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 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 $|G|$.

Solución: Esta demostración se encuentra en la clase 21.

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:

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

Solución: Sean $d \equiv n^{-1} \mod m$ y $e = m^{-1} \mod n$. Definimos $c = a \cdot n \cdot d + b \cdot m \cdot e$, podemos ver que:

$$\begin{aligned} c &\equiv a \cdot n \cdot d + b \cdot m \cdot e \mod m \\ &\equiv a \cdot n \cdot d \mod m \\ &\equiv a \cdot n \cdot n^{-1} \mod m \\ &\equiv a \mod m \end{aligned}$$

Además, de forma análoga, podemos demostrar que $c \equiv b \mod n$.

2. Demuestre que la solución anterior es única bajo $\equiv \mod(m \cdot n)$.

Solución: Sean x, y tales que $x \equiv y \equiv a \mod m$, $x \equiv y \equiv b \mod n$. Es claro que:

$$\begin{aligned} & m|(x-y) \ \wedge \ n|(x-y) \\ \Rightarrow\ & m \cdot n|(x-y) \\ \Rightarrow\ & x \equiv y \mod (m \cdot n) \end{aligned}$$

3. Demuestre que a es primo relativo con m y b es primo relativo con n ssi c es primo relativo con $m \cdot n$.

Solución: Sup. que $gcd(a, m) = 1$ y $gcd(b, n) = 1$

$$\begin{aligned} & \Rightarrow gcd(c, m) = 1 \ \wedge \ gcd(b, n) = 1 \\ & \Rightarrow \exists s, t, u, v.\ sc + tm = 1 \ \wedge \ uc + vn = 1 \end{aligned}$$

$$\begin{aligned}\Rightarrow 1 &= (sc+tm)\cdot(uc+vn)\\ &= suc^2+tmuc+scvn+tmvn\\ &= c(suc+tmu+svn)+mn(tv)\\ &\Rightarrow gcd(c,mn)=1\end{aligned}$$

Por otra parte, sup. que $gcd(c,mn)=1$, esto significa necesariamente que $gcd(c,m)=1$ y $gcd(c,n)=1$, lo que a su vez implica que $gcd(a,m)=1$ y $gcd(b,n)=1$.

4. Utilice lo anterior para demostrar que si $gdc(m,n)=1$, entonces $\phi(m\cdot n)=\phi(m)\cdot\phi(n)$, donde $\phi(n)=|\mathbb{Z}_n^*|$.

   Solución: Podemos definir las siguientes funciones entre $\mathbb{Z}_m^*\times\mathbb{Z}_n^*$ y $\mathbb{Z}_{mn}^*$:

$$\begin{aligned}f((a,b)) &= and+bme\\ f^{-1}(c) &= (c \mod m, c \mod n)\end{aligned}$$

   con $d=n^{-1} \mod m$ y $e=m^{-1} \mod n$. Luego, es fácil ver que ambas funciones son biyecciones, por tanto:

$$\begin{aligned}|\mathbb{Z}_m^*\times\mathbb{Z}_n^*| &= |\mathbb{Z}_{mn}^*|\\ \Rightarrow \phi(m)\cdot\phi(n) &= \phi(m\cdot n)\end{aligned}$$

5. Demuestre que si p es primo, entonces $\phi(p^k)=p^{k-1}(p-1)$

   Solución: Sea $q\neq p$ un número tal que $gcd(q,p^k)\neq 1$. Para que lo anterior se cumpla, q debe ser múltiplo de p, pues los únicos divisores de p son 1 y p.

   Luego, los números de $\mathbb{Z}_{p^k}$ que son coprimos a p^k son:

$$0\cdot p,\ 1\cdot p,\ 2\cdot p,\ ...,\ (p^{k-1}-1)\cdot p$$

   Lo que significa que exactamente p^{k-1} números no coprimos a p^k en $\mathbb{Z}_{p^k}$:

$$\Rightarrow \phi(p^k)=|Z_{p^k}^*|=|Z_{p^k}|-p^{k-1}=p^k-p^{k-1}=p^{k-1}(p-1)$$

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:

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

   Solución:

$$\begin{aligned}\phi(n) &= \phi(p_1^{e_1}\cdot p_2^{e_2}\cdot ...\cdot p_q^{e_q})\\ &= \phi(p_1^{e_1})\cdot\phi(p_2^{e_2})\cdot ...\cdot\phi(p_q^{e_q})\\ &= p_1^{e_1-1}(p_1-1)\cdot ...\cdot p_q^{e_q-1}(p_q-1)\\ &= p_1^{e_1}\left(1-\frac{1}{p_1}\right)\cdot ...\cdot p_q^{e_q}\left(1-\frac{1}{p_q}\right)\\ &= \prod_{i=1}^{q}p_i^{e_i}\cdot\prod_{i=1}^{q}\left(1-\frac{1}{p_q}\right)\\ &= n\cdot\prod_{i=1}^{q}\left(1-\frac{1}{p_i}\right)\end{aligned}$$

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:

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

Solución: Para demostrar esto, necesitamos demostrar que $gcd(d_1, ..., d_n) = gcd(d_1, gcd(d_2, ..., d_n))$. Sean $g = gcd(d_1, ..., d_n)$ y $h = gcd(d_1, gcd(d_2, ..., d_n))$. Tenemos:

$$\begin{aligned} & g|d_1, ..., d_n \\ \Rightarrow & g|d_1 \wedge g|gcd(d_2..., d_n) \\ \Rightarrow & g|gcd(d_1, gcd(d_2..., d_n)) \\ \Rightarrow & g|h \end{aligned}$$

Similarmente:

$$\begin{aligned} & h|d_1 \wedge h|gcd(d_2, ..., d_n) \\ \Rightarrow & h|d_1, ..., d_n \\ \Rightarrow & h|gcd(d_1, ..., d_n) \\ \Rightarrow & h|g \end{aligned}$$

Por tanto, se debe cumplir que $g = h$. Utilizando esto, podemos usar inducción para demostrar lo que queremos, donde los casos base son $n = 1$ y $n = 2$ (que se cumplen trivialmente) y el paso inductivo es:

$$\begin{aligned} gcd(d_1, ..., d_n) &= gcd(d_1, gcd(d_2, ..., d_n)) \\ &= x_1 \cdot d_1 + x_2' \cdot gcd(d_2, ..., d_n)) \\ &= x_1 \cdot d_1 + x_2' \cdot (y_2 \cdot d_2 + ... + y_n \cdot d_n) \\ &= x_1 \cdot d_1 + x_2 \cdot d_2 + ... + x_n \cdot d_n \end{aligned}$$

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:

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

Solución: Sea $a \in J$ tal que $a \neq 0$ (si J solamente contiene al 0, la proposición se cumple trivialmente). Por definición de J, es claro que $-a \in J$, por lo que podemos definir el conjunto:

$$J^+ = \{b \in J \mid b > 0\}$$

Sea $d = min(J^+)$ y $c \in J$ un elemento cualquiera de J. Sabemos que existe t entero y $0 \leq r < d$ tales que:

$$\begin{aligned} & c = t \cdot d + r \\ \Rightarrow & r = c - t \cdot d \end{aligned}$$

Como $c \in J$ y $d \in J$, entonces $td \in J$ y $r \in J$. Sin embargo, sabemos que $0 \leq r < d$, por tanto $r = 0$ y como esto se cumple para cualquier $c \in J$:

$$J \subseteq \{dt | t \in \mathbb{Z}\}$$

Además, por la definición de J, se cumple que $\{dt | t \in \mathbb{Z}\} \subseteq J$, por lo tanto $J = \{dt | t \in \mathbb{Z}\}$, es decir, 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 $S(d_1, ..., d_n)$.

Solución: Por la parte 1, $g = gcd(d_1, ..., d_n) \in S(d_1, ..., d_n)$ y además g será el menor entero positivo en S.

Por otra parte, podemos ver que $S(d_1, ..., d_n)$ cumple las propiedades que pedimos para J, lo que significa que:

$$S(d_1, ..., d_n) = \{gt \mid t \in \mathbb{Z}\}$$

Luego, dados $X, d_1, ..., d_n$, el algoritmo deberá calcular $g = gcd(d_1, ..., d_n)$, y responder `True` ssi $g|X$.