Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC2283 - Diseño y Análisis de Algoritmos
Profesor: Nicolás Van Sint Jan
Ayudante: Dante Pinto

Ayudantía 10

Algoritmos aleatorizados y teoría de números

Problema 1: Pequeño teorema de Fermat

Demuestre que si p es un número primo y a es un número natural, entonces:

$$a^p \equiv a \mod p$$

Hint: Demuestre que para x, y enteros y p primo se cumple $(x+y)^p \equiv x^p + y^p \mod p$

Problema 2: Comunicación aleatorizada

Una persona A desea enviarle un mensaje M, codificado como un string binario de m bits, pero por problemas de conexión solo puede enviar $n < m$ bits.

Para resolver lo anterior, A define $p = \frac{M}{2^m}$ y envía n bits, eligiendo un 1 con probabilidad p y un 0 con probabilidad $1 - p$, de manera independiente para cada bit.

1. Entregue un algoritmo que decodifica el mensaje de A a partir de los n bits y el largo m del mensaje.
2. Acote la probabilidad de que el mensaje decodificado sea incorrecto.
3. ¿Cuántos bits debe enviar A para que la probabilidad de error sea menor a ε? ¿Es eficiente la solución de A?