Título: ARITMÉTICA MODULAR E APLICAÇÕES

Profa.: Flávia Morgana.

Resumo: Na divisão euclidiana entre dois números inteiros dados, onde um não é múltiplo do outro, aparecem os restos não nulos. Historicamente, muitos matemáticos se ocuparam em estudar a aritmética dos restos na divisão por um número fixo, o que levou ao início de um ramo da teoria dos números chamado de congruência modular. Neste minicurso abordaremos suas principais propriedades e algumas de suas aplicações, tais como em sistemas de codificação como o ISBN (*International Standard Book Number*), o CPF (*Cadastro de Pessoa Física*) e o Código de Barras, bem como nas chaves usadas pela Criptografia.