doi:10.20396/revpibic.v0i0.id

XXVI Congresso de Iniciação Científica Unicamp
17 a 19 de outubro Campinas | Brasil

Criptografia e matemática na escola

Guilherme Zanni Pestana*, Laura Rifo.

Resumo
Pretendemos, neste projeto, pensar o ensino de matemática, em particular alguns conceitos de teoria dos números envolvidos no estudo dos números primos e aritmética modular. Usando como motivação a criptografia, ou seja, o desafio de codificar mensagens e os vários métodos já elaborados, desde os mais antigos até os mais atuais, e eficientes, pretendemos entender como essas técnicas avançaram ao longo do tempo, dentro de um contexto histórico, relacionando o estudo da matemática com o de história.

Palavras-chave:
Ensino de matemática, Criptografia, Números Primos.

Introdução

A criptografia, que estuda técnicas que buscam codificar mensagens, de modo que apenas seu destinatário consiga ler, tem sido utilizada ao longo dos últimos milhares de anos e sempre foi muito importante para se trocar informações com segurança. Nos últimos séculos, são vários os exemplos de seu uso para codificar e decifrar mensagens codificadas. Um desses exemplos é a máquina Enigma, usada para criptografar mensagens pelo exército alemão durante a segunda guerra mundial. Outro exemplo é datado de 1822, quando os hieróglifos egípcios foram decifrados usando a "Pedra da Roseta", uma pedra que continha o mesmo texto em três formas de escrita, duas delas conhecidas. Assim, um dos objetivos deste trabalho é relacionar o ensino de matemática com o estudo de história, buscando entender a relevância que a matemática teve em conflitos e avanços tecnológicos à nível mundial.

Hoje a importância da criptografia é ainda mais evidente, com cada vez mais as trocas de mensagens, lojas e transações financeiras se concentrando em operações online. Além disso, com recentes escândalos de vazamento e venda de informações pessoais, esse é um assunto que atrai a atenção de muitos estudantes. Os métodos de criptografia se aperfeiçoaram muito e, ao contrário dos métodos anteriores, que eram de chave privada (para decifrar uma mensagem é necessário fazer o processo inverso do ciframento), passaram a ser de chave pública e muito mais difíceis de se quebrar. Um dos mais eficientes, o RSA, tem por trás conceitos matemáticos que podem ser ensinados no ensino básico. Os números primos, que são ensinados desde o sexto ano do ensino fundamental e tira o sono dos matemáticos há milhares de anos, passam a ter uma importância ainda maior. Aprofundando o seu estudo e introduzindo novos conceitos de teoria dos números (aritmética modular) é possível que um aluno no ensino médio entenda como funciona a criptografia RSA e através desse estímulo, desenvolva o gosto pela matemática.

Resultados e Discussão

O projeto está na fase inicial de elaboração de uma sequência didática que possa ser aplicada em oficinas de matemática, a nível de Ensino Fundamental II ou Médio. Algumas das construções ou atividades propostas têm sido apresentadas para alunos do ensino médio participantes de um cursinho pré-vestibular popular e para uma turma de estágio com alunos de licenciatura de cursos de humanas, biológicas e artes.

Percebemos, neste estágio do projeto, que a recepção por parte dos alunos foi boa, demonstrando interesse ao conhecer alguns dos grandes problemas e curiosidades que desencadeiam a partir dos números primos (algo bem simples e que é conhecido desde o começo do ensino fundamental II). Por outro lado, alguns tópicos de aritmética modular, como congruência entre números e o Pequeno Teorema de Fermat, geraram uma certa dificuldade num primeiro momento.

Conclusões

De acordo com os resultados obtidos até o momento, pensamos que devemos fortalecer conhecimentos básicos prévios à aritmética modular, como critérios de divisibilidade e fatoração de números naturais. Propor atividades relacionadas com fenômenos periódicos e que trabalhem com os restos de divisões entre números naturais. Além disso, pretendemos aprofundar o cruzamento entre matemática e história, aprofundando as pesquisas sobre a história da criptografia.

Agradecimentos

O aluno é bolsista PICME, CNPq, por ter sido medalhista da OBMEP entre os anos de 2007 e 2013.

Gardner, Martin. *Codes, ciphers and secret writing*. Nova York: Dover, **1984**.
Coutinho, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, **2009.**