Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 04 - Conceitos básicos de Teoria dos Números e Corpos Finitos
Para apresentação e discussão em sala de aula, em **31/10/2023**.

Nome Completo: _____

Questões retiradas do livro-texto da disciplina.
Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

1. Defina resumidamente, um grupo, um anel, um corpo.
2. O que significa dizer que b é um divisor de a?
3. Para cada uma das seguintes equações, encontre um inteiro x que satisfaça:
   (a) $5x \equiv 4 \pmod 3$
   (b) $7x \equiv 6 \pmod 5$
   (c) $9x \equiv 8 \pmod 7$
4. Encontre o inverso multiplicativo de cada elemento diferente de zero em Z_5.
5. Determine os MDC:
   (a) mdc(24140, 16762):
   (b) mdc(4655, 12075).
6. Usando o algoritmo de Euclides estendido, encontre o inverso multiplicativo de:
   (a) 1234 mod 4321;
   (b) 24140 mod 40902;
   (c) 550 mod 1769.
7. Determine o inverso multiplicativo de $x^3 + x + 1$ em GF(2^4), com $m(x) = x^4 + x + 1$.
8. Para a aritmética de polinômios com coeficientes em Z_{10}, realize os seguintes cálculos:
   (a) $(7x + 2) - (x^2 + 5)$
   (b) $(6x^2 + x + 3) \times (5x^2 + 2)$
9. Estruture uma calculadora simples de quatro funções em GF(2^4). Você pode usar uma tabela com valores pré-calculados para os inversos multiplicativos.

Livro-texto da disciplina:
STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.