

Examen - Matemática Discreta II

Cada ejercicio de desarrollo correcto vale 25 puntos.

El parcial se realiza sin materiales de consulta, ni calculadora.

La duración del parcial es de cuatro horas.

Ejercicio 1

- (a) Enunciar el Teorema Fundamental de la Aritmética.
- (b) Demostrar que existen infinitos números primos.

Ejercicio 2

- (a) Enunciar el Teorema Chino del Resto, para el caso de dos congruencias.
- (b) Hallar el menor natural congruente con 53^{901} módulo 100.

Ejercicio 3

Sea $(G, *)$ un grupo finito de orden n . Consideremos el conjunto formado por todos los isomorfismos $\text{Sim}(G) = \{\varphi : G \rightarrow G, \varphi \text{ biyectiva}\}$.

- (a) Probar que $\text{Sim}(G)$ equipado con la composición de funciones es un grupo, denominado el grupo simétrico de G .
- (b) Probar que $f : G \rightarrow \text{Sim}(G)$ tal que $f(g)(x) = g * x$, es un homomorfismo inyectivo.
- (c) Demostrar que todo grupo finito es isomorfo a un subgrupo de algún grupo simétrico.

Ejercicio 4

Un reconocido músico que sabe de criptografía ha decidido cifrar una palabra dirigida a su amada. Esta palabra oculta es, al mismo tiempo, su principal elemento de seducción.

Este músico utiliza el cifrado afín $E(x) = ax + b \pmod{28}$, y su palabra cifrada resulta:

$GQDQPFJF$

Sabiendo que las letras A y E son las más frecuentes en nuestro idioma y que $a \not\equiv 4 \pmod{7}$, se pide:

- (a) Encontrar la palabra que fue cifrada. Es una palabra válida de nuestro idioma.
- (b) Hallar la función de encriptación $E(x)$.
- (c) Hallar la función de descryptación $D(x)$.

Vale destacar que el mapeo de letras a números en \mathbb{Z}_{28} se realiza en base a la siguiente tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	\tilde{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	27

Importante: justificar detalladamente los razonamientos, citando los teoremas utilizados.