

Examen de Matemática Discreta II

24 de febrero de 2010

Número de Examen	Cédula	Nombre y Apellido

1. (25 puntos)

- a) (5 puntos) Enunciar el Teorema Chino del Resto.
- b) Sea $A = \{a_0, a_1, \dots, a_{10}\}$ un conjunto de once enteros positivos de hasta dos cifras y coprimos dos a dos. Un entero positivo se dice que es A -coherente si verifica la siguiente condición:

$$\frac{n + a_{i-1}}{a_i} \text{ es entero para } i = 1, 2, \dots, 10.$$

- i) (15 puntos) Probar que existe un entero positivo A -coherente con a lo sumo 20 dígitos (es decir menor a 10^{20}).
- ii) (5 puntos) Probar que existen al menos 9 números A -coherentes con exactamente 21 dígitos.

2. (30 puntos)

- a) Sean G y H dos grupos finitos tal que $|G| = m$ y $|H| = n$, y consideramos $d = \text{mcd}(m, n)$. Consideramos $\varphi : G \rightarrow H$ morfismo de grupos. Probar que $x^d \in \ker(\varphi)$, para todo $x \in G$.
- b) Sean G_1 y G_2 grupos finitos tales que $\text{mcd}(|G_1|, |G_2|) = 1$, y sean $\varphi_1 : G_1 \rightarrow H$, $\varphi_2 : G_2 \rightarrow H$. Probar que $\text{Im}(\varphi_1) \cap \text{Im}(\varphi_2) = \{e_H\}$.

3. (45 puntos)

- i) Describa el método de Diffie-Hellmann para intercambio de claves.
- ii) Usted intercambia con su interlocutor una clave por el método Diffie-Hellmann: fijan el primo $n = 61$, y la base $g = 5$. Usted elige el entero 4 y su interlocutor le envía el número 15 (módulo 61). ¿A qué clave común k arriban usted y su interlocutor?
- iii) Fijada la clave se comunicarán mediante el método de cifrado de Vigenère. La palabra clave se obtiene a partir de k (punto anterior) del siguiente modo: se descompone el entero k en factores primos, y se ordenan en forma creciente (poniendo los repetidos tantas veces como aparecen en la descomposición de k). Mediante la tabla siguiente se transforman los factores primos ordenados en caracteres y se obtiene la palabra clave. ¿Cuál es la palabra clave que se obtiene a partir de k ?

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	27

- iv) Descripte el siguiente mensaje, que le ha enviado su interlocutor:

ÑCUGXC�LBRCPTQGGOBSCOQGSWGGEKGTBXQRCOFV

- v) Respóndale a su interlocutor **SABIAS PALABRAS** encriptando el mensaje de acuerdo al método de cifrado pactado.