

EXAMEN DE MATEMÁTICA DISCRETA II

Ejercicio 1.

- A. Enunciar el teorema de Bezout.
- B. Sean a, b y c números enteros no nulos. Demostrar que la ecuación $ax + by = c$ tiene al menos una solución entera si y solo si $\text{mcd}(a, b) | c$.
- C. Hallar $x, y \in \mathbb{Z}$, $x \geq 5$, $y \leq 16$ tales que $35x - 15y = 80$.

Ejercicio 2. Sean G y H grupos y considérese $K = G \times H = \{(g, h) : g \in G, h \in H\}$ con la operación $*$ definida como

$$(g, h) * (g', h') = (gg', hh') \quad \text{si } g, g' \in G \text{ y } h, h' \in H.$$

- A. Probar que K es un grupo con la operación $*$.
- B. Probar que $N = \{(g, e_H) : g \in G\}$ es un subgrupo normal de K .
- C. Probar que N es isomorfo a G . [Sugerencia: encontrar un isomorfismo entre ambos grupos.]
- D. Probar que K/N es isomorfo a H . [Sugerencia: considerar $\varphi: K \rightarrow H$, $\varphi(g, h) = h$.]

Ejercicio 3.

- A. Hallar el menor $x \in \mathbb{N}$ que verifica
$$\begin{cases} x \equiv 10 \pmod{13} \\ x \equiv 91 \pmod{101} \end{cases}$$
- B. Si E es la función de encriptado con el método RSA con clave (n, e) , describir D la función de desencriptado y demostrar que desencripta.
- C. Si $(n, e) = (1313, 271)$ calcular $E(10)$.

Ejercicio 4.

- A. Sea $G = \langle g \rangle$ un grupo cíclico de orden n .
 - (i) Probar que $\forall m \in \mathbb{Z}$, $\langle g^m \rangle = \langle g^{\text{mcd}(m, n)} \rangle$.
 - (ii) Si $d | n$, hallar el orden de g^d .
 - (iii) Probar que si H y K son dos subgrupos de G tal que $|H| = |K|$, entonces $H = K$.
- B. Sea $k \in \mathbb{Z}$, $k > 2$.
 - (i) Probar que $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$. [Sugerencia: inducción en k .]
 - (ii) Hallar el $o(1 + 2^{k-1})$ y $o(5)$ en $U(2^k)$.
- C. Concluir que no existen raíces primitivas módulo 2^k . [Sugerencia: encontrar dos subgrupos de orden 2 en $U(2^k)$.]