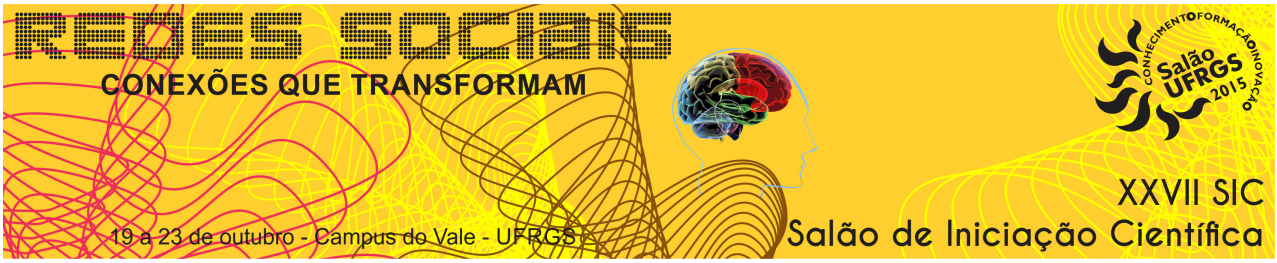

Evento	Salão UFRGS 2015: SIC - XXVII SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2015
Local	Porto Alegre - RS
Título	Trabalhando com o Esquema de Imagens Homomórficas Múltiplas
Autor	PAOLA ROSSATO BERNARDO
Orientador	VILMAR TREVISAN

Título: Trabalhando com o Esquema de Imagens Homomórficas Múltiplas
Autor: Paola Rossato Bernardo
Orientador: Vilmar Trevisan
Instituição: UFRGS

O objetivo deste estudo é encontrar $h = e(a_1, \ldots, a_s)$, nos quais: $h \in H$, $a_i \in H$, $i \in \mathbb{Z}$, H é um anel com divisão e $e(a_1, \ldots, a_s)$ é uma expressão. O método para tal seria avaliar $e(a_1, \ldots, a_s)$ sobre H. Porém, o esquema de imagens homomórficas, propõe avaliar h por seu resto $r \; mod \; m$: computamos $r = h \; mod \; m$, para algum $mod \; m$ apropriado, e recuperamos h. A vantagem é que este método pode ser computado sobre corpos, no qual a estrutura e aritmética modular sejam aproveitados para a rapidez e eficiência do método.
Um dos objetivos principais deste método é a recuperação de h com m suficientemente grande através de uma aritmética rápida. Porém, pode acontecer deste m ser grande demais, tornando o processo lento, contradizendo o seu objetivo principal. O que será apresentado neste trabalho é uma solução para este problema: estender este esquema de imagens homomórficas *singulares* para um *múltiplo*. Fazemos isto ao computar uma família de restos r_k de h tal que $r_k = h \; mod \; m_k$, para uma família de módulos m_k apropriados, no qual obtemos h a partir desses $r_k's$. Para tal, nossa principal ferramenta será o Teorema Chinês dos Restos.

Como exemplos de aplicações, 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, interpolando os valores de $y(k_i)$ para n valores distintos k_i. Ele também é uma ferramenta computacional importante para a manipulação polinomial.