

Examen de Matemática Discreta II
30 de julio de 2013. Duración 3:30 horas.

Número de Examen	Cédula	Nombre y Apellido

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

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

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

Ejercicio 2 (22 **puntos**)

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

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

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

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.

- ¿Cuál es la clave privada que acuerdan?

- b)* Usando la correspondencia de la tabla inicial del ejercicio, la clave privada escrita en base 27 determina una palabra. ¿Cuál es esa palabra?
- c)* *B* envía a *A* el siguiente mensaje: H CVDHROPTOCQ, el cuál está encriptado mediante el método de Vigenère, usando la palabra hallada en *b)*. Determinar el mensaje original encriptado por *B*.
- d)* *A* responderá a *B*: LO CONOZCO. Encriptar este mensaje mediante el mismo método usado por *A*.

Ejercicio 4 (20 **puntos**)

- a)* Enunciar y demostrar el Teorema de Lagrange.
- b)* Obtener el Teorema de Fermat como corolario del Teorema de Lagrange.