

# Soluciones del primer parcial de Matemática Discreta 2 - Curso 2006 - IMERL

Lunes 15 de Mayo de 2006

## Ejercicio 1.

1. Teorema: El sistema de ecuaciones 
$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad \text{con } \text{mcd}(m_i, m_j) = 1 \text{ si } i \neq j$$

con  $i, j \in \{1, \dots, k\}$  tiene una única solución  $x$  módulo  $M = m_1 \times m_2 \times \dots \times m_k$ .

**Demostración:** ♦ Existencia. Sean  $M_1 = m_2 \dots m_k$ ,  $M_2 = m_1 m_3 \dots m_k$ , ...,  $M_k = m_1 m_2 \dots m_{k-1}$ . Entonces  $M_j$  es múltiplo de  $m_i$  para todo  $i \neq j$  y  $\text{MCD}(M_j, m_j) = 1$ . Entonces por el algoritmo de Euclides existen números  $b_j, n_j$  tales que  $b_j M_j + n_j m_j = 1$ . Definimos el número  $x = \sum_{j=1}^k a_j b_j M_j$ . Entonces  $x$  es la solución buscada.

En efecto, dada una ecuación cualquiera  $x \equiv a_i \pmod{m_i}$ , sustituyendo  $x$  por  $\sum_{j=1}^k a_j b_j M_j$  tenemos que todos los sumandos excepto el  $i$ -ésimo son múltiplos de  $m_i$  por lo que esos sumandos son 0 módulo  $m_i$ .

Queda solo  $a_i b_i M_i$ . Pero  $b_i M_i \equiv 1 \pmod{m_i}$  por lo que queda  $a_i b_i M_i \equiv a_i \pmod{m_i}$ .

♦ Unicidad. Si  $x \equiv a_j \pmod{m_j}$  e  $y \equiv a_j \pmod{m_j} \quad \forall j = 1, \dots, k$ , entonces  $x - y \equiv 0 \pmod{m_j} \quad \forall j = 1, \dots, k$ .

Como  $\text{mcd}(m_i, m_j) = 1$  si  $i \neq j$ , se tiene  $x - y \equiv 0 \pmod{m_1 m_2 \dots m_k}$  o sea  $x \equiv y \pmod{M}$ .

2. 
$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{3} \end{cases}$$
 . Al ser 4, 5 y 3 coprimos, sabemos por el teorema chino del resto que este sistema tiene solución

única módulo  $4 \times 5 \times 3 = 60$ .

Tenemos  $M = 4 \times 5 \times 3 = 60$ ,  $M_1 = 15$ ,  $M_2 = 12$ ,  $M_3 = 20$ .

$b_j$  es el inverso de  $M_j$  en  $\mathbb{Z}_{m_j}$ . Obtenemos  $b_1 = -1$ ,  $b_2 = 3$  y  $b_3 = 2$ .

Entonces  $x = 2 \times 15 \times (-1) + 3 \times 12 \times 3 + 2 \times 20 \times 2 = 158 \equiv 38 \pmod{60}$ .

## Ejercicio 2.

1. Si  $[a] \in \mathbb{Z}_n$  es tal que existe su inverso  $[b] \in \mathbb{Z}_n$  entonces  $[a][b] = 1$  en  $\mathbb{Z}_n$  o sea  $ab \equiv 1 \pmod{n}$  lo cual es equivalente en decir que existe  $k \in \mathbb{Z}$  tal que  $ab - 1 = kn$ , o lo que es lo mismo  $ab - kn = 1$  de donde  $\text{MCD}(a, n) = 1$ .

Si  $\text{MCD}(a, n) = 1$  podemos hallar usando el algoritmo de Euclides números  $b, c \in \mathbb{Z}$  tales que  $ab + nc = 1$ . Entonces  $ab \equiv 1 \pmod{n}$  lo cual es lo mismo escribir  $[ab] = 1$  en  $\mathbb{Z}_n$ , y por definición del producto  $[a][b] = 1$ , es decir  $[a]$  es invertible.

2.  $30523 = 131 \times 233$  y 131 y 233 son primos.

$[524]$  no es invertible en  $\mathbb{Z}_{30523}$  pues  $131 \mid 524$ , o sea  $\text{mcd}(30523, 524) \neq 1$ .

$\text{mcd}(30523, 63) = 1$  entonces usando el algoritmo de Euclides se prueba que  $1 = 969 \times 63 - 2 \times 30523$ , es decir  $[63]^{-1} = [969]$ .

3. La cantidad de elementos invertibles en  $\mathbb{Z}_{30523}$  está dado por  $\phi(30523)$  siendo  $\phi$  la función phi de Euler.

$\phi(30523) = \phi(131 \times 233) = 130 \times 232 = 30160$ .

4.  $10000^{3016000} = (10000^{30160})^{100} = (10000^{\phi(30523)})^{100} \equiv 1^{100} = 1 \pmod{30523}$  usando el teorema de Euler.

## Ejercicio 3.

1.  $H_n$  es el conjunto de las potencias  $n$ -ésimas de  $G$ , o sea  $H_n = \{g \in G / \exists h \in G \text{ tal que } g = h^n\}$ .

$H_n$  es un subgrupo de  $G$  pues:

- es no vacío:  $e_G \in H_n$  pues  $e_G = e_G^n$ .

- es cerrado con el producto:  $g_1, g_2 \in H_n$  entonces  $g_1 = h_1^n$  y  $g_2 = h_2^n$ .  $g_1 g_2 = h_1^n h_2^n = (h_1 h_2)^n \in H_n$ .

- El inverso de cada elemento de  $H_n$  pertenece a  $H_n$  y si  $g \in H_n$  entonces  $(g^{-1})^n = (g^n)^{-1}$ .

Entonces  $H_n < G$ . Por el teorema de Lagrange el orden de  $H_n$  divide al orden de  $G$  o sea  $\kappa = |G|/|H_n| \in \mathbb{N}$ .

2. Sea  $\{y_1, y_2, \dots, y_p\}$  el conjunto de soluciones de la ecuación  $y^n = e$ .

Si  $g \in H_n$  entonces existe  $h \in G$  tal que  $h^n = g$ . Luego la ecuación  $x^n = g$  se transforma en  $x^n = h^n$ , es decir  $(xh^{-1})^n = e$ , o sea  $xh^{-1} \in \{y_1, y_2, \dots, y_p\}$ . Entonces  $x \in \{y_1 h, y_2 h, \dots, y_p h\}$  y la ecuación  $x^n = g$  tiene entonces  $p$  soluciones.

Si  $H_n = \{g_1, g_2, \dots, g_s\}$ , entonces  $H_n$  tiene  $s$  elementos y la unión de las soluciones de las ecuaciones  $x^n = g_1, x^n = g_2, \dots, x^n = g_s$  es todo el grupo  $G$ . Entonces  $|G| = p + p + \dots + p = sp$ . Como  $s = |H_n|$  se deduce que  $p = \kappa$ .

3. Al ser  $H_n$  un subgrupo de  $G$  tenemos que  $H_n \subset G$ . Probemos ahora que todo elemento de  $G$  es un elemento de  $H_n$ .

Sea  $g \in G$ . Como  $\text{mcd}(|G|, n) = 1$  existen  $s, t \in \mathbb{Z}$  tales que  $t|G| + sn = 1$ .

Entonces  $g = g^1 = g^{t|G| + sn} = (g^{|G|})^t (g^s)^n = (g^s)^n$  (aquí usamos que si  $x \in G$  entonces  $x^{|G|} = e$ ). Luego si  $h = g^s$  entonces  $g = h^n$  para algún  $h \in G$ , es decir  $g \in H_n$ . Concluimos entonces que  $G \subset H_n$  y finalmente que  $G = H_n$ .

**Ejercicio 4.**

1.  $13^{663} \equiv (-1)^{663} \equiv -1 \equiv 6 \pmod{7}$

2.  $276 = 2 \times 2 \times 3 \times 23$ . Como  $10 < d < 30$  y  $d$  es divisor de 276 entonces las únicas posibilidades son 12 o 23.

Si  $d = 12$  entonces  $m + 36 = 276$  o sea  $m = 240$ . Sean  $a = 12a'$  y  $b = 12b'$  con  $\text{mcd}(a', b') = 1$ .

Entonces  $m = 12a'b' = 240$ , es decir  $a'b' = 20$ . Las posibilidades para  $a'$  y  $b'$  son:

$a' = 1$  y  $b' = 20$ ;

$a' = 2$  y  $b' = 10$  no puede ser pues no serían primos entre sí;

$a' = 4$  y  $b' = 5$ .

Tenemos entonces las soluciones:  $a = 12, b = 240$  y  $a = 48, b = 60$ .

Si  $d = 23$  entonces  $m + 69 = 276$  o sea  $m = 207$ . Sean  $a = 23a'$  y  $b = 23b'$  con  $\text{mcd}(a', b') = 1$ .

Entonces  $m = 23a'b' = 207$ , es decir  $a'b' = 9$ . Las posibilidades para  $a'$  y  $b'$  son:

$a' = 1$  y  $b' = 9$ ;

$a' = 3$  y  $b' = 3$  no puede ser pues no serían primos entre sí;

Tenemos entonces la solución :  $a = 23, b = 207$ .