

**Solución Examen de Matemática Discreta II**

30 de julio de 2013

Ejercicio 1 (28 puntos) Sea  $a \in \mathbb{N}$  tal que el resto de dividir  $a$  entre 12 es 5.

- a) (10 puntos) Probar que  $a^3 + 4 \equiv 21 \pmod{36}$
- b) (8 puntos) Hallar  $y$  el resto de dividir  $53^3 + 11$  entre 36.
- c) (10 puntos) Siendo  $y$  el hallado en la parte anterior, resolver:

$$\begin{cases} x \equiv -1 \pmod{10} \\ x + 3 \equiv y \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

**Solución Ejercicio 1 (28 puntos)**

- a) (10 puntos) Como  $a$  es congruente con 5 módulo 12, entonces existe  $t \in \mathbb{Z}$  tal que  $12t = a - 5$ . Luego  $(12t)^3 = (a - 5)^3 = a^3 - 3a^2 \cdot 5 + 3a \cdot 5^2 - 5^3 = a^3 - 5^3 - 3a \cdot 5(a - 5)$ . Esto implica que  $a^3 - 5^3 = (12t)^3 + 3a \cdot 5(a - 5)$ . Como  $(a - 5)$  es múltiplo de 12, el segundo término de la igualdad es múltiplo de 36. Esto implica que  $a^3 - 5^3 \equiv 0 \pmod{36}$ , o sea  $a^3 \equiv 125 \pmod{36}$  por lo tanto  $a^3 \equiv 17 \pmod{36}$ .
- b) (8 puntos) Como 53 verifica la hipótesis del ejercicio, tenemos que  $53^3 \equiv 17 \pmod{36}$ . Luego  $53^3 + 11 \equiv 28 \pmod{36}$ , o sea que el resto de dividir  $53^3 + 11$  entre 36, es 28.
- c) (10 puntos)  
El sistema queda:

$$\begin{cases} x \equiv -1 \pmod{10} \\ x + 3 \equiv 28 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

Este sistema es equivalente a

$$\begin{cases} x \equiv -1 \pmod{10} \\ x \equiv 1 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

y éste, a su vez, es equivalente a:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv -1 \pmod{5} \\ x \equiv 1 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

Este último sistema es compatible y equivalente a:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{8} \\ x \equiv 4 \pmod{9} \end{cases}$$

Por el Teorema chino del resto, hay solución: 49, única módulo  $5 \times 8 \times 9 = 360$ .

Ejercicio 2 (22 puntos)

Sea  $G := \{e, a, b, c, d\}$  y una operación binaria  $\star : G \times G \rightarrow G$ , tal que:

$$\begin{aligned} a \star b &= d \\ b \star c &= e \\ d \star a &= e \end{aligned}$$

- a) (6 puntos) Hallar la tabla de Cayley de la operación, sabiendo que  $(G, \star)$  es un grupo y  $e$  es su neutro.
- b) (4 puntos) Demostrar que  $(G, \star)$  es abeliano.
- c) (7 puntos) Describir todos los morfismos de grupos  $f : (G, \star) \longrightarrow (\mathbb{Z}_{12}, +)$ .
- d) (5 puntos) Demostrar que existe  $n \in \mathbb{N}$  tal que  $(G, \star)$  es isomorfo a  $(\mathbb{Z}_n, +)$ . Justificar.

Solución Ejercicio 2 (22 puntos)

- a) (6 puntos) La tabla de Cayley es:

$\star$	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b

- b) (4 puntos) Basta observar que la tabla de Cayley es simétrica.
- c) (7 puntos) Como  $|G| = 5$  y  $|\mathbb{Z}_{12}| = 12$ , entonces la  $\text{Im}(f)$  solo puede tener un elemento (recordar que  $|\text{Im}(f)|$  divide a al orden del grupo dominio y al orden del grupo codominio, si todos son finitos).
- d) (5 puntos) Como  $|G| = 5$  el único  $n$  posible es  $n = 5$ . Ahora bien, definiendo  $g : (G, \star) \longrightarrow (\mathbb{Z}_5, +)$ , tal que  $g(a) = 1, g(c) = 2, g(b) = 3, g(d) = 4, g(e) = 0$ , se obtiene una función biyectiva, que se puede comprobar revisando las tablas de ambos grupos que es un morfismo.

Ejercicio 3 (30 puntos)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Dos interlocutores  $A$  y  $B$  acuerdan comunicarse estableciendo una clave privada mediante el método de Diffie-Hellman. Acuerdan usar el módulo primo  $p = 97$  y como base  $g = 5$ .  $A$  elige además el entero  $m = 3$ , enviándole a  $B$   $g^m$  y recibiendo de éste 36.

- a) (5 puntos) ¿Cuál es la clave privada que acuerdan?
- b) (8 puntos) Usando la correspondencia de la tabla inicial del ejercicio, la clave privada escrita en base 27 determina una palabra. ¿Cuál es esa palabra?

- c) ( $\alpha$  puntos)  $B$  envía a  $A$  el siguiente mensaje: H CVDHROPTOCQ, el cual está encriptado mediante el método de Vigenère, usando la palabra hallada en b). Determinar el mensaje original encriptado por  $B$ .
- d) ( $\beta$  puntos)  $A$  responderá a  $B$ : LO CONOZCO. Encriptar este mensaje mediante el mismo método usado por  $A$ .

(De tal manera que  $\alpha + \beta = 17$  y ambos son menores o iguales a 12).

### Solución Ejercicio 3 (30 puntos)

- a) (5 puntos) En este caso, la forma de hallar la clave es resolver  $36^3 \bmod (97) = 96$ .
- b) (8 puntos) Como  $96 = 3 \times 27^1 + 15 \times 27^0$ , entonces la palabra es  $DP$  (ver en la tabla  $D=3$ , y  $P=15$ ).
- c) ( $\alpha$  puntos) Empecemos observando que el opuesto de  $D$  es  $Y$  (el opuesto de 3 es 24), y el opuesto de  $P$  es  $M$  (el opuesto de 15 es 12) en  $\mathbb{Z}_{27}$ . Se arma la tabla de descryptado Vigenère:

H		C	V	D	H	R	O	P	T	O	C	Q
7	26	2	21	3	7	17	14	15	19	17	2	16
24	12	24	12	24	12	24	12	24	12	24	12	24
4	11	26	6	0	19	14	26	12	4	11	14	13
E	L		G	A	T	O		M	E	L	Ó	N

- d) ( $\beta$  puntos) Para encriptar hay que usar la palabra hallada en b):  $DP$ , que, usando la tabla inicial, es 3 15.

L	O		C	O	N	O	Z	C	O
11	14	26	2	14	13	14	25	2	14
3	15	3	15	3	15	3	15	3	15
14	2	2	17	17	1	17	13	5	2
O	C	C	R	R	B	R	N	F	C

### Ejercicio 4 (20 puntos)

- a) (15 puntos) Enunciar y demostrar el Teorema de Lagrange.  
Ver Teórico.
- b) (5 puntos) Obtener el Teorema de Fermat como corolario del Teorema de Lagrange.  
Simplemente aplicar el Teorema de Lagrange para el grupo  $(U(p), \cdot)$  con  $p$  primo. Dado un elemento  $a \in U(p)$ , sabemos que  $o(a) = |\langle a \rangle|$ , o sea el orden de un elemento coincide con el orden (cardinal) del grupo que elemento genera. Por el Teorema de Lagrange tenemos entonces que  $o(a) = |\langle a \rangle|$  divide a  $|U(p)| = p - 1$ . O sea  $p - 1 = o(a) \cdot t$ , con  $t \in \mathbb{Z}^+$ . Por lo tanto  $a^{p-1} = (a^{o(a)})^t \equiv 1 \bmod (p)$ .