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

MC538 – Projeto e Análise de Algoritmos II

Lista 7

1. Mostre a corretude do algoritmo de Euclides estendido.
2. Prove que se $(S, \oplus)$ é um grupo finito e S' é um subconjunto de S tal que $ab \in S'$ para todo $a, b \in S'$, então $(S', \oplus)$ é um subgrupo de $(S, \oplus)$.
3. Ache todas as soluções da equação $35x \equiv 10\ (mod\ 50)$.
4. Mostre que a equação $ax \equiv ay\ (mod\ n)$ implica que $x \equiv y\ (mod\ n)$ quando $\text{mdc}(a, n) = 1$. Mostre que a condição $\text{mdc}(a, n) = 1$ é necessária dando um contra exemplo para o caso onde $\text{mdc}(a, n) > 1$.
5. Considere que no algoritmo que resolve equações modulares trocamos a solução inicial $x_0 \leftarrow x'(b/d)\ mod\ n$ por $x_0 \leftarrow x'(b/d)\ mod\ (n/d)$. O algoritmo continuará funcionando corretamente? Argumente sua resposta.
6. Ache todas as soluções das equações $x \equiv 4\ (mod\ 5)$ e $x \equiv 5\ (mod\ 11)$.
7. Ache todos os inteiros x que tem resto 1, 2, 3, 4 e 5 quando dividido respectivamente por 2, 3, 4, 5 e 6.
8. Construa uma tabela mostrando a ordem de cada elemento em (Z_{11}^*). Para a menor raiz primitiva g encontrada compute uma tabela que mostra $\text{ind}_{11,g}(x)$ para todo $x \in (Z_{11}^*)$.
9. Faça um algoritmo de exponenciação modular que examina os bits de b da direita para a esquerda.
10. Mostre como achar $a^{-1}\ mod\ n$ para qualquer $a \in Z_n^*$ usando o procedimento de exponenciação modular, assumindo que você saiba $\phi(n)$.
11. Considere um sistema RSA com $p = 11$, $q = 29$, $n = 319$ e $e = 3$. Qual valor d deve ser usado na chave secreta? Mostre a mensagem $M = 100$ encriptada.