

Examen de Matemática Discreta II

13 de julio de 2009

Número de Examen	Cédula	Nombre y Apellido

1. (28 puntos)

- Encontrar $h, k \in \mathbb{Z}$ tales que $35 \times h + 66 \times k = 1$ con $0 \leq h \leq 60$.
- Mostrar que 85 es invertible en $(\mathbb{Z}_{101}^*, \cdot)$ y hallar su inverso.
- Se sabe que $a^{35} = 44 \pmod{101}$ y $a^{66} \equiv -16 \pmod{101}$. Calcular $a \pmod{101}$.

2. (40 puntos)

Sea $p \in \mathbb{Z}^+$, primo impar.

- Probar que $\psi : U(p) \rightarrow U(p)$ tal que $\psi(x) = x^2$ es un morfismo de grupos.
- Calcular $N(\psi)$.
- Probar que $\frac{U(p)}{\{-1, +1\}} \cong \text{Im}(\psi)$ y concluir que $|\text{Im}(\psi)| = \frac{p-1}{2}$.
- A los elementos de $\text{Im}(\psi)$ se les llama *restos cuadráticos*. Probar que los restos cuadráticos no son raíces primitivas.
- Sean $h \in \mathbb{N}$ y $p = 2^{2^h} + 1$ un primo de Fermat. Calcular el número de raíces primitivas en $U(p)$.
- Demostrar que todo elemento de $U(p)$ es una raíz primitiva o un resto cuadrático si p es un primo de Fermat.

3. (32 puntos)

- Describir el protocolo Diffie-Hellman para acuerdo de claves.
- Ana y Pedro desean acordar una clave común utilizando el protocolo Diffie-Hellman. Eligen como primo $p = 89$ y $g = 17$. Pedro elige el número secreto $m = 41$ y Ana le envía $34 \pmod{p}$. ¿Cuál es la clave secreta K que acuerdan Ana y Pedro?
- Una vez elegida la clave común K , Ana y Pedro se comunican utilizando el sistema Vigenère. La clave K se expresa en base 11 se expresa en base 11, es decir, $K = K_0 11 + K_1$, con $0 \leq K_0 \leq 10$ y $0 \leq K_1 \leq 10$. A cada letra del mensaje se le asocia un número de la siguiente tabla:

B	C	E	H	I	N	O	P	S	U	
0	1	2	3	4	5	6	7	8	9	10

El último cuadrado en blanco está representando el espacio en blanco. La clave común resulta de sustituir en $K_0 K_1$ por sus respectivas letras. Descriptar el mensaje: SPEEUSPHS.