UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

É um método de resolver sistemas de equações com s incógnitas: encontrar $h = e(a_1, \ldots, a_s)$, nos quais: $h \in H$,, H é um anel com divisão e $e(a_1, \ldots, a_s)$ é uma expressão.
O método propõe avaliar h por seu resto: computamos $r = h \, mod \, m$, para algum módulo m apropriado, e recuperamos h.

O módulo para a recuperação de h pode ser demasiadamente "grande", tornando o processo para o Esquema de Imagem Única lento. Isso muda quando passamos para o Esquema de Imagens Múltiplas, pois então podem e são utilizados módulos apropriados e que tornam o processo rápido.

Homomosfismo entre aplicações (em particular o Epimorfismo); Inverso de um elemento módulo m; Resolução de Sistemas pelo Teorema Chinês dos Restos;

O que é?

Como ele funciona?

Qual a sua diferença para "Única"?

Quais os conteúdos prévios para compreensão do algoritmo?

ESQUEMA DE IMAGENS HOMOMORFAS MÚLTIPLAS

Quando ele é eficaz?

Quais são suas possíveis aplicações?

Qual o principal Teorema?

Em sistemas em que os coeficientes das incógnitas são números relativamente grandes, que ultrapassem 10^5 digitos

Podemos utilizar este método para transformar números modulares em decimais, resolver sistemas lineares sobre conjuntos numéricos e corpos e, no caso especifico dos polinômios, serve para calcular o polinômio característico $y(k) = det\,(KI - A)$, para qualquer matriz A nxm

Teorema Chinês do Resto

$$\begin{cases} u \equiv x_1 \, (mod \, m_1) \\ u \equiv x_1 \, (mod \, m_1) \\ \vdots \\ u \equiv x_{n-1} \, (mod \, m_{n-1}) \end{cases}$$

Autora: Paola Rossato Bernardo, Orientador: Profº Dr. Vilmar Trevisan