

Aplicação do estudo de divisibilidade, congruência, máximo divisor comum, corpo de  $P$  elementos ( $P$  um número primo) e Teorema Chinês de Restos em exemplos da Teoria de Códigos (Cifra de César, Transformação Afim, Sistemas Poligráficos, Sistemas de Chaves Públicas). Nestes exemplos apresenta-se ainda um tipo de cifra, que parece não constar na bibliografia, a qual envolve potências  $k$ -ésimas módulo  $P$  ( $P$  primo). Esta nova cifra mantém a simplicidade de envolver apenas duas chaves e apresenta vantagens em relação à Cifra de César e à Transformação Afim por evitar espaçamento constante entre as cifras, dificultando ainda mais a descoberta das chaves, e como consequência a quebra do segredo. (CNPq).