Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Métodos de Fatoração de Polinômios e Cálculo de suas Raízes sobre Corpos Finitos: Uma Abordagem Computacional com GAP

Túlio Joaquim Altoé[1]
Graduando em Matemática do Instituto de Ciências Exatas, UFF, Volta Redonda, RJ
Rosemary Miguel Pires[2]
Departamento de Matemática, Instituto de Ciências Exatas, UFF, Volta Redonda, RJ

1 Introdução

Nas últimas décadas, a Teoria de Corpos Finitos vêm recebendo grande atenção dos matemáticos. Isto se deve muito ao fato das diversas aplicações desta teoria tanto na Matemática quanto na Tecnologia. São encontradas aplicações na Teoria de Criptografia, Teoria dos Números, Álgebra Abstrata e Teoria de Códigos. Como à teoria é bastante ampla, focamos no cálculo de raízes de polinômios sobre corpos finitos. Este trabalho é árduo para ser feito manualmente. Por isto, é necessário a utilização de alguma ferramenta computacional que auxilie no processo dos cálculos e, também, na ilustração e simulação dos teoremas matemáticos.

O sistema computacional que será utilizado é o GAP (Groups, Algorithms and Programming), disponível no endereço http://www.gap-system.org/. Este sistema foi criado para programar e/ou computar estruturas algébricas.

2 Métodos de Fatoração e Aplicações com GAP

Neste trabalho apresentamos métodos para o cálculo de raízes de polinômios sobre corpos finitos, desenvolvidos com auxílio do GAP. Para isso, são introduzidos conceitos preliminares sobre polinômios irredutíveis e também algoritmos para a decomposição de polinômios sobre corpos finitos em polinômios irredutíveis.

Existem na literatura, vários resultados relacionados a determinação de polinômios irredutíveis e fatoração de polinômios, como por exemplo os teoremas apresentados abaixo. As demonstrações podem ser encontradas em [1] e [2], respectivamente.

Teorema 2.1. *Considere $\mathbb{F}_q$ um corpo finito com q elementos. Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau n, então $f(x)$ divide $(x^{q^k} - x)$ se, e somente se n divide k.*

[1] tulioaltoe@id.uff.br
[2] rosemarypires@id.uff.br

Teorema 2.2. *Para cada corpo finito $\mathbb{F}_q$ e cada $k \in \mathbb{N}$, o produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujo grau divide k é igual a $x^{q^k} - x$.*

Uma consequência do Teorema 2.2, conforme [3], é o algoritmo de Rabin, que consiste basicamente em três passos: o primeiro deles é gerar um polinômio $g(x)$ aleatório de grau d sobre o corpo finito $\mathbb{F}_q$; o segundo, verificar se $g(x)$ divide $(x^q - x)$ e o terceiro, testar se o mínimo múltiplo comum entre $g(x)$ e $(x^{p^{n_i}} - x)$ é igual a 1 para todo $n_i = \frac{n}{k_i}$ onde k_i são todos os divisores primos de n. Se esses três passos obtiverem sucesso significa que encontramos um polinômio irredutível.

Existem métodos de fatoração que são custosos quando executados algebricamente, um exemplo disso, é o método de Kronecker, que nos permite fatorar um polinômio $p(x) \in \mathbb{Z}[x]$. Porém, este método exige muitos cálculos, o que o torna extenso e nada eficiente algebricamente. Mas com auxílio computacional mostramos exemplos de como pode ser implementado de maneira eficiente.

3 Conclusões

Neste trabalho apresentamos algoritmos para a fatoração de polinômios sobre corpos finitos e como consequência dessa fatoração, obtemos as raízes. Implementamos esses métodos e aplicamos com auxílio do GAP.

O trabalho faz parte de um projeto maior de pesquisa que está sendo desenvolvido no Instituto de Ciências Exatas, UFF, em que estudamos vários métodos de fatoração de polinômios sobre corpos finitos, construção e otimização de algoritmos, cálculo de raízes de polinômios, construção de Corpos Finitos e aplicações da Teoria de Corpos.

Agradecimentos

Agradeço a minha orientadora Dr[a] Rosemary Miguel Pires pelo apoio e dedicação e, ao CNMAC (Congresso Nacional de Matemática Aplicada e Computacional) pela oportunidade que estão fornecendo aos alunos para a divulgação de seus trabalhos científicos.

Referências

[1] A. Masuda e D. Panario, *Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos*. IMPA, Rio de Janeiro, 2007.

[2] S. F. Zanoello, Raízes Polinomiais em Corpos Finitos, Dissertação de Mestrado, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2004.

[3] L. M. Zatesko, Irredutibilidade Polinomial e Algoritmos em Corpos Finitos, Monografia de Bacharelado em Ciência da Computação, Universidade Federal do Paraná, Curitiba, 2008.