# ECM – Multiplicação escalar usando coordenadas projetivas

**Souza, Igor Alexandre Cardena de**[1] (iaxcsouza@gmail.com); **MOLGORA, Adriana Betânia de Paula**[2] (adrianamolgora@gmail.com)

[1]Discente do curso de Ciência da Computação da UEMS – Dourados;
[2]Docente do curso de Ciência da Computação da UEMS – Dourados;

A fatoração de números inteiros é um dos antigos problemas matemáticos ainda sem solução. A aplicação de fatoração de inteiros é muito importante em algumas áreas como, por exemplo, na criptografia. A criptografia RSA tem sua segurança pautada na inexistência de solução para o problema de fatoração de inteiros. Ou seja, caso seja desenvolvido um método que fatore qualquer inteiro dado, em tempo computacional viável, a segurança do RSA será comprometida. Assim, torna-se necessário o estudo sobre métodos de fatoração de inteiros. Um dos métodos de fatoração que merecem atenção, devido a sua importância, é o método ECM (Elliptic Curve Method). Esse método utiliza a estrutura de grupo dos pontos de uma curva elíptica para encontrar um fator de um número inteiro dado. Um estudo do método ECM envolve o conhecimento de aspectos teóricos e computacionais. A operação de multiplicação escalar é fundamental no processo de fatoração pelo método ECM e é imprescindível que a mesma seja realizada de forma eficiente. Nesse sentido, este projeto de iniciação científica teve como objetivo realizar um estudo teórico e prático da operação multiplicação escalar utilizando-se coordenadas projetivas. Como o método ECM trabalha com números grandes (até mesmo acima de100 dígitos), é importante que esse cálculo seja realizado de forma eficiente. Para isso, foi estudado o funcionamento da biblioteca GMP, que possibilitou a adaptação destes algoritmos por meio de suas funções. Apesar de seu grande potencial, a linguagem C possui recursos muito limitados para lidar com números gigantes, o que levou ao surgimento de bibliotecas específicas para este fim, sendo a GNU Multiple-Precision Library, conhecida como GMP, a principal delas. Foi implementado um algoritmo que apresentou resultados eficientes, utilizando números com até 60 digitos. O desenvolvimento dessa pesquisa demandou o estudo de conceitos teóricos e práticos, relacionados à teoria dos números e à ciência da computação. Esses estudos proporcionaram a aquisição de conhecimentos matemáticos e computacionais permitindo a aplicação dos conceitos teóricos na prática computacional.

**Palavras-chave:** fatoração de inteiros, coordenadas projetivas, curvas elípticas.

Agradecimentos: **Ao Programa de Iniciação Científica da UEMS pela concessão de bolsa de iniciação científica ao primeiro autor**