Irredutibilidade de polinômios em Z_5

Uma das propriedades fundamentais dos números inteiros é a existência de números primos, e o Teorema Fundamental da Aritmética que diz que, dado um número inteiro diferente de -1, 0 e 1, ou ele é primo, ou pode ser fatorado de forma única como um produto de números primos. Com polinômios, ocorre algo semelhante. Dado um polinômio p(x) e um corpo K, dizemos que p(x) é irredutível sobre K se não há como fatorar p(x) como um produto de dois polinômios não-constantes f(x) e g(x) pertencentes a K[x]. De fato, se p(x) não é irredutível, então ele pode ser fatorado como um produto de polinômios irredutíveis, semelhante aos números inteiros. No caso dos polinômios, esta fatoração, para ser completa, depende do corpo onde se está trabalhando. No trabalho que será apresentado, partimos do artigo Irreducible Cubics Modulo 5 da revista The American Mathematical Monthly, Vol 117 de Novembro de 2010, que estuda a irredutibilidade de polinômios em Z_5. Neste artigo, é dada a seguinte idéia de demonstração: um polinômio p(x) é irredutível em Z_5 se existem dois polinômios f(x) e g(x) tais que p(x) = f(x) + g(x) e cada elemento de Z_5 é raiz de exatamente um destes dois polinômios. É provado, em seguida, que esta demonstração pode ser utilizada em todos os casos de irredutibilidade de Z_5. A demonstração é bastante interessante, já que utiliza métodos combinatórios juntamente à álgebra. Por fim, são dados ainda algoritmos para construir polinômios de grau 3 e irredutíveis em Z_5, bem como os polinômios f(x) e g(x) que provam sua irredutibilidade.