MATEMÁTICA discreta

Maria Regina Carvalho Macieira Lopes
Jotair Kwiatkowski

Caros alunos

Esse ebook é um pdf interativo. Para conseguir acessar todos os seus recursos, é recomendada a utilização do programa *Adobe Reader 11*.

Caso não tenha o programa instalado em seu computador, segue o link para download:

http://get.adobe.com/br/reader/

Para conseguir acessar os outros materiais como vídeos e sites, é necessário também a conexão com a internet.

O menu interativo leva-os aos diversos capítulos desse ebook, enquanto a barra superior ou inferior pode lhe redirecionar ao índice ou às páginas anteriores e posteriores.

Nesse pdf, o professor da disciplina, através de textos próprios ou de outros autores, tece comentários, disponibiliza links, vídeos e outros materiais que complementarão o seu estudo.

Para acessar esse material e utilizar o arquivo de maneira completa, explore seus elementos, clicando em botões como flechas, linhas, caixas de texto, círculos, palavras em destaque e descubra, através dessa interação, que o conhecimento está disponível nas mais diversas ferramentas.

Boa leitura!

Índice

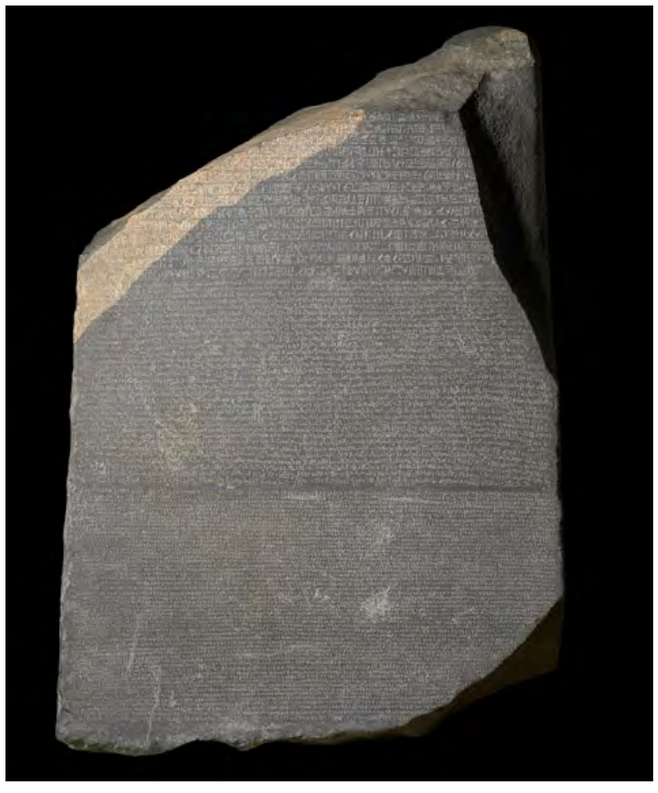
Apresentação

A criptografia é a ciência de codificar mensagens. Com relação aos conteúdos do ensino médio, à criptografia estão relacionados os assuntos: análise combinatória, função injetora e sobrejetora, função inversa e inversão de matrizes, entre outros. Apesar de ser utilizada atualmente em sistemas da *Web*, transações financeiras e comunicação, a criptografia é tão antiga quanto a escrita. Foi depois da Segunda Guerra Mundial que algoritmos complexos foram desenvolvidos para cifrar/decifrar códigos, formando a base do que hoje chamamos de Ciência da Computação. Neste *e-book*, inicialmente será apresentado um breve histórico da criptografia e, na sequência, sugestões de atividades para sala de aula, incluindo a utilização do *software* livre GeoGebra.

Espero que aproveitem este material! Bom curso a todos!

Informações históricas

Figura 1: Pedra de Roseta



Há relatos de aplicação da criptografia em hieróglifos egípcios que datam de cerca de 1900 A.C. No Museu Britânico está a Pedra de Roseta, de basalto negro, pesando cerca de ¾ de tonelada, encontrada pelo exército de Napoleão em 1799 na província egípcia de Al-Buhaira. Somente depois de 23 anos de sua descoberta o código foi decifrado pelo francês Jean-François Campollion. A mensagem foi escrita na pedra em três colunas nas seguintes línguas: grego, hieróglifos e demótico. O texto foi escrito por sacerdotes egípcios e trata de elogios ao faraó Ptolomeu V Epifânio pela isenção de impostos. No texto também constam instruções de como compartilhar a mensagem.

Os gregos antigos usavam o Bastão de Licurgo ou scytalae para transmitir mensagens em suas campanhas militares em V a.C . A citala era um bastão de madeira no qual se enrolava uma tira de couro com a mensagem codificada. A tira era enviada ao destinatário que, para decodificar a mensagem, enrolava a tira de couro em um citale de diâmetro igual ao original.

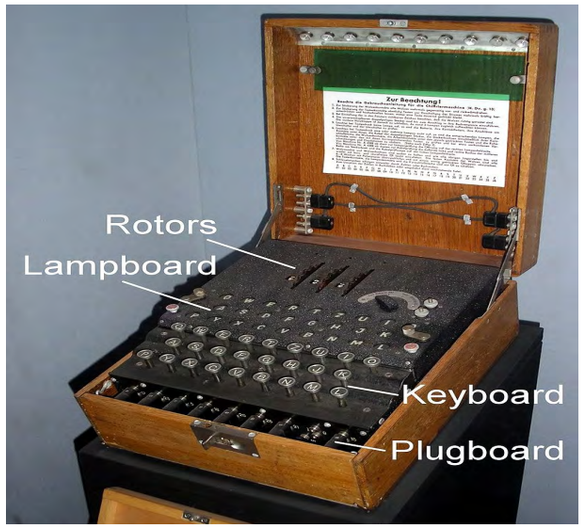
Figura 2: Bastão de Licurgo

Fonte: Wikimedia

Notas
(clique para abrir)

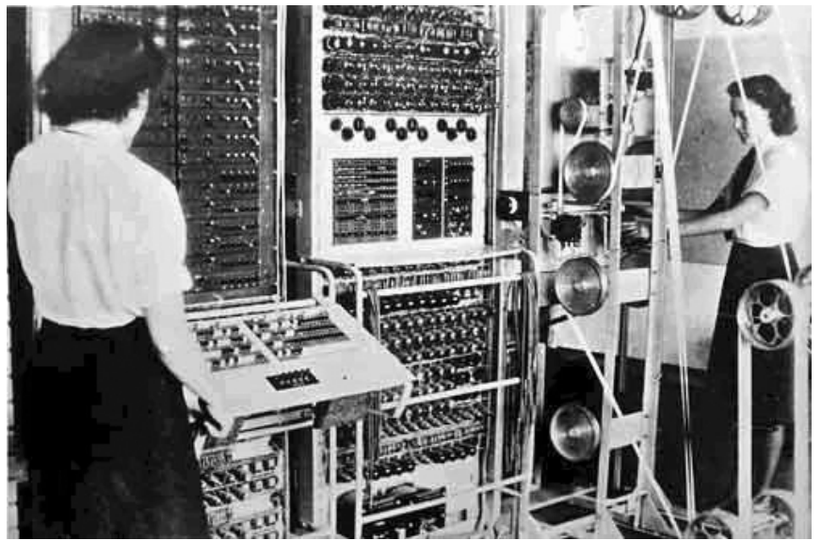
Na Segunda Guerra Mundial, os alemães criaram a máquina de criptografar chamada Enigma, com um sextilhão de possibilidades de senhas. Alan Turing e sua equipe criaram a máquina Colossus, com a finalidade de decifrar essas mensagens. Essa máquina é considerada a precursora do computador e, por isso, Alan Turing é considerado o pai da Computação.

Figura 2: Máquina Enigma



Fonte: Wikipedia

Figura 3: Máquina Colossus



Fonte: Wikipedia

Notas
(clique para abrir)

Até a década de 70 as cifras eram simétricas, isto é, a chave usada para criptografar era a mesma chave para decodificar. Recentemente, com o avanço da ciência da computação, começaram a ser utilizada duas chaves: a pública para criptografar e a privada para decodificar. Atualmente, a criptografia é usada na web na proteção de transações financeiras, segurança da informação e da comunicação.

No Brasil, o órgão responsável por criar meios criptográficos de proteção e do sigilo das comunicações do governo brasileiro é o Centro de Pesquisa e Desenvolvimento para Segurança das Comunicações (CEPESC), vinculado à Agência Brasileira de Inteligência.

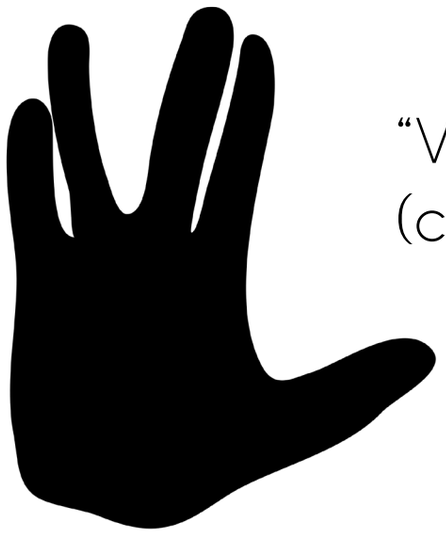
Informações históricas

A criptografia, por ser um assunto intrigante, pode ser uma via didática para o estudo de funções e matrizes inversas. Vejamos alguns exemplos:

1) FUNÇÃO AFIM

Cifrar mensagens é permutar números por meio de uma regra f. Essa regra, pode, por exemplo ser representada por uma função afim $f(x) = ax + b$

Vamos codificar a mensagem



"VIDA LONGA E PRÓSPERA"
(capitão Kirk)

Notas
(clique para abrir)

Usando a tabela 1

Tabela 1: Associação de números às letras do alfabeto

*	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

e a função de $f(x)=3x-2$, fica, conforme tabela 2:

Tabela 1: Associação de números às letras do alfabeto

Mensagem original	V	I	D	A	*	L	O	N	G	A	*	E	*	P	R	Ó	S	P	E	R	A
Associação à tabela 1	22	9	4	1	0	12	15	14	7	1	0	5	0	16	18	17	19	16	5	18	1
Mensagem codificada	64	25	10	1	-2	34	43	40	19	1	-2	13	-2	46	52	49	55	46	13	52	1

O destinatário, ao recebê-la, deverá usar a função inversa para decodificá-la:

$$f(x)=\frac{x+2}{3}$$

Notas
(clique para abrir)

Pergunta: Será que toda função tem inversa?

Definição 1: Uma função $f : x \rightarrow y$ que é injetora e sobrejetora é dita uma bijeção. Se f é uma bijeção, então tem inversa f^{-1}

2) MATRIZ INVERSA

Para mesma mensagem: "VIDA LONGA E PRÓSPERA", usando a associação da tabela 1, podemos montar a matriz M em colunas, completando com zeros, se necessário:

$$M = \begin{pmatrix} 22 & 4 & 0 & 15 & 7 & 0 & 0 & 18 & 19 & 5 & 1 \\ 9 & 1 & 12 & 14 & 1 & 5 & 16 & 17 & 16 & 18 & 0 \end{pmatrix}$$

Combinamos previamente com o destinatário que usaremos a matriz chave para codificar:

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

Notas
(clique para abrir)

A matriz encriptada A*M é:

$$AM=\begin{pmatrix}40 & 6 & 24 & 43 & 9 & 10 & 32 & 52 & 51 & 41 & 1\\ 31 & 5 & 12 & 29 & 8 & 5 & 16 & 35 & 35 & 23 & 1\end{pmatrix}$$

O remetente transmitirá a mensagem:

40 31 6 5 24 12 43 29 9 8 19 5 32 16 52 35 51 35 41 23 1 1

O destinatário deve calcular a inversa da matriz A (note que ele conhece a matriz A):

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

e, para recuperar a mensagem original, fará a operação:

$$M=A^{-1}(AM)$$

Pergunta: Será que toda matriz tem inversa?

Uma condição necessária e suficiente para que a matriz tenha inversa é que seu determinante seja diferente de zero.

Notas
(clique para abrir)

Atividades no GeoGebra

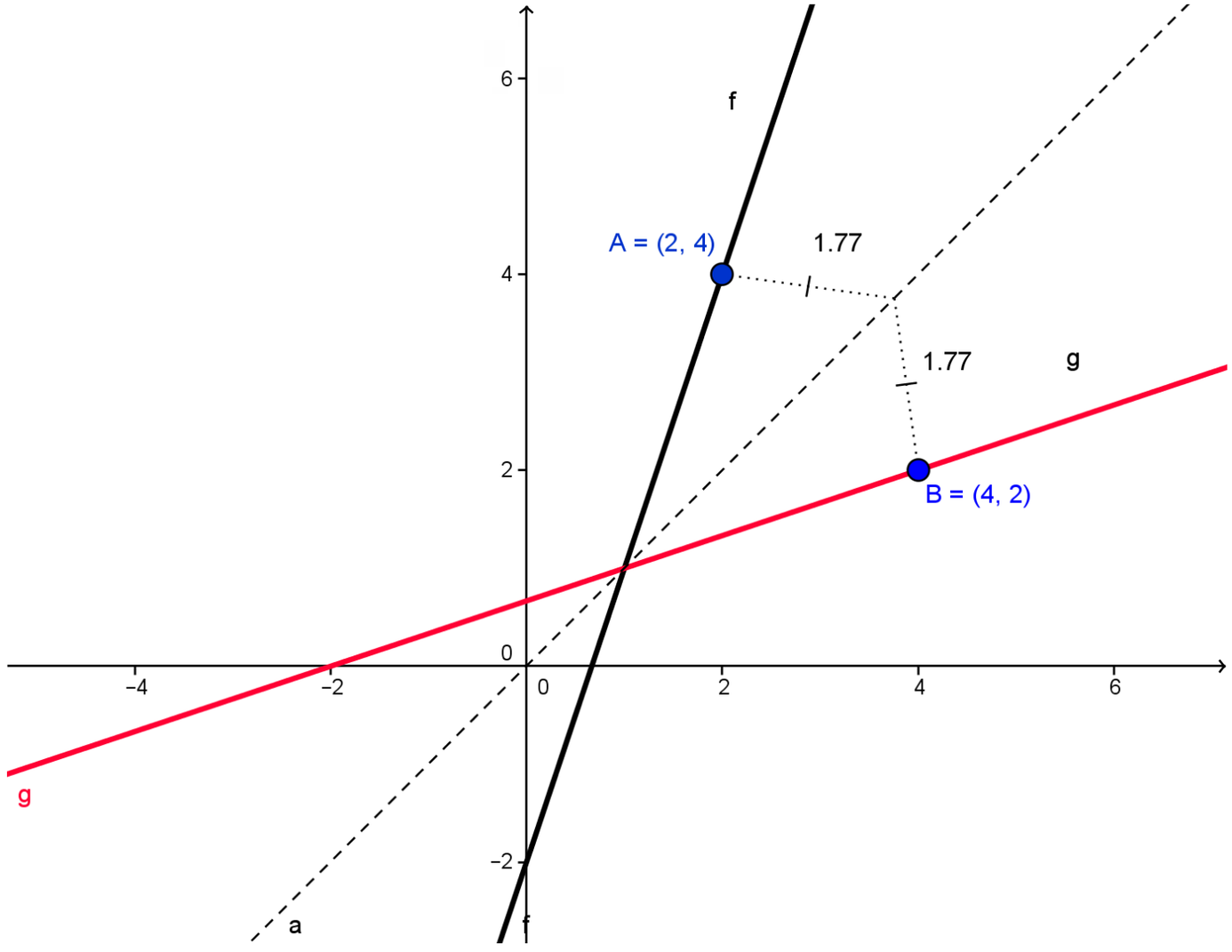
Criado por Markus Hohenwarter, o GeoGebra é um software livre de geometria dinâmica e álgebra desenvolvido para o ensino e aprendizagem da matemática. O software possui recursos para desenvolver atividades desde a educação básica até o nível universitário. No GeoGebra podem ser construídos gráficos, tabelas, textos, cálculos simbólicos, entre outros. Escrito em JAVA e disponível em português é multiplataforma, podendo ser instalado em computadores com Windows, Linux ou Mac OS.

FUNÇÕES INVERSAS

No GeoGebra podemos construir o gráfico das funções $f(x)=3x-2$ e a inversa $g(x)=f^{-1}(x)=\frac{x+2}{3}$

Na janela de álgebra digitamos a função f e a função inversa que chamamos de g. Com o ponteiro sobre o gráfico e o botão direito, podemos mudar as “propriedades” dos gráficos como a cor e espessura da linha.

Figura 4 – Função inversa construída no GeoGebra



Fonte: Autoria Própria

Notas
(clique para abrir)

Observe que foi construído o gráfico $y = x$ (identidade).

Os pontos $A(2,4) \in Graf_f$ e $B(4,2) \in Graf_g$

são simétricos em relação à reta . Geometricamente, comprovamos pelo cálculo das distâncias apresentadas na figura 4.

Importante: Se uma função f admite uma inversa g, então g também admite uma inversa que é a própria f. Nesse caso, g é denominada a função inversa de f e, portanto, f é a inversa de g. Então,

$$(f \circ g)(x) = (g \circ f)(x) = x$$

No nosso exemplo,

$$f(g(x)) = 3\left(\frac{x+2}{3}\right) - 2 = x$$

$$g(f(x)) = \frac{(3x-2)+2}{3} = x$$

Notas
(clique para abrir)

MATRIZ INVERSA

A introdução de matrizes no GeoGebra é feita pela janela de entrada. A matriz

$$B=\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\end{pmatrix}$$

deve ser digitada na janela de entrada como:

$$B=\{\{1,2,3\},\{4,5,6\}\}$$

Voltando ao nosso exemplo da codificação da mensagem: “VIDA LONGA E PRÓSPERA” na qual

$$M=\begin{pmatrix}22 & 4 & 0 & 15 & 7 & 0 & 0 & 18 & 19 & 5 & 1\\ 9 & 1 & 12 & 14 & 1 & 5 & 16 & 17 & 16 & 18 & 0\end{pmatrix} \quad \text{e} \quad A=\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}$$

introduzimos essa duas matrizes no GeoGebra tal que:

$$M=\{\{22,4,0,15,7,0,0,18,19,5,1\},\{9,1,12,14,15,16,17,16,18,0\}\}$$

$$A=\{\{1,1\},\{2,1\}\}$$

Notas
(clique para abrir)

Na sequência, na janela de entrada, fazemos a multiplicação

$$AM = A * M$$

Pergunta: A matriz A tem inversa?

Com o comando Determinante [A] calculamos o **determinante (D)** da matriz.

Nesse caso:

$D = -1 \neq 0$ de onde concluímos que a matriz tem inversa.

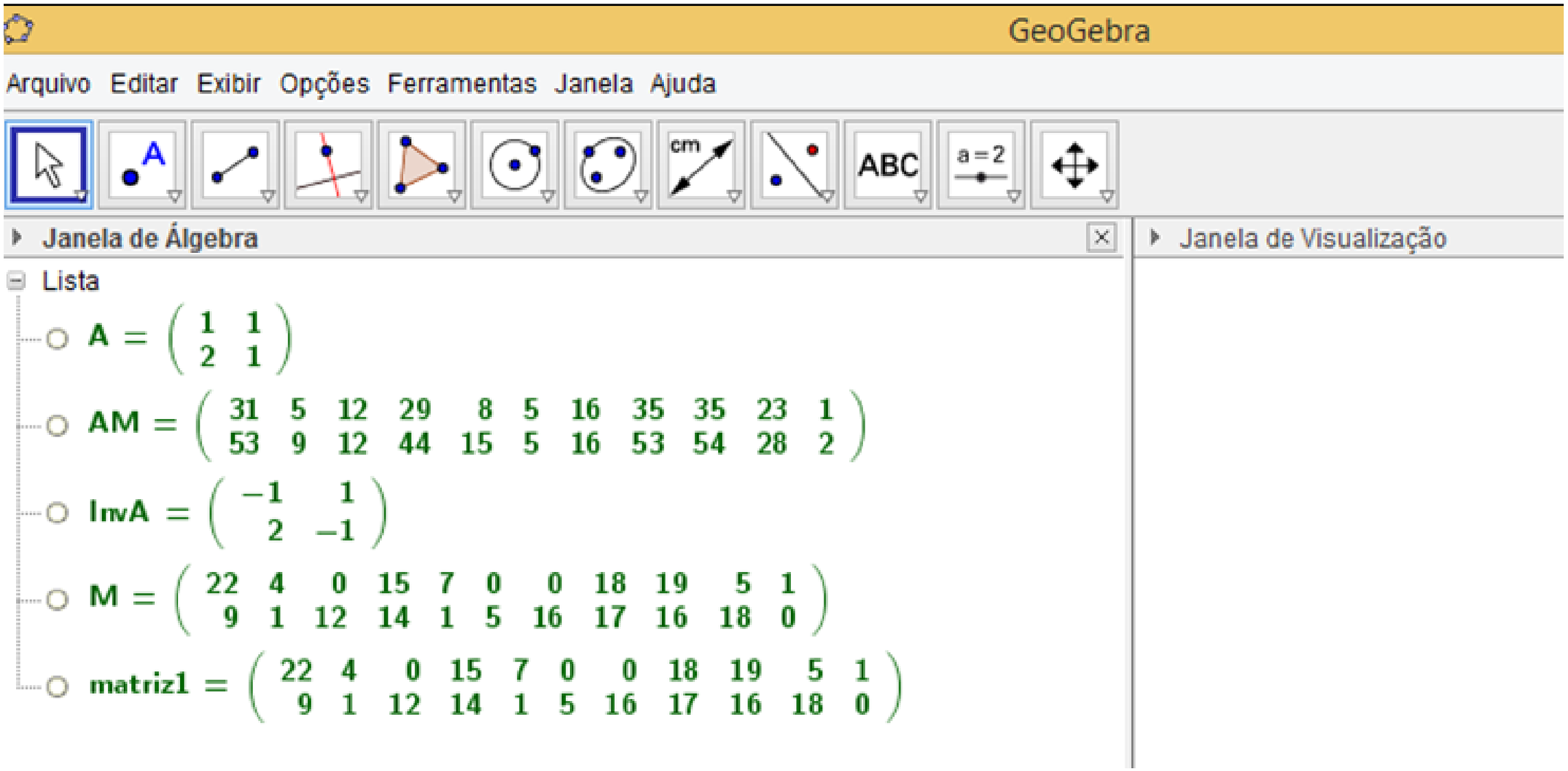
Calculamos a inversa de A com o comando **MatrizInversa [A]** que chamamos de **Inv**.

Para decodificar, fazemos a operação

$$M = Inv * (AM)$$

Na figura 5 são apresentadas essas matrizes. Observe que matriz1 é a matriz M resultante da decodificação.

Figura 5 – Matrizes no GeoGebra



Fonte: Autoria Própria

Notas
(clique para abrir)

Podemos trabalhar ainda no GeoGebra questões:

1) Qual o resultado de $A * InvA$?

2) É possível encontrar a inversa da matriz $A=\begin{pmatrix}1 & 3 & 3\\ 4 & 5 & 6\end{pmatrix}$? Por quê?

Pergunta: E se, por uma distração, escolhêssemos uma matriz com $D=0$ o que aconteceria na codificação?

Tomando a matriz, por exemplo, $T=\begin{pmatrix}1 & 2\\ 3 & 6\end{pmatrix}$ como chave para codificar a matriz $W=\begin{pmatrix}2 & 4\\ 4 & 3\end{pmatrix}$ ao fazer $T*W=\begin{pmatrix}10 & 10\\ 30 & 30\end{pmatrix}$ o que não é desejável.

Nesse caso, dois elementos do domínio têm a mesma imagem e a transformação obtida pela multiplicação da matriz W por uma matriz com determinante diferente de zero **não é injetora.**

Notas
(clique para abrir)

Considerações Finais

O estudo da criptografia é muito interessante e pode ser utilizado como aplicação para vários conteúdos do Ensino Médio. Há, além, do experimentos e vídeos apresentados neste e-book, materiais relacionados à criptografia e análise combinatória. Esse assunto pode resultar em um excelente projeto de pesquisa!

Obrigada pela consulta ao material,

Prof. Maria Regina C. M. Lopes

Prof. Jotair Kwiatkowski Jr

Notas
(clique para abrir)

Referências

BOLDRINI, L., ALVES, J. A. R. Álgebra Linear, Ed. Harbra 3ª Edição, São Paulo, 1980.

COUTINHO, S. C., Números Inteiros e. Criptografia RSA, IMPA/SBM. Rio de. Janeiro: 2000

LOUREIRO, F., O. Tópicos de Criptografia para o Ensino Médio. 2014. 43f. Dissertação (Mestrado em Matemática). Centro de Ciências e Tecnologia. Universidade Estadual no Norte Fluminense Darcy Ribeiro. Rio de Janeiro, 2014.

Recursos educacionais multimídia para a matemática do ensino médio. UNICAMP. Disponível em http://m3.ime.unicamp.br/recursos

TAMAROZZI, A C., Codificando e decifrando mensagens. In Revista do Professor de Matemática 45, São Paulo: Sociedade Brasileira de Matemática, 2001.

WIKIPEDIA. Colossus. In: Wikipedia: a enciclopedia livre. Disponível em: < https://pt.wikipedia.org/wiki/Colossus> Acesso em: 10 out 2015

WIKIPEDIA. Enigma machine. In: Wikipedia: a enciclopedia livre. Disponível em: < https://en.wikipedia.org/wiki/Enigma_machine> Acesso em: 10 out 2015

WIKIPEDIA. Roseta StonePedra de Roseta In: Wikipedia: a enciclopedia livre. Disponível em: <https://en.wikipedia.org/wiki/Rosetta_Stone#/media/File:Rosetta_Stone.JPG> Acesso em: 10 out 2015

WIKIPEDIA. Skytale. In: Wikipedia: a enciclopedia livre. Disponível em: <: https://commons.wikimedia.org/wiki/File:Skytale.png> Acesso em: 10 out 2015