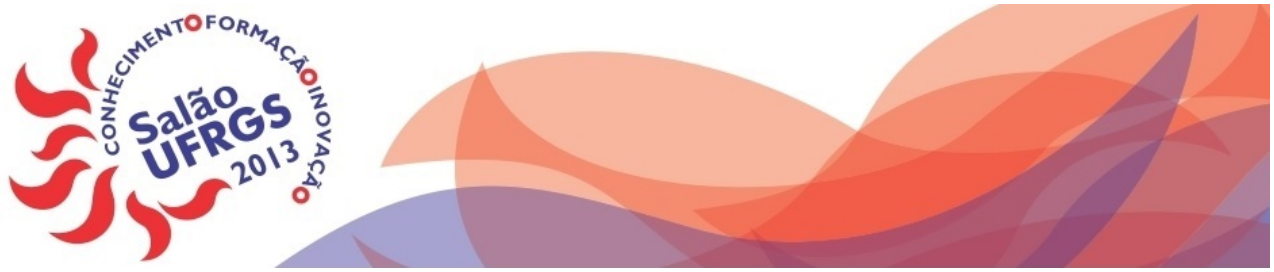

Evento	Salão UFRGS 2013: SIC - XXV SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2013
Local	Porto Alegre - RS
Título	Algoritmo de Berlekamp
Autor	MAIKON MACHADO TOLEDO
Orientador	MARIA CRISTINA VARRIALE

O algoritmo de Berlekamp é um método bem conhecido para fatoração de polinômios univariados sobre pequenos corpos finitos, foi inventado por Elwyn Berlekamp em 1967, sendo o algoritmo dominante para resolver o problema até o surgimento de um algoritmo mais eficiente do Cantor-Zassenhaus de 1981. É um algoritmo recursivo que com o suporte das ferramentas "Teorema Chinês dos Restos", "Morfismo de Frobenius", e com algumas técnicas da álgebra linear e o cálculo GCD's, lineariza o problema e obtém os fatores irredutíveis do polinômio. Neste trabalho vou dar uma ideia geral de como funciona o algoritmo de Berlekamp.