

170

O MDC DE POLINÔMIOS DE UMA VARIÁVEL. *Fabio S. Azevedo, Vilmar Trevisan* (Departamento de Matemática Pura e Aplicada, Instituto de Matemática-UFRGS)

Para a determinação do Máximo Divisor Comum (MDC) de polinômios a uma variável, pode-se aplicar o algoritmo de Euclides. Entretanto, sua aplicação direta pode gerar coeficientes intermediários muito grandes. A alternativa apresentada neste trabalho é o uso de métodos modulares, onde o algoritmo euclidiano é aplicado em corpos finitos, evitando-se o crescimento das expressões intermediárias. A recuperação do MDC é obtida via o Teorema Chinês dos Restos e a determinação, a priori, de cotas superiores para o tamanho dos coeficientes.