Algoritmos Probabilísticos

Segundo semestre de 2006

Lista 5

1. (a) Prove todas as propriedades do símbolo de Jacobi do Teorema 2 das notas de aula de primalidade.

   (b) Usando essas propriedades, projete um algoritmo polinomial para calcular $\left[\frac{a}{n}\right]$ sem conhecer a decomposição em primos de n ou a.

2. Assuma que seja dado um algoritmo S para calcular raiz quadrada módulo um número primo. Usando tal algoritmo como uma caixa preta, projete um algoritmo probabilístico eficiente (RP) para COMPOSTO. (*Dica:* A idéia é escolher um elemento aleatório $a \in \mathbf{Z}_n^*$ e executar o algoritmo S com $b = a^2$. Se S não encontrar a raiz quadrada, então n não é primo. Por outro lado, se S encontrar uma raiz quadrada distinta de a ou $-a$, então novamente n não é primo.)