Pontificia Universidad Católica de Chile
Facultad de Ingenieria
Departamento de Ciencias de la Computación
IIC2283 - Diseño y Análisis de Algoritmos

# Ayudantía 8

19 de octubre, 2018

---

## Problema 1

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

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

**Solución:**

Lo primero es demostrar que $MCD(d_1, ..., d_n) = MCD(d_1, MCD(d_2, ..., d_n))$. Sean $f = MCD(d_1, ..., d_n)$, $e = MCD(d_1, MCD(d_2, ..., d_n))$. Tenemos que

$$\begin{aligned} f \mid d_1, ..., d_n &\implies f \mid d_1, f \mid MCD(d_2, ..., d_n) \\ &\implies f \mid MCD(d_1, MCD(d_2, ..., d_n)) \\ &\implies f \mid e \end{aligned}$$

$$\begin{aligned} e \mid d_1, e \mid MCD(d_2, ..., d_n) &\implies e \mid d_1, ..., d_n \\ &\implies e \mid MCD(d_1, ..., d_n) = f \\ &\implies e \mid f \end{aligned}$$

Como $e \mid f$ y $f \mid e$, se concluye que $e = f$.

Utilizando esto se puede hacer inducción para demostrar la proposición original:

- Casos base: para $n = 1$ es trivial, para $n = 2$ se desprende directamente del lema de Bezout
- Paso Inductivo:

$$\begin{aligned} MCD(d_1, ..., d_n) &= MCD(d_1, MCD(d_2, ..., d_n)) \\ &= x_1 \cdot d_1 + x_2 \cdot MCD(d_2, ..., d_n) && \text{(Lema de Bezout)} \\ &= x_1 \cdot d_1 + x_2 \cdot (y_2 \cdot d_2 + ... + y_n \cdot d_n) && \text{(Hipotesis de Induccion)} \\ &= z_1 \cdot d_1 + z_2 \cdot d_2 + ... + z_n \cdot d_n \end{aligned}$$

□

2. Sea $J \subseteq \mathbb{Z}$, $J \neq \emptyset$ 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 $a \in \mathbb{Z}$ tal que

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

**Solución:**

Si $J = \{0\}$ entonces es trivialmente verdadero. Si $J \neq \{0\}$, tomemos $a \in J$ que cumpla $a \neq 0$. Por definición de $J$, tenemos que $a \in J$ y $-a \in J$, de los cuales uno es positivo. Por lo tanto, $J' = \{b \mid b > 0 \wedge b \in J\}$ es no vacío. Sea $d = \min(J')$.

La idea es intentar demostrar que $J$ corresponde precisamente al conjunto de múltiplos de $d$. Sea $c$ un elemento cualquiera de $J$. Tenemos que

$$\begin{aligned} & c = qd + r, 0 \leq r < d \\ \implies & r = c - qd \\ \implies & r \in J, r < d \\ \implies & r = 0 \\ \implies & d \mid c \\ \implies & J \subseteq \{dt \mid t \in \mathbb{Z}\} \end{aligned}$$

Pero por definición de $J$ tenemos que $\{dt \mid t \in \mathbb{Z}\} \subseteq J$

Por lo tanto, $J = \{dt \mid t \in \mathbb{Z}\}$.

3. Dados enteros positivos $d_1, ..., d_n$, se define el conjunto $S$ como

$$S(d_1, ..., d_n) = \{d_1x_1 + ... + d_nx_n \mid x_1, ..., x_n \in \mathbb{Z}\}$$

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, $g = MCD(d_1, ..., d_n) \in S(d_1, ..., d_n)$. Además, $g$ es el mínimo positivo de $S(d_1, ..., d_n)$ pues $g$ divide a todos los elementos de $S(d_1, ..., d_n)$.

Por el otro lado, $S(d_1, ..., d_n)$ cumple las propiedades de la parte 2.

$$\implies S(d_1, ..., d_n) = \{gt | g = MCD(d_1, ..., d_n) \wedge t \in \mathbb{Z}\}$$

Así, el algoritmo es:

`Input:` $X, d_1, ..., d_n$

- Calcular $g = MCD(d_1, ..., d_n)$
- Verificar si $g \mid X$

# Problema 2

Los computadores en general realizan las operaciones de resta, chequeo de paridad y dividir por 2 más rápido que computar restos y divisiones arbitrarias. En este problema se desarrolla un algoritmo para calcular el MCD de dos números utilizando solo las operaciones mencionandas anteriormente.

1. Demuestra que si $a$ y $b$ son pares, entonces $MCD(a, b) = 2 \cdot MCD(a/2, b/2)$

**Solución:**

Por el lema de Bezout, tenemos que

$$\begin{aligned} x \cdot \frac{a}{2} + y \cdot \frac{b}{2} &= d = MCD(a/2, b/2) \\ ax + by &= 2d \end{aligned}$$

¿Es $2d$ el mínimo de $\{ax_0 + by_0 \mid x_0, y_0 \in \mathbb{Z}, ax_0 + by_0 > 0\}$? Si lo fuera, el lema de bezout nos diría que $MCD(a, b) = 2d$

Supongamos por contradicción que no lo es, es decir, tenemos que

$$w = ax' + by', 0 < w < 2d$$

$$\implies \frac{w}{2} = \frac{a}{2}x' + \frac{b}{2}y', \text{ con } \frac{w}{2} < d \rightarrow\leftarrow$$

$$\therefore 2 \cdot MCD(a/2, b/2) = MCD(a, b)$$

2. Demuestra que si $a$ es impar y $b$ es par, entonces $MCD(a, b) = MCD(a, b/2)$

   **Solución:**

   Sean $d = MCD(a, b/2)$ y $d' = MCD(a, b)$, donde $2 \nmid d'$ (Si 2 dividiera a $d'$, entonces tambien dividiría a $a$, lo que es una contradicción).

   Tenemos que $d \mid a, b$, por lo que se cumple que $d \mid d'$. Además, tenemos que

$$\begin{aligned}
b = k_2 \cdot d' &\implies \frac{b}{2} = \frac{k_2 d'}{2} \\
&\implies 2 \mid k_2 \qquad \left(\frac{b}{2} \in \mathbb{Z}, \text{ 2 es primo y } 2 \nmid d'\right) \\
&\implies \frac{b}{2} = k_3 d', k_3 \in \mathbb{Z} \\
&\implies d' \mid \frac{b}{2} \\
&\implies d' \mid d \\
&\implies d = d'
\end{aligned}$$

3. Demuestra que si $a$ y $b$ son ambos impares, entonces $MCD(a, b) = MCD((a - b)/2, b)$

   Basta demostrar que $MCD(a, b) = MCD(a - b, b)$. Luego $a - b$ es par, por lo que se puede utilizar la proposición del item 2 para demostrar lo pedido.

   Sean $d = MCD(a, b)$ y $d' = MCD(a - b, b)$. Tenemos que

$$d \mid a, b \implies d \mid a - b, b \implies d \mid d'$$

   Además,

$$\begin{aligned}
d' \mid a - b, b &\implies a - b = k_1 d', \quad b = k_2 d' \\
&\implies a = (k_1 + k_2) d' \\
&\implies d' \mid a \\
&\implies d' \mid d \\
&\implies d' = d
\end{aligned}$$

4. Diseña un algoritmo para calcular el máximo común divisor entre dos números $a$ y $b$ que utilice solamente las operaciones

   - Resta
   - Dividir por 2
   - Multiplicar por 2
   - Chequeo de paridad

   El algoritmo debe correr en tiempo $O(\log(a))$. Asume que cada una de las 3 operaciones anteriores toma tiempo unitario.

   **Solución:**

   El algoritmo consiste simplemente en aplicar las reglas anteriores de manera recursiva:

   **procedure** BGCD($a, b$)
   **if** $b > a$ **then** swap(a,b)

**if** $b == 0$ **then return** $a$
**if** $a\%2 == 0$ and $b\%2 == 0$ **then return** $2 \cdot \text{BGCD}(a/2, b/2)$
**if** $a\%2 == 1$ **then return** $\text{BGCD}(a/2, b)$
**if** $b\%2 == 1$ **then return** $\text{BGCD}(a, b/2)$
**return** $\text{BGCD}((a-b)/2, b)$

# Problema 3

1. (Teorema Chino del Resto) Sean $m, n$ tales que $MCD(m, n) = 1$. 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 $d = n^{-1} \mod m$, $e = m^{-1} \mod n$.

Tomemos $c = a \cdot n \cdot d + b \cdot m \cdot e$. Tenemos que

$$\begin{aligned} c &\equiv and + bme \mod m \\ c &\equiv and \mod m \\ c &\equiv ann^{-1} \mod m \\ c &\equiv a \mod m \end{aligned}$$

De manera análoga se cumple que $c \equiv b \mod n$.

2. Demuestre que la solución anterior es única $\mod m \cdot n$.

**Solución:**

Sean $x, y$ soluciones $\mod m \cdot n$. Tenemos que

$$\begin{aligned} x \equiv y \equiv a &\mod m \\ x \equiv y \equiv b &\mod n \\ \implies & \begin{matrix} m \mid (x-y) \\ n \mid (x-y) \end{matrix} \\ \implies & m \cdot n \mid (x-y) \\ \implies & x \equiv y \mod m \cdot n \end{aligned}$$

donde el penúltimo paso es válido pues $MCD(m, n) = 1$.

3. Demuestre que $a$ es relativamente primo con $m$ y $b$ es relativamente primo con $n$ si y solo si la solución $c$ al sistema de congruencias es relativamente primo a $m \cdot n$.

**Solución:**

p.d. $MCD(a, m) = 1 \wedge MCD(b, n) = 1 \implies MCD(c, mn) = 1$

$$\begin{matrix} MCD(a,m) = 1 \\ MCD(b,n) = 1 \end{matrix} \implies \begin{matrix} MCD(c,m) = 1 \\ MCD(c,n) = 1 \end{matrix} \implies \begin{matrix} s_1c + t_1m = 1 \\ s_2c + t_2n = 1 \end{matrix}$$

$$\implies c(s_1s_2c + s_1t_2n + s_2t_1m) + mn(t_1t_2) = 1 \implies MCD(c, mn) = 1$$

p.d. $MCD(c, mn) = 1 \implies MCD(a, m) = 1 \wedge MCD(b, n) = 1$

$$MCD(c,mn) = 1 \implies \begin{matrix} MCD(c,m) = 1 \\ MCD(c,n) = 1 \end{matrix} \implies \begin{matrix} MCD(a,m) = 1 \\ MCD(b,n) = 1 \end{matrix}$$

4. Utilice lo anterior para demostrar que si $MCD(m,n) = 1$, entonces $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$. Recordar: $\phi(n) = |\mathbb{Z}_N^*|$, $\mathbb{Z}_N^* = \{a \in \{1, ..., n-1\} \mid MCD(a,n) = 1\}$.

   **Solución:**

   Por las partes 1,2 y 3, hay una biyección entre $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ y $\mathbb{Z}_{mn}^*$ dada por

$$f((a,b)) = and + bme$$

$$f^{-1}(c) = (c \mod m, c \mod n)$$

   donde $d = n^{-1} \mod m$, $e = m^{-1} \mod n$.

   Por lo tanto, tenemos que

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

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

   **Solución:**

   Dado $x < p$, para que $MCD(x, p^k) \neq 1$ debe cumplirse que $x$ sea múltiplo de $p$ (pues $p$ es primo, sus únicos divisores son 1 y $p$).

   Por lo tanto, los números no coprimos a $p^k$ en $\mathbb{Z}_{p^k}$ son

$$0 \cdot p, 1 \cdot p, 2 \cdot p, 3 \cdot p, ..., (p^{k-1} - 1) \cdot p$$

   Esto implica que hay $p^{k-1}$ números no coprimos a $p^k$ en $\mathbb{Z}_{p^k}$.

$$\implies \phi(p^k) = |\mathbb{Z}_{p^k}^*| = |\mathbb{Z}_{p^k}| - p^{k-1} = p^k - p^{k-1} = p^{k-1}(p-1)$$

6. Demuestre que si $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdot ... \cdot p_q^{e_q}$, donde $i \neq j \implies p_i \neq p_j$ y para todo $i$ se cumple que $p_i$ es primo y $e_i > 0$, entonces

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

   **Solución:**

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