

Examen de Matemática Discreta II
20 de julio de 2007

Número de Examen	Cédula	Nombre y Apellido

1. **(30 puntos)**

Consideramos \mathbb{Z}_n el conjunto de los enteros módulo n con la suma y el producto habituales. Sea \mathbb{U}_n el conjunto de los invertibles respecto del producto.

- a) Probar que $[a] \in \mathbb{Z}_n$ es invertible (respecto del producto) si y sólo si $\text{mcd}(a, n) = 1$.
- b) Supongamos que $n = 117 \times 263 = 36031$. Determinar si $[2502]$ y $[512]$ tienen inverso en \mathbb{Z}_{36031} y en caso afirmativo hallarlo(s).
- c) ¿Cuántos elementos tiene \mathbb{U}_{36031} ?
- d) Calcular $1500^{9432} \pmod{36031}$.

2. **(35 puntos)**

Un subgrupo H de G es característico si para todo $f \in \text{Aut}(G) = \{h : G \rightarrow G / h \text{ es morfismo biyectivo}\}$ (automorfismos de G) se cumple que $f(H) \subseteq H$.

- a) Probar que el $Z(G)$ es un subgrupo característico de G .
- b) Probar que cualquier subgrupo característico es un subgrupo normal.
- c) Consideremos $\text{Int}(G) = \{i_a : a \in G\}$ donde $i_a : G \rightarrow G$ es tal que $i_a(x) = axa^{-1}$.
Probar: 1) $\text{Int}(G) \triangleleft \text{Aut}(G)$; 2) $G/Z(G) \cong \text{Int}(G)$.
- d) Considerar S_n con $n \geq 3$.
Probar: 1) $Z(S_n) = \{id\}$; 2) $\text{Int}(S_n) \cong S_n$.

3. **(35 puntos)**

- a) Describir el método de Diffie - Hellman para acuerdo de clave.
- b) Edubijes y Tomás se ponen de acuerdo en el primo $p = 71$ y $g = 7$. Tomás elige el número secreto $n = 69$ y Edubijes le envía $g^m = 23$. ¿Cuál es la clave secreta que acuerdan Edubijes y Tomás?
- c) Asignamos valores a algunos caracteres según la tabla siguiente:

A	C	L	O	H	U	M	R	S	E	T
0	1	2	3	4	5	6	7	8	9	10

Definimos el criptosistema afín de la siguiente manera: para $a, b \in \mathbb{Z}$ con $1 \leq a \leq 10, 0 \leq b \leq 10$ definimos la siguiente función de encriptado $E : \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11} / E(x) = ax + b \pmod{11}$.

Sea K ($0 \leq K < 71$) la clave acordada por Edubijes y Tomás en la parte anterior, escribamos $K = a \cdot 11 + b$ con $0 \leq a < 11$ y $0 \leq b < 11$. Para encriptar un texto se encripta letra a letra usando la función de encriptado. Encriptar el texto HOLA.

- d) Supongamos ahora que somos espías y que sabemos que Edubijes le envía a Tomás un mensaje encriptado según el criptosistema anterior (esta vez desconocemos los valores a y b de la función de encriptado). Espías ayudantes han descubierto que el mensaje original (sin encriptar) comienza con la letra C y termina con la letra U y que el mensaje encriptado es ESLH.
 - i) Hallar la función de encriptar (o sea los valores de a y b) que usan Edubijes y Tomás.
 - ii) Desencriptar el mensaje ESLH.