

**Universidad de la República - Facultad de Ingeniería - IMERL: Matemática  
Discreta 2**

SOLUCIÓN PRIMER PARCIAL - 27 DE ABRIL DE 2017.

**Ejercicio 1.** Encontrar todos los  $a, b \in \mathbb{N}$  tales que  $a + b = 407$  y  $\text{mcm}(a, b) = 210 \text{mcd}(a, b)$ .

**Solución:** Sean  $d = \text{mcd}(a, b)$  y  $a = da^*$ ,  $b = db^*$ . Como

$$d(a^* + b^*) = a + b = 11 \cdot 37$$

entonces  $d \mid 407$  y  $d \in \{1, 11, 37, 407\}$ .

Por otro lado, como  $\text{mcm}(a, b) \text{mcd}(a, b) = ab$ , tenemos

$$d^2 a^* b^* = ab = 210 \text{mcd}(a, b)^2 = 2 \cdot 3 \cdot 5 \cdot 7 d^2.$$

Por lo tanto

$$a^* b^* = 2 \cdot 3 \cdot 5 \cdot 7.$$

Recordemos que  $\text{mcd}(a^*, b^*) = 1$  por lo tanto  $a^* \in \{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\}$ .  
Veamos para que  $d$  hay alguna solución.

- Si  $d = 1$  entonces  $a^* + b^* = 407$ , y mirando entre las opciones para  $a^*$  y  $b^*$  vemos que ninguna llega a sumar 407.
- Si  $d = 11$  entonces  $a^* + b^* = 37$ , dentro de las opciones para  $a^*$  y  $b^*$ , recordar que  $a^* b^* = 210$ , las únicas que funcionan son  $(a^*, b^*) = (7, 30)$  y  $(a^*, b^*) = (30, 7)$ .
- Si  $d = 37$  entonces  $a^* + b^* = 11$ , ninguna de las opciones para  $a^*$  y  $b^*$  funcionan.
- Si  $d = 407$  entonces  $a^* + b^* = 1$  y ninguna de las opciones para  $a^*$  y  $b^*$  funcionan.

Por lo tanto las soluciones son  $(a, b) = (7 \cdot 11 = 77, 30 \cdot 11) = (77, 330)$  y  $(a, b) = (330, 77)$ .

**Ejercicio 2.** Sean  $a, b, c \in \mathbb{Z}$  con  $(a, b) \neq (0, 0)$ . Probar que la ecuación diofántica

$$ax + by = c$$

tiene solución si y solo si  $\text{mcd}(a, b) \mid c$ .

**Solución:** Sea  $d = \text{mcd}(a, b)$ . Como  $(a, b) \neq (0, 0)$  tenemos que  $d \neq 0$ .

( $\longrightarrow$ ) Si la ecuación tiene solución, entonces existen  $x_0, y_0 \in \mathbb{Z}$  tales que  $ax_0 + by_0 = c$ . Como  $d \mid a$  y  $d \mid b$ , entonces  $d \mid ax_0 + by_0 = c$ .

( $\longleftarrow$ ) Supongamos que  $d \mid c$  y veamos que la ecuación tiene solución:

Como  $d \mid c$  existe  $k \in \mathbb{Z}$  tal que  $c = dk$ . Por la identidad de Bezout existen  $x', y' \in \mathbb{Z}$  tales que  $ax' + by' = d$ . Multiplicando ambos lados de la ecuación por  $k$ , obtenemos que  $a(x'k) + b(y'k) = c$ , y por lo tanto  $x_0 = x'k$ ,  $y_0 = y'k$  es una solución de la ecuación  $ax + by = c$ .

**Ejercicio 3.**

- a. Hallar el menor  $x$  natural que verifica

$$\begin{cases} x \equiv 6 & (\text{mód } 13) \\ x \equiv 62 & (\text{mód } 103) \end{cases}$$

- b. Si  $(n, e) = (1339, 311)$  calcular  $E(11)$ , donde  $E$  es la función de cifrado del criptosistema RSA con clave pública  $(n, e)$ .
- c. Sabiendo que  $1339 = 13 \cdot 103$  calcular la función de descifrado  $D$  del criptosistema RSA para la clave pública  $(n, e)$  de la parte anterior.
- d. Sean  $n = p \cdot q$ , con  $p, q$  primos, y  $0 < e < \varphi(n)$  con  $\text{mcd}(e, \varphi(n)) = 1$ . Dadas las funciones de cifrado  $E$  y descifrado  $D$  del criptosistema RSA para  $(n, e)$ , probar que  $D(E(x)) \equiv x \pmod{n}$  cuando  $\text{mcd}(x, n) = 1$ .

**Solución:**

- a. Sabemos que el sistema tiene solución por TCR ya que 13 y 103 son coprimos. Combinando las dos congruencias obtenemos que

$$x = 62 + 103k \equiv 6 \pmod{13}.$$

Ahora, como  $103 \equiv -1 \pmod{13}$  y  $62 \equiv -3 \pmod{13}$  vemos que  $k = 4$  y  $x \equiv 474 \pmod{13 \cdot 103}$ . Por lo tanto, la solución buscada es

$$x = 474.$$

- b. Tenemos que calcular  $x \equiv 11^{311} \pmod{1339}$ , con  $0 \leq x < 1339$ . Como  $1339 = 13 \cdot 103$  y TCR, esto es equivalente a resolver el sistema

$$\begin{cases} x \equiv 11^{311} & (\text{mód } 13) \\ x \equiv 11^{311} & (\text{mód } 103) \end{cases}, x \in \mathbb{Z}.$$

En la primer congruencia podemos aplicar el teorema de Euler ya que 11 y 13 son coprimos. Como  $311 \equiv -1 \pmod{12}$  y  $\varphi(13) = 12$  tenemos que

$$11^{311} \equiv 11^{-1} \pmod{13} \equiv (-2)^{-1} \pmod{13} \equiv -7 \pmod{13} \equiv 6 \pmod{13}.$$

Para la segunda congruencia también podemos aplicar Euler y como  $311 \equiv 5 \pmod{102}$  entonces

$$11^{311} \equiv 11^5 \pmod{103} \equiv 18 \cdot 18 \cdot 11 \pmod{103} \equiv 15 \cdot 11 \pmod{103} \equiv 62 \pmod{103}.$$

Entonces, por lo visto en la primer parte del ejercicio vemos que

$$E(x) = 474.$$

- c. Para hallar  $D$  tenemos que hallar  $0 \leq d < \varphi(n) = 1224$  tal que  $e \cdot d \equiv 1 \pmod{1339}$ . O sea, hallar el inverso de  $e$  módulo 1339. Para ello aplicamos el algoritmo extendido de Euclides para hallar la identidad de Bezout

$$1224 \cdot (-140) + 311 \cdot 511 = 1,$$

y por lo tanto  $d = 551$  y  $D(y) = y^{551} \pmod{1339}$ .

- d. Como  $D(E(x)) \equiv x^{ed} \pmod{n}$ , debemos probar que  $x^{ed} \equiv x \pmod{n}$ . Por la construcción del sistema RSA tenemos que  $ed \equiv 1 \pmod{\varphi(n)}$ , es decir que  $ed = \varphi(n)k + 1$ .

Ahora como  $\text{mcd}(x, n) = 1$ , el Teorema de Euler dice que

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Entonces

$$x^{ed} = x^{\varphi(n)k+1} = (x^{\varphi(n)})^k \cdot x \equiv 1^k \cdot x \equiv x \pmod{n}.$$

**Ejercicio 4.** Demostrar la siguiente versión del teorema chino del resto.

Sean  $m_1, m_2$  enteros coprimos y  $a_1, a_2 \in \mathbb{Z}$ , entonces el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}, x \in \mathbb{Z},$$

tiene solución y es única módulo  $m_1 m_2$ .

**Solución:** La primer congruencia es equivalente a que existe  $s \in \mathbb{Z}$  tal que  $x = a_1 + m_1 s$ , y la segunda congruencia a que exista  $t \in \mathbb{Z}$  tal que  $x = a_2 + m_2 t$ . Igualando ambas ecuaciones obtenemos

$$a_1 + m_1 s = a_2 + m_2 t,$$

o lo que es lo mismo

$$m_1 s - m_2 t = a_2 - a_1.$$

Como  $\text{mcd}(m_1, m_2) = 1$ , esta ecuación siempre tiene solución en  $\mathbb{Z}$  (por el ejercicio 2). Ahora si  $s_0, t_0 \in \mathbb{Z}$  es una solución, tenemos que  $x = a_1 + m_1 s_0 = a_2 + m_2 t_0$  es una solución al sistema de congruencias planteado.

Para ver la unicidad de la solución módulo  $m_1 m_2$ , consideremos  $x_0$  y  $x_1$  dos soluciones. Entonces  $x_0 \equiv x_1 \pmod{m_1}$  y  $x_0 \equiv x_1 \pmod{m_2}$ . Dicho de otro modo,  $m_1 \mid (x_0 - x_1)$  y  $m_2 \mid (x_0 - x_1)$ . Pero como  $\text{mcd}(m_1, m_2) = 1$  esto implica que  $m_1 m_2 \mid (x_0 - x_1)$ , es decir que  $x_0 \equiv x_1 \pmod{m_1 m_2}$ .