Universidade Federal do
Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
T +55 (87) 3764-5500
m 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 29 de junho de 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.

Grupo:

Um conjunto não vazio de elementos algébricos com uma operação binária denominada multiplicação, e que deve satisfazer algumas propriedades:

1. Fechamento
2. Associatividade
3. Identidade
4. Inverso

Anel:

Um conjunto não vazio de elementos algébricos com duas operações binárias denominadas adição e multiplicação, e que deve satisfazer algumas propriedades:

1. O conjunto com a operação de adição possui todas as propriedades que o grupo tem para a multiplicação
2. O conjunto com a operação multiplicativa é associativo e distributivo

Corpo:

É o mesmo que um anel porém com uma propriedade adicional do inverso para elementos não nulos.

2. O que significa dizer que *b* é um divisor de *a*?

R:

Significa que b divide a de forma exata, em outras palavras, o resto da divisão de a por b é zero.

3. Para cada uma das seguintes equações, encontre um inteiro x que satisfaça:

(a) $5x \equiv 4 \pmod 3$ **(2)**
(b) $7x \equiv 6 \pmod 5$ **(3)**
(c) $9x \equiv 8 \pmod 7$ **(4)**

4. Encontre o inverso multiplicativo de cada elemento diferente de zero em Z_5.

1^{-1} mod 5 = 1*1 mod 5 = 1

2^{-1} mod 5 = 2*3 mod 5 = 6 mod 5 =1

3^{-1} mod 5 = 3*2 mod 5 = 6 mod 5 =1

4^{-1} mod 5 = 4*4 mod 5 = 16 mod 5 =1

5. Determine os MDC:

(a) mdc(24140, 16762):

24.140 mod (16.762) = 7.378
16.762 mod (7.378) = 2.006
7.378 mod (2.006) = 1.360
2.006 mod (1.360) = 646
1.360 mod (646) = 68
646 mod (68) = 34
68 mod (34) = 0

o mdc(24140, 16762) = 34

(b) mdc(4655, 12075).

12.075 mod (4.655) = 2.765
4.655 mod (2.765) = 1.890
2.765 mod (1.890) = 875
1.890 mod (875) = 140
875 mod (140) = 35
140 mod (35) = 0

o mdc(4655, 12075) = 35

6. Usando o algoritmo de Euclides estendido, encontre o inverso multiplicativo de:

(a) 1234 mod 4321;

passo 1: algoritmo de Euclides:

4321 = 3 * 1234 + 619
1234 = 1 * 619 + 615
619 = 1 * 615 + 4
615 = 153 * 4 + 3
4 = 1 * 3 + 1

passo 2: Euclides extendido

1 = 4 - 3
3 = 615 - 153 * 4
1 = 4 - 615 + 153 * 4 = (-1) 615 + 154 * 4
1 = (-1) 615 + 154 (619-615)
615 = 1234 - 619
1 = (-1) (1234 - 619) + 154 (619-615)
619 = 4321 - (3 * 1234)
1 = (-1) (1234 - (4321 - (3 * 1234))) + 154 ((4321 - (3 * 1234) - 615)
1 = (- 4321 + 4 * 1234) + 154 (3706 - 3 * 1234)
1 = - 4321 + (4 * 1234) - (462 * 1234) + 570724

(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) $(7x + 2) - (x^2 + 5)$

$((7x + 2) - (x^2 + 5))$ mod 10

$= (7x + 2 - x^2 - 5) \bmod 10$

$= (-x^2 + 7x + 3) \bmod 10$

$= -x^2 + 7x + 3$

(b) $(6x^2 + x + 3) \times (5x^2 + 2)$

$((6x^2 + x + 3) \times (5x^2 + 2)) \bmod 10$

$=(30x^4+12x^2+5x^3+2x+15x^2+6) \bmod 10$

$= (30x^4+5x^3+27x^2+2x+6) \bmod 10$

$= 0x^4+5x^3+7x^2+2x+6$

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.