

EXAMEN - 24 DE JULIO DE 2014. DURACIÓN: 3 HORAS.

Nº de examen	Cédula	Apellido y nombre

Ejercicio 1.

- a. Sean $a, b \in \mathbb{Z}$ enteros no nulos. Probar que:

$$\text{mcd}(a, b) = \min \{c > 0 : c = ax + by, x, y \in \mathbb{Z}\}.$$

- b. Hallar todos los a, b enteros positivos que cumplen $a \equiv 4 \pmod{b}$ y $\text{mcm}(a, b) = 675 \times \text{mcd}(a, b)$.

Ejercicio 2.

- a. Hallar todas las soluciones $x \in \mathbb{Z}$ del siguiente sistema:

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 4 \pmod{6} \\ x \equiv 0 \pmod{11} \end{cases}$$

- b. Hallar el resto de dividir 22^{300} entre 4290.

Ejercicio 3.

- a. Probar que si $f : G \rightarrow K$ es un homomorfismo de grupos y G es un grupo finito, entonces $|G| = |\ker(f)| |\text{Im}(f)|$. Si utiliza algún teorema de grupos, debe probarlo.
- b. Probar que si G y K son grupos y $f : G \rightarrow K$ es un homomorfismo de grupos, entonces $|\text{Im}(f)|$ divide a $\text{mcd}(|G|, |K|)$.
- c. Hallar todos los subgrupos del grupo dihedral D_3 .
- d. i) Sean p un primo impar y x un entero impar coprimo con p . Probar que x es raíz primitiva módulo p si y sólo si x es raíz primitiva módulo $2p$.
 ii) Probar que 11 es raíz primitiva módulo 82.
 iii) Hallar todos los homomorfismos $f : U(82) \rightarrow D_3$. *Sugerencia: utilizar las partes anteriores.*

Ejercicio 4. Sean $n = 209$ y $e = 17$.

- a. Utilizando el método de cifrado RSA y la clave (n, e) cifrar $x = 5$.
- b. Hallar $\varphi(n)$.
- c. Hallar la función de descifrado D .
- d. Descifrar $y = 10$.