**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 31/10/2023.** |
| --- |

**Nome Completo:**

* Izabel Yale Neves Nascimento
* Jonas Ferreira Leal Junior

**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.**

Grupos

Conjunto de elementos que possui uma operação de combinação entre dois elementos quaisquer, formando um terceiro elemento. Deve obedecer aos axiomas de A1 a A5.

#### Anéis

São grupos com duas operações binárias, adição e multiplicação, que obedecem aos axiomas de A1 a A5 e M1 a M6.

#### Corpos

Um corpo e um conjunto que é possível somar, subtrair, multiplicar e dividir por números não nulos e que satisfazem os axiomas de A1 a A5 e M1 a M7.

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

"b" divide "a" se "a" e "b" são inteiros, "b != 0" e o resultado não terá resto.

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

**(a) 5*x ≡* 4 (mod 3)**  X = 2

**(b) 7*x ≡* 6 (mod 5)** X = 3

**(c) 9*x ≡* 8 (mod 7)** X= 9

**4. Encontre o inverso multiplicativo de cada elemento diferente de zero em *Z*5.**

0 não tem

1 \* 1 mod 5 = 1

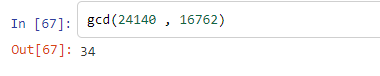
2 \* 3 mod 5 = 1

3 \* 2 mod 5 = 1

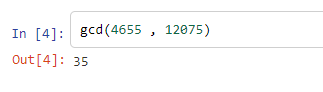
4 \* 4 mod 5 = 1

**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(24), com *m*(*x*) = *x*4 + *x* + 1.**

**8. Para a aritmética de polinômios com coeficientes em *Z*10, realize os seguintes cálculos:**

**(a) (7*x* + 2) *−* (*x*2 + 5)**

= 7x + 2 -x² -5

= -x² + 7x - 3

**(b) (6*x*2 + *x* + 3) *×* (5*x*2 + 2)**

=30x4 + 12x² + 5x³ + 2x + 15x² + 6

=30x4 + 5x³ + 27x² + 2x + 6

**9. Estruture uma calculadora simples de quatro funções em GF(24). Você pode usar uma tabela com valores pré-calculados para os inversos multiplicativos.**