CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA

GT 02 – Educação Matemática no Ensino Médio e Superior

Radael de Souza Parolin – UNIJUÍ – radaelsp@gmail.com
Fernando Tosini –UNIJUÍ – fernandotosini@hotmail.com

Resumo

A educação matemática enfrenta diversos desafios na busca de aliar o interesse discente e a formação do cidadão, partindo do pressuposto que a educação se concretiza nesta relação. Portanto, aproximar a realidade da linguagem matemática é o foco de estratégias educacionais, para que os alunos se tornem cidadãos conscientes com conhecimentos matemáticos, e através destes tenham criticidade matemática e possam incorporar estes conhecimentos em suas atividades humanas, sejam elas simplesmente corriqueiras do dia-a-dia, ou de âmbito profissional.

Nesta perspectiva, as aplicações exploram os conhecimentos matemáticos no contexto da realidade do aluno, validando a importância da ciência matemática como desenvolvimento tecnológico e humano.

Dessa forma, propomos o uso do tema Criptografia para a exploração de conceitos matemáticos aplicados. No entanto, o tema é amplo e complexo, e pretendemos dar ênfase ao estudo que abrange a educação matemática no Ensino Médio, valorizando a aplicabilidade da matemática neste contexto.

Sendo assim, segundo Silva (2008) temos que Criptografia é a arte ou ciência de escrever mensagens em cifra ou em código, de modo que somente a pessoa autorizada possa decifrar e ler as mensagens.

Silva (2008) ainda complementa:

> A criptografia é tão antiga quanta a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalhas. 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 para decifração de mensagens.

> Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

A mensagem para ser enviada é chamada de texto-original e a mensagem codificada é chamada de texto-cifrado. O texto original e o texto-cifrado são escritos em algum alfabeto específico consistindo de um certo número de símbolos. O processo de converter um texto-original para um texto-cifrado é chamado de codificação ou cifragem, e o processo de reverter é chamado de decodificação ou decifragem.

Com o intuito de codificar e decodificar mensagens, o mini-curso envolve atividades de exploração dos conteúdos matemáticos: funções, matrizes, inversão de funções e inversão de matrizes. Pretende-se também abordar possibilidades do uso de tecnologias como complemento no ensino/aprendizagem deste tema.

Para codificar uma mensagem escrita, nos baseamos na associação do alfabeto utilizado com um conjunto de números, em que cada letra é associada à um número deste conjunto. Na alteração da mensagem, o processo de conversão obedece uma lei matemática, que neste mini-curso é abordado através de uma função ou uma matriz. Através dessa alteração, o novo conjunto de dados é novamente associado com o alfabeto da mensagem original, caracterizando uma mensagem codificada. Dessa forma, a mensagem pode ser decodificada somente com o conhecimento da lei de codificação. Se a lei que codifica é uma função, a decodificação será dada pela inversa desta função. E se a lei que codifica é uma matriz, a decodificação será dada pela inversa desta matriz. Sendo assim, é possível retornar à mensagem original.

Esse processo de criptografia é estudado e discutido através de atividades com embasamento teórico e vinculado à prática deste processo, para que o participante desenvolva esta prática valendo das propriedades e conceitos matemáticos abordados.

Como complemento das atividades, sugerimos uma discussão das possibilidades do uso de tecnologias no estudo da criptografia, analisando a viabilidade no contexto aplicado, já que é um paradigma para muitos professores o uso de tecnologias nas aulas de matemática, e em muitos casos, a estrutura escolar não supre atividades diferenciadas pela falta de tais tecnologias, como por exemplo, um laboratório de informática.

Propomos este tema diferenciado com intuito de motivar o uso da matemática em novas atividades que possam cativar o interesse dos alunos, tornando as atividades escolares aplicadas e prazerosas, tendo em vista uma forma de diferenciar o ensino massante da matemática tradicional.

Por fim, o mini-curso discute o uso da criptografia em diferentes níveis de ensino, dos quais cada professor pode adaptar as atividades, ou mesmo reorganizá-las de acordo com a ênfase desejada, seja pela turma ou pelos conceitos matemáticos trabalhados. Sendo assim, a amplitude do tema pode também contemplar outras áreas, buscando envolver um estudo contextualizado e multidisciplinar.

Referências

SILVA, A. A. *Números, Relações e Criptografia*. Departamento de Matemática - UFPB, Paraíba, 2000. Disponível em: <http://www.mat.ufpb.br/me_aas.zip>. Acessado em: <27/08/2008>.