MINI-CURSO DE CRIPTOGRAFIA; UMA APLICAÇÃO DA TEORIA DOS NÚMEROS

RESUMO

Priscila Roque de Almeida[1], Laís Mayara Azevedo Barroso[2], Leandro Roberto Macedo[3], Ricardo Barbosa Lima Mendes Oscar[4], Vinicius Roberto Gomes Domingues [5]

Introdução

A criptografia é um assunto atual, presente em nosso dia-a-dia, e que na maioria das vezes passa despercebida. Seu principal objetivo é transmitir uma mensagem a um determinado destinatário sem que outro possa compreender seu conteúdo. Estruturado a partir de uma vasta pesquisa bibliográfica e em *sites* na *Internet*, foi organizado um mini-curso intitulado "A Teoria dos Números aplicada à Criptografia", direcionado a alunos dos cursos de Matemática. Durante a graduação, normalmente, os alunos não conseguem associar os conceitos abordados na disciplina "Teoria dos Números" às suas possibilidades de aplicação. Este mini-curso visa fixar os conceitos de Congruência – conceito fundamental para os estudos mais aprofundados em Teoria dos Números – e mostrar o funcionamento do método de Criptografia mais utilizado atualmente, o Método RSA. Tal mini-curso, que foi ministrado para um grupo de alunos que estavam cursando o quinto período do curso de Matemática da Universidade Estadual de Minas Gerais (UEMG), está dividido em três partes: a princípio, uma pequena revisão dos conceitos e teoremas necessários para desenvolvimento do método; posteriormente é apresentada uma contextualização e a concepção do processo, além de um exemplo para melhor entendimento; e para finalizar é proposta uma atividade de codificação e decodificação de mensagem para que os alunos possam colocar em prática o que foi demonstrado e fixar o conhecimento adquirido.

Objetivos

Durante a execução deste mini-curso, os alunos apresentaram muitas dificuldades, tanto no tocante aos conceitos elementares da Teoria de Números quanto relacionados ao uso da calculadora para auxilio na resolução de exercícios. Mediante tais dificuldades, a reformulação do mini-curso, tendo em vista, não somente diminuir as deficiências mencionadas, mas também, apresentar uma aplicação prática de fácil compreensão sobre a Teoria dos Números, incentivando o aprendizado e estudo do tema.

Metodologia

Elaboramos um questionário, envolvendo o tema de Teoria dos Números, direcionados aos alunos do curso de Matemática da UFV. A análise das respostas obtidas pretende subsidiar a reformulação do mini-curso que será aplicado a alunos de graduação em Licenciatura em Matemática da UFV.

1 Universidade Federal de Viçosa - Departamento de Matemática *priscila.almeida@ufv.br*
2 Universidade Federal de Viçosa - Departamento de Matemática *laís.barroso@ufv.br*
3 Universidade Federal de Viçosa - Departamento de Matemática *leandro.macedo@ufv.br*
4 Universidade Federal de Viçosa - Departamento de Matemática *ricardo.oscar@ufv.br*
5 Universidade Federal de Viçosa - Departamento de Matemática *vinicius.domingues@ufv.br*

Conclusões

O mini-curso foi muito bem aceito entre os alunos de graduação em Licenciatura em Matemática da UEMG, assim como pelo Departamento de Matemática da UFV, que pretende, com o auxilio do questionário, reformulá-lo e aplicá-lo ao maior número possível de estudantes de Licenciatura em Matemática da UFV que possam ter interesse na área.

Referências

[1] COUTINHOS, S.C. **PROGRAMA DE INICIAÇÃO CIENTÍFICA DA OBMEP 2007** - IMPRINTA EXPRESS GRÁFICA E EDITORA LTDA.

[2] VIDIGAL, A.; AVRITZER, D.; SOARES, E. F.; BUENO, H. P.; FERREIRA, M. C. C.; FARIA, M. C.; **FUNDAMENTOS DE ÁLGEBRA** - EDITORA UFMG, 2005.

[3] BORGES, F. **CRIPTOGRAFIA COMO FERRAMENTA PARA O ENSINO DE MATEMÁTICA** – PETRÓPOLIS, RJ: LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA – LNCC.

[4] LEMOS, M. **CRIPTOGRAFIA, NÚMEROS PRIMOS E ALGORITMOS** – RIO DE JANEIRO, RJ: EDITORA DO IMPA.

[5] COUTINHOS, S.C. **NÚMEROS INTEIROS E CRIPTOGRAFIA RSA** – RIO DE JANEIRO, RJ: IMPA, 2005.

[6] HTTP://WWW.DICAS-L.COM.BR/DICAS-L/20070611.PHP, ACESSADO PELA ÚLTIMA VEZ EM 30 DE NOVEMBRO DE 2009 ÀS 21HS E 33 MIN.