



## “Fundamentos matemáticos”

### Ejercicios propuestos

#### Ejercicio 1 :

Cálculo de Inversos: resolver  $ax=1 \pmod{n}$ , dónde  $\text{m.c.d.}(a,n)=1$

- a) Aplicando el teorema de Fermat. Resolver:  $37x = 1 \pmod{5}$
- b) Aplicando el teorema de Euler. Resolver:  $7x = 1 \pmod{12}$
- c) Aplicando el método de Euclides modificado. Resolver:  $32x = 1 \pmod{5}$

#### Solución:

a)

$a=37$ ,  $n=5$  primo,  $\text{m.c.d.}(37,5)=1$ , por Fermat:  $x=37^{n-2} \pmod{5} \Rightarrow$

$x=37^{5-2} \pmod{5} \Rightarrow x=3 \pmod{5}$

b)

$a=7$ ,  $n=12$  (no primo),  $\text{m.c.d.}(7,12)=1$ , por Euler:  $x=7^{\Phi(12)-1} \pmod{12}$

Aquí,  $12 = 2^2 * 3$ ,  $\Phi(12) = \Phi(2^2) * \Phi(3) = 2^{2-1} * (2-1) * 2 = 4$

$x=7^{4-1} \pmod{12} \Rightarrow x=7^3 \pmod{12} \Rightarrow x=7 \pmod{12}$

c)

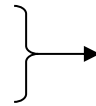
(La solución es inmediata si se realiza una reducción modular de la ecuación, resultando en:  $2x \pmod{5}=1$ ).

Para ilustrar el manejo del método de Euclides modificado se elige calcular el inverso aplicando dicho método:

	6	2	2
32	5	2	1
2	1	0	

$$a = c_1 n + r_1 \Rightarrow r_1 = a - c_1 n$$

$$n = c_2 r_1 + r_2 \Rightarrow r_2 = n - c_2 r_1$$



$$\Rightarrow r_2 = n - c_2 (a - c_1 n) \Rightarrow r_2 = n (1 + c_1 c_2) - c_2 (a - c_1 n) \Rightarrow$$

$$r_2 = n (1 + c_1 c_2) - c_2 a$$

$$\text{entonces: } r_2 = 1 = n (1 + c_1 c_2) - c_2 a \Rightarrow 1 = -c_2 a \text{ mod. } n \Rightarrow$$

$$1 = -2 * 32 \text{ mod. } 5 \Rightarrow x \equiv -2 \text{ mod. } 5 \Rightarrow x = 3 \text{ mod. } 5$$

## Ejercicio 2:

Resolución de ecuaciones del tipo  $ax = b \text{ mod. } n$ , donde  $\text{m.c.d.}(a, n) = 1$

a) Aplicando el teorema de Euler. Resolver  $3x = 3 \text{ mod. } 14$

b) Aplicando el método de Euclides modificado. Resolver  $19x = 4 \text{ mod. } 49$

## Solución:

a)

$$a=3, n=14 \text{ (no primo), m.c.d.}(14,3)=1, \text{ por Euler: } a^{-1} = 3^{\Phi(14)-1} \text{ mod. } 14$$

$$\text{Aquí, } 14 = 7*2, \Phi(14) = \Phi(7) * \Phi(2) = (7-1) * (2-1) = 6*1 = 6$$

$$a^{-1} = 3^{6-1} \text{ mod. } 14 \Rightarrow a^{-1} = 3^5 \text{ mod. } 14 \Rightarrow a^{-1} = 9*9*3 \text{ mod. } 14 = 243 \text{ mod. } 14 = 5 \text{ mod. } 12$$

$$\Rightarrow (\text{Por reducción modular}) a^{-1} = 5 \text{ mod. } 14$$

$$x = a^{-1} * b = 5 * 3 \text{ mod. } 14 = 1$$

b)

$$19y = 1 \text{ mod. } 49, \text{ donde } x = y * 4 \text{ mod. } 49$$

$$n = c * a + r_1$$

$$49 = 19 * 2 + 11$$

$$19 = 11 * 1 + 8$$

$$11 = 8 * 1 + 3$$

---

$$8 = 3 \cdot 2 + 2$$

$$3 = 2 \cdot 1 + 1$$

-----

$$r_1 = n - 2a$$

$$r_2 = a - r_1 = a - n + 2a = 3a - n$$

$$r_3 = r_1 - r_2 = n - 2a - (3a - n) = -5a + 2n$$

$$r_4 = r_2 - 2r_3 = 3a - n - 2(-5a + 2n) = 13a - 5n$$

$$1 = r_3 - r_4 = -5a + 2n - 13a + 5n = -18a + 7n$$

$$1 = -18a \pmod{49}$$

$$y = -18 \pmod{49} = 31 \pmod{49}$$

$$x = 4 \cdot y \pmod{49} = 4 \cdot 31 \pmod{49} = 26 \pmod{49}$$

### Ejercicio 3:

Resolución de ecuaciones del tipo  $ax = b \pmod{n}$ , donde  $\text{m.c.d.}(a, n) = m \neq 1$

a) Aplicando el teorema de Euler. Resolver  $15x = 6 \pmod{9}$

### Solución:

a)

La ecuación es equivalente a ésta otra:  $6x = 6 \pmod{9}$

$$a = 6, n = 9, \text{m.c.d.}(6, 9) = m = 3$$

$$b = 6 = 2 \cdot m$$

Se calcula y:

$$2y \pmod{3} = 1$$

$$\text{por Euler } y = 21 \pmod{3}; y = 2$$

Por lo tanto:

$$x = (6/3) \cdot 2 + (9/3)k ;$$

$$x = 4 + 3k \pmod{9}, \text{ para } k = \{0, 1, 2\}$$

---

#### Ejercicio 4:

Ejercicios misceláneos de aritmética modular

a) Sin indicar el método.

i) Resolver:  $2x = 1 \pmod{4}$

ii) Resolver:  $37x = 1 \pmod{10}$

iii) Resolver  $3x = 5 \pmod{8}$

iv) Resolver  $5x = 10 \pmod{15}$

v) Resolver  $63x = 2 \pmod{110}$

b) Demostración de propiedades

i) Demuestre que:

Dados  $M$  y  $n$  tales  $\text{m.c.d.}(M,n) = 1$ , y

Dados  $e, d \in \mathbb{Z} - \{0\}$  tales que  $e \cdot d = 1 \pmod{\Phi(n)}$ , entonces:

$$M^{e \cdot d} \pmod{n} = M$$

ii) Establezca y razone si son verdaderas o falsas las siguientes igualdades:

ii.a)  $16^{16} + 16^{17} \pmod{17} = 1 \pmod{17}$

ii.b)  $16^{17} * 16^{16} \pmod{17} \equiv -1 \pmod{17}$

iii) Demuestre que:

Si  $a$  y  $n$  son dos enteros tales que,  $\text{m.c.d.}(a,n) = 1$ , entonces:

$$a^x = a^y \pmod{n} \Leftrightarrow x = y \pmod{\Phi(n)}.$$

iv) Demuestre que:

$$\text{Dados } a, b, c, n \in \mathbb{Z} - \{0\} \text{ tales que } \text{m.c.d.}(a,n)=d, \text{ si } ab \equiv ac \pmod{n} \Leftrightarrow b \equiv c \pmod{n/d}.$$

v) Demuestre que:

Demuestre que el sistema de ecuaciones siguiente no tiene solución:

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{9} \end{cases}$$

---

**Solución:**

a)

i) Resolver:  $2x = 1 \pmod{4}$

$a=2, n=4, \text{m.c.d.}(2,4) \neq 1$ , por lo que no existe solución.

ii) Resolver:  $37x = 1 \pmod{10}$

$a=37, n=10, \text{m.c.d.}(37,10)=1$ , por Euler:  $x = 37^{\Phi(10)-1} \pmod{10}$

Aquí,  $10 = 2 * 5, \Phi(10) = \Phi(2) * \Phi(5) = 1 * 4 = 4$

$x = 37^{4-1} \pmod{10} \Rightarrow x = 37^3 \pmod{10} \Rightarrow x = 7^3 \pmod{10} \Rightarrow x = 63 \pmod{10} \Rightarrow$

$x = 3 \pmod{10}$

iii) Resolver  $3x = 5 \pmod{8}$

Transformamos a  $3y \pmod{8} = 1$  donde  $x=y*5 \pmod{8}$ .

Para resolverlo aplicamos el teorema de Euler  $x = a^{\phi(n)-1} \pmod{n}$

Por  $\phi(n) = n^{k-1} (n-1)$  se obtiene que  $\phi(8) = 4$ ,

$y = 3^{\phi(8)-1} \pmod{8} = 3^3 \pmod{8} \Rightarrow y = 3 \pmod{8}$

Despejamos en  $x = by \pmod{n}$ , y resolvemos:

$x = 15 \pmod{8} \Rightarrow x = 7 \pmod{8}$

iv) Resolver  $5x = 10 \pmod{15}$

$\text{m.c.d.}(15,5) = 5 = m$

$y \pmod{3} = 1$

por Euler  $y = 1 \pmod{3}; y = 1$

Por lo tanto:

$x = (10/5).1 + (15/5).k ;$

$x = 2 * 1 + 3.k, \text{ para } k = \{0,1,2,3,4\}$

v) Resolver  $63x = 2 \text{ mod. } 110$

	1	1	2	1	15
110	63	47	16	15	<u>1</u>
47	16	15	<u>1</u>	<u>0</u>	

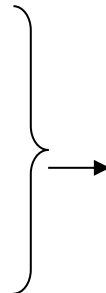
$$n = c_1a + r_1 \Rightarrow r_1 = n - c_1a$$

$$a = c_2r_1 + r_2 \Rightarrow r_2 = a - c_2r_1$$

$$r_1 = c_3r_2 + r_3 \Rightarrow r_3 = r_1 - c_3r_2$$

$$r_2 = c_4r_3 + r_4 \Rightarrow r_4 = r_2 - c_4r_3 = \underline{1}$$

$$r_3 = c_5r_4 + r_5 \Rightarrow r_5 = \underline{0}, c_5 = \underline{1}$$



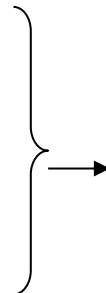
$$\underline{110} = 1 \cdot \underline{63} + 47 \Rightarrow \underline{47} = \underline{110} - 1 \cdot \underline{63}$$

$$\underline{63} = 1 \cdot \underline{47} + 16 \Rightarrow \underline{16} = \underline{63} - 1 \cdot \underline{47}$$

$$\underline{47} = 2 \cdot \underline{16} + 15 \Rightarrow \underline{15} = \underline{47} - 2 \cdot \underline{16}$$

$$\underline{16} = 1 \cdot \underline{15} + 1 \Rightarrow \underline{1} = \underline{16} - 1 \cdot \underline{15}$$

$$\underline{15} = 15 \cdot 1 + \underline{0}$$



$$\underline{1} = \underline{16} - 1 \cdot \underline{15} =$$

$$= (\underline{63} - 1 \cdot \underline{47}) - 1 \cdot (\underline{47} - 2 \cdot \underline{16}) =$$

$$= (\underline{63} - 1 \cdot (\underline{110} - 1 \cdot \underline{63})) - 1 \cdot (\underline{110} - 1 \cdot \underline{63} - 2 \cdot (\underline{63} - 1 \cdot \underline{47})) =$$

$$= (\underline{63} - 1 \cdot (\underline{110} - 1 \cdot \underline{63})) - 1 \cdot (\underline{110} - 1 \cdot \underline{63} - 2 \cdot (\underline{63} - 1 \cdot (\underline{110} - 1 \cdot \underline{63}))) =$$

$$= -4 \cdot \underline{110} + 7 \cdot \underline{63}$$

$$1 = -4 \cdot \underline{110} + 7 \cdot \underline{63} \text{ mod. } 110 = 7 \cdot 63 \text{ mod. } 110$$

$$63^{-1} \text{ mod. } 110 = 7$$

$$X = 7 \cdot 2 \text{ mod } 110 = 14$$

---

b)

i)

(Ésta es la demostración del algoritmo RSA)

$$e \cdot d = 1 \bmod \Phi(n) \rightarrow e \cdot d = k \cdot \Phi(n) + 1$$

$$\text{m.c.d}(M, n) = 1 \Rightarrow (\text{por T}^{\text{ma}} \text{ Euler}) M^{\Phi(n)} = 1 \bmod n \Rightarrow M^{k \cdot \Phi(n)} = 1 \bmod n$$

Entonces:

$$M^{e \cdot d} \bmod n = M^{(k \cdot \Phi(n) + 1)} \bmod n = M^{k \cdot \Phi(n)} \cdot M \bmod n = M \bmod n$$

ii)

Se aplica el teorema de Fermat:  $a^{16} \bmod 17 = 1$  para  $\text{m.c.d}(a, 17) = 1$

ii.a) (falso = 0)

ii.b) Verdadero (la igualdad no hubiera sido verdadera)

iii)

Partimos:

$$a^x = a^y \bmod n ;$$

$$a^{x-y} = 1 \bmod n ;$$

$$a^{\Phi(n)} = 1 \bmod n; \text{ Teorema de Euler}$$

Entonces:  $x - y = k \cdot \Phi(n)$  ; para  $k$  entero.

$$\text{Entonces: } x = y \bmod \Phi(n)$$

iv)

$$ab \equiv ac \bmod n \Rightarrow \text{existe } k \text{ entero tal que } ab - ac = kn \quad (1)$$

$$\text{m.c.d}(a, n) = d \Rightarrow \text{existe } k_a \text{ entero tal que } k_a = a/d$$

$$\text{m.c.d}(a, n) = d \Rightarrow \text{existe } k_n \text{ entero tal que } k_n = n/d \text{ y además } \text{m.c.d}(k_a, k_n) = 1$$

Dividimos (1) entre  $d$ :

$$a/d(b - c) = k n/d \Rightarrow k_a (b - c) = k k_n \Rightarrow k_a \text{ divide a } k \Rightarrow$$

$$(b - c) = k/k_a n/d \Rightarrow b \equiv c \bmod n/d$$

---

v)

$x \equiv 2 \pmod{6} \Rightarrow$  existe  $k$  entero tal que  $x = 6k + 2$

$6k + 2 \equiv 3 \pmod{9} \Rightarrow 6k \equiv 1 \pmod{9}$ ,  $\text{m.c.d.}(6,9)=3 \neq 1 \Rightarrow$  No existe solución a esta ecuación