A Matemática dos Códigos[1]

Nalva A. M. Batista **Astride G. C. Giraldello***
Instituto de Ciências Exatas, UNIFAL-MG
37130-000, Alfenas, MG
E-mail: nalvaalf@hotmail.com, tidegiraldello@hotmail.com

Andréa Cardoso
Instituto de Ciências Exatas, UNIFAL-MG
37130-000, Alfenas, MG
E-mail: andreac74@uol.com.br

RESUMO

A ideia de se compreender a Matemática como uma disciplina em que o aprendizado é resultante de um processo de investigação e resolução de problemas, é compartilhada por [2] que atesta, ainda, a importância desta compreensão por parte dos professores.

A metodologia utilizada na aplicação de certos conteúdos, muitas vezes, acarreta um distanciamento deste com sua aplicação, tornando a matemática cada vez mais abstrata para os alunos. Esta metodologia deve ser substituída por uma que propicie ao aluno compreender os fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, como estabelece [1]. Assim se torna necessário haver uma transposição didática, que de acordo com [3], é uma transformação do conhecimento científico em conhecimento escolar. Porém, na formação de professores, muitas vezes as disciplinas são ministradas isoladamente, sem correlação com outras disciplinas ou com suas aplicações ou ainda sem evidenciar quais transposições poderiam ser feitas para que o futuro professor possa se aproveitar e se apropriar deste conhecimento.

O trabalho aqui exposto foi desenvolvido na disciplina de Álgebra Linear, em um curso de formação de professores, com o intuito de apresentar a estes professores uma ligação entre o conteúdo da matemática acadêmica com a matemática escolar, a partir de assuntos da atualidade como é o caso da criptografia.

A importância do tema criptografia é evidenciada pela necessidade de codificar e decodificar mensagens de forma rápida e segura devido à demanda resultante do avanço tecnológico. Em tempos de celulares e internet a palavra criptografia provavelmente não é estranha à maioria das pessoas, entretanto poucos compreendem as teorias matemáticas que garantem a segurança e o sigilo das informações na rede mundial de comunicação. Civilizações antigas já utilizavam textos cifrados para garantir o sigilo das mensagens, e desde então a criptografia restringiu-se ao ambiente militar sendo considerada uma arma de guerra. Um exemplo que entrou para a história foi a Enigma, uma máquina criptográfica eletromecânica de fundamental importância para as comunicações militares e de inteligência da Alemanha nazista na Segunda Guerra Mundial.

A criptografia, que é conhecida como "a arte dos códigos secretos", estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la, o que pode vir a ser um estímulo para os alunos do ensino médio no estudo de matrizes.

Neste texto, será apresentada uma breve abordagem de classe de sistemas poligráficos chamados Cifras de Hill, que são baseados em Transformações Matriciais e Aritmética Modular. O nome é em referência a Lester S. Hill, que introduziu estes sistemas poligráficos.

O sistema consiste em fazer m combinações lineares dos $\boldsymbol{n}$ caracteres do texto comum, produzindo os $\boldsymbol{m}$ caracteres do texto cifrado. Para a codificação foi utilizado o $Z_{36,}$ englobando as 26 letras do alfabeto e os números naturais no intervalo [0; 9], como mostra a tabela a seguir:

[1]O presente trabalho foi realizado com apoio financeiro da Fundação de Amparo a Pesquisa do Estado de Minas Gerais (FAPEMIG) e do Programa Institucional de Bolsa de Iniciação à Docência (PIBID), da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Brasil.

* Bolsista de Iniciação à docência PIBID/CAPES.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
S	T	U	V	X	Y	W	Z	0	1	2	3	4	5	6	7	8	9
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	0

A partir de uma matriz codificadora, que deverá possuir inversa no Z_{36}, é possível obter a mensagem codificada através do seguinte procedimento: as letras do texto comum são agrupadas em ternos, no caso de um terno incompleto devem ser adicionadas letras fictícias; cada letra do texto comum será substituída pelo seu valor numérico correspondente; os ternos resultantes são dispostos em um vetor coluna; ao multiplicar o vetor coluna pela matriz codificadora obtém-se o correspondente vetor cifrado; por fim, converte-se cada vetor cifrado em seu equivalente alfabético. A matriz inversa serve para a decodificação da mensagem. Quando ocorrer inteiros maiores do que 35 basta substituir pelo seu resto na divisão por 36. Esta técnica é chamada de Aritmética Modular.

Em um curso de formação de professores, as disciplinas podem ser oferecidas sem que haja qualquer ligação entre os conteúdos e suas aplicações, porém quando as disciplinas evidenciam estas aplicações, o curso se torna mais proveitoso para o aluno que vivencia a ligação entre a matemática acadêmica e a matemática escolar. Para o grupo que desenvolveu este trabalho, além do aprendizado na disciplina, outro ganho foi o conhecimento cultural de um assunto que, no exercício da profissão, poderá despertar o interesse em seus futuros alunos.

Embora o método das cifras de Hill tenha sido desenvolvido no século XX, sua ideia é relativamente simples e fornece uma excelente oportunidade para que o professor do ensino médio trabalhe os conceitos de Matrizes, Operações Matriciais, Determinantes, Transformações Lineares, Divisibilidade, Máximo Divisor Comum e Algoritmo da Divisão, além de mostrar uma bela aplicação envolvendo Matrizes e Determinantes que são alvos de questionamentos sobre a importância destes por parte dos alunos. Assim, se torna possível apresentar uma matemática desfragmentada, passível de proporcionar ao professor em formação estabelecer significação para os conteúdos aprendidos.

Palavras-chave*: Matrizes, Criptografia, Formação de Professores.*

Referências

[1] Brasil, "Lei de Diretrizes e Bases da Educação Nacional". Lei Nº. 9.394, de 20 de dezembro de 1996. Brasília, 23 de dezembro de 1996.

[2] B. S. D'Ambrósio, Formação de professores de matemática para o século XXI: o grande desafio, Campinas. Pro - Posições, vol. 4 nº. 1 [10], pp. 35-41, (1993).

[3] E. T. Menezes, T. H. Santos, "Transposição didática" (verbete). Dicionário Interativo da Educação Brasileira - EducaBrasil. São Paulo: Midiamix Editora, 2002. Disponível em: http://www.educabrasil.com.br/eb/dic/dicionario.asp?id=23, acessado em: 25/2/2014.

