

Examen de Matemática Discreta II

22 de julio de 2008

Número de Examen	Cédula	Nombre y Apellido

1. (35 puntos)

Sea Q el grupo generado por las matrices complejas:

$$w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad z = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \text{ donde } i^2 = -1.$$

- Calcular wz , zw , w^n y z^n , para todo $n \in \mathbb{N}$.
- Probar que:
 - Q no es abeliano;
 - Q es de orden 8;
 - todo subgrupo de Q es normal.
- Calcular $Z(Q)$.
- Probar que $Q/Z(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. (35 puntos)

- Dado $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_t^{\alpha_t}$, definimos $\delta(n) = \text{mcm}\{\phi(p_1^{\alpha_1}), \dots, \phi(p_t^{\alpha_t})\}$ donde ϕ es la función de Euler. Probar que, si $\text{mcd}(a, n) = 1$, entonces $a^{\delta(n)} \equiv 1 \pmod{n}$.
- Concluir que para todo $a \in \mathbb{N}$ tal que $\text{mcd}(a, 30) = 1$, vale que $a^4 \equiv 1 \pmod{120}$.
- Se define por recurrencia la sucesión $(a_n)_{n \in \mathbb{N}}$, para todo $n \in \mathbb{N}$, tal que $a_{n+2} = 7a_{n+1} + 40a_n$, con $a_1 = 21$, y $a_0 = 3$.
 - Probar que a_n es múltiplo de 3, para todo $n \in \mathbb{N}$.
 - Calcular $a_{2008} \pmod{120}$.

3. (30 puntos)

- Describir el método de Diffie - Hellman para acuerdo de clave.
- Alex y Pedro se ponen de acuerdo en el primo $p = 73$ y $g = 11$. Pedro elige el número secreto $n = 70$ y Alex le envía $g^m = 17$. ¿Cuál es la clave secreta que acuerdan Alex y Pedro?
- Asignamos valores a algunos caracteres según la tabla siguiente:

B	D	E	G	I	N	O	X	Q	Y	Z	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12

Definimos el criptosistema afín de la siguiente manera: para $a, b \in \mathbb{Z}$ con $1 \leq a \leq 12$, $0 \leq b \leq 12$ definimos la siguiente función de encriptado $E : \mathbb{Z}_{13} \rightarrow \mathbb{Z}_{13}/E(x) = ax + b \pmod{13}$.

Sea $K(0 \leq K < 73)$ la clave acordada por Alex y Pedro en la parte anterior, escribamos $K = a \cdot 13 + b$ con $0 \leq a < 13$ y $0 \leq b < 13$. Para encriptar un texto se encripta letra a letra usando la función de encriptado. Encriptar el texto BIEN.

- Supongamos ahora que somos espías y que sabemos que Alex le envía a Pedro 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 G y termina con la letra D y que el mensaje encriptado es BQQU.
 - Hallar la función de encriptar (o sea los valores de a y b) que usan Alex y Pedro.
 - Desencriptar el mensaje BQQU.