

Examen de Matemática Discreta II  
28 de febrero de 2009

SOLUCIÓN

- Ejercicio 1.**
- 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  $\sigma$  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  $(\theta\tau\delta)^{2009}$ .

**Solución:**

- i) Se tiene que  $\sigma(x_1, x_2)(y_1, y_2, y_3)\sigma^{-1} = \sigma(x_1, x_2)\sigma^{-1}\sigma(y_1, y_2, y_3)\sigma^{-1}$ . Luego basta probar el resultado para un ciclo cualquiera:  $\sigma(z_1, z_2, \dots, z_n)\sigma^{-1} \stackrel{?}{=} (\sigma(z_1), \sigma(z_2), \dots, \sigma(z_n))$ . Y esta última igualdad es fácil de probar, calculando ambas permutaciones en los elementos  $\{\sigma(z_1), \sigma(z_2), \dots, \sigma(z_n)\}$ .
- ii) (*letra original corregida*)  
Se tiene que  $\tau\theta\tau^{-1}$  transforma los elementos así:  $7 \rightarrow 4 \rightarrow 5 \rightarrow c$  y  $6 \rightarrow 1 \rightarrow 3 \rightarrow a$ , dejando fijo al 2, siendo:

Caso (1):  $a = 6$  y  $c = 7$  con  $\tau\theta\tau^{-1} = (7, 4, 5)(6, 1, 3)$ ;

Caso (2):  $a = 7$  y  $c = 6$  con  $\tau\theta\tau^{-1} = (7, 4, 5, 6, 1, 3)$ .

Calculando  $\tau^{-1}(\tau\theta\tau^{-1})\tau$  se obtiene  $\theta$  en ambos casos:

Caso (1):  $\theta = (7, 4, 3)(5, 1, 6)$ ;

Caso (2):  $\theta = (7, 4, 3, 5, 1, 6)$ .

Entonces el único caso posible es el (2),  $a = 7$ ,  $c = 6$ ,  $b = 5$  y  $d = 4$ .

- iii) (*letra original*)  
Tenemos que  $(\theta\tau\delta)^{2009} = (16573)^{2009} = (16573)^4$  por ser un 5-ciclo. Luego  $(\theta\tau\delta)^{2009} = (16573)^{-1} = (37561)$ .

*La solución usando la matriz  $\theta = (165)(374)$ , que se fijó durante el desarrollo del examen sería:  $(\theta\tau\delta)^{2009} = (7316)^{2009} = (7316)$  por ser un 4-ciclo.*

- Ejercicio 2.**
- 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  $(x_1 + n_1 x_3, x_2 + n_2 x_3)$  es un par de enteros coprimos.
- 1) Mostrar que  $(6, 10, 15)$  es reducible.
- 2) Demostrar que toda terna de coprimos es reducible.

### Solución:

- a) 1) Ejemplo:  $(7, 3)$ , pues  $7 + (-2) \times 3 = 1$ .
- 2) Ejemplo:  $(3, 7)$ , pues  $3 + n \times 7 = 1$  implicaría que 7 divide a 2, absurdo.
- b) 1) Ejemplo:  $(6, 10, 15)$ , pues  $1 \times 6 + 1 \times 10 + (-1) \times 15 = 1$ , y  $\text{mcd}(6, 10) = 2$ ;  $\text{mcd}(10, 15) = 5$ ;  $\text{mcd}(6, 15) = 3$ .
- 2) Directo:  
Si  $(x_1, x_2, x_3)$  son coprimos, existen, por definición,  $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$  tal que  $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 1$ . Si  $m \in \mathbb{Z}$  divide a  $x_1, x_2, x_3$ , entonces  $m$  divide a  $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 1$ . Luego  $m = \pm 1$ . Esto prueba el directo.  
Recíproco:  
Sea  $d = \text{mcd}(x_1, x_2)$ . Entonces, por el Lema de Bezout, existen  $\beta_1, \beta_2 \in \mathbb{Z}$  tal que  $d = \beta_1 \times x_1 + \beta_2 \times x_2$ . Por hipótesis  $\text{mcd}(d, x_3) = 1$ . Entonces existen  $\gamma, \alpha_3 \in \mathbb{Z}$  tal que  $\gamma \times d + \alpha_3 \times x_3 = 1$ . Sustituyendo obtenemos:  $\gamma \times (\beta_1 \times x_1 + \beta_2 \times x_2) + \alpha_3 \times x_3 = 1$ . Luego definiendo  $\alpha_1 = \gamma \times \beta_1$  y  $\alpha_2 = \gamma \times \beta_2$ , y se obtiene el resultado.
- c) 1) Hay muchas formas de hacer esto. Una forma es considerar  $(6, 10 + 3 \times 15) = (6, 55)$ . O sea  $n_1 = 0$  y  $n_2 = 3$ .
- 2) Sea  $(x_1, x_2, x_3)$  una terna de coprimos cualquiera.  
Afirmación: la terna es reducible.  
Si  $x_1 = p_1^{s_1} \times p_2^{s_2} \times \dots \times p_k^{s_k} \times \dots \times p_n^{s_n}$ , siendo  $p_1, \dots, p_k$ , los factores primos en común entre  $x_1$  y  $x_2$ , consideramos el par  $(x_1, x_2 + p_{k+1} \times \dots \times p_n \times x_3)$ . Este es un par de enteros coprimos. Justificación: si un primo  $q \in \mathbb{Z}$  divide a  $x_1$  y a  $x_2$ , por ser  $(x_1, x_2, x_3)$  una terna de coprimos,  $q$  no puede dividir a  $x_3$ . Luego  $q$  divide a  $x_1$  pero no a  $x_2 + p_{k+1} \times \dots \times p_n \times x_3$ . Ahora si  $q$  divide a  $x_1$  pero no divide a  $x_2$ , entonces  $q$  divide, por construcción, a  $p_{k+1} \times \dots \times p_n \times x_3$ , con lo cual se concluye que  $q$  no divide a  $x_2 + p_{k+1} \times \dots \times p_n \times x_3$ . Entonces  $(x_1, x_2 + p_{k+1} \times \dots \times p_n \times x_3)$  es un par de enteros coprimos.

**Ejercicio 3.** 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 |

### Solución:

- i) Comenzamos observando que, como  $a^{p-1} \equiv 1 \pmod{p}$ , entonces  $a \not\equiv 0 \pmod{p}$ .  
 Sea  $a = x(p-1) + y$  con  $0 \leq y < p-1$ , la división entera de  $a$  por  $p-1$ .  
 $(\Rightarrow)$  Tenemos que  $1 \equiv r^a = (r^{p-1})^x r^y \equiv r^y \pmod{p}$  pero como  $0 \leq y < p-1$  solo puede ser  $y = 0$  (por definición de raíz primitiva) y por lo tanto  $a \equiv 0 \pmod{p-1}$ .  
 $(\Leftarrow)$  Si  $a \equiv 0 \pmod{p-1}$  entonces  $y = 0$  y por lo tanto  $r^a = (r^{p-1})^x \equiv 1 \pmod{p}$ .
- ii) Se tiene que  $r^a \equiv r^b \pmod{p} \Leftrightarrow r^{a-b} \equiv 1 \pmod{p} \Leftrightarrow a-b \equiv 0 \pmod{p-1} \Leftrightarrow a \equiv b \pmod{p-1}$ , donde en el “segundo si y solo si” se usó la parte a.
- iii) La inyectividad se desprende de la parte anterior y como  $\mathbb{Z}_{p-1}$  y  $\mathbb{Z}_p^*$  son conjuntos finitos del mismo cardinal,  $e$  también deberá ser biyectiva.
- iv) Sea  $x = \log_r a$  e  $y = \log_r a^n$  entonces  $r^x \equiv a \pmod{p-1}$  y  $r^y \equiv a^n \pmod{p-1}$ . Se tiene que  $r^{nx} = (r^x)^n \equiv a^n \equiv r^y \pmod{p-1}$  así que  $y \equiv nx \pmod{p-1}$  como se quería probar.
- v) Recordemos que si Marta le manda a Pepe  $a^n \pmod{p}$  y Pepe le manda a Marta  $a^m \pmod{p}$  entonces la clave secreta es  $k = a^{mn} \pmod{p}$ . Tenemos entonces que  $996 \equiv 820^n \pmod{5003} \Leftrightarrow \log_2 996 \equiv n \log_2 820 \pmod{5002} \Leftrightarrow 697 \equiv 123n \pmod{5002} \Leftrightarrow 17 \equiv 3n \pmod{122} \Leftrightarrow n \equiv 41 \cdot 17 \equiv 87 \pmod{122}$ .

Ahora calculamos  $k = a^{mn} = (a^m)^n \equiv 872^{87} = 872^{1+2+4+16+64} \equiv 872 \cdot 4931 \cdot 181 \cdot 4540 \cdot 2255 = 4299832 \cdot 821740 \cdot 2255 \equiv 2255 \cdot 1248 \cdot 2255 = 2814240 \cdot 2255 \equiv 2554 \cdot 2255 = 5759270 \equiv 817 \pmod{5003}$ .

La clave secreta acordada es  $k = 817$ .