Fatoração de polinômios univariados

Pelo Teorema Fundamental da Álgebra, podemos escrever um inteiro como o produto de primos. O mesmo pode ser feito com um polinômio univariado f sobre um corpo finito F_q, escrevendo-o como o produto de polinômios irredutíveis.

Para fazer essa fatoração, geralmente é utilizado um algoritmo formulado da seguinte maneira.

Utiliza-se a fatoração Livre de Quadrados tomando, por exemplo, o polinômio $f = g^2h$, g, h Є $F_q[x]$ e eliminando o fator quadrático de g, obtendo assim f* = gh. A partir de f*, utiliza-se a fatoração de grau distinto para dividi-lo em blocos de polinômios de graus menores, agrupando estes blocos de acordo com o grau dos polinômios e assim, pode-se escrever f* como $f^* = f_1f_2f_3...f_k$ onde cada f_i, i = 1,...,k é um bloco de polinômios irredutíveis de grau i. Partindo de $f^* = f_1f_2f_3...f_k$ utiliza-se a fatoração de mesmo grau onde, para cada bloco f_i, i = 1,...,k obtém-se a fatoração em polinômios irredutíveis.

Nesta apresentação, partindo de um polinômio livre de quadrados, ou seja, partindo, por exemplo, de f* = gh, iremos mostrar como é feita a aplicação do método.