

En todos los ejercicios deben justificar los resultados a los que llegan.

**Ejercicio 1.**

- a. Enunciar y demostrar el Lema de Euclides.

**Solución:** Ver notas teóricas.

- b. Sean  $a, b$  enteros positivos, probar que

$$\text{mcm}(a, b) = \frac{a \cdot b}{\text{mcd}(a, b)}.$$

*En esta parte deben probar cualquier propiedad que utilicen.*

**Solución:** Ver notas teóricas.

- c. Encontrar todos los  $a, b$  enteros positivos que cumplan  $a \cdot b = 792$  y  $\text{mcm}(a, b) = 132$ .

**Solución:** Multiplicando la segunda igualdad por  $\text{mcd}(a, b)$ , y utilizando la parte anterior obtenemos que  $a \cdot b = 132 \text{mcd}(a, b)$ . Igualando con la primer igualdad dada vemos que  $132 \text{mcd}(a, b) = 792$ , por lo que  $\text{mcd}(a, b) = 6$ . Escribimos  $a = 6a'$  y  $b = 6b'$ , y substituyendo obtenemos que  $a' \cdot b' = 22 = 2 \cdot 11$ . Como sabemos que  $\text{mcd}(a', b') = 1$  vemos que todas las soluciones tienen que ser  $(a', b') = (1, 22), (2, 11), (11, 2), (22, 2)$ . Y  $(a, b) = (6, 132), (12, 66), (66, 12), (132, 6)$ .

**Ejercicio 2.** Para los siguientes sistemas de congruencias, determinar si tienen solución y en caso de que tengan solución hallarlas todas.

a. 
$$\begin{cases} x \equiv 17 \pmod{44} \\ x \equiv 50 \pmod{99} \\ x \equiv 5 \pmod{12} \end{cases}.$$

b. 
$$\begin{cases} x \equiv 18 \pmod{44} \\ x \equiv 52 \pmod{99} \\ x \equiv 10 \pmod{12} \end{cases}.$$

**Solución:**

- a. Escribimos  $44 = 2^2 \cdot 11$ ,  $99 = 3^2 \cdot 11$  y  $12 = 2^2 \cdot 3$ . Luego de verificar que el sistema es compatible, vemos que es equivalente a: 
$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 5 \pmod{9} \\ x \equiv 6 \pmod{11} \end{cases}.$$
 De las dos primeras congruencias

es fácil ver que  $x \equiv 5 \pmod{4 \cdot 36}$ , y el sistema es equivalente a: 
$$\begin{cases} x \equiv 6 \pmod{11} \\ x \equiv 5 \pmod{36} \end{cases}.$$
 De la segunda congruencia obtenemos  $x = 36k + 5$  y si substituímos en la primera:  $36k + 5 \equiv 6 \pmod{11}$ . Por lo que  $3k \equiv 1 \pmod{11}$  y  $k \equiv 4 \pmod{11}$ . Por lo que  $x \equiv 36 \cdot 4 + 5 \pmod{4 \cdot 9 \cdot 11} \equiv 149 \pmod{396}$ .

- b. De la primera congruencia vemos que  $x \equiv 7 \pmod{11}$  y de la segunda vemos que  $x \equiv 8 \pmod{11}$ . Concluimos entonces que el sistema no tiene solución.

**Ejercicio 3.** Sea el grupo de invertibles módulo 803,  $K = U(803)$ .

- a. Calcular  $2^{90} \pmod{803}$ .

**Solución:** Observamos que  $803 = 11 \cdot 73$ , entonces por el Teorema Chino del Resto, vemos que  $x \equiv 2^{90} \pmod{803}$  si y solo si 
$$\begin{cases} x \equiv 2^{90} \pmod{11} \\ x \equiv 2^{90} \pmod{73} \end{cases}$$
 En la primera equivalencia aplicamos el Teorema de Fermat, como sabemos que  $2^{10} \equiv 1 \pmod{11}$  concluimos que  $2^{90} = (2^{10})^9 \equiv 1^9 \pmod{11} \equiv 1 \pmod{11}$ .

Podemos hacer lo mismo con la segunda congruencia,  $2^{90} \equiv 2^{18} \pmod{73}$ . Para hallar la potencia anterior usamos el método de exponenciación rápida. Para ello calculamos la

	$k$	$2^{2^k} \pmod{73}$	
	0	2	
siguiente tabla:	1	4	. Como $18 = 16 + 2 = 2^4 + 2^1$ vemos que $2^{18} = 2^{2^4} 2^{2^1} \equiv$
	2	16	
	3	37	
	4	55	

$55 \cdot 4 \pmod{73} \equiv 220 \pmod{73} \equiv 1 \pmod{73}$ . Concluimos que  $2^{90} \equiv 1 \pmod{803}$ .

- b. Hallar el orden de  $\bar{4} \in K$ .

**Solución:** Por la parte anterior sabemos que  $4^{45} = 2^{90} \equiv 1 \pmod{803}$ . Por lo que el orden de  $\bar{4}$  tiene que ser un divisor de  $45 = 3^2 \cdot 5$ . Los divisores de 45 son 1, 3, 5, 9, 15, 45. Claramente  $4^1, 4^3, 4^5$  no son 1 módulo 803. Si  $4^9 \equiv 1 \pmod{803}$  entonces  $2^{18} \equiv 4^9 \pmod{11} \equiv 1 \pmod{11}$ , pero  $2^{18} \equiv 2^8 \not\equiv 1 \pmod{11}$ , concluyendo que  $4^9 \not\equiv 1 \pmod{803}$ . De igual manera, supongamos que  $4^{15} \equiv 1 \pmod{803}$ , entonces  $2^{30} \equiv 1 \pmod{73}$ , pero utilizando la tabla del ejercicio anterior vemos que  $2^{30} = 2^{16} 2^8 2^4 2^2 \equiv 55 \cdot 37 \cdot 16 \cdot 4 \pmod{73} \equiv 8 \pmod{73}$ , entonces  $4^{15} \not\equiv 1 \pmod{803}$  y el orden de  $\bar{4}$  tiene que ser 45.

- c. Sabiendo que  $2^{45} \not\equiv 1 \pmod{803}$ , deducir el orden de  $\bar{2} \in K$ .

**Solución:** Utilizamos la fórmula:

$$45 = o(\bar{4}) = o(\bar{2}^2) = \frac{o(\bar{2})}{\gcd(o(\bar{2}), 2)}.$$

Ahora,  $\gcd(o(\bar{2}), 2)$  puede ser 1 o 2, si es 1 entonces tendríamos que  $o(\bar{2}) = 45$ , pero por el dato dado eso no puede pasar. Concluimos que  $\gcd(o(\bar{2}), 2) = 2$  y  $o(\bar{2}) = 90$ .

- d. Para los siguientes grupos  $G$  verificar si existen homomorfismos no triviales  $f: G \rightarrow K$ .

$$\text{i) } G = \mathbb{Z}_{803}. \quad \text{ii) } G = \mathbb{Z}_{45}. \quad \text{iii) } G = \mathbb{Z}_2. \quad \text{iv) } G = S_3.$$

**Solución:**

- i) Como  $|\mathbb{Z}_{803}| = 803$  es coprimo a  $|U(803)| = \varphi(803) = \varphi(11)\varphi(73) = 720$ , vemos que no hay morfismos no triviales entre  $G$  y  $K$ .
- ii) Como  $G$  es cíclico de orden 45 y  $\bar{1}$  es un generador, tenemos el morfismo no trivial dado por  $f(k\bar{1}) = \bar{4}^k$ , ya que  $o(\bar{4}) = 45$ .
- iii) Como  $G$  es cíclico de orden 2 y  $\bar{1}$  es un generador, tenemos el morfismo no trivial dado por  $f(k\bar{1}) = \overline{-1}^k$ , ya que  $o(\overline{-1}) = 2$ .
- iv) Dados dos elementos  $\tau$  y  $\sigma$  de  $S_3$  de orden 2 y 3 respectivamente, vemos que  $S_3 = \{\text{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ . Podemos definir el morfismo dado por  $f(\tau) = \overline{-1}$  y  $f(\sigma) = \bar{1}$  (verificar que funciona).

#### Ejercicio 4.

- a. Sean  $n$  y  $e$  datos utilizados por el protocolo RSA, y las funciones de cifrado  $E$  y descifrado  $D$ . Probar que  $D$  descifra correctamente.

**Solución:** Ver notas teóricas.

- b. Sean  $n = 187$  y  $e = 7$ , hallar la función de descifrado  $D$ .

**Solución:** Tenemos que hallar  $d \equiv e^{-1} \pmod{\varphi(187)}$ . Para ello aplicamos el Algoritmo de Euclides Extendido. Primero vemos que  $187 = 11 \cdot 17$ , por lo que  $\varphi(187) = 160$ . Vemos entonces que:

$$\begin{aligned} 160 &= 7 \cdot 22 + 6 \\ 7 &= 6 \cdot 1 + 1 \end{aligned}$$

Entonces  $1 = 7 \cdot 23 + 160 \cdot (-1)$ , por lo que  $7^{-1} \equiv 23 \pmod{160}$ , y  $D(y) = y^{23} \pmod{187}$ .