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

Ayudantía 11

Teoría de números

Problema 1: Teorema de Lagrange

Demuestre que si $(G, \circ)$ es un grupo finito y $(H, \circ)$, es un subgrupo de $(G, \circ)$, entonces $|H|$ divide a $|G|$.

Problema 2: Teorema Chino de los Restos

1. Sean m, n tales que $gcd(m, n) = 1$. Demuestre que para todo a, b existe c tal que:

$$\begin{aligned} c &\equiv a \mod m \\ c &\equiv b \mod n \end{aligned}$$

2. Demuestre que la solución anterior es única bajo $\equiv \text{mod}(m \cdot n)$
3. Demuestre que a es primo relativo con m y b es primo relativo con n ssi c es primo relativo con $m \cdot n$.
4. Utilice lo anterior para demostrar que si $gdc(m, n) = 1$, entonces $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$, donde $\phi(n) = |\mathbb{Z}_n^*|$.
5. Demuestre que si p es primo, entonces $\phi(p^k) = p^{k-1}(p-1)$
6. Demuestre que si $n = p^{e_1} \cdot p^{e_2} \cdot ... \cdot p^{e_q}$, donde $i \neq j \Rightarrow p_i \neq p_j$, todo p_i es primo y $e_i > 0$, entonces:

$$\phi(n) = n \prod_{i=1}^{1} \left(1 - \frac{1}{p_i}\right)$$

Problema 3

1. Dados enteros $\{d_1, ..., d_n\}$, se define $gcd(d_1, ..., d_n)$ como el menor entero positivo que divide a todos los d_i. Demuestre que existen enteros $\{x_1, ..., x_n\}$ tales que:

$$gcd(d_1, ..., d_n) = d_1 \cdot x_1 + ... + d_n x_n\}$$

2. Sea $J \subseteq \mathbb{Z}$, con $J \neq \emptyset$, tal que para todo $x \in J$ y para todo $z \in \mathbb{Z}$ se cumple que $xz \in J$. Además si $a, b \in J$, entonces $a + b \in J$. Demuestre que existe $z \in \mathbb{Z}$ tal que:

$$J = \{zt \mid t \in \mathbb{Z}\}$$

3. Dados enteros positivos $\{d_1, ..., d_n\}$ se define el conjunto S como:

$$S(d_1, ..., d_n) = \{d_1 \cdot x_1 + ... + d_n x_n \mid x_1, ..., x_n \in \mathbb{Z}\}$$

Desarrolle y analice un algoritmo que dado un entero X y enteros $d_1, ..., d_n$ determine si X pertenece o no a $S(d_1, ..., d_n)$.