Complejidad computacional

Problemas de Criptología - Hoja 5

Curso 07-08

1 **Complejidad de una conversión.** Dado un entero de k bits en base 2, calcula la complejidad de la conversión del entero a base 10.

2 **Complejidades diversas.** Obtén la complejidad del cálculo de $n!$, 3^n y n^n.

3 **Complejidades en $\mathbb{Z}_n$.** Calcula la complejidad de:

(a) La suma $a + b \bmod n$, donde a, b son dos enteros positivos arbitrarios.
(b) La suma $a + b \bmod n$, donde a, b son dos enteros positivos menores que n.
(c) La resta de a y b en los dos casos anteriores.
(d) El producto en los dos casos primeros.

4 **Complejidades asociadas al algoritmo de Euclides.** Calcula la complejidad de:

(a) El algoritmo de Euclides para dos enteros positivos a, b con $a > b$.
(b) Hallar dos números s, t tales que $as + bt = (a, b)$.
(c) Hallar el inverso de $a \bmod m$, donde m es un entero positivo.

5 **Clasificación de problemas.** Clasifica los siguientes problemas como polinómicos o exponenciales.

(a) La conversión de un entero representado en base 2 a su representación en base 10.
(b) Cálculo de $n!$.
(c) Cálculo del inverso de $a \bmod n$.
(d) Producto de dos enteros a, b en $\mathbb{Z}_n$, donde $a, b \leq n$.
(e) Cálculo de n^n.
(f) Cálculo de la suma de los n primeros enteros.

6 **Reducción de problemas.** Prueba que el problema de encontrar un ciclo hamiltoniano se puede reducir en tiempo polinómico al problema del viajante.

7 **El problema de la suma de un subconjunto.** Dado el conjunto $S = \{1, 3, 2, 5, 11, -7, 9, 4, -23, 10\}$ y $m = 0$, resuelve a mano el problema de la suma de un subconjunto.