

Examen de Matemática Discreta II
28 de febrero de 2009

Número de Examen	Cédula	Nombre y Apellido

Ejercicio 1. (30 puntos)

- i) Probar que $\sigma(x_1, x_2)(y_1, y_2, y_3)\sigma^{-1} = (\sigma(x_1), \sigma(x_2))(\sigma(y_1), \sigma(y_2), \sigma(y_3))$, siendo σ una permutación de S_n , con $x_i \neq y_j$, $i = 1, 2$; $j = 1, 2, 3$.
- ii) Se consideran las permutaciones $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ c & 2 & b & 3 & 1 & a & d \end{pmatrix}$ y $\tau = (3, 5, 6)$ donde $\{a, b, c, d\} = \{4, 5, 6, 7\}$. Hallar a, b, c y d sabiendo que $\tau\theta\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & a & 5 & c & 1 & 4 \end{pmatrix}$.
- iii) Sea $\delta = (7, 4)$. Calcular $(\theta\tau\delta)^{2009}$.

Ejercicio 2. (35 puntos)

- a) Diremos que un par de enteros coprimos (x_1, x_2) es *reducible* si existe $n_1 \in \mathbb{Z}$ tal que $x_1 + n_1x_2 = 1$.
 - 1) Dar un ejemplo de un par de coprimos reducible.
 - 2) Dar un ejemplo de un par de coprimos no reducible (justificar).
- b) Diremos que una terna de enteros (x_1, x_2, x_3) son coprimos si existen $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$ tal que $\alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 = 1$.
 - 1) Dar un ejemplo de una terna de coprimos tal que cada par de enteros (x_i, x_j) , con $1 \leq i, j \leq 3$, no sean coprimos.
 - 2) Demostrar que (x_1, x_2, x_3) son coprimos si y solamente si no existe un primo p que divida a x_i para $i = 1, 2, 3$.
- c) Se dice que una terna (x_1, x_2, x_3) de coprimos es *reducible* si existen $n_1, n_2 \in \mathbb{Z}$ tal que $(x_1 + n_1x_3, x_2 + n_2x_3)$ es un par de enteros coprimos.
 - 1) Mostrar que $(6, 10, 15)$ es reducible.
 - 2) Demostrar que toda terna de coprimos es reducible.
(Sugerencia: multiplicar a x_3 por los factores primos de x_1 no comunes a x_2 .)

Ejercicio 3. (35 puntos)

Si p un primo impar, decimos que r es una raíz primitiva módulo p si se verifica:

$$\min\{n \in \mathbb{Z}^+ / r^n \equiv 1 \pmod{p}\} = p - 1$$

Sea p primo impar y r una raíz primitiva módulo p .

- i) Probar que $r^a \equiv 1 \pmod{p} \Leftrightarrow a \equiv 0 \pmod{p-1}$.
- ii) Probar que $r^a \equiv r^b \pmod{p} \Leftrightarrow a \equiv b \pmod{p-1}$.

- iii) Probar que la función $e : \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^*$ definida por $e(a \pmod{p-1}) = r^a \pmod{p}$ es biyectiva (sug: probar que es inyectiva). A la función inversa de e la llamamos logaritmo discreto en base r y se caracteriza por la propiedad $\log_r a = \beta \Leftrightarrow r^\beta \equiv a \pmod{p}$.
- iv) Probar que si $a \not\equiv 0 \pmod{p}$ y $n \in \mathbb{Z}^+$ entonces $\log_r(a^n) \equiv n \log_r a \pmod{p-1}$.
- v) Supongamos que Marta y Pepe quieren utilizar el método Diffie-Hellmann de intercambio de clave usando el primo $p = 5003$ y $a = 820$. Marta le envía a Pepe el número $x = 996$, Pepe luego le envía a Marta el número $y = 872$. Si se sabe que 2 es una raíz primitiva módulo 5003 y los siguientes logaritmos $\log_2 820 = 123$ y $\log_2 996 = 697$, hallar la clave común acordada por Marta y Pepe (puede serle de ayuda el cuadrado de abajo).

n	0	1	2	3	4	5	6
$872^{2^n} \pmod{5003}$	872	4931	181	2743	4540	4243	2255