Professores: Cid Carvalho de Souza e Zanoni Dias   Primeiro semestre de 2005

MC538 – Projeto e Análise de Algoritmos II

Lista 6

1. Mostre que se $a|b$ e $b|c$ então $a|c$.

2. Mostre que se p é primo e $0 < k < p$, então $\text{mdc}(k, p) = 1$.

3. Mostre que para todos os inteiros positivos n, a e b, se $n|ab$ e $\text{mdc}(a, n) = 1$ então $n|b$.

4. Mostre que as seguintes propriedades são válidas:
   (a) $\text{mdc}(a, b) = \text{mdc}(b, a)$.
   (b) $\text{mdc}(a, b) = \text{mdc}(-a, b)$.
   (c) $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$.
   (d) $\text{mdc}(a, 0) = |a|$.
   (e) $\text{mdc}(a, ka) = |a|$ para todo inteiro k.

5. Mostre passo a passo a execução do algoritmo de Euclides para a entrada $(121, 78)$.

6. Compute os valores (d, x, y) que são a saída do algoritmo estendido de Euclides para a entrada $(899, 493)$. Mostre os passos de execução do algoritmo.

7. Mostre que para todos os inteiros a, k e n temos que $\text{mdc}(a, n) = \text{mdc}(a + kn, n)$.

8. Reescreva o algoritmo recursivo de Euclides como um algoritmo iterativo, de forma que ele utilize um número constante de variáveis inteiras.

9. Seja $\text{mmc}(a, b)$ o mínimo múltiplo comum de a e b. Mostre como calcular $\text{mmc}(a, b)$ utilizando o algoritmo de Euclides.

10. Desenhe tabelas de operações para os grupos $(Z_4, +_4)$ e $(Z_5^*, \cdot_5)$.

11. Mostre que $\phi(p^e) = p^{e-1}(p - 1)$, onde p é um número primo e e é um inteiro positivo.

12. Liste todos os subgrupos de Z_9 e Z_{13}^*.

13. Prove que existem infinitos números primos. Dica: Mostre que nem um dos primos $p_1, \ldots, p_k$ divide o número $(p_1 p_2 \ldots p_k) + 1$.

14. Mostre que se a e b são inteiros tal que $a|b$ e $b > 0$, então
    $(x \ mod \ b) \ mod \ a = x \ mod \ a$
    para qualquer inteiro x. Mostre também que
    $x \equiv y \ (mod \ b)$ implica que $x \equiv y \ (mod \ a)$
    para quaisquer inteiros x e y.