Bacharelado em Ciência da Computação

CCMP3079 Segurança de Redes de Computadores

Atividade Cap. 04

Prof. Sérgio Mendonça

Nome Completo: Luan Valentino Sampaio Marques

Data: 31/10/2023

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

Questões

1. Defina resumidamente, um grupo, um anel, um corpo.

- **Grupo:** Um grupo é um conjunto G com uma operação binária associativa, que possui um elemento identidade e tal que todo elemento de G tem um inverso em G.
- **Anel:** Um anel é um conjunto R equipado com duas operações, adição e multiplicação, onde R é um grupo abeliano sob adição, a multiplicação é associativa, e a multiplicação distribui-se sobre a adição.
- **Corpo:** Um corpo é um anel comutativo K em que todo elemento diferente de zero tem um inverso multiplicativo.

2. O que significa dizer que b é um divisor de a?
Significa que existe um número inteiro k tal que $a = b \times k$.
3. Para cada uma das seguintes equações, encontre um inteiro x que satisfaça:
(a) $5x \equiv 4 \pmod 3$
$5 \equiv 2 \pmod 3$, logo:

$$2x \equiv 4 \pmod 3$$

Dividindo ambos os lados por 2:

$$x \equiv 2 \pmod 3$$

(b) $7x \equiv 6 \pmod 5$
$7 \equiv 2 \pmod 5$, logo:

$$2x \equiv 6 \pmod 5$$

$6 \equiv 1 \pmod 5$, então:

$$2x \equiv 1 \pmod 5$$

Multiplicando por 3 (o inverso de 2 mod 5):

$$x \equiv 3 \pmod 5$$

(c) $9x \equiv 8 \pmod 7$
$9 \equiv 2 \pmod 7$, logo:

$$2x \equiv 8 \pmod 7$$

$8 \equiv 1 \pmod 7$, então:

$$2x \equiv 1 \pmod 7$$

Multiplicando por 4 (o inverso de 2 mod 7):

$$x \equiv 4 \pmod 7$$

4. Encontre o inverso multiplicativo de cada elemento diferente de zero em Z_5.
Os inversos multiplicativos em Z_5 são:

$$1^{-1} \equiv 1 \pmod 5$$

$$2^{-1} \equiv 3 \pmod 5$$

$$3^{-1} \equiv 2 \pmod 5$$
$$4^{-1} \equiv 4 \pmod 5$$

5. Determine os MDC:

(a) $\text{mdc}(24140, 16762)$

Utilizando o algoritmo de Euclides:

$$24140 = 16762 \times 1 + 7380$$

$$16762 = 7380 \times 2 + 2$$

$$7380 = 2 \times 3690$$

Portanto, $\text{mdc}(24140, 16762) = 2$.

(b) $\text{mdc}(4655, 12075)$

$$12075 = 4655 \times 2 + 2765$$

$$4655 = 2765 \times 1 + 1890$$

$$2765 = 1890 \times 1 + 875$$

$$1890 = 875 \times 2 + 140$$

$$875 = 140 \times 6 + 35$$

$$140 = 35 \times 4$$

Portanto, $\text{mdc}(4655, 12075) = 35$.

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

(a) $1234 \mod 4321$

Aplicando o algoritmo de Euclides estendido, obtemos:

$$1234 \times (-1403) + 4321 \times 401 = 1$$

Logo, o inverso de $1234 \mod 4321$ é $-1403 \mod 4321 = 2918$.

(b) $24140 \mod 40902$

Aplicando o algoritmo de Euclides estendido, obtemos:

$$24140 \times (-5158) + 40902 \times 3039 = 1$$

Logo, o inverso de $24140 \mod 40902$ é $-5158 \mod 40902 = 35744$.

(c) $550 \mod 1769$

Aplicando o algoritmo de Euclides estendido, obtemos:

$$550 \times (-257) + 1769 \times 80 = 1$$

Logo, o inverso de $550 \mod 1769$ é $-257 \mod 1769 = 1512$.

7. Determine o inverso multiplicativo de $x^3 + x + 1$ em $GF(2^4)$, com $m(x) = x^4 + x + 1$.

Para determinar o inverso multiplicativo, precisamos encontrar um polinômio $g(x)$ tal que:

$$(x^3 + x + 1) \times g(x) \equiv 1 \pmod{x^4 + x + 1}$$

Esse processo envolve a divisão polinomial e cálculos em corpos finitos, que fornecem:

$$g(x) = x^2 + 1$$

8. Para a aritmética de polinômios com coeficientes em Z_{10}, realize os seguintes cálculos:

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

$$(7x + 2) - (x^2 + 5) = -x^2 + 7x - 3$$

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

$$= 30x^4 + 12x^2 + 15x^2 + 6x + 6$$

Reduzindo os coeficientes modulo 10:

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

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.