CÓDIGOS E SENHAS NO ENSINO BÁSICO[1]

Codes and Passwords in Basic Education

Claudia Lisete Oliveira Groenwald
Rosvita Fuelber Franke
Clarissa de Assis Olgin

Resumo

Criptografia é a arte de escrever mensagens cifradas que, nos dias atuais, é muito utilizada em processos eletrônicos, transmissão digital de informações, transações bancárias *on-line*, sistemas de compras eletrônicos, entre outras aplicações muito utilizadas na vida moderna. Neste artigo, apresentamos o tema criptografia utilizando códigos e senhas como motivadores e geradores de situações didáticas para o desenvolvimento do processo de ensino e aprendizagem da Matemática no ensino básico. Esse tema pode contribuir para enriquecer as aulas de Matemática, pois coloca à disposição do professor atividades e jogos de codificação e decodificação envolvendo os conteúdos, sendo um material útil para exercícios e fixação dos conteúdos matemáticos trabalhados no ensino básico. Este artigo é fruto da pesquisa "Teoria dos Números", que vem sendo desenvolvida na Universidade Luterana do Brasil, desde 2002, vinculada ao Grupo de Estudos Curriculares em Educação Matemática (GECEM).

Palavras-chave: Criptografia. Ensino e Aprendizagem. Educação Matemática.

Abstract

Cryptography is the art of writing ciphered messages which, nowadays, is way too much used in electronic processes, digital information transmission, online banking transactions, purchasing electronic systems, among other applications extremely used in modern life. In this work we present the subject cryptography in a code-password-cipher use as a didactic situation motivator and creator for the development of the Mathematics Teaching/Learning process, in Basic Education. This subject can contribute to enrich the Mathematics classes, because it disposes to the teacher codification and decoding activities and games involving the contents, being a useful material for exercises and setting of the worked mathematical contents in Basic Education. This work is based on the research "Theory of the Numbers" that has been developed at Universidade Luterana do Brasil, since 2002, tied with the Group of Curricular Studies in Mathematics Education (GECEM).

Keywords: Cryptography. Teaching and learning. Mathematics Education.

1 Introdução

O ponto de referência do processo de ensino e aprendizagem da Matemática deve ser a abordagem de assuntos de interesse do aluno, que estimulem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos. A Matemática torna-se interessante e motivadora para a aprendizagem quando

[1] Projeto inserido no convênio de pesquisa ULBRA/HP Calculadoras.

desenvolvida de forma integrada e relacionada a outros conhecimentos, trazendo o desafio de desenvolver competências e habilidades formadoras do pensamento matemático.

Este artigo visa salientar a importância da utilização de atividades didáticas adequadas para o desenvolvimento do pensamento matemático, apresentando o tema criptografia, utilizando códigos e senhas, como motivador e gerador de situações didáticas que permitam o aprofundamento da compreensão dos conceitos matemáticos, possibilitando ao aluno perceber a utilização do conhecimento matemático em situações práticas.

O trabalho é um recorte da pesquisa Teoria dos Números, que vem sendo desenvolvida na Universidade Luterana do Brasil, desde 2002, e está vinculada ao Grupo de Estudos Curriculares em Educação Matemática (GECEM).

2 Justificativa do tema

O tema Criptografia tem um papel importante nos dias atuais, pois é utilizado nos recursos humanos (auditoria eletrônica e lacre de arquivos de pessoal e pagamentos), em compras e vendas (autenticação de ordens eletrônicas de pagamento), nos processos jurídicos (transmissão digital e custódia de contratos), na automação de escritórios (autenticação e privacidade de informações), no código de verificação do ISBN, nos navegadores de Internet, entre outras situações da vida cotidiana.

Para Terada (1988), o meio de comunicação digital, controlado por computadores, trouxe flexibilidade e eficiência em gravação, recuperação e distribuição de informações, sendo utilizado em sistemas de transações bancárias *on-line,* sistema de compras a distância, saques e transferências de fundos com cartões eletrônicos. Porém, segundo o autor, à medida que se intensificam as transmissões de numerosas informações (como transferência de fundos, registros financeiros, médicos, militares etc.) através de meios eletrônicos (satélites, linhas telefônicas, fitas magnéticas etc.), as possibilidades de quebra de segurança e de privacidade aumentam, pois essas transações podem ser modificadas, gerando fraudes. A maneira mais segura de ter uma garantia de que informações transmitidas não serão copiadas, modificadas ou falsificadas é o uso da criptografia.

Esse tema pode, também, servir como um instrumento de ensino e aprendizagem no ensino básico, contribuindo para enriquecer as aulas de Matemática, pois coloca à disposição do professor atividades e jogos de codificação e decodificação, envolvendo conteúdos que são trabalhados no ensino básico. De acordo com Cantoral et al. (2000), a criptografia pode ser um elemento motivador para o processo de ensino e aprendizagem da Matemática. Para Tamarozzi (2001), exemplos elementares de processos criptográficos podem constituir, para os professores, um material útil para exercícios e fixação de conteúdos matemáticos.

As atividades apresentadas neste artigo envolvem os conteúdos relativos às funções quadrática, exponencial e logarítmica, possibilitando ao aluno observar as relações e as propriedades algébricas dessas funções, abrindo espaço para discussões sobre os conceitos de domínio, contradomínio, imagem e função inversa. Há, também, atividades envolvendo códigos e senhas, que envolvem os conceitos aritméticos desenvolvidos no ensino básico.

O desenvolvimento das atividades aqui propostas possibilita, também, o uso de calculadoras na sala de aula. Segundo Krist (1995), as calculadoras podem servir de laboratório para os alunos, pois, com esse instrumento, eles podem realizar experiências e desenvolver suas próprias ideias e estratégias. O professor de Matemática pode utilizá-la em sala de aula, de forma planejada, e, assim, ela pode tornar-se um recurso que contribui para o aprendizado dos conteúdos matemáticos, liberando tempo e energia gastos em operações repetitivas, possibilitando que o foco da aula seja a resolução de problemas. Para D'Ambrosio (2009), a calculadora permite a primazia do raciocínio qualitativo (criatividade – busca do novo) sobre o raciocínio quantitativo (rotina). Segundo Silva (1991), a calculadora deve fazer parte dos recursos que os professores devem utilizar em sala de aula, acompanhada da reflexão das suas potencialidades e de um profundo exame da Matemática que se ensina, por que ensinamos e a forma como ensinamos.

3 Criptografia e sua história

Criptografia vem do grego *krypto,* que significa secreto, oculto, e *grapho,* que significa grafia. Consiste em codificar informações usando uma chave antes que essas sejam transmitidas, e em decodificá-las, após a recepção, através de um processo de codificação. A criptografia torna possível o envio de mensagens incompreensíveis para uma terceira pessoa que, eventualmente, venha a interceptá-las, mas que poderão ser lidas pelo seu destinatário, que conhece o critério para decifrar o texto encriptado. (TERADA, 1988; TAMAROZZI, 2001; SCHEINERMAN, 2003; ZATTI; BELTRAME, 2009).

Para Tamarozzi (2001), o princípio básico da criptografia é encontrar uma transformação (função) injetiva *f* entre um conjunto de mensagens escritas em um determinado alfabeto (de letras, números ou outros símbolos) para um conjunto de mensagens codificadas. O desafio de um processo criptográfico é ocultar eficientemente os mecanismos (chaves) para a inversão de *f*, de modo que estranhos não possam fazê-lo.

Na linguagem da criptografia, os códigos são denominados cifras, as mensagens não codificadas são textos comuns e as mensagens codificadas são textos cifrados ou criptogramas. O processo de converter um texto comum em cifrado é chamado cifrar ou criptografar, e o processo inverso, de converter um texto cifrado em comum, é chamado decifrar (ZATTI; BELTRAME, 2009).

A criptografia é uma arte bastante antiga, presente desde o sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. E, o mais interessante, é que a tecnologia de criptografia não mudou muito até meados deste século.

Depois da segunda guerra mundial, com a invenção do computador, a área realmente floresceu, incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços na decifração de códigos utilizados. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

O citale espartano foi o primeiro aparelho criptográfico militar utilizado durante o século V a.C. Era um bastão de madeira em que se enrolava uma tira de couro e escrevia-se a mensagem em todo o comprimento desse bastão. 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.

Outro tipo de cifra foi utilizada por Júlio César, que consistia em substituir cada letra da mensagem original por outra que estivesse três casas à frente no mesmo alfabeto. César utilizava o alfabeto normal para escrever a mensagem e o alfabeto cifrado para codificar a mensagem que mais tarde seria enviada. Esse método de criptografia ficou conhecido como Cifra de César.

Como as cifras de substituição monoalfabéticas eram muito simples e facilmente decifradas por criptoanalistas, através da análise de frequência de cada letra, no texto cifrado, surgiu a necessidade de criar novas cifras, mais elaboradas e mais difíceis de serem descobertas. A solução encontrada, no século XVI, pelo diplomata francês Blaise Vigenère, foi uma cifra de substituição polialfabética. Um exemplo de cifra de substituição polialfabética foi a Cifra de Vigenère, que utilizava 26 alfabetos cifrados diferentes para codificar uma mensagem.

Alberti, citado por Singh (2003), foi o criador da primeira máquina criptográfica, o Disco de Cifras, um misturador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado. Seu inventor, porém, sugeriu que fosse mudada a disposição do disco durante uma mensagem, o que iria gerar uma cifra polialfabética, o que 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.

Em 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 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, computador utilizado durante a Segunda Guerra Mundial para decodificar os códigos criados pela Enigma. O Colossus deu início a uma era moderna da criptografia, em que 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, começaram a utilizar os computadores, os quais 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 neles contidos. Para solucionar esse problema, foram criados dois algoritmos de codificação: o DES (sistema de chave secreta) e o RSA (sistema de chave pública).

4 Objetivo da investigação

O objetivo geral deste trabalho foi investigar o tema criptografia e suas aplicações para o desenvolvimento de atividades didáticas aplicáveis no currículo de Matemática do ensino básico.

5 Metodologia da investigação

Este trabalho foi desenvolvido em duas etapas. A primeira, desenvolvida através de reuniões de estudos, foi um estudo exploratório em torno dos conceitos de criptografia e sua utilização na vida das pessoas. A segunda etapa foi o desenvolvimento de atividades didáticas para o ensino básico que possam ser utilizadas pelos professores de Matemática como exercícios de revisão e fixação dos conteúdos. Foi realizada uma ampla revisão bibliográfica em livros, revistas da área de Educação Matemática, anais de congressos e documentos *on-line*.

6 Atividades didáticas com o tema criptografia

6.1 Código ISBN

Será você capaz de descobrir o dígito verificador do padrão ISBN cujo código é 85-01-05598?

O código é escrito como quatro blocos de dígitos separados por hífens ou por espaços em branco. Lendo da esquerda para 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 10. Sendo a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 os 9 primeiros dígitos do ISBN, para calcular o dígito verificador usamos a seguinte fórmula: $\left[\sum_{i=1}^{9} i(a_i)\right]_{\text{mod } 11}$

Por exemplo: com o número de ISBN 852440124-X, o dígito de verificação X é calculado por:

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

6.2 Código de César

Esse método de criptografia ficou conhecido como Cifra de César. O alfabeto da Cifra de César está apresentado na Figura 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
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 1: quadro do método de substituição utilizado por Júlio César.

Utilizando a Figura 1 e considerando como texto original a frase "A vida é bela", teremos o seguinte texto cifrado "DYLGDHEOD".

Na Cifra de César, para dificultar a decodificação, caso a mensagem seja interceptada por um inimigo, é comum remover os espaços entre as letras no texto cifrado.

6.3 A Cifra de Vigenère

A Cifra de Vigenère utiliza 26 alfabetos, cifrados diferentes, para codificar uma mensagem. A Figura 2, a seguir, é conhecida como o Quadro de Vigenère.

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 2: quadro de Vigenère conforme Singh 2003.

No Quadro de Vigenère, temos 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.

Para escrever uma mensagem codificada pelo Quadro de Vigenère, o codificador e a pessoa que recebem o texto combinam uma palavra-chave, por exemplo: MATEMÁTICA.

A frase a ser codificada será OS NÚMEROS DOMINAM O MUNDO.

Para codificar a mensagem, temos que escrever a palavra-chave quantas vezes for necessário, pois cada letra da palavra MATEMÁTICA equivale a uma letra na frase, apresentada na Figura 3.

M	A	T	E	M	A	T	I	C	A	M	A	T	E	M	A	T	I	C	A	M	A
O	S	N	U	M	E	R	O	S	D	O	M	I	N	A	M	O	M	U	N	D	O

Figura 3: exemplo do uso do quadro de Vigenère.

Para codificar as letras da frase, é necessário usar a linha correspondente à letra da palavra-chave relacionada. Para M, por exemplo, usa-se o alfabeto da linha 12. Assim, o primeiro “O” da frase será traduzido como A. Para A, usamos a linha 1 e o “S” seria traduzido como “S”.

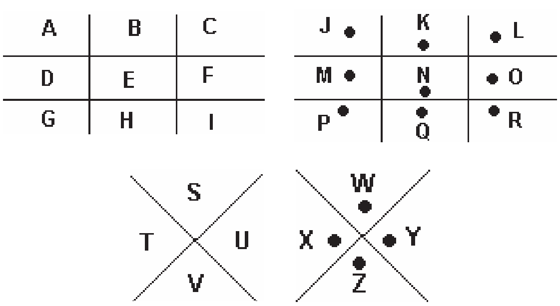
A frase codificada ficará conforme a Figura 4.

Palavra-chave	M	A	T	E	M	A	T	I	C	A	M	A	T	E	M	A	T	I	C	A	M	A
Mensagem	O	S	N	U	M	E	R	O	S	D	O	M	I	N	A	M	O	M	U	N	D	O
Mensagem codificada	A	S	G	Y	Y	E	K	W	U	D	A	M	B	R	M	M	H	U	W	N	P	O

Figura 4: exemplo do uso da cifra de Vigenère.

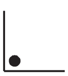
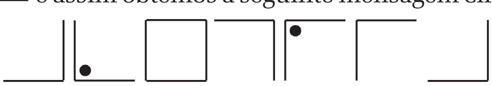
Para decodificar as letras da frase, é necessário verificar, na mesma coluna, a letra da palavra-chave e a letra da mensagem codificada. Na linha da letra codificada, a intersecção com a segunda coluna, encontramos a letra resultante. Por exemplo, na coluna da letra M, procuramos a letra A na intersecção com a segunda coluna e encontramos a letra O.

6.4 Atividades com códigos: a cifra do chiqueiro



Este código não substitui uma letra por outra, mas por um símbolo, de acordo com o seguinte padrão:

Por exemplo, para codificar a palavra ALEGRIA, localizamos a letra A no padrão acima e substituímos pelo símbolo onde ela se localiza.

Veja: , a letra L será representada pelo símbolo  e assim obtemos a seguinte mensagem cifrada: .

6.5 Atividade didática com letras que viram números

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.

Então, a verificação da hipótese verdadeira é: 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 $2\,786 + 2\,786 + 2\,786 = 8\,358$.

6.6 Código com função quadrática

Primeiro, relacionamos cada letra do alfabeto a um número, conforme a Figura 5.

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 5: valor numérico de cada letra utilizada na criptografia para função.

A seguir, escolhemos uma função cifradora, que pode ser, por exemplo, a função: $f(x) = ax^2 + bx + c$.

Escolhemos então um texto qualquer para ser criptografado: Liberdade.

A sequência numérica que corresponde ao texto é: 12 – 9 – 2 – 5 – 18 – 4 – 1 – 4 – 5.

A mensagem a ser transmitida ao receptor deve ser a sequência numérica obtida pela imagem da função.

A seguir apresentamos um exemplo: depois de relacionar para cada letra do alfabeto um número, escolhemos uma função chave: $f(x) = x^2 + 2x + 6$, com $1 \leq x \leq 26$.

O texto a ser criptografado é: O livro é uma caixa mágica.

A sequência 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, substituímos cada número da sequência numérica na função escolhida. Por exemplo: A letra *O* corresponde ao número 15, portanto, calculamos

$f(15) = 15^2 + 2.15 + 6$

$f(15) = 225 + 30 + 6$

$f(15) = 261$

Sendo a sequência 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:

$f^{-1}(x) = \dfrac{-2 \pm \sqrt{-20 + 4x}}{2}$, como $x \in Z$ e $9 \leq x \leq 734$,

então $f^{-1}(x) = \dfrac{-2 + \sqrt{-20 + 4x}}{2}$.

6.7 Código com funções exponenciais e logarítmicas

Considere a Figura 5, combine com o seu colega uma função exponencial, que será a função cifradora.

Crie uma mensagem a ser enviada: MATEMÁTICA.

Cifre essa mensagem utilizando a função escolhida.

Entregue a mensagem cifrada para que seu colega a decifre.

Seja a função $f(x) = 2^x$, calculamos a imagem da função para cada algarismo da sequência numérica, conforme a Figura 6.

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 6: quadro do processo de codificação da mensagem.

Decifrando o texto, conforme Figura 7.

Sequência numérica recebida	Imagem da inversa da função codificadora x = log2 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 7: quadro do processo de decodificação da mensagem.

Considere a Figura 5 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 e decodifique a palavra ALEGRIA.

Seja a função $f(x) = 2^x.2^1$, calculamos a imagem da função para cada algarismo da sequência numérica, conforme Figura 8.

Letra	Sequência numérica	Imagem da função $f(x) = 2^x.2^1$
A	1	$f(x) = 2^{x+1} = 2^{1+1} = 2^2 = 4$
L	12	$f(x) = 2^{x+1} = 2^{1+12} = 2^{13} = 8192$
E	5	$f(x) = 2^{x+1} = 2^{1+5} = 2^6 = 64$
G	7	$f(x) = 2^{x+1} = 2^{1+7} = 2^8 = 256$
R	18	$f(x) = 2^{x+1} = 2^{1+18} = 2^{19} = 524288$
I	9	$f(x) = 2^{x+1} = 2^{1+9} = 2^{10} = 1024$

Figura 8: quadro do processo de codificação da mensagem.

Decifrando o texto, como segue na Figura 9.

Sequência numérica recebida	Imagem da inversa da função codificadora $x + 1 = \log_2 y$	Letra encontrada no alfabeto inicial
4	$2^{x+1} = 4 \rightarrow x = 1$	A
8192	$2^{x+1} = 8192 \rightarrow x = 12$	L
64	$2^{x+1} = 64 \rightarrow x = 5$	E
256	$2^{x+1} = 256 \rightarrow x = 7$	G
524288	$2^{x+1} = 524288 \rightarrow x = 18$	R
1024	$2^{x+1} = 1024 \rightarrow x = 9$	I
4	$2^{x+1} = 4 \rightarrow x = 1$	A

Figura 9: quadro do processo de decodificação da mensagem.

Considere a Figura 5 e a função cifradora $f(x) = 3^x:3^2$

Utilize a propriedade ($a^x : a^y = a^{x-y}$) na função dada e codifique e decodifique a palavra LIBERDADE.

Seja a função $f(x) = 3^x:3^2$, calculamos a imagem da função para cada algarismo da sequência numérica, conforme Figura 10.

Letra	Sequência numérica	Imagem da função $f(x) = 3^x:3^2$
L	12	$f(x) = 3^{x-2} = 3^{12-2} = 3^{10} = 59049$
I	9	$f(x) = 3^{x-2} = 3^{9-2} = 3^7 = 2187$
B	2	$f(x) = 3^{x-2} = 3^{2-2} = 3^0 = 1$
E	5	$f(x) = 3x^{x-2} = 3^{5-2} = 3^3 = 27$
R	18	$f(x) = 3^{x-2} = 3^{18-2} = 3^{16} = 43046721$
D	4	$f(x) = 3^{x-2} = 3^{4-2} = 3^2 = 9$
A	1	$f(x) = 3^{x-2} = 3^{1-2} = 3^{-1} = \frac{1}{3}$

Figura 10: quadro do processo de codificação da mensagem.

Decifrando o texto, como observamos na Figura 11.

Sequência numérica recebida	Imagem da inversa da função codificadora $x - 2 = \log_3 y$	Letra encontrada no alfabeto inicial
59049	$3^{x-2} = 59049 \rightarrow x = 12$	L
2187	$3^{x-2} = 2187 \rightarrow x = 9$	I
1	$3^{x-2} = 1 \rightarrow x = 2$	B
27	$3^{x-2} = 27 \rightarrow x = 5$	E
43046721	$3^{x-2} = 43046721 \rightarrow x = 18$	R
9	$3^{x-2} = 9 \rightarrow x = 4$	D
$\frac{1}{3}$	$3^{x-2} = \frac{1}{3} \rightarrow x = 1$	A
9	$3^{x-2} = 9 \rightarrow x = 4$	D
27	$3^{x-2} = 27 \rightarrow x = 5$	E

Figura 11: quadro do processo de decodificação da mensagem.

Considere a Figura 5 e a função cifradora $f(x) = (2^x)^2$.

Utilize a propriedade ($(a^x)^y = a^{xy}$) na função dada e codifique e decodifique a palavra FELICIDADE.

Seja a função $f(x) = (2^x)^2$, calculamos a imagem da função para cada algarismo da sequência numérica observada na Figura 12.

Letra	Sequência numérica	Imagem da função $f(x) = (2^x)^2$
F	6	$F(x) = 2^{2x} = 2^{2.6} = 2^{12} = 4096$
E	5	$F(x) = 2^{2x} = 22.5 = 2^{10} = 1024$
L	12	$F(x) = 2^{2x} = 2^{2.12} = 2^{24} = 16777216$
I	9	$F(x) = 2^{2x} = 2^{2.9} = 2^{18} = 262144$
C	3	$F(x) = 2^{2x} = 2^{2.3} = 2^6 = 64$
D	4	$F(x) = 2^{2x} = 2^{2.4} = 2^8 = 256$
A	1	$F(x) = 2^{2x} = 2^{2.1} = 2^2 = 4$

Figura 12: quadro do processo de codificação da mensagem.

Decifrando o texto, como observamos na Figura 13.

Sequência numérica recebida	Imagem da inversa da função codificadora $2x = \log_2 y$	Letra encontrada no alfabeto inicial
4096	$2^{2x} = 4096 \rightarrow x = 6$	F
1024	$2^{2x} = 1024 \rightarrow x = 5$	E
16777216	$2^{2x} = 16777216 \rightarrow x = 12$	L
262144	$2^{2x} = 262144 \rightarrow x = 9$	I
64	$2^{2x} = 64 \rightarrow x = 3$	C
262144	$2^{2x} = 262144 \rightarrow x = 9$	I
256	$2^{2x} = 256 \rightarrow x = 4$	D
4	$2^{2x} = 4 \rightarrow x = 1$	A
256	$2^{2x} = 256 \rightarrow x = 4$	D
1024	$2^{2x} = 1024 \rightarrow x = 5$	E

Figura 13: quadro do processo de decodificação da mensagem.

Considere a Figura 5 e a função cifradora $f(x) = \log_2 x$

Crie uma mensagem a ser enviada ao seu colega.

Cifre essa mensagem, utilizando a função dada.

Entregue a mensagem cifrada juntamente com a função, para que seu colega a decifre.

Foi possível decifrar a mensagem? Por quê?

Seja a função cifradora $f(x) = \log_2 x$. Crie uma mensagem a ser enviada, por exemplo, A CASA É BELA.

A sequência numérica do texto, conforme a Figura 14, é:

A	C	A	S	A	É	B	E	L	A
1	3	1	19	1	5	2	5	12	1

Figura 14: quadro da sequência numérica do texto.

Cifre essa mensagem utilizando a função dada.

Seja a função $f(x) = \log_2 x$, calculamos a imagem da função para cada algarismo da sequência numérica. Para que o aluno chegue mais próximo de um número inteiro na resolução das atividades, optamos por trabalhar com números de até três casas decimais, após a vírgula, conforme a Figura 15.

Letra	Sequência numérica	Imagem da função $x = \log_2 y$
A	1	$x = \log_2 1 \rightarrow 2^x = 1 \rightarrow x = 0$
C	3	$x = \log_2 3 \rightarrow 2^x = 3 \rightarrow x = \frac{\log 3}{\log 2} \rightarrow x = 1{,}585$
S	19	$x = \log_2 19 \rightarrow 2^x = 19 \rightarrow x = \frac{\log 19}{\log 2} \rightarrow x = 4{,}248$
E	5	$x = \log_2 5 \rightarrow 2^x = 5 \rightarrow x = \frac{\log 5}{\log 2} \rightarrow x = 2{,}322$
B	2	$x = \log_2 2 \rightarrow 2^x = 2 \rightarrow x = 1$
L	12	$x = \log_2 12 \vee 2^x = 12 \rightarrow x = \frac{\log 12}{\log 2} \rightarrow x = 3{,}585$

Figura 15: processo de codificação da mensagem.

Entregue a mensagem cifrada juntamente com a função, para que seu colega a decifre.

Decifrando o texto, conforme Figura 16.

Sequência numérica recebida	Imagem da inversa da função codificadora $x = 2^y$	Letra encontrada no alfabeto inicial
0	$2^0 \rightarrow x \cong 1$	A
1,585	$2^{1,585} \rightarrow x \cong 3$	C
4,248	$2^{4,248} \rightarrow x \cong 19$	S
2,322	$2^{2,322} \rightarrow x \cong 5$	E
1	$2^1 \rightarrow x \cong 2$	B
3,585	$2^{3,585} \rightarrow x \cong 12$	L

Figura 16: processo de decodificação da mensagem.

6.8 Atividade de código

Qual é o número de telefone com sete dígitos em que todos os dígitos são distintos e, formando arranjos de três dígitos seguidos, resulta em um número divisível por 17?

Para resolver essa atividade, escrevemos as cifras dos números com as 7 primeiras letras do alfabeto: A, B, C, D, E, F, G. A seguir, escreveremos todos os múltiplos de 17 que possuem 2 e 3 dígitos, conforme Figura 17.

017	102	204	306	408	510	612	714	816	901
034	119	221	323	425	527	629	731	833	918
051	136	238	340	442	544	646	748	850	935
068	153	255	357	459	561	663	765	865	952
085	170	272	374	476	574	680	782	884	969
	187	289	391	493	595	697	799		986

Figura 17: quadro dos divisores de 17 com três algarismos.

Eliminamos os números que têm dois dígitos iguais, que são: 119, 221, 255, 272, 323, 442, 544, 595, 646, 663, 799, 833, 884, 969.

Como ABC não pode começar por zero, é possível eliminar os números 037, 034, 051, 068, 085.

Eliminamos, também, os números 102, 136, 153, 170, 187, 204, 238, 289, pois os dígitos ABC não podem ser da forma 02d.

Concluímos que B não pode ser nenhum dos números: 2, 3, 5, 7, 8, 0, mas pode ser: 1, 4, 6, 9. Listando todos os números que tenham como B 1, 4, 6 e 9, temos: 510, 612, 714, 816, 918, 340, 748, 561, 867, 391, 493, 697.

Quando chegamos ao número 306, podemos utilizar como dígito "D" o número 8, porque 068 aparece na lista. Podemos continuar utilizando como dígito "E" o número 0, porque 680 é múltiplo de 17, mas não serve, porque os dígitos seriam 30680, que repete o 0.

Formando a lista dos números restantes, tirando os números que formam a lista ABC, temos: 102, 136, 153, 170, 187, 204, 238, 289, 306, 357, 374, 408, 425, 459, 476, 527, 578, 629, 680, 731, 765, 782, 850, 901, 935, 952 e 986.

Concluímos, então, que o número de telefone com 7 dígitos é 4935782.

Porque: 493→935 resulta em 4935;

4935→357 resulta em 49357;

49357→578 resulta em 493578;

493578→782 resulta em **4935782**.

Conclusão

As atividades apresentadas neste artigo são sugestões que o professor pode utilizar para revisar, exercitar e aprofundar os conteúdos desenvolvidos no ensino médio (funções quadrática, exponencial e logarítmica) e conceitos de aritmética básica, bem como uma oportunidade de incentivar o desenvolvimento de estratégias de resolução de problemas (sistematizar os dados relevantes no problema, formular hipóteses, prever resultados, analisar as hipóteses levantadas e revisar os resultados).

Outro ponto importante a ser ressaltado é a utilização da calculadora na sala de aula, pois as atividades com exponencial e logaritmo apresentam cálculos longos e desnecessários de serem realizados sem o uso de calculadora. É uma oportunidade de incentivar a utilização desse recurso desenvolvendo atividades didáticas que incentivam o seu uso. Smole e Diniz (2004) destacam que a utilização da calculadora permite aos alunos ganharem mais confiança para trabalhar com problemas e buscarem novas experiências de aprendizagem.

Referências

CANTORAL, Ricardo et al. **Desarrollo del pensamiento matemático.** México: Trillas, 2000.

D'AMBROSIO, Ubiratan. **O uso da calculadora**. Disponível em: www.ima.mat.br/ubi/pdf/uda_006.pdf. Acesso em 26 ago. 2009.

KRIST, Betty J. Logaritmos, Calculadoras e o Ensino de Álgebra Intermediária. In: COXFORD, A. F.; SHULTE, A. P. **As ideias da álgebra.** São Paulo: Atual, 1995.

SCHEINERMAN, Edward R. **Matemática discreta:** uma introdução. São Paulo: Thompson, 2003.

SILVA, A. V. **A calculadora no percurso de formação de professores de Matemática.** Portugal: APM, 1991.

SINGH, Simon. **O livro dos códigos:** a ciência do sigilo – do Antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2003.

SMOLE, Kátia Stocco; DINIZ, Maria Ignez. **Matemática – Ensino médio**. 4.ed. São Paulo: Saraiva, 2004, v.1.

TAMAROZZI, Antônio Carlos. Codificando e decifrando mensagens. **Revista do Professor de Matemática (RPM)**, São Paulo, n.45, 41-43, 2001.

TERADA, Routo. Criptografia e a importância das suas aplicações. **Revista do Professor de Matemática (RPM),** São Paulo, n.12, 1-6, 1988.

ZATTI, Sandra Beatriz; BELTRAME, Ana Maria. **A presença da álgebra linear e da teoria dos números na criptografia**. Disponível em: <*www.unifra.br/eventos/.../2006/matematica.htm*> Acesso 26 ago. 2009.

Claudia Lisete Oliveira Groenwald – Dra. em Ciências da Educação pela Pontifícia de Salamanca (Espanha) e professora do curso de Matemática e do Programa de Pós-Graduação em Ensino e Ciências e Matemática da Universidade Luterana do Brasil. E-mail: claudiag@ulbra.br

Rosvita Fuelber Franke – Mestre em Matemática pela UFRGS e professora do curso de Matemática da Universidade Luterana do Brasil. E-mail: rosvitafranke@ig.com.br

Clarissa de Assis Olgin – Formada em Matemática pela Universidade Luterana do Brasil, mestranda do Programa de Pós-Graduação em Ensino de Ciências e Matemática da ULBRA e professora da E. E. de Ensino Fundamental, no Bairro Santo Afonso. E-mail: clarissa_olgin@yahoo.com.br

RECEBIDO em: 02/07/2009
CONCLUÍDO em: 20/10/2009