamente, decodificando a mensagem, isto é, multiplicando a matriz (AM) com A^{-1}, ou seja, $(AM).A^{-1} =$

$$\begin{pmatrix} 27 & 51 & 33 & 11 & 23 \\ 26 & 48 & 39 & 8 & 24 \end{pmatrix} \cdot \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix} = \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}$$

b) Considere a tabela da figura 29 e codifique a mensagem “Conhecer o caminho não é o mesmo que o percorrer!”, sabendo que a matriz codificadora é $A = \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix}$.

Possível solução dos alunos

O aluno deve observar que uma das informações relevantes apresentada na questão é a matriz codificadora $A = \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix}$.

Tomando por base a figura xx, o aluno deverá montar a sequência numérica da mensagem: “3 – 15 – 14 – 8 – 5 – 3 – 5 – 18 – 15 – 3 – 1 – 13 – 9 – 14 – 8 – 15 – 14 – 1 – 15 – 5 – 15 – 13 – 5 – 19 – 13 – 15 – 17 – 21 – 5 – 15 – 16 – 5 – 18 – 3 – 15 – 18 – 18 – 5 – 18”.

Em seguida, deve fazer a matriz da mensagem:

$$M = \begin{pmatrix} 3 & 14 & 5 & 5 & 15 & 1 & 9 & 8 & 14 & 15 & 15 & 5 & 13 & 17 & 5 & 16 & 18 & 15 & 18 & 18 \\ 15 & 8 & 3 & 18 & 3 & 13 & 14 & 15 & 1 & 5 & 13 & 19 & 15 & 21 & 15 & 5 & 3 & 18 & 5 & 18 \end{pmatrix}$$

Para codificar, o aluno deverá realizar multiplicação de matrizes, em que ele multiplicará a matriz A com a matriz M:

$$AM = \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} . \begin{pmatrix} 3 & 14 & 5 & 5 & 15 & 1 & 9 & 8 & 14 & 15 & 15 & 5 & 13 & 17 & 5 & 16 & 18 & 15 & 18 & 18 \\ 15 & 8 & 3 & 18 & 3 & 13 & 14 & 15 & 1 & 5 & 13 & 19 & 15 & 21 & 15 & 5 & 3 & 18 & 5 & 18 \end{pmatrix}$$

$$AM = \begin{pmatrix} 66 & 60 & 22 & 82 & 42 & 54 & 74 & 76 & 32 & 50 & 82 & 86 & 86 & 118 & 70 & 52 & 48 & 102 & 56 & 108 \\ 78 & 54 & 20 & 95 & 30 & 66 & 79 & 83 & 19 & 40 & 80 & 100 & 88 & 122 & 80 & 41 & 33 & 105 & 43 & 108 \end{pmatrix}$$

Os elementos da matriz AM corresponderão à mensagem codificada.

Verificação das hipóteses: o aluno poderá verificar se realizou o procedimento corretamente, decodificando a mensagem, isto é, multiplicando a matriz (AM) com A^{-1}.

$$A^{-1}(AM) = \begin{pmatrix} \frac{5}{6} & -\frac{2}{3} \\ -\frac{1}{6} & \frac{1}{3} \end{pmatrix} . \begin{pmatrix} 66 & 60 & 22 & 82 & 42 & 54 & 74 & 76 & 32 & 50 & 82 & 86 & 86 & 118 & 70 & 52 & 48 & 102 & 56 & 108 \\ 78 & 54 & 20 & 95 & 30 & 66 & 79 & 83 & 19 & 40 & 80 & 100 & 88 & 122 & 80 & 41 & 33 & 105 & 43 & 108 \end{pmatrix}$$

$$A^{-1}(AM) = \begin{pmatrix} 3 & 14 & 5 & 5 & 15 & 1 & 9 & 8 & 14 & 15 & 15 & 5 & 13 & 17 & 5 & 16 & 18 & 15 & 18 & 18 \\ 15 & 8 & 3 & 18 & 3 & 13 & 14 & 15 & 1 & 5 & 13 & 19 & 15 & 21 & 15 & 5 & 3 & 18 & 5 & 18 \end{pmatrix}$$

c) Considere a tabela da figura 29 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26, que considera como zero a letra Z e decodifique a mensagem "10/ 106/ 132/ 54/ -60/ 86/ 58/ 98/ -70/ 94/ 86/ 30/ 108/ 58/ 81/ 72/ 15/ 26/ 5/ 34/ 121/ 40/ 16/ 10/ 38/ 114/ 10/ 106/ 87/ 90/ 50/ 112/ -73/ 66/ -88/ 78/ 113/ 54/ 10/ 106", sabendo que a matriz codificadora é $A = \begin{pmatrix} 7 & -5 \\ 2 & 4 \end{pmatrix}$.

Possível solução dos alunos

O aluno deve observar que uma das informações relevantes apresentada na questão é a matriz codificadora $A = \begin{pmatrix} 7 & -5 \\ 2 & 4 \end{pmatrix}$.

Em seguida, deverá saber que deve realizar o cálculo da matriz inversa da matriz A:

$$A^{-1} = \begin{pmatrix} 7 & -5 \\ 2 & 4 \end{pmatrix} . \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} \frac{2}{19} & \frac{5}{38} \\ -\frac{1}{19} & \frac{7}{38} \end{pmatrix}$$

Para decodificar, o aluno deverá realizar multiplicação de matrizes, em que ele multiplicará a matriz A^{-1} com a matriz AM:

$$A^{-1}.(AM)=\begin{pmatrix} \frac{2}{19} & \frac{5}{38} \\ -\frac{1}{19} & \frac{7}{38} \end{pmatrix}.\begin{pmatrix} 10 & 132 & -60 & 58 & -70 & 86 & 108 & 81 & 15 & 5 & 121 & 16 & 38 & 10 & 87 & 50 & -73 & -88 & 113 & 10 \\ 106 & 54 & 86 & 98 & 94 & 30 & 58 & 72 & 26 & 34 & 40 & 10 & 114 & 106 & 90 & 112 & 66 & 78 & 54 & 106 \end{pmatrix}$$

$$A^{-1}(AM)=\begin{pmatrix} 15 & 21 & 5 & 19 & 5 & 13 & 19 & 18 & 5 & 5 & 18 & 3 & 19 & 15 & 21 & 20 & 1 & 1 & 19 & 15 \\ 19 & 3 & 19 & 15 & 21 & 1 & 5 & 9 & 3 & 6 & 1 & 1 & 19 & 19 & 12 & 18 & 16 & 19 & 4 & 19 \end{pmatrix}$$

Assim, encontrará como mensagem a frase “O sucesso é uma série de fracassos ultrapassados.”.

d) Considere a tabela da figura 29 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26, que considera como zero a letra Z, e codifique a mensagem “Viver é a arte de sorrir cada vez que o mundo diz não.”, sabendo que a matriz codificadora é $A = 2.\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$.

Possível solução dos alunos

O aluno deve observar que uma das informações relevantes apresentada na questão é a matriz codificadora $A = 2.\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$.

Tomando por base a figura 29, o aluno deverá montar a sequência numérica da mensagem: “22 – 9 – 22 – 5 – 18 – 5 – 1 – 1 – 18 – 20 – 5 – 4 – 5 – 19 – 15 – 18 – 18 – 9 – 18 – 3 – 1 4 – 1 – 22 – 5 – 0 – 17 – 21 – 5 – 15 – 13 – 21 – 14 – 4 – 15 – 4 – 9 – 0 – 14 – 1 – 15”.

Em seguida, deve fazer a matriz mensagem:

$$M = \begin{pmatrix} 22 & 22 & 18 & 1 & 18 & 5 & 5 & 15 & 18 & 18 & 14 & 22 & 0 & 21 & 15 & 21 & 4 & 4 & 0 & 1 \\ 9 & 5 & 5 & 1 & 20 & 4 & 19 & 18 & 9 & 3 & 1 & 5 & 17 & 5 & 13 & 14 & 15 & 9 & 14 & 15 \end{pmatrix}$$

Para codificar, o aluno deverá realizar multiplicação de matrizes, multiplicando a matriz A com a matriz M:

$$AM = \begin{pmatrix} 4 & 6 \\ 8 & 10 \end{pmatrix}.\begin{pmatrix} 22 & 22 & 18 & 1 & 18 & 5 & 5 & 15 & 18 & 18 & 14 & 22 & 0 & 21 & 15 & 21 & 4 & 4 & 0 & 1 \\ 9 & 5 & 5 & 1 & 20 & 4 & 19 & 18 & 9 & 3 & 1 & 5 & 17 & 5 & 13 & 14 & 15 & 9 & 14 & 15 \end{pmatrix}$$

$$AM = \begin{pmatrix} 142 & 118 & 102 & 10 & 192 & 44 & 134 & 168 & 126 & 90 & 62 & 118 & 103 & 114 & 138 & 168 & 106 & 70 & 84 & 94 \\ 266 & 226 & 194 & 18 & 344 & 80 & 230 & 300 & 234 & 174 & 122 & 226 & 170 & 218 & 250 & 308 & 182 & 122 & 140 & 158 \end{pmatrix}$$

Os elementos da matriz AM corresponderão à mensagem codificada.

Verificação das hipóteses: o aluno poderá verificar se realizou o procedimento corretamente, decodificando a mensagem, isto é, multiplicando a matriz (AM) com A^{-1}.

$$A^{-1}(AM)=\begin{pmatrix} -\frac{5}{4} & \frac{3}{4} \\ 1 & -\frac{1}{2} \end{pmatrix}.\begin{pmatrix} 142 & 118 & 102 & 10 & 192 & 44 & 134 & 168 & 126 & 90 & 62 & 118 & 103 & 114 & 138 & 168 & 106 & 70 & 84 & 94 \\ 266 & 226 & 194 & 18 & 344 & 80 & 230 & 300 & 234 & 174 & 122 & 226 & 170 & 218 & 250 & 308 & 182 & 122 & 140 & 158 \end{pmatrix}$$

$$A^{-1}(AM)=\begin{pmatrix} 22 & 22 & 18 & 1 & 18 & 5 & 5 & 15 & 18 & 18 & 14 & 22 & 0 & 21 & 15 & 21 & 4 & 4 & 0 & 1 \\ 9 & 5 & 5 & 1 & 20 & 4 & 19 & 18 & 9 & 3 & 1 & 5 & 17 & 5 & 13 & 14 & 15 & 9 & 14 & 15 \end{pmatrix}$$

e) Considere a tabela da figura 29 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26, que considera como zero a letra Z, e decodifique a mensagem “101/ -63/ 89/ -53/ -3/ 3/ 93/ -58/ -47/ -40/ 27/ 5/ -3/ 68/ -41/ 29/ -18/ 83/ -50/ -13/ 10/ 109/ -68/ 107/ -65/ -49/ 33/ 6/ -1/ -4/ 3/ 60/ -37/ 141/ -88/ -19/ 13”, sabendo que a matriz codificadora é $A=\begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix}+\begin{pmatrix} 0 & 6 \\ 1 & 3 \end{pmatrix}$.

Possível solução dos alunos

O aluno deve observar que uma das informações relevantes apresentada na questão é a matriz codificadora $A=\begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix}+\begin{pmatrix} 0 & 6 \\ 1 & 3 \end{pmatrix}$.

Em seguida, deverá saber que deve realizar o cálculo da matriz inversa da matriz A:

$$A^{-1}=\begin{pmatrix} 5 & 8 \\ 2 & 3 \end{pmatrix}.\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^{-1}=\begin{pmatrix} -3 & 8 \\ 2 & -5 \end{pmatrix}$$

Para decodificar, o aluno deverá realizar multiplicação de matrizes, multiplicando a matriz A^{-1} com a matriz AM:

$$A^{-1}.(AM)=\begin{pmatrix} -3 & 8 \\ 2 & -5 \end{pmatrix}.\begin{pmatrix} 101 & 89 & -3 & 93 & 77 & -40 & 5 & 68 & 29 & 83 & -13 & 109 & 107 & -49 & 6 & -4 & 60 & 141 & -19 \\ -63 & -53 & 3 & -58 & -47 & 27 & -3 & -41 & -18 & -50 & 10 & -68 & -65 & 33 & -1 & 3 & -37 & -88 & 13 \end{pmatrix}$$

$$A^{-1}(AM)=\begin{pmatrix} 1 & 21 & 9 & 1 & 9 & 16 & 1 & 12 & 1 & 15 & 15 & 1 & 15 & 19 & 22 & 4 & 4 & 1 & 9 \\ 13 & 19 & 3 & 12 & 13 & 1 & 1 & 13 & 4 & 16 & 4 & 14 & 19 & 1 & 9 & 1 & 9 & 18 & 1 \end{pmatrix}$$

Assim, encontrará como mensagem a frase “A música limpa a alma do pó da nossa vida diária.”.

f) Considere a tabela da figura 29 que, para cada letra do alfabeto, associa um número inteiro de 1 a 26, que considera como zero a letra Z, e decodifique a mensagem “16 – 3 – 21 – 9 – 43 – 42 – 24 – 27 – 33 – 42 – 39 – 57 – 51 – 54 – 30 – 15 – 55 – 60 – 36 – 27 – 49 – 42 – 36 – 45 – 16 – 3 – 25 – 9 – 13 – 12 – 25 – 36 – 61 – 60 – 1 – 0”, sabendo que a matriz codificadora é a matriz transposta de A e a matriz $A = \begin{pmatrix} 1 & 0 \\ 3 & 2 \end{pmatrix}$.

Possível solução dos alunos

O aluno deve observar que uma das informações relevantes apresentada na questão é a matriz codificadora, transposta de A, que é $A^t = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$.

Em seguida, deverá saber que deve realizar o cálculo da matriz inversa da matriz A^t:

$$A^{-1} = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} . \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$$

Para decodificar, o aluno deverá realizar multiplicação de matrizes, multiplicando a matriz A^{-1} com a matriz AM:

$$A^{-1}.(AM) = \begin{pmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{2} \end{pmatrix} . \begin{pmatrix} 16 & 21 & 43 & 24 & 33 & 39 & 51 & 30 & 55 & 36 & 16 & 25 & 13 & 25 & 61 & 1 \\ 3 & 9 & 42 & 27 & 42 & 57 & 54 & 15 & 60 & 45 & 3 & 9 & 12 & 36 & 60 & 0 \end{pmatrix}$$

$$A^{-1}.(AM) = \begin{pmatrix} 14 & 15 & 15 & 6 & 5 & 1 & 15 & 20 & 15 & 18 & 21 & 6 & 14 & 19 & 5 & 1 & 21 & 1 \\ 1 & 3 & 14 & 9 & 44 & 19 & 18 & 5 & 20 & 9 & 14 & 15 & 1 & 3 & 4 & 12 & 20 & 0 \end{pmatrix}$$

Assim, encontrará como mensagem a frase “Não confie na sorte. O triunfo nasce da luta.”.

3.3 FASE DA EXPERIMENTAÇÃO

Neste capítulo, apresenta-se a turma em que foi realizado o experimento e a descrição das aulas desenvolvidas durante a fase da experimentação.

3.3.1 A turma 231 do 3º ano do Ensino Médio

O experimento foi aplicado pela professora/pesquisadora na turma 231, 3º ano do Ensino Médio da Escola Técnica Estadual 31 de Janeiro, no turno da manhã, em dois períodos a cada dia, totalizando 14 horas aula, no período de agosto a setembro de 2010.

A turma é formada por 44 alunos, sendo 29 do sexo feminino e 15 do sexo masculino, na faixa etária de 16 a 18 anos.

Nessa classe, um aluno repetiu a 1ª série do Ensino Médio e outro parou de estudar um ano, 17 trabalham no turno da tarde com carga horária entre 5 e 6 horas diárias.

O questionário foi aplicado em 40 alunos, pois 4 não compareceram à aula no dia da aplicação do mesmo. O questionário possibilitou observar que as aulas propostas pela professora titular são expositivas e dialogadas. Como recurso didático, utiliza desafios matemáticos. Os trabalhos são realizados em grupos e individuais, proporcionando aos alunos materiais impressos e mimeografados.

Ao serem questionados sobre a utilização da Matemática no seu cotidiano, 33 alunos responderam que a utilizam em diversas situações, por exemplo, fazer compras, em atividades profissionais, na ida ao banco, no troco recebido, entre outras, e 7 colocaram que não a utilizam.

Quando questionados quanto à importância de estudar Matemática, os alunos colocaram que ela é importante, porque desenvolve o intelecto, pelo fato de fazerem contas quase todos os dias, por utilizá-la no dia-a-dia, para adquirir mais conhecimento, porque desenvolve o raciocínio e a lógica, está presente na maioria das profissões, possibilita serem exatos nos cálculos. Também disseram que ela melhora o aprendizado, porque no futuro podem vir a precisar dessa matéria, porque qualquer emprego exigirá conhecimento matemático.

Com relação ao estudo da disciplina de Matemática, 14 alunos não estudam além do que a professora passa em sala de aula e 26 estudam.

Na turma, 27 alunos possuem calculadoras científicas e 13 não possuem, sendo que 30 utilizam-na frequentemente fora do ambiente escolar e 10 não a utilizam. Quanto ao uso da calculadora científica, mais da metade dos alunos não sabem colocar uma expressão nela e nem utilizar algumas funções, como a de potência e logaritmo. A escola não apresenta restrições quanto ao uso de calculadora e a professora da turma faz uso desse recurso sempre que acha oportuno.

Nos corredores da escola, nas paredes, foram desenhados temas e o de matemática é um desenho de uma pessoa utilizando calculadora (figura 30).

Figura 30: caricatura no corredor da escola.

Os alunos apresentaram um bom relacionamento entre si durante toda a realização do experimento. Conforme pode ser observado na figura 31, eles trabalharam em grupos, formando-se na turma 5 grupos, que foram denominados grupos A, B, C, D e E. Os grupos receberam uma apostila (apêndice C) com todas as atividades didáticas a serem desenvolvidas durante o experimento. O trabalho em grupo possibilitou que os mesmos interagissem entre si e entre os grupos para realização das atividades didáticas, realizando um trabalho cooperativo.

Figura 31: turma 231.

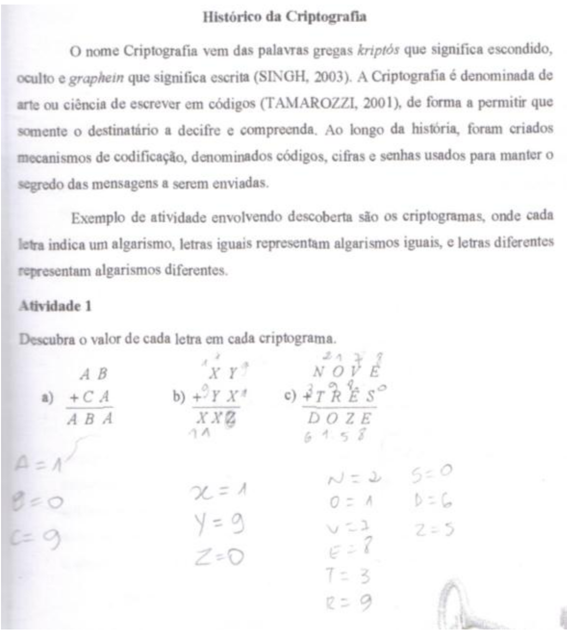
3.3.2 O experimento

Neste item, apresenta-se o que foi trabalhado em cada encontro com os alunos da turma 231 durante a fase da experimentação.

Primeira aula

Em primeiro lugar, foram distribuídos aos alunos questionários prévios para conhecer a turma e determinar o perfil da turma na qual seria aplicado o experimento.

Em seguida, foi distribuída uma apostila com as atividades didáticas que seriam desenvolvidas durante o experimento. Em seguida, introduziu-se a história da Criptografia, pela professora/pesquisadora, e foram desenvolvidas as atividades propostas, conforme figura 32.



Histórico da Criptografia

O nome Criptografia vem das palavras gregas *kriptós* que significa escondido, oculto e *graphein* que significa escrita (SINGH, 2003). A Criptografia é denominada de arte ou ciência de escrever em códigos (TAMAROZZI, 2001), de forma a permitir que somente o destinatário a decifre e compreenda. Ao longo da história, foram criados mecanismos de codificação, denominados códigos, cifras e senhas usados para manter o segredo das mensagens a serem enviadas.

Exemplo de atividade envolvendo descoberta são os criptogramas, onde cada letra indica um algarismo, letras iguais representam algarismos iguais, e letras diferentes representam algarismos diferentes.

Atividade 1

Descubra o valor de cada letra em cada criptograma.

a) $\begin{array}{r} A\ B \\ +\ C\ A \\ \hline A\ B\ A \end{array}$ b) $\begin{array}{r} X\ Y \\ +\ Y\ X \\ \hline X\ X\ Z \end{array}$ c) $\begin{array}{r} N\ O\ V\ E \\ +\ T\ R\ E\ S \\ \hline D\ O\ Z\ E \end{array}$

A = 1
B = 0
C = 9

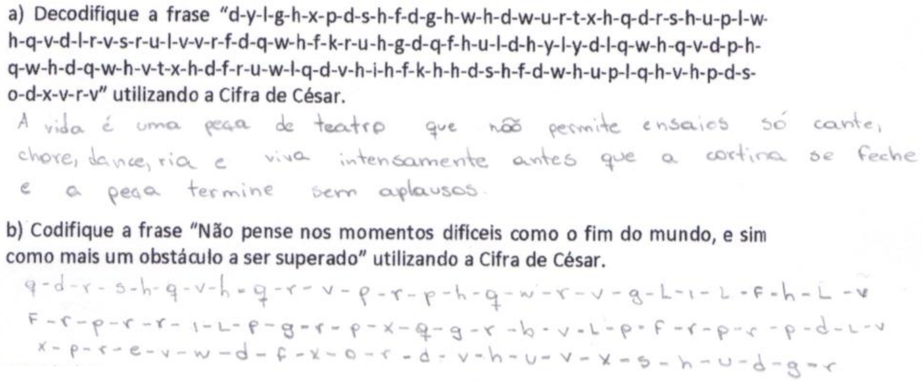
x = 1
Y = 9
Z = 0

N = 2
O = 1
V = 7
E = 8
T = 3
R = 9

S = 0
D = 6
Z = 5

Figura 32: exemplo de atividades de criptogramas realizadas pelos alunos do grupo B.

Após, foi proposto a cada grupo o desafio de um criptograma diferente, que deveria ser realizado como tema de casa e entregue na aula seguinte. Em seguida, os alunos resolveram algumas atividades envolvendo o uso da Criptografia ao longo da história. A atividade proposta foi codificar e decodificar, utilizando a Cifra de César, conforme figura 33.



a) Decodifique a frase "d-y-l-g-h-x-p-d-s-h-f-d-g-h-w-h-d-w-u-r-t-x-h-q-d-r-s-h-u-p-l-w-h-q-v-d-l-r-v-s-r-u-l-v-v-r-f-d-q-w-h-f-k-r-u-h-g-d-q-f-h-u-l-d-h-y-l-y-d-l-q-w-h-q-v-d-p-h-q-w-h-d-q-w-h-v-t-x-h-d-f-r-u-w-l-q-d-v-h-i-h-f-k-h-h-d-s-h-f-d-w-h-u-p-l-q-h-v-h-p-d-s-o-d-x-v-r-v" utilizando a Cifra de César.

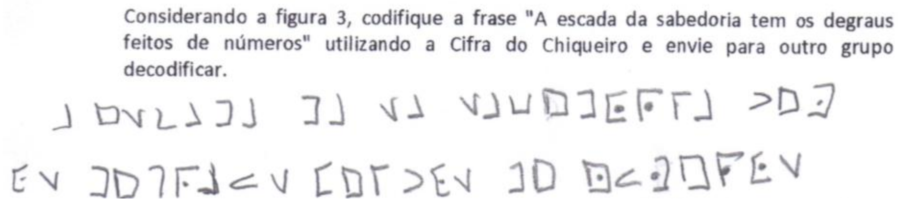
A vida é uma peça de teatro que não permite ensaios só cante, chore, dance, ria e viva intensamente antes que a cortina se feche e a peça termine sem aplausos.

b) Codifique a frase "Não pense nos momentos difíceis como o fim do mundo, e sim como mais um obstáculo a ser superado" utilizando a Cifra de César.

q-d-r-s-h-q-v-h-q-r-v-p-r-p-h-q-w-r-v-g-l-i-l-f-h-l-v-f-r-p-r-r-i-l-p-g-r-p-x-q-g-r-h-v-l-p-f-r-p-r-p-d-l-v-x-p-r-e-v-w-d-f-x-o-r-d-v-h-u-v-x-s-h-u-d-g-r

Figura 33: exemplo de atividades envolvendo Cifra de César, resolvida pelo grupo D.

Outra atividade desenvolvida foi a codificação de uma frase, utilizando a Cifra do Chiqueiro, conforme figura 34.

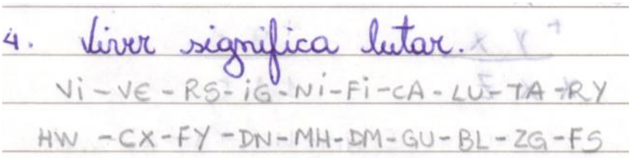


Considerando a figura 3, codifique a frase "A escada da sabedoria tem os degraus feitos de números" utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

Figura 34: exemplo de atividades envolvendo Cifra do Chiqueiro, resolvida pelo grupo C.

Segunda aula

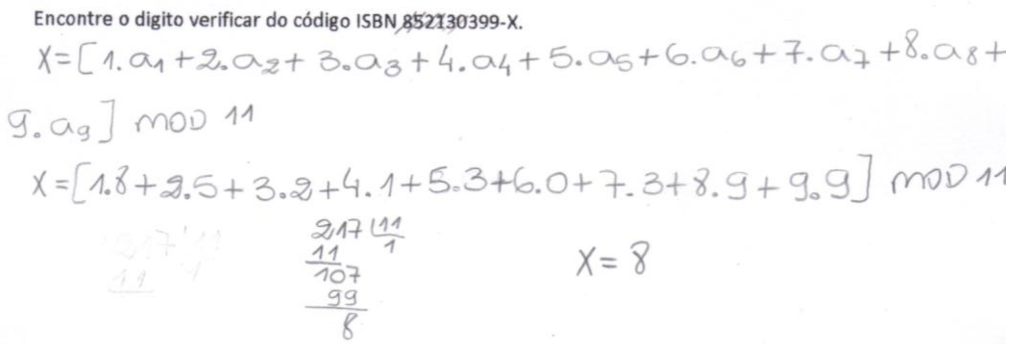
Iniciou-se a aula com os alunos entregando o desafio proposto na aula anterior e tirando-se dúvidas referentes à atividade do desafio. Os alunos organizaram-se nos grupos, formados na primeira aula e foi dado seguimento à história da Criptografia, explicando a Cifra de Vigènere e a Cifra de Playfair. Foi proposto aos alunos que realizassem uma atividade de codificação, utilizando a Cifra de Playfair, conforme figura 35.



4. Viver significa lutar.
VI-VE-RS-IG-NI-FI-CA-LU-TA-RY
HW-CX-FY-DN-MH-DM-GU-BL-ZG-FS

Figura 35: exemplo de atividades envolvendo Cifra de Playfair, resolvida pelo grupo C.

Após a realização da atividade deu-se continuidade à história da Criptografia e foi exposto aos alunos que era possível descobrir o dígito verificador do Código ISBN e os mesmos realizaram a atividade envolvendo o Código ISBN, conforme figura 36.



Encontre o digito verificar do código ISBN 852130399-X.

$X = [1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9]$ MOD 11

$X = [1.8 + 2.5 + 3.2 + 4.1 + 5.3 + 6.0 + 7.3 + 8.9 + 9.9]$ MOD 11

217 | 11
11   1
107
99
8

$X = 8$

Figura 36: exemplo de atividades envolvendo Código ISBN, resolvida pelo grupo A.

Outra atividade proposta nesta aula foi o código com Função Linear. Para resolver essa atividade, os alunos fizeram uso da calculadora científica 35s da HP (figura 37), com o objetivo de aprender a utilizar essa ferramenta, já presente em seu cotidiano. As calculadoras utilizadas na fase de experimentação foram disponibilizadas pelo Laboratório de Matemática da Universidade Luterana do Brasil, através da parceria UBRA e HP Calculadoras. Cada grupo recebeu uma calculadora, para resolver as atividades propostas. Os grupos combinaram que cada um faria uma parte da atividade, utilizando a calculadora para possibilitar a todos o seu uso.

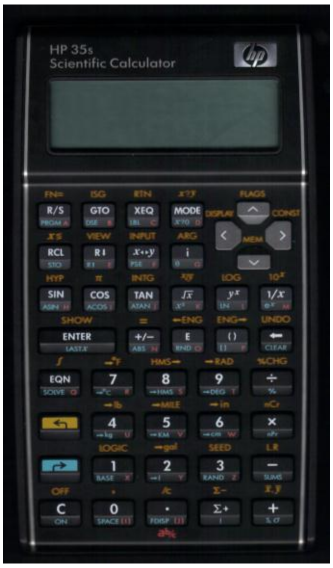


Figura 37: imagem da calculadora 35s da HP utilizada pelos alunos no experimento.

Terceira aula

No início da aula, os alunos organizaram-se em grupos, foram distribuídas as calculadoras e as apostilas com as atividades para continuação da resolução da atividade de codificação e decodificação com código com função linear, conforme a figura 38.

Figura 38: imagem dos alunos resolvendo as atividades com o auxílio da calculadora.

Quarta aula

Nessa aula, os alunos realizaram a atividade didática envolvendo o conteúdo de função quadrática. Os grupos, cuja atividade era codificar, não tiveram dificuldade em realizar a atividades, pois sabiam que teriam que realizar o cálculo da imagem.

Os grupos que deveriam decodificar apresentaram dificuldade, pois não lembravam qual o procedimento para encontrar a função quadrática inversa. Após o auxílio da professora/pesquisadora, explicando como determinar a inversa de uma função quadrática, os alunos conseguiram resolver a atividade proposta. Salienta-se, aqui, que essa atividade possibilitou aos alunos conhecer um novo conteúdo, calcular a inversa de uma função quadrática.

Quinta aula

Iniciou-se a aula com a atividade didática de codificação com função exponencial e logarítmica, em que a professora/pesquisadora explicou a atividade e, em seguida, os alunos reuniram-se, conforme os grupos formados na primeira aula e começaram a resolver a atividade. Quando encontravam dificuldades, os alunos discutiam entre os grupos para solucionar o problema. Se a dúvida persistisse, pediam auxílio da professora.

Sexta aula

Os alunos continuaram a resolução da atividade de codificação com função exponencial e logarítmica. Após o término dessa atividade, a professora/pesquisadora explicou o código com matrizes e os alunos começaram a realizar essa atividade. Como a frase proposta era muito extensa, os alunos a dividiram e cada elemento do grupo codificou uma parte, depois construíram uma única matriz. Foi desenvolvido um trabalho cooperativo.

Sétima aula

Nessa aula, deu-se prosseguimento à atividade didática de codificação e decodificação com matrizes. Os alunos realizaram cálculo de multiplicação de matrizes para codificar. Também realizaram o cálculo da matriz inversa para decodificar. Os estudantes não tiveram dificuldade nessa atividade, pois haviam estudado matrizes no trimestre anterior.

3.4 ANÁLISES *A POSTERIORI* E VALIDAÇÃO

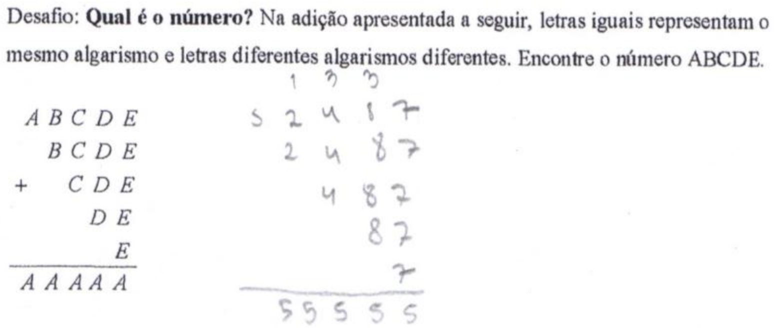
Os dados para análise foram coletados durante a fase de experimentação, através das observações da professora/pesquisadora, dos registros realizados pelos alunos durante o experimento e pelas respostas dos alunos ao questionário aplicado.

Nas atividades envolvendo Criptogramas, os alunos tiveram que formular hipóteses e verificá-las, para conseguir resolver as questões. Essa atividade também exigiu dos mesmos a discussão em grupo das hipóteses levantadas (figura 39).

Figura 39: imagem dos alunos resolvendo as atividades.

Na realização das atividades envolvendo Criptogramas, os alunos utilizaram seus conhecimentos de operações algébricas para encontrar a solução do problema. Depois de discussões e reflexões eles resolveram a atividade de Criptogramas (figura 40), partindo da hipótese que A poderia ser zero ou cinco e começaram a testar suas hipóteses. Então, eles perceberam que, atribuindo para letra E valor igual a zero, a letra A seria igual a zero, então descartaram essa possibilidade, visto que cada letra representa um algarismo distinto. Logo, a letra A corresponderia ao algarismo cinco. Após encontrar o algarismo da letra A, os alunos verificaram quais seriam os algarismos das outras letras, para que a adição ficasse correta. Para encontrar os demais algarismos, os alunos foram testando as possibilidades.

Resolução do grupo B

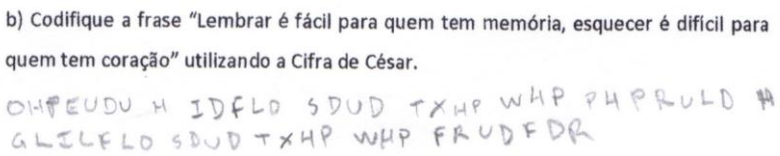

Desafio: **Qual é o número?** Na adição apresentada a seguir, letras iguais representam o mesmo algarismo e letras diferentes algarismos diferentes. Encontre o número ABCDE.

$$
\begin{array}{rr}
 & A\,B\,C\,D\,E \\
 & B\,C\,D\,E \\
+ & C\,D\,E \\
 & D\,E \\
 & E \\
\hline
 & A\,A\,A\,A\,A
\end{array}
\qquad
\begin{array}{r}
1\;3\;3\;\; \\
5\,2\,4\,1\,7 \\
2\,4\,8\,7 \\
4\,8\,7 \\
8\,7 \\
7 \\
\hline
5\,5\,5\,5\,5
\end{array}
$$

Figura 40: exemplo da resolução da atividade envolvendo a Criptogramas.

Na realização das atividades didáticas envolvendo a Cifra de César e a Cifra do Chiqueiro, os alunos não encontraram dificuldade na resolução. Para cifrar, utilizando a Cifra de César, o grupo utilizou a tabela dada na atividade e escrevem o texto codificado, como se observa na figura 41.

Resolução do grupo B


b) Codifique a frase "Lembrar é fácil para quem tem memória, esquecer é difícil para quem tem coração" utilizando a Cifra de César.

OHPEUDU H IDFLO SDUD TXHP WHP PHPRULD H
GLILFLO SDUD TXHP WHP FRUDFDR

Figura 41: exemplo da resolução da atividade envolvendo a Cifra de César.

Para cifrar utilizando a Cifra do Chiqueiro, o grupo utilizou a tabela dada na atividade e codificou a frase proposta, conforme se observa na figura 42.

Resolução do grupo B

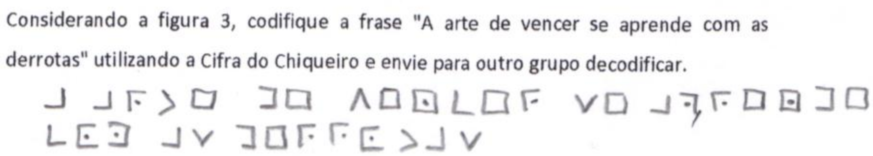

Considerando a figura 3, codifique a frase "A arte de vencer se aprende com as derrotas" utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

Figura 42: exemplo da resolução da atividade envolvendo a Cifra do Chiqueiro.

Na atividade envolvendo a Cifra de Playfair, os alunos tiveram que prestar mais atenção, para poder resolver a atividade, pois é uma cifra que exige concentração, porque a codificação é realizada aos pares e tem várias regras a serem seguidas para codificar e decodificar. Para cifrar utilizando a Cifra de Playfair, o grupo organizou a frase em pares e, utilizando o quadro da Cifra de Playfair e as normas para codificação, resolveram a atividade, como se observa na figura 43.

Resolução do grupo E

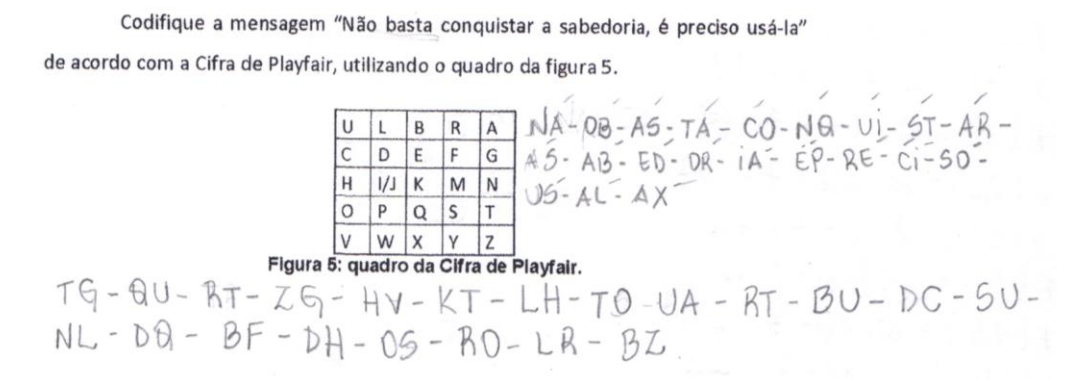


Figura 43: exemplo da resolução da atividade envolvendo a Cifra de Playfair.

Na atividade envolvendo o código ISBN, os alunos não apresentaram dificuldade, utilizaram corretamente a fórmula, encontrando o dígito verificador. Os alunos não haviam trabalhado anteriormente com aritmética modular, mas compreenderam que era necessário realizar divisão da soma encontrada por 11 e que o resto seria o dígito verificador do código ISBN. Para encontrar o dígito verificador do código ISBN, os alunos do grupo utilizaram a fórmula dada, em que atribuíram para cada dígito da fórmula o valor dos algarismos dados no código, como se observa na figura 44.

Resolução do grupo B

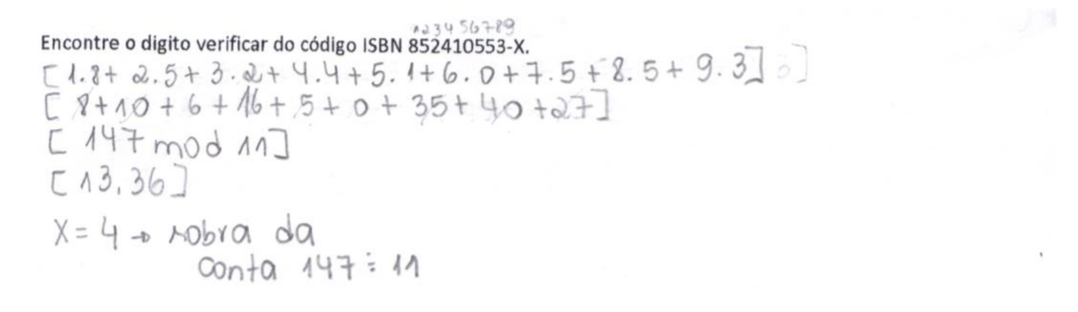


Figura 44: exemplo da resolução da atividade do Código ISBN.

No código com função linear, os alunos utilizaram a calculadora como um recurso facilitador nos cálculos. Tiveram que se concentrar, pois precisavam conhecer os recursos que ela apresentava para resolver os cálculos, conforme a figura 45.

Figura 45: imagem dos alunos resolvendo as atividades.

Na atividade de codificação com função linear, os alunos atribuíram para cada letra do alfabeto um número e realizaram o cálculo da imagem da função para cada algarismo da sequência da mensagem (figura 46).

Resolução do grupo D

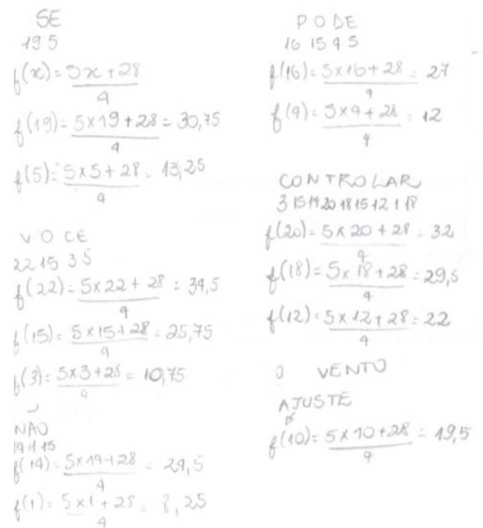
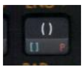
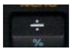
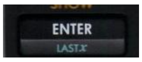


Figura 46: exemplo da resolução da atividade de codificação com Função Linear.

Nessa atividade, o grupo utilizou a calculadora científica da seguinte forma: primeiro, apertaram a tecla dos parênteses , em seguida digitaram 5, a tecla da multiplicação, o algarismo 19, depois apertaram a tecla da operação de adição, o algarismo 28 e apertaram a tecla da seta para direita . Para sair dos parênteses, apertaram a tecla da operação de divisão  e, em seguida, apertaram a tecla do algarismo 4 e, para encontrar o resultado, apertaram a tecla .

Na atividade didática envolvendo decodificação com o conteúdo de função linear, o grupo realizou o cálculo da função inversa e calculou a imagem de cada letra (figura 47). Em seguida, observou o quadro que atribui para cada letra um número e substituiu o número pela letra, encontrando o texto decodificado.

Resolução do grupo B

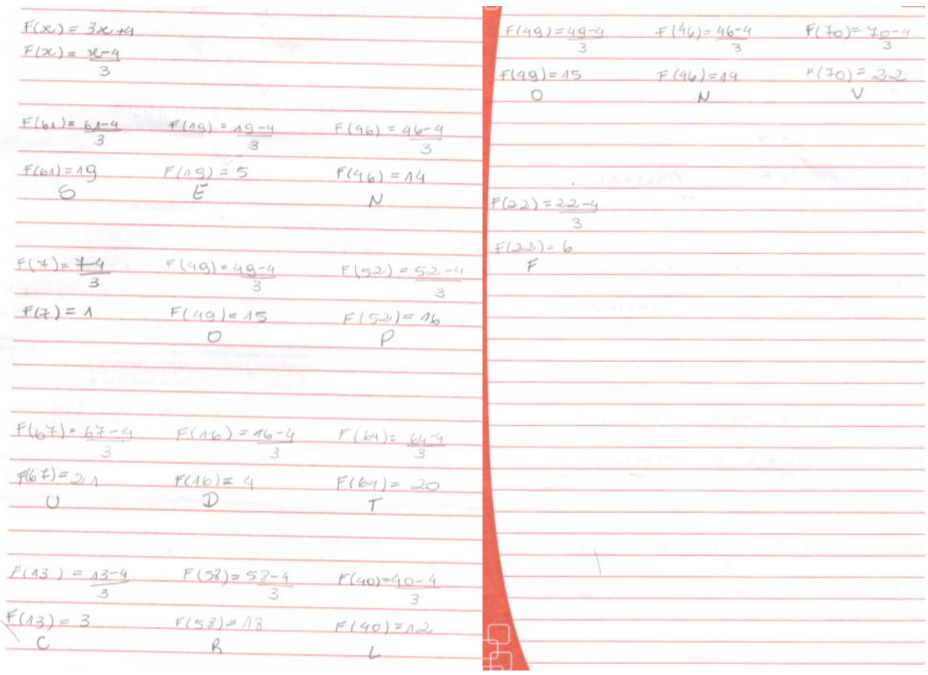
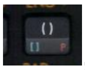
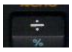
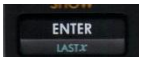


Figura 47: exemplo da resolução da atividade do Código com Função Linear.

Nessa atividade, o grupo utilizou a calculadora científica da seguinte forma: primeiro, apertaram a tecla dos parênteses , em seguida, digitaram 61 – 4, apertaram a tecla da seta para direita , depois apertaram a tecla da operação de divisão  e, em seguida, a tecla do algarismo 3 e, para encontrar o resultado, apertaram a tecla , encontrando na calculadora a expressão da figura 48.

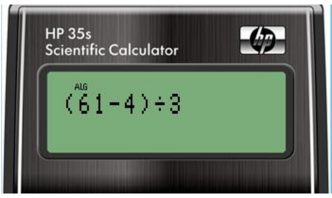


Figura 48: exemplo da atividade resolvida com a calculadora 35s da HP.

Cabe salientar que, para encontrar as demais imagens, os alunos utilizaram a tecla da seta para esquerda  e foram até o símbolo da operação. Apertaram a tecla *clear* , para apagar o número 61 e colocar outro nesta posição. Com isso, verificou-se que os alunos perceberam que a variável estava naquela posição.

Na atividade de codificação com função quadrática, os alunos atribuíram para cada letra da mensagem um algarismo e revisaram o conteúdo de função quadrática, realizando o cálculo da imagem da função dada na atividade para cada algarismo correspondente à mensagem, conforme a figura 49.

Resolução do grupo D

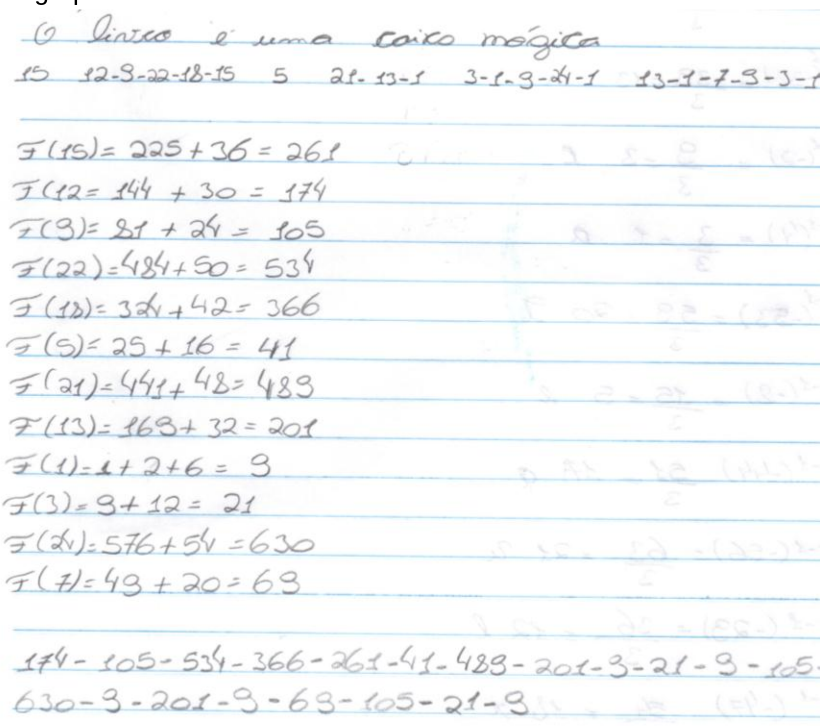


Figura 49: exemplo da resolução da atividade do Código com Função Quadrática.

A atividade didática com o conteúdo de função quadrática oportunizou aos alunos revisar o conteúdo de função quadrática inversa, pois eles não lembravam qual o procedimento para encontrar a função inversa. Também oportunizou o uso da função de potência da calculadora científica. Para decodificar a mensagem utilizando o conteúdo de função quadrática, o grupo realizou o cálculo da função inversa e calculou a imagem de cada letra (figura 50), em seguida, observou o quadro que atribui para cada letra um número e encontrou o texto decodificado.

Resolução do grupo C

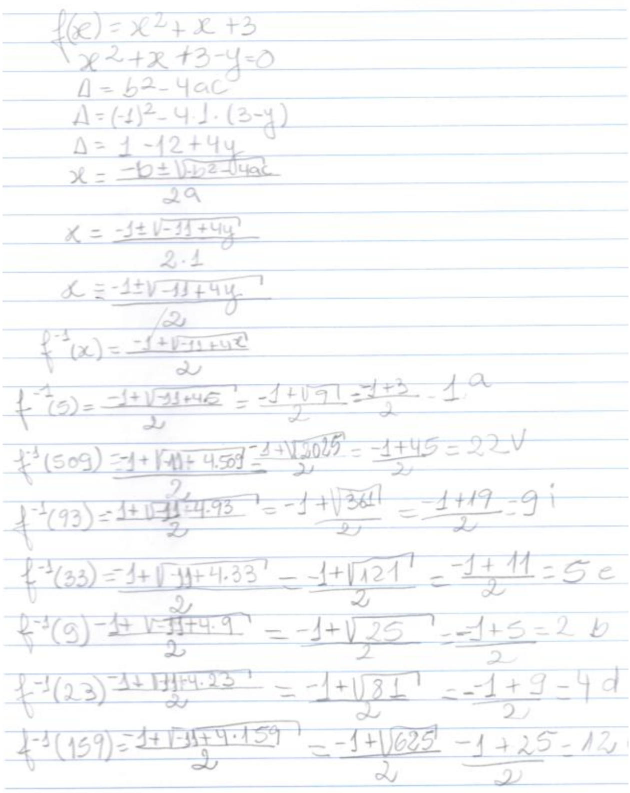
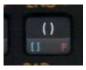
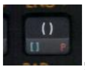
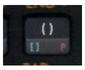
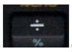
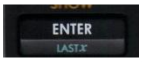


Figura 50: exemplo da resolução da atividade do Código com Função Quadrática.

Nessa atividade, o grupo utilizou a calculadora científica da seguinte forma: primeiro, apertaram a tecla dos parênteses , em seguida, digitaram o algarismos 1, a tecla , a tecla de deslocamento para direita , a operação de adição , a tecla dos parênteses , a operação de radiciação , a tecla dos parênteses , o algarismo 11, a tecla , a operação de adição , o algarismo 4, a tecla da operação de multiplicação , o algarismo 5, a tecla de deslocamento para direita  até sair de todos os parênteses. Apertaram na operação de divisão 

, no algarismo 2 e, para encontrar o resultado, apertaram a tecla 

, encontrando na calculadora a expressão da figura 51, que apresenta parte da expressão no primeiro visor e outra parte no segunda visor, conforme foi visualizado pelos alunos que deslocavam o cursor para direita ou esquerda, para visualizar toda expressão. Com relação à variável, os alunos utilizaram o mesmo procedimento da atividade com o conteúdo função linear, substituindo somente a variável.

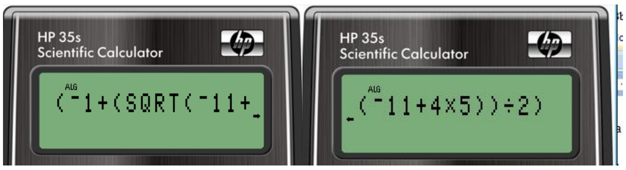


Figura 51: exemplo da atividade resolvida com a calculadora 35s da HP.

Durante a aplicação da sequência didática, os alunos mostraram-se mais concentrados nas atividades (figura 52), diminuindo, assim, a agitação da turma.

Figura 52: imagem dos alunos durante a experimentação.

Também permitiu a discussão em grupo de considerações relevantes sobre as atividades propostas, figura 53.

Figura 53: imagem dos alunos durante a experimentação.

Os alunos resolveram as atividades didáticas envolvendo função exponencial e logarítmica, explorando os recursos da calculadora científica. Para codificar a mensagem "Por mais longa que seja a caminhada, o mais importante é dar o primeiro passo.", utilizando a função cifradora $f(x) = \log_2 x$, os alunos utilizaram logaritmo mudança de base, conforme a figura 54.

Resolução do grupo E

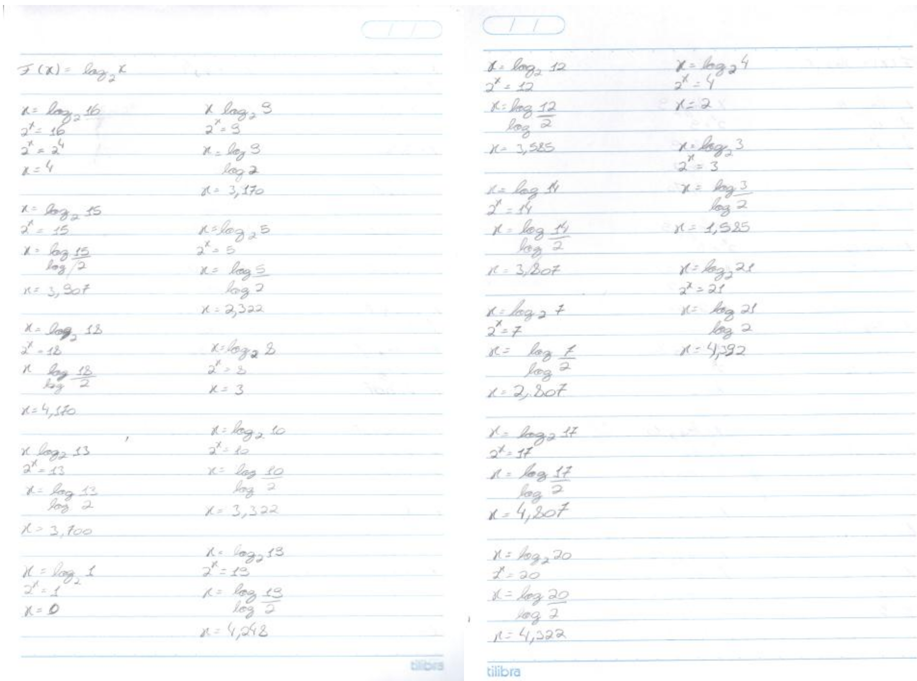
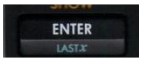


Figura 54: exemplo da resolução da atividade envolvendo função exponencial e logarítmica.

Utilizaram a calculadora da seguinte forma: primeiro, apertaram a tecla,  para habilitar função logaritmo, a tecla do logaritmo de base 10 

, o algarismo 15, a tecla da operação de divisão, a tela , o algarismo 2 e apertaram a tecla 

, encontrando na calculadora a expressão da figura 55.

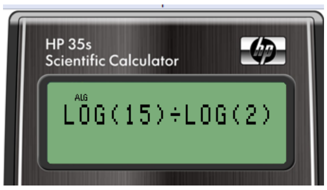
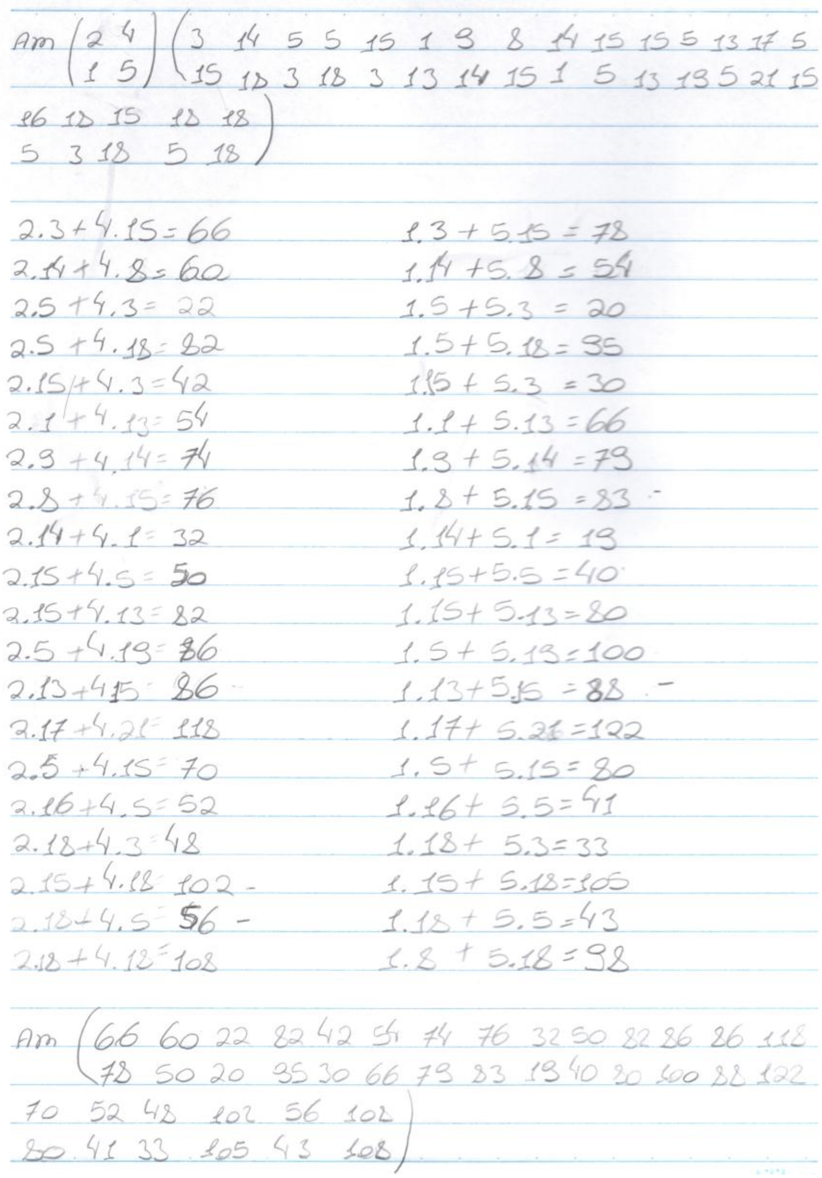


Figura 55: exemplo da atividade resolvida com a calculadora 35s da HP.

Na atividade de codificação com matrizes, os alunos atribuíram para cada letra da mensagem um algarismo e construíram a matriz mensagem. Para codificar, eles multiplicaram a matriz mensagem pela matriz codificadora, como se observa na figura 56.

Resolução do grupo C



$$Am \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 3 & 14 & 5 & 5 & 15 & 1 & 3 & 8 & 14 & 15 & 15 & 5 & 13 & 17 & 5 & 26 & 12 & 15 & 12 & 18 \\ 15 & 12 & 3 & 18 & 3 & 13 & 14 & 15 & 1 & 5 & 13 & 13 & 5 & 21 & 15 & 5 & 3 & 18 & 5 & 18 \end{pmatrix}$$

2.3+4.15=66	1.3+5.15=78
2.14+4.8=60	1.14+5.8=54
2.5+4.3=22	1.5+5.3=20
2.5+4.18=82	1.5+5.18=95
2.15+4.3=42	1.15+5.3=30
2.1+4.13=54	1.1+5.13=66
2.3+4.14=74	1.3+5.14=79
2.8+4.15=76	1.8+5.15=83
2.14+4.1=32	1.14+5.1=19
2.15+4.5=50	1.15+5.5=40
2.15+4.13=82	1.15+5.13=80
2.5+4.19=86	1.5+5.19=100
2.13+4.15=86	1.13+5.15=88
2.17+4.21=118	1.17+5.21=122
2.5+4.15=70	1.5+5.15=80
2.26+4.5=52	1.26+5.5=41
2.18+4.3=48	1.18+5.3=33
2.15+4.18=102	1.15+5.18=105
2.18+4.5=56	1.18+5.5=43
2.18+4.18=108	1.8+5.18=98

$$Am \begin{pmatrix} 66 & 60 & 22 & 82 & 42 & 54 & 74 & 76 & 32 & 50 & 82 & 86 & 26 & 118 & 70 & 52 & 48 & 102 & 56 & 102 \\ 78 & 50 & 20 & 35 & 30 & 66 & 79 & 83 & 19 & 40 & 80 & 100 & 88 & 122 & 80 & 41 & 33 & 105 & 43 & 108 \end{pmatrix}$$

Figura 56: exemplo da resolução da atividade de codificação com matrizes.

Na atividade didática envolvendo o conteúdo de matrizes, os alunos se organizaram para codificar e decodificar. Cada aluno do grupo ficou responsável pela codificação de uma parte da frase para otimizar o tempo de resolução da atividade. Isso oportunizou que cada membro do grupo fizesse a atividade. O grupo começou a decodificação com matrizes, encontrando a matriz inversa da matriz A (figura 57). Depois realizaram a multiplicação da matriz inversa com a matriz da mensagem codificada, encontraram a matriz decodificada, substituíram os números pelas letras, conforme o quadro dado e encontraram a mensagem.

Resolução do grupo A

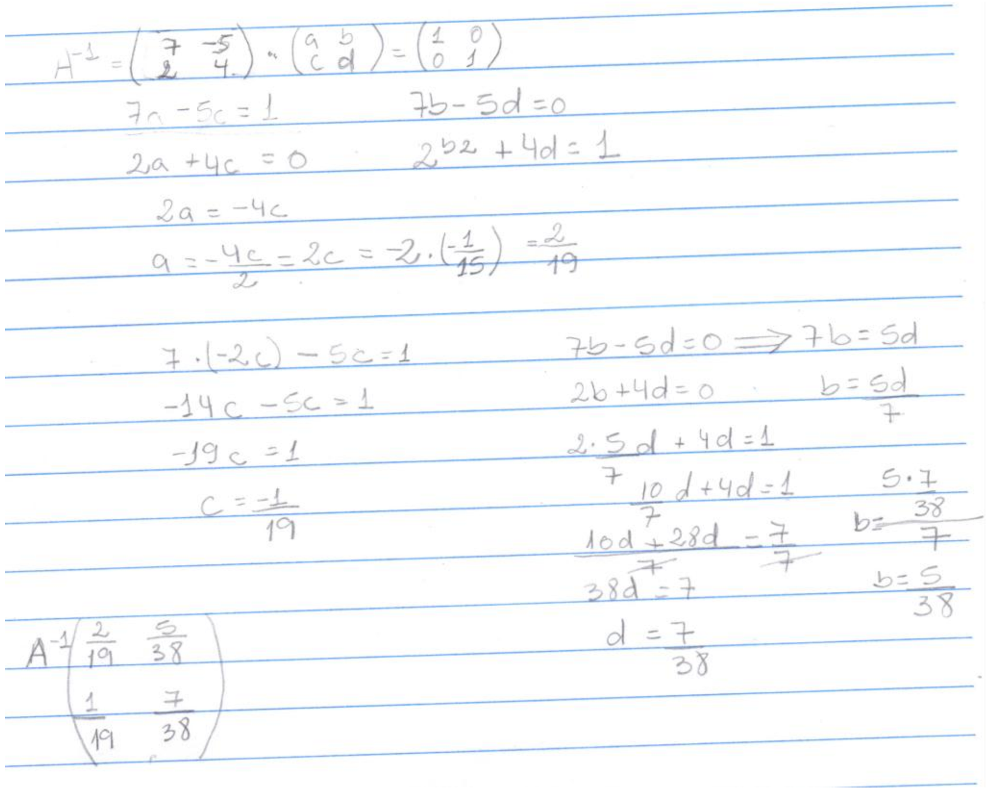


Figura 57: exemplo da resolução da atividade envolvendo o conteúdo de matrizes.

As atividades didáticas desenvolvidas no experimento relacionaram o tema proposto aos conteúdos matemáticos do Ensino Médio, que são: função linear, função quadrática, função exponencial, função logarítmica e matrizes, além das atividades envolvendo a Cifra de César, Cifra do Chiqueiro e Cifra de Playfair.

Constatou-se, ainda, através das análises dos dados coletados, durante o experimento, que os alunos compreenderam a proposta das atividades e conseguiram resolvê-las, demonstrando interesse e concentração durante a realização das mesmas, conforme figura 58.

Figura 58: imagem dos alunos resolvendo as atividades.

Percebeu-se que, na turma em que foi aplicada a sequência didática, os alunos conseguiram realizar as atividades didáticas propostas envolvendo aplicações do tema Criptografia ao longo de sua história, corretamente, mas para isso precisaram se concentrar nas atividades, pois a Cifra de Playfair apresenta muitas regras e codifica os pares de letras, o que dificulta a sua codificação.

No exercício envolvendo o dígito verificador do Código ISBN, os alunos não haviam trabalhado o conteúdo de aritmética modular e essa atividade proporcionou-lhes esse conhecimento e uma aplicação do mesmo. Percebeu-se que, após a explicação para encontrar o dígito verificador, os alunos conseguiram resolver a tarefa, aplicando a fórmula.

Durante as atividades didáticas percebeu-se que os alunos conseguiram desenvolver os conteúdos, mas é importante salientar que alguns foram desenvolvidos com mais facilidade do que em outros. As atividades de codificação com função linear, nas quais os alunos deveriam ter conhecimento de imagem da função e cálculo da função inversa foi facilmente relembrada pelos alunos. Porém, na atividade didática que envolvia codificação e decodificação com função quadrática, para codificar, os alunos utilizaram o conhecimento de função linear e calcularam a imagem, mas para decodificar não lembraram como realizar o cálculo da função inversa quadrática, o que teve que ser explicado pela professora/pesquisadora, que também chamou a atenção dos mesmos para a questão do domínio da função, visto que na função quadrática os alunos encontram duas variáveis.

As atividades didáticas com funções exponenciais e logarítmicas possibilitaram aos estudantes perceberem que essas funções são inversas, pois, para codificar, realizaram o cálculo da imagem da função e, para decodificar, envolvendo essas funções, a professora/pesquisadora teve que auxiliá-los, para que eles encontrassem a função inversa e conseguissem dar continuidade à atividade proposta. Essa atividade possibilitou a ampliação da compreensão desse conteúdo, conforme indicação dos alunos.

Nas atividades didáticas envolvendo matrizes, eles realizaram o cálculo de multiplicação de matrizes, matriz transposta, adição de matrizes e matriz inversa, sem encontrar dificuldades. Quando ocorria alguma dúvida, os próprios alunos se ajudavam e tentavam encontrar a razão da diferença nos resultados.

Com base nas atividades didáticas pesquisadas, elaborou-se uma sequência didática para aplicação em uma turma do 3º ano do Ensino Médio, que aliou os conteúdos matemáticos ao tema Criptografia e possibilitou aos alunos conhecer o conceito de Criptografia, através de atividades envolvendo: a história da Criptografia, a descoberta de algarismos (criptogramas) e os conteúdos matemáticos de funções e matrizes.

Também, foi possível perceber, durante a aplicação das atividades didáticas, na turma 231, que houve o diálogo, o trabalho em equipe e a troca de conhecimento entre os alunos, conforme figura 59.

Figura 59: imagem dos alunos realizando as atividades.

Percebeu-se, ainda, que as atividades, com esse tema, abrem a discussão acerca da introdução, em sala de aula, da utilização de tecnologias da informação e comunicação, como a calculadora, que no experimento serviu de facilitador para cálculos longos. Esse item também foi uma ampliação aos conhecimentos dos alunos, pois já utilizavam a calculadora, mas, não sabiam utilizar as teclas de potência, parênteses, cursores e não a utilizavam para resolver expressões.

Pode-se constatar que, na turma em que foi realizada a aplicação das atividades com o tema Criptografia, desenvolvidas para o Ensino Médio, permitiu que os alunos revisitassem conteúdos estudados no Ensino Médio, ampliando a compreensão daqueles já desenvolvidos, os quais foram abordados na sequência didática.

Portanto, as atividades didáticas propostas na sequência elaborada pela professora/pesquisadora, oportunizaram aos alunos a abordagem de conteúdos novos, por exemplo, o conteúdo de Aritmética Modular e o cálculo da inversa de uma função quadrática. Também possibilitou trabalhar com um tema de interesse dos estudantes, aliando os conteúdos matemáticos a um tema atual, tornando possível ampliar e revisar conteúdos já desenvolvidos. As atividades didáticas da forma, como foram conduzidas pelas professora/pesquisadora, em sala de aula, proporcionaram o trabalho em grupo e cooperativo. Além disso, os alunos conheceram aplicações da Matemática, na vida Moderna, como a atividade de encontrar o dígito verificador do Código ISBN.

CONCLUSÃO

Neste trabalho, observou-se que as atividades com códigos e senhas possibilitaram aos alunos trabalhar o conceito de Criptografia, aliado aos conteúdos de Matemática do Ensino Médio. Também tornou viável desenvolver as capacidades de concentração nas atividades, trabalho em grupo, desenvolver estratégias de resolução de problemas e validação das mesmas. As atividades didáticas desenvolvidas, nesta investigação, aliam os conteúdos matemáticos a um tema atual, apresentando diferentes situações e aplicações, bem como a utilização desse tema ao longo da história.

As atividades desenvolvidas e aplicadas são exemplos de material didático que pode ser utilizado pelos professores para exercitar, aprofundar, fixar e revisar conteúdos, fazendo uso de códigos e senhas, conforme as indicações de Tamarozzi (2001).

A sequência didática desenvolvida permitiu que os alunos explorassem os diversos recursos da calculadora científica, facilitando-lhes os cálculos longos e a compreensão de conceitos matemáticos. Esse foi um fato novo para os alunos, pois aprenderam a utilizar melhor os recursos da calculadora científica.

A metodologia de Engenharia Didática possibilitou que a pesquisa fosse analisada internamente, verificando a validade das atividades desenvolvidas. Também salienta-se que o desenvolvimento de uma sequência didática, utilizando a metodologia Engenharia Didática, é muito importante para o aperfeiçoamento do professor de sala de aula, pois permite uma análise profunda das atividades que são desenvolvidas com os alunos e isso foi possível comprovar nessa investigação.

Pode-se verificar que as hipóteses propostas, nesta investigação, foram comprovadas, através da sequência didática proposta para o 3º ano do Ensino Médio, e das análises realizadas na fase de análise *a posteriori* e validação. Também observa-se que, durante o desenvolvimento da Engenharia Didática, foram alcançados os objetivos traçados na investigação, em que investigou-se a relação do tema em estudo com os conteúdos de Matemática. Foram pesquisadas atividades didáticas com o tema, realizado um experimento em uma turma do 3º ano do Ensino Médio e verificaram-se, através das atividades desenvolvidas, que os alunos estabelecem relações com o tema.

As atividades didáticas propostas aliando o tema Criptografia aos conteúdos matemáticos do Ensino Médio, utilizando funções e matrizes, podem ser exploradas utilizando *softwares* como o *Excel*. Também, fica como sugestão, para futuros trabalhos, que o professor proponha atividades didáticas de codificação e decodificação, onde as funções não sejam bijetoras para que os alunos verifiquem que, nesses casos, não é possível decodificar as mensagens, o que possibilita trabalhar com o conceito de função não bijetora e consequentemente que não tem inversa em todo o domínio.

Entende-se que a busca de temas de interesse e que permitem o desenvolvimento de atividades didáticas devem ser incentivadas, pois o Currículo de Matemática que deve ser desenvolvido no Ensino Médio necessita ser de interesse do aluno, além de motivador e instigante, incentivando-o ao estudo dos conteúdos. Também deve proporcionar a compreensão do uso da Matemática em assuntos da vida moderna. Fatores, que podem ser observados no tema Criptografia, desenvolvido nesta investigação.

REFERÊNCIAS

ANTON, Howard; RORRES, Chris, tradução: DOERING, Claus I. **Álgebra linear com aplicações**. Porto Alegre: Bookman, 2001.

ANTON, Howard; BUSBY, Robert C., tradução: DOERING, Claus I. **Álgebra linear contemporânea**. Porto Alegre: Bookman, 2006.

ARTIGUE, Michèle; DOUADY, Régine; MORENO, Luis. **Ingeniería Didática en Educación Matemática:** Un esquema para la investigación y la innovavación en La enseñanza y el aprendizaje de las matemáticas.Venezuela: Pedro Gómez, 1995.

BRASIL, LEI 10172, de 09/01/2001. **Plano Nacional de Educação**.

BRASIL, LEI 9394, de 20/12/1996. **Diretrizes e Bases da Educação Nacional**.

BRASIL, Ministério da Educação, Secretaria de Educação Média e Tecnológica (Semtec). **Parâmetros Curriculares Nacionais para o Ensino Médio.** Brasília: MEC/Semtec, 2006.

CANTORAL, Ricardo et al. **Desarrollo del pensamiento matemático**. México, Trillas: ITESM, Universidade Virtual, 2003.

COLL, César. **Psicologia e Currículo:** uma aproximação psicopedagógica à elaboração do currículo escolar. São Paulo: Ática, 1999.

COLL, César; POZO, Juan Ignacio; SARABIA, Bernabé; VALLS, Enric. **Os conteúdos na Reforma:** ensino e aprendizagem de conceitos, procedimentos e atitudes. Porto Alegre: Artes Médicas, 2000.

D'AMBROSIO, Ubiratan. **Educação Matemática:** da teoria à prática. 2. Ed. Campinas: Papirus, 1997.

DANTE, Luiz Roberto. **Tudo é Matemática**. São Paulo: Ática, 2004.

GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber. **Currículo de Matemática e o tema Criptografia no Ensino Médio.** Educação Matemática em Revista – RS. 2008, 51-57.

GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber; OLGIN, Clarissa de Assis. **Códigos e senhas no Ensino Básico.** Educação Matemática em Revista – RS. 2009, 41-50.

GROENWALD, Claudia Lisete Oliveira; NUNES, Giovanni da Silva. **Currículo de Matemática no Ensino Básico:** a importância do desenvolvimento dos pensamentos de alto nível. Revista Latinoamericana de Investigación en Matemática Educativa. 2007, 97-116.

GROENWALD, Claudia Lisete Oliveira; RUIZ, Lorenzo Moreno. **Formação de professores de Matemática**: uma proposta de ensino com novas tecnologias. Revista de Ciências Naturais e Exatas. ACTA – SCIENTIAE. Volume 8. Número 2. Julho/Dezembro 2006, 19 – 28.

MACHADO, Silvia Dias Alcântara et al. **Educação Matemática:** uma (nova) introdução. 2.ed. São Paulo: EDUC, 2008.

NIETO, Solange dos Santos ; LOPES, C. M. C. ; SILVA, A. F. . **Criptografia:** uma aplicação de álgebra linear. In: X Internacional Conference on Engineering and Technology Education, 2008, Peruibe - SP- Brasil. The New Technology for the Engineering and Technology Education, 2008.

OBMEP. **BANCO DE QUESTÕES**: Olimpíada Brasileira de Matemática. 2009.

PAIS, Luiz Carlos. **Didática da Matemática –** Uma análise da influência francesa. 2.ed. Belo Horizonte: Autêntica, 2005.

PANNUTI, M.R.V. Caminhos da prática pedagógica. TVE Brasil. Rio de Janeiro, p. 01- 05, jun. 2004.

PIRES, C. M. C. **Currículo de Matemática**: da organização linear à idéia de rede. São Paulo: FTD, 2000.

SECRETARIA DE EDUCAÇÃO BÁSICA. **Orientações curriculares para o ensino médio.** Brasília: Ministério da Educação, Secretaria de Educação Básica, 2006.

SILVA, Marcio Antonio da. **Currículo de Matemática no Ensino Médio: em busca de critérios para escolha e organização de conteúdos.** Tese de doutorado. Pontifícia Universidade Católica de São Paulo, 2009.

SINGH, Simon. **O Livro dos Códigos:** A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro, Record, 2003.

SHOKRANIAN, Salahoddin. **Criptografia para Iniciantes.** Brasília: UnB, 2005.

TABACOW, Luiz Samuel. Contribuições da neurociência cognitiva para a formação de professores e pedagogos. Dissertação. Campinas, 2006. Disponível em: < http://www.bibliotecadigital.puc-campinas.edu.br/tde_arquivos/3/TDE-2006-06-30T115909Z-1178/Publico/Luiz%20Tabacow.pdf> Acesso em: 18 de maio de 2009.

TAMAROZZI, Antônio Carlos. **Codificando e decifrando mensagens**. In Revista do Professor de Matemática 45, São Paulo: Sociedade Brasileira de Matemática, 2001.

TERADA, Routo. **Criptografia e a importância das suas aplicações.** Revista do Professor de Matemática (RPM). Nº 12, 1º semestre de 1988, 1-6.

ZABALA, Antoni. **A prática educativa:** como ensinar. Porto Alegre: ARTMED, 1998.

APÊNDICES

APÊNDICE A: QUESTIONÁRIO PRÉVIO

Neste apêndice apresenta-se o questionário aplicado antes do desenvolvimento das atividades didáticas.

Questionário

1) Quantos anos você tem?

2) Você exerce atividade profissional?
( ) sim ( ) não
3) Onde você trabalha?

4) Quantas horas você trabalha por dia?

5) Você já repetiu alguma série? Qual? Que disciplina você não aprovou para passar de ano?

6) Em sua opinião as aulas de Matemática motivam os alunos a buscarem novos conhecimentos?

7) Você utiliza matemática no seu dia-a-dia? Em quais situações?

8) Você considera importante estudar matemática? Por quê?

9) Como as aulas de matemática costumam ser ministradas?
( ) aula expositiva dialogada
( ) utilização de recursos didáticos
( ) trabalhos individuais ou em grupos
( ) utilizando material impresso ou mimeografado
10) Você costuma estudar além do que lhe é ensinado em sala de aula?

11) Nas aulas de matemática são utilizados desafios?
( ) sim ( ) não
12) Com que regularidade?

( ) semanalmente ( ) mensalmente ( ) trimestralmente

13) Você possui uma calculadora científica?

( ) sim ( ) não

14) Você utiliza calculadora frequentemente fora do ambiente escolar?

( ) sim ( ) não

15) Você sabe colocar uma expressão na calculadora científica e modificar somente a variável?

( ) sim ( ) não

16) Você utiliza as funções de potência e logaritmo?

( ) sim ( ) não

APÊNDICE B: QUESTIONÁRIO PÓS EXPERIMENTO

Neste apêndice apresenta-se o questionário aplicado após a resolução das atividades didáticas aplicadas.

Questionário

1) O que você achou das aulas envolvendo o tema Criptografia? Justifique.

2) Você encontrou dificuldade nos conteúdos matemáticos trabalhados? Quais conteúdos e por quê?

3) O que poderia melhorar nas atividades aplicadas? Por quê?

4) Nos desafios propostos você resolveu sozinho, com a ajuda de um familiar ou com um amigo?

5) O uso da calculadora facilitou na resolução das atividades? Por quê?

6) Que funções você não conhecia e aprendeu a utilizar na calculadora científica? Essas funções ajudaram na resolução?

APÊNDICE C: APOSTILA

Apostila confeccionada contendo as atividades didáticas da fase da experimentação.

UNIVERSIDADE LUTERANA DO BRASIL

ULBRA

DESCUBRA OS SEGREDOS DAS CODIFICAÇÕES

MESTRANDA CLARISSA DE ASSIS OLGIN

ORIENTADORA: PROFª CLAUDIA LISETE OLIVEIRA GROENWALD

Histórico da Criptografia

O nome Criptografia vem das palavras gregas *kriptós* que significa escondido, oculto e *graphein* que significa escrita (SINGH, 2003). A Criptografia é denominada de arte ou ciência de escrever em códigos (TAMAROZZI, 2001), de forma a permitir que somente o destinatário a decifre e compreenda. Ao longo da história, foram criados mecanismos de codificação, denominados códigos, cifras e senhas usados para manter o segredo das mensagens a serem enviadas.

Exemplo de atividade envolvendo descoberta são os criptogramas, onde cada letra indica um algarismo, letras iguais representam algarismos iguais, e letras diferentes representam algarismos diferentes.

Atividade 1

Descubra o valor de cada letra em cada criptograma.

a) $\begin{array}{r} A\ B \\ +\ C\ A \\ \hline A\ B\ A \end{array}$ b) $\begin{array}{r} X\ Y \\ +\ Y\ X \\ \hline X\ X\ Z \end{array}$ c) $\begin{array}{r} N\ O\ V\ E \\ +\ T\ R\ \hat{E}\ S \\ \hline D\ O\ Z\ E \end{array}$

Desafio: Encontre o valor de cada letra no Criptograma a seguir:

$\begin{array}{l|l} D\ O\ C\ E & D\ O \\ \cline{2-2} & T\ I\ O \end{array}$

Uma das primeiras formas de codificar foi o *Citale* Espartano (SINGH, 2003), que era um aparelho criptográfico militar, que consistia em um bastão de madeira, onde se enrolava uma tira de couro e se escrevia a mensagem em todo o comprimento desse bastão. Segundo o autor, para enviar a mensagem, de forma despercebida, a tira de couro era desenrolada do *Citale* e utilizada como um cinto, com a mensagem voltada para dentro. Como na tira de couro a mensagem ficava sem sentido, para decifrá-la era necessário que o receptor tivesse um *Citale* de mesmo diâmetro para enrolar a tira de couro e ler a mensagem, conforme figura 1.

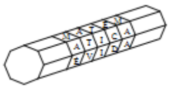
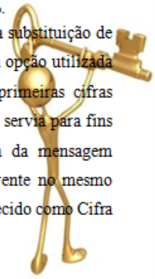


Figura 1: exemplo de *Citale* Espartano.

A cifra monoalfabética, caracterizada pela substituição de uma letra por outra ou por um símbolo, era outra opção utilizada para criptografar uma mensagem. Uma das primeiras cifras monoalfabéticas era a utilizada por Júlio César, servia para fins militares e consistia em substituir cada letra da mensagem original por outra que estivesse três casas à frente no mesmo alfabeto. Esse método de criptografia ficou conhecido como Cifra de César.



Vamos conhecer como era codificar utilizando essa cifra?

Para codificar utilizando a Cifra de César desloca-se cada letra do alfabeto original três casas a frente, conforme apresentado na figura 2:

Alfabeto Normal	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
Alfabeto Cifrado	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

Figura 2: quadro do método de substituição utilizado por Júlio César.

Fonte: Adaptado de Singh (2003, p.27)

Utilizando a figura 2 e considerando como texto original a frase "MATEMÁTICA É PARA VIDA", tem-se o seguinte texto cifrado: "PDWHPDWLFDHSDUDYLGD", de onde foram retirados os espaços entre as palavras para dificultar a decodificação.

Atividade 2

a) Decodifique a frase "d-y-l-g-h-x-p-d-s-h-f-d-g-h-w-h-d-w-u-r-t-x-h-q-d-r-s-h-u-p-l-w-h-q-v-d-l-r-v-s-r-u-l-v-v-r-f-d-q-w-h-f-k-r-u-h-g-d-q-f-h-u-l-d-h-y-l-y-d-l-q-w-h-q-v-d-p-h-q-w-h-d-q-w-h-v-t-x-h-d-f-r-u-w-l-q-d-v-h-i-h-f-k-h-h-d-s-h-f-d-w-h-u-p-l-q-h-v-h-p-d-s-o-d-x-v-r-v" utilizando a Cifra de César.

b) Codifique a frase "Não pense nos momentos difíceis como o fim do mundo, e sim como mais um obstáculo a ser superado" utilizando a Cifra de César.

Outro exemplo de Cifra de substituição monoalfabética, foi a Cifra do Chiqueiro utilizada pelos maçons livres para guardar seus segredos (SINGH, 2003). A cifra consiste em substituir uma letra por um símbolo, seguindo o padrão apresentado na figura 3.

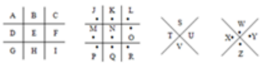


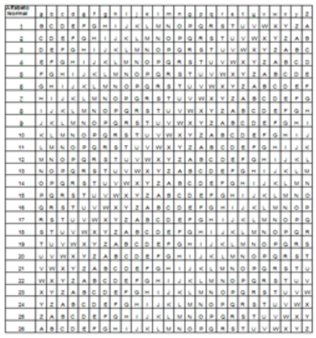
Figura 3: exemplo do padrão utilizado pela Cifra do Chiqueiro.

A codificação da Cifra do Chiqueiro é realizada encontrando a posição da letra em uma das quatro grades da figura 3 e desenhando a porção da grade que representa a letra a ser codificada, por exemplo, a letra **E** corresponde ao símbolo □.

Atividade 3

Considerando a figura 3, codifique a frase "A felicidade não está no fim da jornada, e sim em cada curva do caminho que percorremos para encontrá-la" utilizando a Cifra do Chiqueiro e envie para outro grupo decodificar.

Como a Cifra de César era de substituição de letras, facilmente decodificada por criptoanalistas por apresentar 26 chaves em potencial, a solução encontrada no século XVI, foi a cifra polialfabética, criada pelo diplomata francês Blaise Vigenère, denominada Cifra de Vigenère e que seguia o mesmo princípio da Cifra de César, porém eram utilizados 26 alfabetos cifrados para codificar e decodificar uma mensagem, conforme mostra a figura 4.



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

Figura4: Quadro de vigènere

Como os jovens apaixonados da Inglaterra vitoriana não podiam expressar seu amor publicamente, eles começaram a trocar mensagens codificadas através dos jornais, em colunas dedicadas às mensagens dos leitores. Essas colunas ficaram conhecidas como "colunas de óbito" (SINGH, 2003). Charles Babbage e seus amigos Sir Wheatstone e o barão Lyon Playfair foram os criadores da Cifra de Playfair.

A Cifra de Playfair substitui cada par de letras da mensagem a ser codificada por outro par de letras. Para codificar, primeiramente escolhe-se uma palavra-chave, por exemplo, ULBRA. Antes da cifragem, as letras do alfabeto são escritas em um quadrado 5X5, começando com a palavra chave e combinando as letras I e J em um único elemento, conforme a figura 5.

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

Figura 5: quadro da Cifra de Playfair.

A mensagem original é escrita em pares de letras, ou dígrafos. As duas letras em qualquer dígrafo devem ser diferentes, o que se consegue inserindo, por exemplo, uma letra *x* caso apareçam letras iguais ou se o número de letras for ímpar. A cifragem começa da seguinte forma: se as duas letras estiverem na mesma linha, elas são substituídas pela letra imediatamente à direita de cada uma delas, se uma delas estiver no final da linha, ela é substituída pela letra que está no começo da linha. Se ambas as letras estiverem na mesma coluna, elas serão substituídas pela letra que está imediatamente abaixo de cada uma e, neste caso, se uma das letras for a última letra da coluna, será substituída pela letra que está no topo da coluna.

Se as letras no dígrafo não estiverem nem na mesma linha, nem na mesma coluna, seguimos a seguinte regra: para cifrar a primeira letra olhe ao longo de sua linha até chegar à coluna em que está a segunda letra; a letra que estiver nesta intersecção irá substituir a primeira letra. Para cifrar a segunda letra, utilize o mesmo raciocínio.

A figura 6 apresenta um exemplo de codificação utilizando a cifra referida.

Texto original	A vida é bela
Texto original em pares	AV – ID – AE – BE – LA
Texto Codificado	UZ – PI – BG – EK – BU

Figura 6: exemplo de cifragem utilizado pela Cifra de Playfair.

Para codificar o par AV, tem-se que, como não estão na mesma linha e nem na mesma coluna, utilizar-se a regra de olhar primeiro ao longo da linha até chegar à coluna onde está a segunda letra, e a letra que estiver na intersecção irá substituir a primeira letra. Para cifrar a segunda letra, utiliza-se o mesmo raciocínio, conforme figura 7.

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

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

Figura 7: exemplo da cifragem do par AD utilizando a Cifra de Playfair.

Atividade 4

Codifique a mensagem "Podemos escolher o que semear, mas somos obrigados a colher aquilo que plantamos" de acordo com a Cifra de Playfair, utilizando o quadro da figura 5.

Em 1918, foi introduzido o ADFGVX, uma cifra de guerra que se acreditava dar maior segurança às mensagens a serem enviadas, pois se tratava de uma cifra de substituição e transposição (consiste em rearranjar as letras da mensagem, gerando um anagrama). Foi utilizada pelos alemães, que acreditavam fosse imbatível, mas o criptoanalista Georges Painvin quebrou a Cifra ADFGVX e descobriu onde os alemães atacariam (SINGH, 2003). As letras ADFGVX foram escolhidas porque quando traduzidas para os pontos e traços do código Morse diminui a possibilidade de erros durante a transmissão.

A Cifra ADFGVX para codificar utiliza uma grade 6x6, preenchida com 36 quadrados, onde se coloca as 26 letras do alfabeto e 10 algarismos. Na primeira linha e coluna colocam-se as letras A, D, F, G, V e X, conforme figura 8.

	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	O	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	0	F	Q

Figura 8: quadro da Cifra ADFGVX.

Inicia-se a codificação pegando cada letra da mensagem a ser enviada, localizando a sua posição na grade, e substitui-se pelas letras da linha e da coluna, por exemplo, **d** será substituído por **AG**. Uma mensagem codificada por esta cifra ficará conforme a figura 9.

Palavra original	Lógica
Palavra codificada	DADGGVVGFGDV

Figura 9: exemplo de codificação da Cifra ADFGVX.

Para cifrar a letra L, localiza-se sua posição na grade e se substitui pelas letras que estão na sua linha e coluna, como mostra a figura 10.

	A	D	F	G	V	X
A	8	p	3	d	1	N
D	l	t	4	o	A	H
F	7	k	b	c	5	Z
G	j	u	6	w	G	M
V	x	s	v	i	R	2
X	9	e	y	0	F	Q

l = DA

Figura 10: exemplo de codificação da Cifra ADFGVX.

De acordo com Singh (2003), com o avanço da Criptografia, Alberti foi o criador da primeira máquina criptográfica, o Disco de Cifras (figura 11). São dois discos de cobre, um maior que o outro, com as letras do alfabeto fixas ao longo dos discos, onde uma letra do texto normal se transformava em outra letra no texto cifrado.

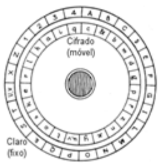


Figura 11: exemplo de Disco de Cifras.

Em 1918, o inventor Artur Scherbius e seu amigo Richard Ritter fundaram uma empresa, e um dos projetos de Artur Scherbius era substituir os sistemas criptográficos, usados na primeira guerra mundial. Então, utilizando a tecnologia do século XX, ele desenvolveu uma máquina criptográfica, que era uma versão elétrica do disco de cifras. Essa máquina recebeu o nome de Enigma. Para decifrar uma mensagem da Enigma o destinatário precisaria ter outra Enigma e uma cópia do livro de códigos, contendo o ajuste inicial dos misturadores para cada dia.

Em 1943, foi projetado o Colossus, esse computador foi utilizado durante a Segunda Guerra Mundial para decodificar os códigos criados pela Enigma. O Colossus deu início a uma era moderna da criptografia, onde os computadores eram programados com chaves de codificação muito mais complexas do que as utilizadas pela Enigma, essa nova técnica de criptografia era de uso exclusivo do governo e de militares para guardar informações.

Como as cifras de substituição sofriam constantes ataques dos criptoanalistas começou-se a utilizar os computadores. Os computadores utilizavam criptografias complexas, mas não apresentavam ainda a segurança necessária para não serem invadidos por pessoas que não deveriam tem acesso aos códigos de criptagem contidos nele. Para solucionar este problema foram criados dois algoritmos de codificação o DES (sistema de chave secreta) e RSA (sistema de chave pública).

Um dos códigos, utilizados nos dias atuais, é o "Código de verificação ISBN" (*International Standard Book Number*). Este código é escrito como quatro blocos de dígitos separados por hífens ou por espaços em branco. Lendo-se da esquerda para a direita, o primeiro bloco identifica o país, a área ou a área da língua entre os participantes, o segundo bloco identifica as editoras daquele grupo e o terceiro bloco é o número atribuído pela editora para a obra. O último bloco, consiste em um único dígito de 0 a 9 ou um X, que representa a_{10}. Sendo os 9 primeiros dígitos do ISBN: $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$. Para calcularmos o dígito verificador do código ISBN, utilizamos a seguinte fórmula: $\left[\sum_{i=1}^{9} i(a_i)\right] \text{mod} 11$. Para encontrar o dígito verificador do código ISBN 852440124-X, procede-se da seguinte forma:

X= $\left[\sum_{i=1}^{9} i(a_i)\right] \text{mod} 11$

X= $[1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9]$ mod11

X= [1.8 + 2.5 + 3.2 + 4.4 + 5.4 + 6.0 + 7.1 + 8.2 + 9.4] mod11

X= [8 + 10 + 6 + 16 + 20 + 0 + 7 + 16 + 36] mod11

X= 119 mod 11

X= 9

Assim, o dígito verificador é 9.

Atividade 5

Encontre o digito verificar do código ISBN 852130206-X.

Assim como na história a Criptografia também pode ser utilizada nas aulas de Matemática, em diversos conteúdos veja alguns exemplos.

Exemplo de codificação com função linear

Primeiro relacionamos cada letra do alfabeto a um número, conforme a figura 12:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figura 12: Valor numérico de cada letra utilizada na criptografia para função

A seguir, escolhemos uma função cifradora, que pode ser, por exemplo, a função: $f(x) = 5x + 1$

O texto a ser criptografado é: A v i d a é b e l a

A seqüência numérica é: 1 22 9 4 1 5 2 5 12 1

Criptografamos a mensagem a ser transmitida substituindo cada número na função escolhida. Sendo a seqüência numérica a imagem da função, isto é: 6 111 46 21 6 26 11 26 61 6

Para decodificar a mensagem o receptor recebe a mensagem e calcula a imagem, dos elementos utilizando a função inversa: $f^{-1}(x) = \frac{x-1}{5}$

Atividade 6

Considere a tabela, da figura 12, que para cada letra do alfabeto associa um número inteiro de 1 à 26 e, utilizando a função f(x) =

6x + 5, codifique a mensagem "O segredo não é correr atrás das borboletas. E sim cuidar do jardim para que elas venham até você".

Nesta atividade como a calculadora ajudou na resolução?

____

____

____

____

Descreva os procedimentos utilizados, na calculadora, para resolução.

____

____

____

____

____

Quais teclas você não conhecia e aprendeu a utilizar?

____

____

____

____

Resolver a atividade com a calculadora facilitou ou não? Por quê?

____

____

____

____

____

____

Exemplo de codificação com função quadrática

Primeiro relaciona-se para cada letra do alfabeto a um número, conforme a figura 13.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figura 13: Valor numérico de cada letra utilizada na criptografia para função

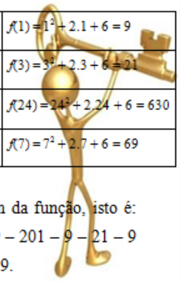
A seguir apresenta-se um exemplo: depois de relacionar para cada letra do alfabeto um número, escolhe-se uma função chave: $f(x) = x^2 + 2x + 6$

O texto a ser criptografado é: O livro é uma caixa mágica.

A seqüência numérica é: 15 – 12 – 9 – 22 – 18 – 15 – 5 – 21 – 13 – 1 – 3 – 1 – 9 – 24 – 1 – 13 – 1 – 7 – 9 – 3 – 1.

Para criptografar a mensagem a ser transmitida, calcula-se a imagem da função para cada número, da sequência numérica, na função escolhida.

$f(15) = 15^2 + 2.15 + 6 = 261$	$f(18) = 18^2 + 2.18 + 6 = 366$	$f(1) = 1^2 + 2.1 + 6 = 9$
$f(12) = 12^2 + 2.12 + 6 = 174$	$f(5) = 5^2 + 2.5 + 6 = 41$	$f(3) = 3^2 + 2.3 + 6 = 21$
$f(9) = 9^2 + 2.9 + 6 = 105$	$f(21) = 21^2 + 2.21 + 6 = 489$	$f(24) = 24^2 + 2.24 + 6 = 630$
$f(22) = 22^2 + 2.22 + 6 = 534$	$f(13) = 13^2 + 2.13 + 6 = 201$	$f(7) = 7^2 + 2.7 + 6 = 69$



Sendo a seqüência numérica a imagem da função, isto é: 261 – 174 – 105 – 534 – 366 – 261 – 41 – 489 – 201 – 9 – 21 – 9 – 105 – 630 – 9 – 201 – 9 – 69 – 105 – 21 – 9.

Para decodificar a mensagem o receptor recebe a mensagem e calcula a imagem, dos elementos utilizando a função inversa: $f^{-1}(x) = \frac{-2 \pm \sqrt{-20+4x}}{2}$, como $x \in Z$ e $1 \leq x \leq 26$, então $f^{-1}(x) = \frac{-2 + \sqrt{-20+4x}}{2} = -1 + \sqrt{-5+x}$.

Atividade 7

Codifique a mensagem "O maravilhoso da fantasia é nossa capacidade de torná-la realidade.", utilizando a função chave: $f(x) = x^2 + x + 1$.

Nesta atividade como a calculadora ajudou na resolução?

____

____

____

____

Descreva os procedimentos utilizados, na calculadora, para resolução.

____

____

____

____

____

Quais teclas você não conhecia e aprendeu a utilizar?

____

____

____

____

Resolver a atividade com a calculadora facilitou ou não? Por quê?

____

____

____

Exemplo de codificação com função exponencial e logarítmica

Primeiramente relacionamos para cada letra do alfabeto um número, que corresponderá aos valores de x na função, conforme a figura 14.

A	B	C/Ç	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

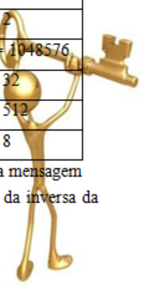
Figura 14: Quadro apresentando o valor numérico de cada letra do alfabeto.

Escolhe-se um texto e uma função exponencial que será a função cifradora, $f(x) = 2^x$, calcula-se a imagem da função para cada algarismo da sequência numérica do texto a ser codificado, conforme a figura 15.

Letra	**Sequência Numérica**	**Imagem da função $f(x) = 2^x$**
M	13	$f(x) = 2^x = 2^{13} = 8192$
A	1	$f(x) = 2^x = 2^1 = 2$
T	20	$f(x) = 2^x = 2^{20} = 1048576$
E	5	$f(x) = 2^x = 2^5 = 32$
I	9	$f(x) = 2^x = 2^9 = 512$
C	3	$f(x) = 2^x = 2^3 = 8$

Figura 15: Quadro do processo de codificação da mensagem

Para decifrar o texto, calcula-se a imagem da inversa da função codificadora, conforme figura **16**.

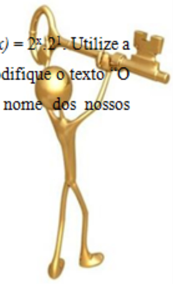


Sequência Numérica Recebida	Imagem da inversa da função codificadora $x = log_2 y$	Letra encontrada no alfabeto inicial
8192	$2^x = 8192 \rightarrow x = 13$	M
2	$2^x = 2 \rightarrow x = 1$	A
1048576	$2^x = 1048576 \rightarrow x = 20$	T
32	$2^x = 32 \rightarrow x = 5$	E
8192	$2^x = 8192 \rightarrow x = 13$	M
2	$2^x = 2 \rightarrow x = 1$	A
1048576	$2^x = 1048576 \rightarrow x = 20$	T
512	$2^x = 512 \rightarrow x = 9$	I
8	$2^x = 8 \rightarrow x = 3$	C
2	$2^x = 2 \rightarrow x = 1$	A

Figura 16: Quadro do processo de decodificação da mensagem

Atividade 8

a) Considere a figura 14 e a função cifradora $f(x) = 2^x.2^1$. Utilize a propriedade ($a^x . a^y = a^{x+y}$) na função dada e codifique o texto "O Bom combate é aquele que é travado em nome dos nossos Sonhos".



b) (Desafio) Considere a figura 14 e a função cifradora $f(x) = \log_2 x$ e codifique a mensagem "Por mais longa que seja a caminhada o mais importante é dar o primeiro passo".

Obs: Utilize ao menos três casas decimais na resolução dos cálculos.

Nesta atividade como a calculadora ajudou na resolução?

____

____

____

____

____

Descreva os procedimentos utilizados, na calculadora, para resolução.

____

____

____

____

Quais teclas você não conhecia e aprendeu a utilizar?

____

____

____

____

Resolver a atividade com a calculadora facilitou ou não? Por quê?

____

____

____

____

____

Exemplo de codificação com matrizes

Relacionamos para cada letra do alfabeto um número, conforme figura 17. Escolhemos uma matriz A e a matriz inversa A^{-1}.

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

Figura 17: Quadro apresentando o valor numérico de cada letra do alfabeto.

$$A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \qquad A^{-1} = \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix}$$

Texto Normal: F E L I C I D A D E

Seqüência Numérica: 6 5 12 9 3 9 4 1 4 5

Montamos a matriz M com a seqüência numérica da mensagem que queremos enviar.

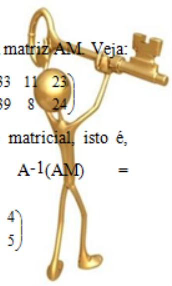
$$M = \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}$$

Para codificar a mensagem encontramos a matriz AM. Veja:

$$AM = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 27 & 51 & 33 & 11 & 23 \\ 26 & 48 & 39 & 8 & 24 \end{pmatrix}$$

Para decodificar usaremos a identidade matricial, isto é, calcularemos a matriz: $M = A^{-1}(AM) =$

$$\begin{pmatrix} 27 & 51 & 33 & 11 & 23 \\ 26 & 48 & 39 & 8 & 24 \end{pmatrix} \cdot \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix} = \begin{pmatrix} 6 & 12 & 3 & 4 & 4 \\ 5 & 9 & 9 & 1 & 5 \end{pmatrix}$$



Obs.: Se o número de letras na mensagem for impar dobra-se a última letra.

Atividade 9

Considere a tabela, da figura 17, que para cada letra do alfabeto associa um número inteiro de 1 à 26 e, que considera como zero a letra Z, e codifique a mensagem "Conhecer o caminho não é o mesmo que o percorrer!", sabendo que a matriz codificadora é $A = \begin{pmatrix} 2 & 4 \\ 1 & 5 \end{pmatrix}$.

Nesta atividade como a calculadora ajudou na resolução?

Descreva os procedimentos utilizados, na calculadora, para resolução.

Quais teclas você não conhecia e aprendeu a utilizar?

Resolver a atividade com a calculadora facilitou ou não? Por quê?