UFV - Universidade Federal de Viçosa
DPI - Departamento de Informática
Prof. André Gustavo dos Santos
INF 230 - Matemática Discreta - 2021/1

Lista de Exercícios 2
Para sexta, 22/out/2021

Teoria dos números

Os exercícios a seguir envolvem problemas de teoria dos números que podem ser feitos "à mão", sem necessidade de implementar programas em computador.

1. Informe o quociente e o resto das seguintes divisões

a) 44 dividido por 8
b) 0 dividido por 19
c) -123 dividido por 19
d) -1 dividido por 4

2. Quantas horas um relógio de formato 24h (que mostra de 0 a 23) marca

a) 80 horas depois de marcar 10 horas?
b) 100 horas depois de marcar 8 horas?

3. Considere a e b dois inteiros, com $a \equiv 11 (\text{mod } 19)$ e $b \equiv 9 (\text{mod } 19)$. Encontre c, com $0 \leq c < 19$ tal que:

a) $c \equiv 13a (\text{mod } 19)$
a) $c \equiv b - a (\text{mod } 19)$
c) $c \equiv 2a + 3b (\text{mod } 19)$
d) $c \equiv a^2 - b^2 (\text{mod } 19)$

4. Encontre o valor do $\text{mdc}(120, 36)$ por três métodos diferentes:

a) listar todos os divisores e selecionar o maior divisor comum
b) fatorar em primos os dois valores e multiplicar as menores potências dos fatores comuns
c) utilizar o algoritmo de Euclides

5. Siga os passos do algoritmo de Euclides estendido para expressar o mdc de cada par de inteiros a seguir por uma combinação linear deles. Por exemplo, $\text{mdc}(252, 198) = 18 = 4 \cdot 252 - 5 \cdot 198$.

a) $21, 44$
b) $33, 44$
c) $35, 78$
d) $1001, 1342$

6. Encontre o inverso de a módulo m para cada par de inteiros primos entre si a seguir.

a) $a = 2, m = 17$
b) $a = 144, m = 233$

7. Use os resultados do exercício anterior para resolver as seguintes congruências.

a) $2x \equiv 5 (\text{mod } 17)$
b) $144x \equiv 4 (\text{mod } 233)$

8. Use o teorema chinês do resto para encontrar todas as soluções do sistema de congruências a seguir:

$x \equiv 2 (\text{mod } 3)$,
$x \equiv 1 (\text{mod } 4)$,
$x \equiv 3 (\text{mod } 5)$.

9. Use o pequeno teorema de Fermat para calcular os seguintes valores:

a) $3^{73} (\text{mod } 5)$
b) $3^{73} (\text{mod } 11)$

10. Use os resultados do exercício anterior e o teorema chinês do resto para calcular $3^{73} \pmod{55}$
(note que $55 = 5 \cdot 11$*)*

11. Seja $(n, e) = (33, 3)$ a chave pública escolhida por alguém no sistema RSA. Qual a chave secreta?

12. Alice e Bob usaram o protocolo de troca de chaves de Diffie-Hellman para gerar uma chave secreta. Eles escolheram o primo $p = 23$ e $a = 5$, que é uma raiz primitiva de 23. Alice escolheu $k_1 = 8$ e Bob escolheu $k_2 = 5$.

a) Que mensagens cada um enviou para o outro?
b) Qual o valor da chave secreta resultante dessa comunicação?

13. Considere que você tenha interceptados as mensagens enviadas por Alice e Bob no exercício anterior, e saiba inclusive os valores de p e a, que foram combinados por canal inseguro.

a) Por que é mais fácil para eles que para você calcular a chave secreta?
b) Mostre os cálculos necessários para descobrir a chave secreta resultante.