Comentarios

Büten Zar

FB

Letra

Ejercicio 1

Ejercicio 2

Ejercicio 3

Ejercicio 4

Ejercicio 5

Ejercicio 6

Ejercicio 7

Ejercicio 8

Ejercicio 9

Ejercicio 1

Menu

[Büten Zar]
B.Sz

1 Sean m_1 y m_2 coprimos.

a) Probar que existen $b_1, b_2 \in \mathbb{Z}$ tales que $b_1 m_2 \equiv 1 \pmod{m_1}$ y $b_2 m_1 \equiv 1 \pmod{m_2}$

$b_1 \cdot m_2 \equiv 1 \pmod{m_1}$, b_1 es el inverso de m_2 mod m_1.

El cual existe pues m_2 y m_1 son coprimos.

$b_2 \cdot m_1 \equiv 1 \pmod{m_2}$, b_2 es el inverso de m_1 mod m_2.

El cual existe pues m_2 y m_1 son coprimos.

b) Probar que para b_1 y b_2 como en la parte anterior, para todo $a_1, a_2 \in \mathbb{Z}$, el entero $x = a_1 b_1 m_2 + a_2 b_2 m_1$ es solución del sistema $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$

$$\left.\begin{array}{l} a_2 b_2 m_1 \equiv 0 \pmod{m_1} \\ b_1 m_2 \equiv 1 \pmod{m_1} \\ a_1 b_1 m_2 \equiv a_1 \pmod{m_1} \end{array}\right\} \Longrightarrow a_1 b_1 m_2 + a_2 b_2 m_1 \equiv a_1 \pmod{m_1}$$

$$\left.\begin{array}{l} a_1 b_1 m_2 \equiv 0 \pmod{m_2} \\ b_2 m_1 \equiv 1 \pmod{m_2} \\ a_2 b_2 m_1 \equiv a_2 \pmod{m_2} \end{array}\right\} \Longrightarrow a_1 b_1 m_2 + a_2 b_2 m_1 \equiv a_2 \pmod{m_2}$$

[Büten Zar]
B.Sz

c) Utilizar lo anterior para hallar todas las soluciones del sistema.

$$\begin{cases} x \equiv 5 \pmod{14} \\ x \equiv 3 \pmod{11} \end{cases}$$

Vamos a hallar b_1 el inverso de m_2 mod m_1

$$b_1 \cdot 11 \equiv 1 \pmod{14} \longrightarrow b_1 = 9$$

Vamos a hallar b_2 el inverso de m_1 mod m_2

$$b_2 \cdot 14 \equiv 1 \pmod{11} \longrightarrow b_2 = 4$$

$$x = (5) \cdot 9 \cdot 11 + 3 \cdot 4 \cdot 14 = 663$$

La solución es $\boxed{x \equiv 663 \pmod{154}}$

[Büten Zar]
B.Sz

2 Sean $m_1, m_2, \dots, m_k$ enteros coprimos 2 a 2

a) Definimos $M_i = \dfrac{m_1 m_2 \cdots m_k}{m_i} = \prod_{j \neq i} m_j$

Probar que existen $b_1, b_2, \dots, b_k \in \mathbb{Z}$ tales que $b_i M_i \equiv 1 \pmod{m_i}$ $\forall i = 1, \dots, k$

$b_1 \cdot m_2 \cdot m_3 \cdots m_k \equiv 1 \pmod{m_k}$

como $m_1 \dots m_k$ son coprimos 2 a 2 $\Longrightarrow$ ningun m_i comparte factores primos con ningún m_j si $i \neq j$

$\Longrightarrow m_2 \cdot m_3 \cdots m_k$ y m_1 son coprimos $\Longrightarrow$ El sistema $b_1 \cdot M_1 \equiv 1 \bmod m_1$ tiene solución.

b) Probar que para $b_1, b_2, \dots, b_k$ como en la parte anterior, para todo $a_1, a_2, \dots, a_k \in \mathbb{Z}$ el entero $x = a_1 b_1 M_1 + a_2 b_2 M_2 + \dots + a_k b_k M_k$ es solución del sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

$$a_1 b_1 M_1 + \underbrace{a_2 b_2 M_2 + \dots + a_k b_k M_k}_{\equiv 0 \pmod{m_1}} \equiv a_1 \pmod{m_1}$$

como $\left.\begin{array}{l} b_1 M_1 \equiv 1 \pmod{m_1} \\ a_1 b_1 M_1 \equiv a_1 \pmod{m_1} \end{array}\right\} \Longrightarrow x \equiv a_1 \pmod{m_1}$

y así con los demás.

c) Utilizar lo anterior para hallar todas las soluciones del sistema:

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{12} \end{cases}$$

Hallemos los inversos.

$\boxed{b_1}$ $\quad M_1 = 7 \cdot 12$ $\qquad b_1 \cdot 7 \cdot 12 \equiv 1 \pmod{11}$

$$b_1 \cdot 84 \equiv 1 \pmod{11} \iff 84\, b_1 + 11k = 1$$

<u>por AEE</u>

$$84 = 11 \cdot 7 + 7 \implies 7 = 84 - 11 \cdot 7$$

$$11 = 7 \cdot 1 + 4 \implies 4 = 11 - 84 + 11 \cdot 7 = -84 + 11 \cdot 8$$

$$7 = 4 \cdot 1 + 3 \implies 3 = 84 - 11 \cdot 7 + 84 - 11 \cdot 8 = 2 \cdot 84 - 11 \cdot 15$$

$$4 = 3 \cdot 1 + 1 \implies 1 = -84 + 11 \cdot 8 - 2 \cdot 84 + 11 \cdot 15 = -3 \cdot 84 + 11 \cdot 23$$

$$\boxed{b_1 = -3}$$

$\boxed{b_2}$ $\quad M_2 = 11 \cdot 12$ $\qquad b_2 \cdot 11 \cdot 12 \equiv 1 \pmod{7}$

$$b_2 \cdot \underset{\overset{\text{|||}}{-1}}{132} \equiv 1 \pmod{7} \qquad \boxed{b_2 = -1}$$

$\boxed{b_3}$ $\quad M_3 = 11 \cdot 7$ $\qquad b_3 \cdot 11 \cdot 7 \equiv 1 \pmod{12}$

$$b_3 \cdot \underset{\overset{\text{|||}}{5}}{77} \equiv 1 \pmod{12} \iff b_3 \cdot 5 \equiv 1 \pmod{12}$$

$$\boxed{b_3 = 5}$$

$$X = (5)(-3)\,84 + 3\,(-1)\,132 + 10 \cdot 5 \cdot 77 = -1260 - 396 + 3850 = 2194$$

$$X \equiv 2194 \pmod{924} \text{ es sol} \iff \boxed{x \equiv 346 \pmod{924}}$$

1) hallar el menor natural que dividido 3 da resto 1, dividido 4 da resto 3 y dividido 7 da resto 5.

$$\begin{cases} n \equiv 1 \pmod 3 \\ n \equiv 3 \pmod 4 \\ n \equiv 5 \pmod 7 \end{cases}$$

$3y + 4z = 1$

$y = -1, \quad z = 1$

$n = 3.(-1).3 + 4.1.1 = -5$

$$\begin{cases} n \equiv -5 \pmod{12} \\ n \equiv 5 \pmod 7 \end{cases}$$

$12y + 7z = 1$

$y = 3, \quad z = -5$

$12 = 7.1 + 5 \rightarrow 5 = 12 - 7$

$7 = 5.1 + 2 \rightarrow 2 = 7 - 12 + 7$

$5 = 2.2 + 1 \rightarrow 1 = 12 - 7 - 4.7 + 2$

$1 = 3.12 - 5.7$

$n = 12.3.5 - 5.-5.7 = 180 + 175 = 355$

$n \equiv 355 \pmod{84}$

$\boxed{n \equiv 19 \pmod{84}}$ $\boxed{n = 19}$

2)

$$\begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 2 \pmod 3 \\ n \equiv 3 \pmod 4 \\ n \equiv 4 \pmod 5 \\ n \equiv 5 \pmod 6 \\ n \equiv 6 \pmod 7 \\ n \equiv 7 \pmod 8 \\ n \equiv 8 \pmod 9 \end{cases} \Longrightarrow \begin{cases} n \equiv -1 \pmod 2 \\ n \equiv -1 \pmod 3 \\ n \equiv -1 \pmod 4 \\ n \equiv -1 \pmod 5 \\ n \equiv -1 \pmod 6 \\ n \equiv -1 \pmod 7 \\ n \equiv -1 \pmod 8 \\ n \equiv -1 \pmod 9 \end{cases}$$

$n \equiv -1 \mod (3^2 . 2^3 . 7 . 5)$

$n \equiv -1 \mod 2520$

$\boxed{n \equiv 2519 \pmod{2520}}$

$\boxed{n = 2519}$

Ejercicio 3 Menu

$$\begin{cases} 2x+3 \equiv 4 \pmod 5 \\ 3x+4 \equiv 3 \pmod 7 \end{cases}$$

$2x \equiv 1 \pmod 5 \longrightarrow 3.2x \equiv 3 \pmod 5$

$\boxed{x \equiv 3 \pmod 5}$

$3x \equiv 6 \pmod 7 \longrightarrow$ cancelo el 3.

$\boxed{x \equiv 2 \pmod 7}$

nuevo sistema:

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

$5y + 7z = 1$

$y = 3$, $z = -2$

$x = 3.5.2 - 7.2.3 = -12$

$x \equiv -12 \pmod{35}$

$\boxed{x \equiv 23 \pmod{35}} \Longleftrightarrow \boxed{x \equiv 268 \pmod{35}}$

$x = 268$ es el menor par mayor a 199 que cumple las condiciones.

Ejercicio 4 Menu [Büten Zar] B.Sz

(1)

$$\begin{cases} x \equiv 8 \pmod{13} \\ x \equiv 3 \pmod{11} \\ x \equiv 5 \pmod{8} \end{cases}$$

$11z + 8y = 1$

$3 \quad -4$

$x = 11.3.5 - 4.8.3 = 165 - 96 = 69$

$$\begin{cases} x \equiv 69 \mod 88 \\ x \equiv 8 \mod 13 \end{cases}$$

$88y + 13z = 1$

$88 = 13.6 + 10 \longrightarrow 10 = 88 - 13.6$

$13 = 10.1 + 3 \longrightarrow 3 = 13 - 88 + 13.6$

$10 = 3.3 + 1 \longrightarrow 1 = 88 - 13.6 - 21.13 + 3.88$

$1 = (4)\,88\,(-27).13$

$x = 4.88.8 - 27.13.69 = 2816 - 24219 = -21403$

$x \equiv -21403 \pmod{1144}$

$\boxed{x \equiv 333 \pmod{1144}}$

Habian 333 monedas

2

$\boxed{x < 400}$

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 0 \pmod 7 \end{cases}$$

$x \equiv 1 \pmod 6 \Longleftarrow x \equiv 1 \pmod 3,\ \cancel{x \equiv 1 \pmod 2}$

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 3 \end{cases} \qquad \boxed{x \equiv 1 \pmod{60}}$$

$$\begin{cases} x \equiv 1 \pmod{60} \\ x \equiv 0 \pmod 7 \end{cases} \qquad 60x + 7y = 1$$

$60 = 7.8 + 4 \longrightarrow 4 = 60 - 7.8$

$7 = 4.1 + 3 \longrightarrow 3 = 7 - 60 + 7.8$

$4 = 3.1 + 1 \longrightarrow 1 = 60 - 7.8 - 7.9 + 60$

$1 = 2.60 - 7.17$

$x = 60.2.0 - 7.17 = -119$

$x \equiv -119 \pmod{420} \Longleftrightarrow \boxed{x \equiv 301 \pmod{420}}$

hay 301 libros

3

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$$

$x < 75$ $\quad$ x cantidad de huevos en ese día

$$3\underset{-3}{y} + 5\underset{2}{z} = 1$$

$$x = 3.(-3)\,4 + 5.2.2 = -36 + 20 = -16$$

$$x \equiv -16 \pmod{15}$$

$$\boxed{x \equiv 14 \pmod{15}}$$

$$\begin{cases} x \equiv 14 \pmod{15} \\ x \equiv 5 \pmod 7 \end{cases}$$

$$15\underset{1}{y} + 7\underset{-2}{z} = 1$$

$$x = 15.5 - 14.14 = 75 - 196 = -121$$

$$x \equiv -121 \pmod{105}$$

$$x \equiv -16 \pmod{105}$$

$$\boxed{x \equiv 89 \pmod{105}}$$

El capataz tiene razón. Es imposible que esto suceda porque $89 > 75$.

[Büten Zar]
B.Sz

4

$X \leqslant 1000$

$$\begin{cases} X \equiv 1 \pmod 7 \\ X \equiv 8 \pmod{11} \\ X \equiv 1 \pmod{13} \end{cases}$$

mod 7 mod 11 el mod 13

$$\boxed{X = 1\,\alpha_1\, 11 \cdot 13 + 8\,\alpha_2\, 7 \cdot 13 + 1\,\alpha_3\, 7 \cdot 11}$$

$$X = \alpha_1 \cdot 11 \cdot 13 + 8 \cdot \alpha_2\, 7 \cdot 13 + \alpha_3 \cdot 7 \cdot 11$$

$$\alpha_1 \cdot \underset{\equiv 4}{11} \cdot \underset{-1}{13} \equiv 1 \pmod 7$$

$$\alpha_1 \cdot (-4) \equiv 1 \pmod 7 \longrightarrow \boxed{\alpha_1 = -2}$$

$$\alpha_2 \cdot \underset{-4}{7} \cdot \underset{2}{13} \equiv 1 \pmod{11}$$

$$\alpha_2 \cdot \underset{3}{-8} \equiv 1 \pmod{11}$$

$$\alpha_2 \cdot 3 \equiv 1 \pmod{11}$$

$$\boxed{\alpha_2 = 4}$$

$$\alpha_3 \cdot \underset{\equiv -2}{7} \cdot 11 \equiv 1 \pmod{13}$$

$$\alpha_3 \cdot (-14) \equiv 1 \pmod{13}$$

$$\boxed{\alpha_3 = -1}$$

$$X = -2 \cdot 11 \cdot 13 + 32 \cdot 7 \cdot 13 - 7 \cdot 11 = -286 + 2912 - 77 = 2549$$

$$X \equiv 2549 \pmod{1001}$$

$$\boxed{X \equiv 547 \pmod{1001}}$$

$$\boxed{X = 547}$$

Ejercicio 5

Menu

1) $\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 6 \pmod{21} \\ x \equiv 11 \pmod{15} \end{cases}$

$\left.\begin{array}{l} x \equiv 6 \pmod{21} \\ 3 \mid 21 \\ 7 \mid 21 \end{array}\right\} \overset{prop}{\Rightarrow} \begin{array}{l} x \equiv 6 \pmod 3 \\ y \\ x \equiv 6 \pmod 7 \end{array}$ es equivalente por el teo chino de los restos para el $(\Leftarrow)$

$\left.\begin{array}{l} x \equiv 11 \pmod{15} \\ 3 \mid 15 \\ 5 \mid 15 \end{array}\right\} \overset{prop}{\Rightarrow} \begin{array}{l} x \equiv 11 \pmod 3 \\ y \\ x \equiv 11 \pmod 5 \end{array}$ es equivalente por el teo chino de los restos para el $(\Leftarrow)$

El nuevo sistema es:

$\begin{cases} \boxed{x \equiv 1 \pmod 7} \\ \boxed{x \equiv 6 \pmod 7} \\ x \equiv 6 \pmod 3 \\ x \equiv 11 \pmod 3 \\ x \equiv 11 \pmod 5 \end{cases}$ → no puede existir x que cumpla con esas ecuaciones pues el resto es único.

$\Rightarrow$ El sistema no tiene solución.

2) $\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 15 \pmod{21} \\ x \equiv 12 \pmod{15} \end{cases}$ el nuevo sistema es $\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 15 \pmod 7 \longrightarrow x \equiv 1 \pmod 7 \\ x \equiv 15 \pmod 3 \longrightarrow x \equiv 0 \pmod 3 \\ x \equiv 12 \pmod 3 \longrightarrow x \equiv 0 \pmod 3 \\ x \equiv 12 \pmod 5 \longrightarrow x \equiv 2 \pmod 5 \end{cases}$

$\Rightarrow \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 0 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases}$

$x \equiv 1 \pmod 7$

$x \equiv 0 \pmod 3$

$0 < x \leq 21$ es único

$7y + 3z = 1$, $\;y = 1$, $\;z = -2$

$7y \equiv 1 \pmod 3$

$3z \equiv 1 \pmod 7$

$x = 0 \cdot 7(1) + 1 \cdot 3(-2) = \boxed{-6}$

$\Rightarrow \begin{cases} x \equiv -6 \pmod{21} \\ x \equiv 2 \pmod 5 \end{cases}$

$21y + 5z = 1$, $\;y = 1$, $\;z = -4$

$21y \equiv 1 \pmod 5$

$5z \equiv 1 \pmod{21}$

$x = -6 \cdot 5 \cdot (-4) + 21 \cdot 2$

$\boxed{x = 162}$

La solucion del sistema es $x = 162 \mod (7 \cdot 3 \cdot 5)$

$\boxed{x = 57 \mod (105)}$

3

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{18} \end{cases} \quad \text{nuevo sistema} \quad \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{3} \\ x \equiv 6 \pmod{5} \\ x \equiv 7 \pmod{9} \\ x \equiv 7 \pmod{2} \end{cases}$$

$$x \equiv 3 \pmod{4} \longrightarrow x \equiv 3 \pmod{2} \Longleftrightarrow x \equiv 7 \pmod{2}$$

Se puede tachar $x \equiv 7 \pmod{2}$

$$\begin{cases} x \equiv 3 \pmod{4} \\ \boxed{x \equiv 0 \pmod{3}} \\ x \equiv 1 \pmod{5} \\ x \equiv 7 \pmod{9} \end{cases} \qquad x \equiv 7 \pmod{9} \longrightarrow \boxed{x \equiv 7 \pmod{3}}$$

sistema incompatible.

4

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 15 \pmod{18} \end{cases} \quad \text{nuevo sistema} \quad \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{3} \longrightarrow x \equiv 0 \pmod{3} \\ x \equiv 6 \pmod{5} \longrightarrow x \equiv 1 \pmod{5} \\ x \equiv 15 \pmod{2} \\ x \equiv 15 \pmod{9} \longrightarrow x \equiv 6 \pmod{9} \end{cases}$$

$$x \equiv 3 \pmod{4} \longrightarrow x \equiv 3 \bmod 2 \Longleftrightarrow x \equiv 15 \pmod{2}$$

Se puede eliminar $x \equiv 15 \pmod{2}$

$$x \equiv 6 \pmod{9} \longrightarrow x \equiv 6 \pmod{3} \Longleftrightarrow x \equiv 0 \pmod{3}$$

Se puede eliminar $x \equiv 0 \pmod{3}$

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{9} \end{cases} \qquad \underset{-1}{4y} + \underset{1}{5z} = 1 \qquad \begin{aligned} 4y &\equiv 1 \pmod{5} \\ 5z &\equiv 1 \pmod{4} \end{aligned} \qquad x = 4(-1)\cdot 1 + 5(1)\cdot 3 = \boxed{11}$$

$$\begin{cases} x \equiv 11 \pmod{20} \\ x \equiv 6 \pmod{9} \end{cases} \qquad \underset{9}{9y} + \underset{-4}{20z} = 1 \qquad \begin{aligned} 9y &\equiv 1 \pmod{20} \\ 20z &\equiv 1 \pmod{9} \end{aligned} \qquad x = 9\cdot 9\cdot 11 - 80\cdot 6 = \boxed{411}$$

La sol es $x \equiv 411 \pmod{180} \longrightarrow \boxed{x \equiv 51 \pmod{180}}$

5

$$\begin{cases} x \equiv 22 \pmod{63} \\ x \equiv 1 \pmod{21} \\ x \equiv 11 \pmod{49} \end{cases}$$

nuevo sist.

$$\begin{cases} x \equiv 22 \pmod{7} \\ x \equiv 22 \pmod{9} \longrightarrow x \equiv 4 \pmod{9} \\ x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{3} \\ x \equiv 11 \pmod{49} \end{cases}$$

$x \equiv 22 \pmod{7} \iff x \equiv 1 \pmod{7}$

$x \equiv 4 \mod 9 \longrightarrow x \equiv 4 \pmod{3} \iff x \equiv 1 \pmod{3}$

$x \equiv 1 \pmod{3}$ se puede tachar.

$x \equiv 11 \pmod{49} \implies \boxed{x \equiv 11 \pmod{7}}$

$$\begin{cases} \boxed{x \equiv 1 \pmod{7}} \\ x \equiv 4 \pmod{9} \\ \boxed{x \equiv 11 \pmod{49}} \end{cases}$$

sistema incompatible.

6

$$\begin{cases} x \equiv 22 \pmod{63} \\ x \equiv 1 \pmod{21} \\ x \equiv 36 \pmod{49} \end{cases}$$

nuevo sistema

$$\begin{cases} x \equiv 22 \pmod{7} \\ x \equiv 22 \pmod{9} \longrightarrow x \equiv 4 \pmod{9} \\ x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{3} \\ x \equiv 36 \pmod{49} \end{cases}$$

$x \equiv 22 \pmod{7} \iff x \equiv 1 \pmod{7}$

$x \equiv 4 \pmod{9} \longrightarrow x \equiv 4 \pmod{3} \iff x \equiv 1 \pmod{3}$

$x \equiv 1 \pmod{3}$ se puede tachar

$x \equiv 36 \pmod{49} \longrightarrow x \equiv 36 \pmod{7} \iff x \equiv 1 \pmod{7}$

$x \equiv 1 \pmod{7}$ se puede tachar

$$\begin{cases} x \equiv 36 \pmod{49} \\ x \equiv 4 \pmod{9} \end{cases}$$

$$\underset{-2}{49y} + \underset{11}{9z} = 1$$

$x = 49 \cdot (-2) \cdot 4 + 9 \cdot 11 \cdot 36 =$

$-392 + 3564 = 3172$

$x \equiv 3172 \pmod{441} \iff \boxed{x \equiv 85 \pmod{441}}$

Ejercicio 6

Menu

(1)
$$\begin{cases} 3x \equiv 13 \pmod{22} \\ 5x \equiv -1 \pmod{31} \end{cases}$$

$$5x \equiv 30 \pmod{31} \xrightarrow{prop} \boxed{x \equiv 6 \pmod{31}}$$

$$\left.\begin{array}{l} b \in \mathbb{Z} \;/\; 3b \equiv 1 \mod 22 \\ \boxed{b = -7} \end{array}\right\} \quad \begin{array}{l} x \equiv 13 \cdot -7 \pmod{22} \\ \boxed{x \equiv 19 \pmod{22}} \end{array}$$

$$\begin{cases} x \equiv 6 \pmod{31} \\ x \equiv 19 \pmod{22} \end{cases} \qquad 31y + 22z = 1$$

$$31 = 22 \cdot 1 + 9 \longrightarrow 9 = 31 - 22$$

$$22 = 9 \cdot 2 + 4 \longrightarrow 4 = 22 - 9 \cdot 2 \longrightarrow 4 = 22 - 31 \cdot 2 + 22 \cdot 2$$

$$9 = 4 \cdot 2 + 1 \longrightarrow 1 = 9 - 4 \cdot 2$$

$$\rightarrow 1 = 31 - 22 - 6 \cdot 22 + 31 \cdot 4$$

$$1 = 31 \cdot 5 - 7 \cdot 22$$

$$31y \equiv 1 \pmod{22}$$

$$22z \equiv 1 \pmod{31}$$

$$x = 31 \cdot 5 \cdot 19 - 7 \cdot 22 \cdot 6 = 465 - 924 = 2021$$

$$x \equiv 2021 \pmod{682}$$

$$\boxed{x \equiv 657 \pmod{682}}$$

(2) $\begin{cases} 11x \equiv 25 \pmod{45} \\ 32x \equiv 6 \pmod{33} \end{cases}$

sistema $\begin{cases} 11x \equiv 25 \pmod{9} \rightarrow 11x \equiv 7 \pmod{9} \\ 11x \equiv 25 \pmod{5} \rightarrow 11x \equiv 0 \pmod{5} \\ 32x \equiv 6 \pmod{3} \rightarrow \boxed{32x \equiv 0 \pmod{3}} \\ 32x \equiv 6 \pmod{11} \end{cases}$

$11x \equiv 7 \pmod{9} \longrightarrow \boxed{11x \equiv 7 \pmod{3}}$

El sistema es incompatible.

(3) $\begin{cases} 5x - 7y \equiv 9 \pmod{12} \\ 2x + 3y \equiv 10 \pmod{12} \end{cases}$

$\times -2 \longrightarrow 5x - 7y \equiv 9 \pmod{12}$

$\times 5 \longrightarrow 2x + 3y \equiv 10 \pmod{12}$

$29y \equiv 32 \pmod{12}$

$b \in \mathbb{Z} \,/\, 29.b \equiv 1 \mod 12$

$12 \mid 29b - 1 \Rightarrow 12n = 29b - 1 \Rightarrow 1 = 29b - 12n$

$29 = 12.2 + 5 \longrightarrow 5 = 29 - 12.2$

$12 = 5.2 + 2 \longrightarrow 2 = 12 - 2.29 + 4.12 = 5.12 - 2.29$

$5 = 2.2 + 1 \longrightarrow 1 = 5 - 2.2 = 29 - 12.2 - 10.12 + 4.29$

$1 = 5.29 - 12.12$

$\boxed{b = 5}$

$29y \equiv 32 \pmod{12}$

$29y \equiv 8 \pmod{12}$

$5.29y \equiv 5.8 \pmod{12}$

$y \equiv 40 \pmod{12}$

$\boxed{y \equiv 4 \mod 12}$

$\begin{cases} 5x - 28 \equiv 9 \pmod{12} \\ 2x + 12 \equiv 10 \pmod{12} \end{cases}$

$x - 52 \equiv -11 \pmod{12}$

$x \equiv 53 \pmod{12}$

$\boxed{x \equiv 5 \pmod{12}}$

[Büten Zar]
B.Sz

4

$$\begin{cases} 11x - 7y \equiv 10 \pmod{45} \\ 4x + 14y \equiv 12 \pmod{45} \end{cases}$$

$\times 2 \longrightarrow 11x - 7y \equiv 10 \pmod{45}$

$4x + 14y \equiv 12 \pmod{45}$

$26x \equiv 32 \pmod{45}$

$b \in \mathbb{Z} \ / \ 26 \cdot b \equiv 1 \pmod{45}$

$\boxed{b = -19}$

$(-19) \cdot 26x \equiv (-19) \cdot 32 \pmod{45}$

$x \equiv 32 \cdot (-19) \pmod{45} \implies \boxed{x \equiv 22 \pmod{45}}$

$$\begin{cases} 22 \cdot 11 - 7y \equiv 10 \pmod{45} \\ 4 \cdot 22 + 14y \equiv 12 \pmod{45} \end{cases} \longrightarrow 14y \equiv 12 - 88 \pmod{45}$$

$14y \equiv -76 \pmod{45}$

$7y \equiv -38 \pmod{45}$

$7y \equiv 7 \pmod{45}$

$\boxed{y \equiv 1 \pmod{45}}$

Ejercicio 7

Menu

1 a) $\boxed{560^{48} \pmod{1001}}$

$1001 = 11 \cdot 13 \cdot 7$

$$\begin{cases} 560^{48} \equiv x \pmod 7 \\ 560^{48} \equiv x \pmod{11} \\ 560^{48} \equiv x \pmod{13} \end{cases}$$

$560^{48} \equiv x \pmod 7 \longrightarrow (7 \cdot 80)^{48} \equiv x \pmod 7 \Longrightarrow \boxed{0 \equiv x \pmod 7}$

$560 \equiv 10 \pmod{11}$

$10 \cdot b \equiv 1 \pmod{11}$

$b = -1$

$10^{48} \equiv x \pmod{11}$

$(-1)^{48} \cdot 10^{48} \equiv (-1)^{48} \cdot x \pmod{11}$

$\boxed{1 \equiv x \pmod{11}}$

$560 \equiv 1 \pmod{13} \Longrightarrow \boxed{1 \equiv x \pmod{13}}$

$$\begin{cases} x \equiv 0 \pmod 7 \\ x \equiv 1 \pmod{11} \\ x \equiv 1 \pmod{13} \end{cases}$$

$11y + 13z = 1$

$13 = 11 \cdot 1 + 2 \longrightarrow 2 = 13 - 11$

$11 = 2 \cdot 5 + 1 \longrightarrow 1 = 11 - 5 \cdot 13 + 5 \cdot 11$

$1 = 6 \cdot 11 - 5 \cdot 13$

$11y \equiv 1 \pmod{13}$

$13z \equiv 1 \pmod{11}$

$x = 11(6) \cdot 1 - 13 \cdot (5) \cdot 1$

$\boxed{x = 1}$

$$\begin{cases} x \equiv 0 \pmod 7 \\ x \equiv 1 \pmod{143} \end{cases}$$

$7\underset{41}{y} + 143\underset{-2}{z} = 1$

$x = 7 \cdot 41 \cdot 1 - 0 = 287$

$\boxed{x \equiv 287 \pmod{1001}}$

$\boxed{560^{48} \equiv 287 \pmod{1001}}$

[Büten Zar]
B.Sz

(b) $\boxed{22^{232} \pmod{36}}$

$$22^{232} \equiv x \pmod{36}$$

$$\begin{cases} 22^{232} \equiv x \pmod 4 \\ 22^{232} \equiv x \pmod 9 \end{cases}$$

$22^{232} \equiv x \pmod 4 \longrightarrow 22 \equiv 2 \pmod 4 \Rightarrow 2^{232} \equiv x \pmod 4$

$2^2 \equiv 0 \pmod 4 \Rightarrow 2^{232} \equiv 0 \pmod 4$

$\Rightarrow \boxed{x \equiv 0 \pmod 4}$

$22 \equiv 4 \pmod 9$

$\Rightarrow 4^{232} \equiv x \pmod 9$

$4^2 \equiv -2 \pmod 9 \Rightarrow (-2)^{116} \equiv x \pmod 9$

$(4)^{58} \equiv x \pmod 9$

$(-2)^{29} \equiv x \pmod 9$

$(-2) \cdot 4^{14} \equiv x \pmod 9$

$(-2) \cdot (-2)^7 \equiv x \pmod 9$

$4 \cdot 4^3 \equiv x \pmod 9 \Rightarrow (-2)^2 \equiv x \pmod 9$

$\boxed{x \equiv 4 \pmod 9}$

$$\begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 4 \pmod 9 \end{cases}$$

$4y + 9z = 1$

$y = -2$

$x = -2 \cdot 4 \cdot 4 = \boxed{-32}$

$$\boxed{22^{232} \equiv 4 \pmod{36}}$$

Ejercicio 1

1 **c)** Hallar el último dígito de $2^{1000000}$ representado en base 13.

$$2^{1000000} = \underbrace{d_m 13^m + \dots + 13^2 d_2 + 13 d_1}_{\dot{13}} + 13^0 . d_0 \qquad 0 \leq d_0 < 13$$

$$\left.\begin{array}{l} 2^{1000000} \equiv d_0 \pmod{13} \\ 0 \leq d_0 < 13 \end{array}\right\} \Rightarrow \quad 2^{12} \equiv 1 \pmod{13}$$

$$2^{12 . n} \equiv 1 \pmod{13}$$

$$2^{12 . 83333} \equiv 1 \pmod{13}$$

$$2^4 \equiv d_0 \pmod{13}$$

$$\boxed{3 \equiv d_0 \pmod{13}}$$

d) idem, en base 10.

$$2^{1000000} \equiv 0 \pmod{2}$$

tco chino

$$2^{1000000} \equiv d_0 \pmod{10} \quad \begin{cases} 2^{1000000} \equiv d_0 \pmod{2} \\ 2^{1000000} \equiv d_0 \pmod{5} \quad \rightarrow \quad 2^4 \equiv 1 \pmod{5} \end{cases}$$

$$2^{1000000} \equiv 1 \pmod{5}$$

$$\begin{cases} d_0 \equiv 0 \pmod{2} \\ d_0 \equiv 1 \pmod{5} \end{cases} \Rightarrow \boxed{d_0 = 6}$$

$$\boxed{2^{1000000} \equiv 6 \mod 10}$$

2 Investigar si 257 es primo y calcular 3^{9990} (mod 257)

$\sqrt{257} = 16, \ldots \qquad 2 \nmid 257 \;,\; 3 \nmid 257 \;,\; 5 \nmid 257 \;,\; 7 \nmid 257 \;,\; 11 \nmid 257 \;,\; 13 \nmid 257$

257 es primo.

$\boxed{3^{9990} \equiv x \mod (257)}$

ptf

$3^{256} \equiv 1 \mod (257) \implies 3^{9984} \equiv 1 \pmod{257}$

$\implies 3^{6} \equiv x \pmod{257}$

$\boxed{x \equiv 215 \pmod{257}}$

3 a) $\boxed{132^{231} \pmod 7}$

$132^{231} \equiv x \pmod 7$

$132 \equiv -1 \pmod 7 \implies (-1)^{231} \equiv x \pmod 7$

$\boxed{x \equiv 6 \pmod 7}$

b) $\boxed{246^{218} \pmod{11}}$

$246^{218} \equiv 4 \mod 11 \implies 4^{218} \equiv x \pmod{11}$

$4^{10} \equiv 1 \pmod{11} \to 4^{8} \equiv x \pmod{11}$

$2^{16} \equiv x \pmod{11}$

$2^{10} \equiv 1 \pmod{11}$

$\to 2^{6} \equiv x \pmod{11}$

$64 \equiv x \pmod{11}$

$\boxed{x \equiv 9 \pmod{11}}$

C $\boxed{2^{69} \pmod{71}}$

$$2^{69} \equiv x \pmod{71}$$

2 es invertible mod 71 y su inverso es 36

$\Downarrow$ ptf

$$2^{70} \equiv 1 \pmod{71}$$

$$\underbrace{36 \cdot 2}_{1} \cdot 2^{69} \equiv 36 \pmod{71} \implies \boxed{2^{69} \equiv 36 \pmod{71}}$$

D $\boxed{3^{279} \pmod{283}}$

$$3^{279} \equiv x \pmod{283}$$

$$3^{282} \equiv 1 \pmod{283}$$

$$27 \cdot 3^{279} \equiv 1 \pmod{283}$$

$$27 \cdot b \equiv 1 \pmod{283}$$

$$27b - 283k = 1$$

$$283 = 27 \cdot 10 + 13 \longrightarrow 13 = 283 - 10 \cdot 27$$

$$27 = 13 \cdot 2 + 1 \longrightarrow 1 = 27 - 2 \cdot 283 + 20 \cdot 27$$

$$\boxed{b = 21}$$

$$\implies \underbrace{21 \cdot 27}_{1} \, 3^{279} \equiv 21 \pmod{283}$$

$$\boxed{3^{279} \equiv 21 \pmod{283}}$$

Ejercicio 7

4 $\boxed{2^{71} \pmod 3}$

$$2^{71} \equiv R \pmod 3$$

$$0 \leq R < 3$$

Pequeño teorema de Fermat

$$\left.\begin{array}{l} p \text{ primo} \quad a \nmid p \end{array}\right\} \Rightarrow a^{p-1} \equiv 1 \ (p)$$

$$\left.\begin{array}{l} a = 2 \\ p = 3 \end{array}\right\} \Rightarrow 2^{2} \equiv 1 \pmod 3 \Rightarrow \boxed{2 \equiv R \pmod 3} \qquad 2^{71} \equiv 2 \pmod 3$$

$\boxed{2^{71} \pmod{37}}$

$$\left.\begin{array}{l} a = 2 \\ p = 37 \end{array}\right\} \xRightarrow{PTF} 2^{36} \equiv 1 \pmod{37} \Rightarrow 2^{72} \equiv 1 \pmod{37}$$

$$b \in \mathbb{Z} \,/\, 2b \equiv 1 \pmod{37} \to 19$$

$$2 \cdot 2^{71} \equiv 1 \pmod{37}$$

$$\underbrace{19 \cdot 2}_{1} \cdot 2^{71} \equiv 19 \pmod{37}$$

$$\boxed{2^{71} \equiv 19 \pmod{37}}$$

$\boxed{2^{71} \pmod{111}}$

teochino

$$2^{71} \equiv R \pmod{111} \quad \begin{cases} 2^{71} \equiv R \pmod{37} \\ 2^{71} \equiv R \pmod 3 \end{cases} \iff \begin{cases} x \equiv 19 \pmod{37} \\ x \equiv 2 \pmod 3 \end{cases}$$

$$\underset{-12}{3y} + \underset{1}{37z} = 1 \qquad \begin{array}{l} 3y \equiv 1 \pmod{37} \\ 37z \equiv 1 \pmod 3 \end{array}$$

$$x = 37 \cdot 1 \cdot 2 - 3 \cdot 12 \cdot 19 = 74 - 684 = -610$$

$$R \equiv -610 \pmod{111}$$

$$\boxed{R \equiv 56 \pmod{111}}$$

5 $\boxed{347^{231} \pmod{35}}$

$$347 \equiv 2 \pmod 5$$

$$347^{231} \equiv x \pmod 5$$

PtFe

$$347^{4} \equiv 1 \pmod 5 \Rightarrow 347^{228} \equiv 1 \pmod 5$$

$$347^{3} \equiv x \pmod 5 \Longrightarrow 2^{3} \equiv x \pmod 5$$

$$\boxed{x \equiv 3 \pmod 5}$$

$$347^{231} \equiv x \pmod 7 \xrightarrow{PTF} 347^{6} \equiv 1 \pmod 7$$

$$347^{234} \equiv 1 \pmod 7$$

$$347^{3} \cdot x \equiv 1 \pmod 7$$

$$347b + 7k = 1$$

$$347 = 7 \cdot 49 + 4 \rightarrow 4 = 346 - 7 \cdot 49$$

$$7 = 4 \cdot 1 + 3 \rightarrow 3 = 7 - 346 + 7 \cdot 49$$

$$4 = 3 \cdot 1 + 1 \rightarrow 1 = 346 - 7 \cdot 49 - 7 \cdot 50 + 346$$

$$\boxed{b = 2}$$

$$2^{3} \cdot 346^{3}\, x \equiv 8 \pmod 7$$

$$\boxed{x \equiv 1 \pmod 7}$$

$$7\underset{-7}{y} + 5\underset{10}{z} = 1$$

$$x = 7 \cdot (-7)\, 3 + 50 \cdot 1 = -97$$

$$x \equiv -97 \pmod{35}$$

$$\boxed{x \equiv 8 \pmod{35}}$$

$$\Longrightarrow \boxed{347^{231} \equiv 8 \pmod{35}}$$

[Büten Zar]
B.Sz

6 a) $\boxed{12^{22} \pmod{100}}$

$$\begin{cases} 12^{22} \equiv x \pmod 4 \\ 12^{22} \equiv x \pmod{25} \end{cases}$$

$12 \equiv 0 \pmod 4 \Longleftarrow 12^{22} \equiv 0 \pmod 4$

$\boxed{x \equiv 0 \pmod 4}$

F-E

$12^{20} \equiv 1 \pmod{25}$

$12^{2} \equiv x \pmod{25}$

$\boxed{x \equiv 19 \pmod{25}}$

$4y + 25z = 1$

$1 \quad 1$

$-6 \quad 1$

$x = -24 \cdot 19 = -456$

$\boxed{x \equiv 44 \pmod{100}}$

$12^{22} \equiv 44 \pmod{100}$

b) $\boxed{70^{151} \pmod{252}}$

$$\begin{cases} 70^{151} \equiv x \pmod 4 \\ 70^{151} \equiv x \pmod 9 \\ 70^{151} \equiv x \pmod 7 \end{cases}$$

$70 \equiv -2 \pmod 4 \Longrightarrow 70^{151} \equiv 2^{151} \pmod 4$

$2^{2} \equiv 0 \pmod 4 \Longrightarrow 2^{151} \equiv 0 \pmod 4$

$\boxed{0 \equiv x \pmod 4}$

$$\left.\begin{array}{l} 70 \equiv 7 \pmod 9 \\ 7 \equiv -2 \pmod 9 \end{array}\right\} \Rightarrow 70 \equiv -2 \pmod 9$$

$70^{151} \equiv (-2)^{151} \pmod 9$

$(-2)^{\varphi(9)} \equiv 1 \pmod 9$

$(-2)^{6} \equiv 1 \pmod 9 \Rightarrow 151 = 6 \cdot 25 + 1$

$(-2)^{150} \cdot -2 \equiv x \pmod 9$

$-2 \equiv x \pmod 9$

$\boxed{x \equiv 7 \pmod 9}$

[Büten Zar]
B.Sz

$$70^{151} = (7.10)^{151} = 7^{151} . 10^{151} \equiv 0 \pmod 7$$

$$\boxed{x \equiv 0 \pmod 7}$$

$$\begin{cases} x \equiv 0 \pmod 4 \\ x \equiv -2 \pmod 9 \\ x \equiv 0 \pmod 7 \end{cases} \longrightarrow \begin{cases} x \equiv 0 \pmod{28} \\ x \equiv -2 \pmod 9 \end{cases}$$

$$\underset{1}{\underset{\uparrow}{28y}} + \underset{-3}{\underset{\uparrow}{9z}} = 1 \qquad x = 28(-2) = -56$$

$$x \equiv -56 \pmod{252} \iff \boxed{x \equiv 196 \pmod{252}}$$

$$\Longrightarrow \boxed{70^{151} \equiv 196 \pmod{252}}$$

7 $\boxed{123^{253} \pmod{490}}$

$$\begin{cases} 123^{253} \equiv x \pmod 2 \\ 123^{253} \equiv x \pmod 5 \\ 123^{253} \equiv x \pmod{49} \end{cases}$$

$$123 \equiv 1 \pmod 2 \longrightarrow 123^{253} \equiv 1 \pmod 2$$

$$\boxed{x \equiv 1 \pmod 2}$$

$$123 \equiv 3 \pmod 5$$

pff

$$\left.\begin{array}{l} 123^4 \equiv 1 \pmod 5 \\ 253 = 4.63 + 1 \end{array}\right\} \quad 123^{253} = (123^4)^{63} . 123 \equiv 123 \text{ mo}$$

$$\boxed{x \equiv 3 \pmod 5}$$

$$123^{\varphi(49)} = 123^{42} \equiv 1 \pmod{49}$$

$$123 \equiv 25 \pmod{49} \qquad 253 = 42.6 + 1$$

$$123^{253} = (123^{42})^6 . 123^3 \equiv 123^3 \pmod{49}$$

$$\equiv 25^3 \pmod{49} \qquad \boxed{x \equiv 25 \pmod{49}}$$

$$\left\{\begin{array}{l} x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 5 \end{array}\right\} \quad x \equiv 3 \pmod{10}$$

$$x \equiv 25 \pmod{49} \longrightarrow x \equiv 25 \pmod{49}$$

$$10y + 49z = 1$$
$$y = 5, \quad z = -1$$

$$x = 10 \cdot 5 \cdot 25 - 49 \cdot 3 = 1250 - 147 = 1103$$

$$x \equiv 1103 \pmod{490} \iff x \equiv 123 \pmod{490}$$

$$\Longrightarrow 123^{253} \equiv 123 \pmod{490}$$

8 $\boxed{24^{253} \pmod{490}}$

$$\left\{\begin{array}{l} 24^{253} \equiv x \pmod 2 \longrightarrow x \equiv 0 \pmod 2 \\ 24^{253} \equiv x \pmod 5 \longrightarrow x \equiv -1 \pmod 5 \\ 24^{253} \equiv x \pmod{49} \end{array}\right.$$

$$24^{42} \equiv 1 \pmod{49} \Rightarrow \left(24^{42}\right)^{6} \cdot 24 \equiv 24 \pmod{49}$$

$$x \equiv 24 \pmod{49}$$

$$\left\{\begin{array}{l} x \equiv 0 \pmod 2 \\ x \equiv 4 \pmod 5 \end{array}\right\} \Rightarrow x \equiv 4 \pmod{10}$$

$$x \equiv 24 \pmod{49} \quad x \equiv 24 \pmod{49}$$

$$49y + 10z = 1$$
$$y = -1, \quad z = 5$$

$$x = -49 \cdot 4 + 50 \cdot 24 = -196 + 1200 = \boxed{1004}$$

$$x \equiv 1004 \pmod{490} \iff x \equiv 24 \pmod{490}$$

$$\boxed{24^{253} \equiv 24 \pmod{490}}$$

Ejercicio 8

Menu

p y q son primos, $p \neq q$ $\quad a^p \equiv a \pmod q$ y $a^q \equiv a \pmod p$

probar que $a^{pq} \equiv a \pmod{pq}$

Por el pequeño teorema de Fermat.

$a^p \equiv a \pmod p$

$a^q \equiv a \pmod q$

$$\left.\begin{array}{l} a^{pq} = (a^p)^q \equiv a^q \pmod p \\ a^{pq} = (a^q)^p \equiv a^p \pmod q \end{array}\right\} \Rightarrow x = a^{pq} \text{ es solución de } \left\{\begin{array}{l} x \equiv a^q \pmod p \\ x \equiv a^p \pmod q \end{array}\right.$$

por (H) $x = a$ también es solución

$\Rightarrow$ por la unicidad del teorema del resto chino

$$a^{pq} \equiv a \pmod{pq}$$

Probar que $\varphi(m.n) = \dfrac{\varphi(m)\varphi(n)\, d}{\varphi(d)}$ donde $d = \text{mcd}(m,n)$ y φ la función de Euler.

$m = p_1^{m_1} \cdots\cdots p_k^{m_k}$

$n = q_1^{\alpha_1} \cdots q_r^{\alpha r}$

Construimos $d = \text{MCD}(m,n)$ tomando los factores primos comunes elevados al menor exponente.

$d = h_1^{\beta_1} \cdots\cdots h_J^{\beta_J}$

$$\frac{\varphi(m).\varphi(n).d}{\varphi(d)} = \frac{\cancel{d}.\, m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\, n\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_r}\right)}{\cancel{d}\left(1-\frac{1}{h_1}\right)\cdots\left(1-\frac{1}{h_J}\right)}$$

Ahora, sea γ un factor común de m y n, entonces el término $\left(1-\frac{1}{\gamma}\right)$ aparece elevado al cuadrado en el numerador. Pero si γ es un factor común de m y n entonces es un factor de d, por lo que $\left(1-\frac{1}{\gamma}\right)$ aparece en el denominador cancelando la potencia al cuadrado.

$$\Rightarrow \frac{\varphi(m)\,\varphi(n).d}{\varphi(d)} = m.n \prod_{\substack{p_i \text{ primo} \\ p_i \mid m.n}} = \varphi(m.n)$$

Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Menu

Matemática Discreta 2
Curso 2012

PRÁCTICO 5: Teorema Chino del Resto- Teorema de Fermat-Euler

Ejercicio 1.

1. Sean m_1 y m_2 enteros coprimos

a) Probar que existen b_1, $b_2 \in \mathbb{Z}$ tales que $b_1 m_2 \equiv 1 (\operatorname{mod} m_1)$ y $b_2 m_1 \equiv 1 (\operatorname{mod} m_2)$.

b) Probar que para b_1 y b_2 como en la parte anterior, para todo a_1, $a_2 \in \mathbb{Z}$, el entero $x = a_1 b_1 m_2 + a_2 b_2 m_1$ es solución del sistema

$$\begin{cases} x \equiv a_1 (\operatorname{mod} m_1) \\ x \equiv a_2 (\operatorname{mod} m_2) \end{cases}$$

c) Utilizar lo anterior para hallar todas las soluciones del sistema

$$\begin{cases} x \equiv 5 (\operatorname{mod} 14) \\ x \equiv 3 (\operatorname{mod} 11) \end{cases}$$

2. Sean $m_1, m_2, \cdots, m_k$ enteros coprimos 2 a 2.

a) Definimos $M_i = \dfrac{m_1 m_2 \cdots m_k}{m_i} = \prod_{j \neq i} m_j$; probar que existen b_1, $b_2, \cdots, b_k \in \mathbb{Z}$ tales que $b_i M_i \equiv 1 (\operatorname{mod} m_i)$ $\forall i = 1, \cdots, k$.

b) Probar que para $b_1, b_2, \cdots, b_k$ como en la parte anterior, para todo a_1, $a_2, \cdots, a_k \in \mathbb{Z}$ el entero $x = a_1 b_1 M_1 + a_2 b_2 M_2 + \cdots + a_k b_k M_k$ es solución del sistema

$$\begin{cases} x \equiv a_1 (\operatorname{mod} m_1) \\ x \equiv a_2 (\operatorname{mod} m_2) \\ \quad \vdots \\ x \equiv a_k (\operatorname{mod} m_k) \end{cases}$$

c) Utilizar lo anterior para hallar todas las soluciones del sistema

$$\begin{cases} x \equiv 5 (\operatorname{mod} 11) \\ x \equiv 3 (\operatorname{mod} 7) \\ x \equiv 10 (\operatorname{mod} 12) \end{cases}$$

Ejercicio 2.

1. Hallar el menor natural que dividido 3 da resto 1, divido 4 da resto 3 y dividido 7 da resto 5.

2. Encontrar el menor natural n que dividido 2 da resto 1, dividido 3 da resto 2, dividido 4 da resto 3, dividido 5 da resto 4, dividido 6 da resto 5, dividido 7 da resto 6, dividido 8 da resto 7 y dividido 9 da resto 8. [Sug. Considerar $n + 1$]

Ejercicio 3. Hallar el menor par $x > 199$ que cumpla $2x + 3 \equiv 4 (\operatorname{mod} 5)$ y $3x + 4 \equiv 3 (\operatorname{mod} 7)$.

Ejercicio 4.

1. Una banda de 13 piratas obtuvo un cierto número de monedas de oro, que trataron de distribuir entre sí equitativamente, pero les sobraban 8 monedas. Imprevistamente dos de ellos fueron expulsados de la banda por intentar robarse todo el botín. Al volver a intentar el reparto, sobraban ahora 3 monedas. Posteriormente, tres de ellos se ahogaron y al intentar distribuir las monedas quedaban 5. ¿Cuántas monedas habían en el botín?

2. Un bibliotecario cuenta los libros de un armario. Si los agrupa de a 4 o de a 5 o de a 6 siempre sobra 1. Si los agrupa de a 7 no le sobra ninguno. Sabiendo que los libros son menos de 400 ¿cuántos libros tiene?

3. La producción diaria de huevos de una granja es inferior a 75 unidades. Cierto día el recolector informa que la cantidad de huevos recogida es tal que contando de a 3 le sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz, que estudia aritmética a escondidas, le dice que eso es imposible. ¿Quién tiene razón?

4. Un mago me pidió que pensara un número natural no mayor que 1000. Yo elegí x. Luego me pidió el resto de la división entre 7. Le dije que era 1. Inmediatamente después me dijo que dividiera el número pensado entre 11 y que también le diera el resto. Le dije que era 8. Y por último la misma operación dividiendo el número pensado entre 13. Le dije que el resto era 1. Entonces el mago dijo que utilizo la fórmula mágica de los restos y con los números 1, 8 y 1, que son los restos, dedujo que el número era x. ¡¡Acertó!!. Hallar el valor de x justificando la respuesta.

Ejercicio 5. Investigar si los siguientes sistemas tienen solución, y en caso de que así sea, hallarlas todas (observar que cuando existen soluciones, son únicas modulo el mínimo común múltiplo de los módulos de cada ecuación).

1. $\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 6 \pmod{21} \\ x \equiv 11 \pmod{15} \end{cases}$ **2.** $\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 15 \pmod{21} \\ x \equiv 12 \pmod{15} \end{cases}$ **3.** $\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{18} \end{cases}$ **4.** $\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 6 \pmod{15} \\ x \equiv 15 \pmod{18} \end{cases}$

5. $\begin{cases} x \equiv 22 \pmod{63} \\ x \equiv 1 \pmod{21} \\ x \equiv 11 \pmod{49} \end{cases}$ **6.** $\begin{cases} x \equiv 22 \pmod{63} \\ x \equiv 1 \pmod{21} \\ x \equiv 36 \pmod{49} \end{cases}$

Ejercicio 6. Resolver los siguientes sistemas.

1. $\begin{cases} 3x \equiv 13 \pmod{22} \\ 5x \equiv -1 \pmod{31} \end{cases}$ **2.** $\begin{cases} 11x \equiv 25 \pmod{45} \\ 32x \equiv 6 \pmod{33} \end{cases}$ **3.** $\begin{cases} 5x - 7y \equiv 9 \pmod{12} \\ 2x + 3y \equiv 10 \pmod{12} \end{cases}$

4. $\begin{cases} 11x - 7y \equiv 10 \pmod{45} \\ 4x + 14y \equiv 12 \pmod{45} \end{cases}$

Ejercicio 7. Cuando pedimos calcular $a \pmod n$ nos referimos a hallar el entero $0 \leq x < n$ tal que $a \equiv x \pmod n$. En los siguientes casos, calcular:

1. **a)** $560^{48} \pmod{1001}$ **b)** $22^{232} \pmod{36}$ **c)** Hallar el último dígito de $2^{1000000}$ representado en base 13.

2. Investigar si 257 es primo y calcular $3^{9990} \pmod{257}$.

3. **a)** $132^{231} \pmod 7$, **b)**$246^{218} \pmod{11}$ **c)** $2^{69} \pmod{71}$ **d)** $3^{279} \pmod{283}$.

4. $2^{71} \pmod 3$ y $2^{71} \pmod{37}$ y utilizarlos para calcular $2^{71} \pmod{111}$.

5. $347^{231} (\bmod 35)$ (sugerencia: imitar lo hecho en la parte anterior)

6. **a)** $12^{22} (\bmod 100)$ **b)** $70^{151} \bmod 252$

7. Hallar el resto de dividir 123^{253} entre 490 (sugerencia: hallar los restos de dividir 123^{253} entre 2, 5 y 49).

8. Hallar el resto de dividir 24^{253} entre 490.

Ejercicio 8. Si p y q son primos distintos tales que $a^p \equiv a (\bmod q)$ y $a^q \equiv a (\bmod p)$, probar que $a^{pq} \equiv a (\bmod pq)$.

Ejercicio 9. Probar que $\varphi(mn) = \frac{\varphi(m)\varphi(n)d}{\varphi(d)}$ donde $d = \operatorname{mcd}(m, n)$ y φ la función de Euler.

Ejercicio 10. Se dice que un entero n es un *Pseudoprimo de Carmichael* si n es compuesto y $a^n \equiv a \bmod n$ para todo $a \in \mathbb{Z}$.

1. Sea a un número entero positivo y coprimo con 561.

   a. Demostrar que $a^2 \equiv 1 (\bmod 3)$, $a^{10} \equiv 1 (\bmod 11)$ y $a^{16} \equiv 1 (\bmod 17)$.

   b. Hallar $a^{560} (\bmod 3)$, $a^{560} (\bmod 11)$ y $a^{560} (\bmod 17)$.

   c. Probar que 561 es un Pseudoprimo de Carmichael (*Sug: hallar* a^{561} *dependiendo si* a *es coprimo o no con 561*).

2. Probar que si n es un entero compuesto tal que $\varphi(n) | n - 1$ entonces n es un pseudoprimo de Carmichael.

3. Sea n compuesto y libre de cuadrados (no es divisible por ningún cuadrado), tal que todo divisor primo p de n cumple que $p - 1 | n - 1$.

   a. Probar que n es un pseudoprimo de Carmichael.

   b. Probar que n es impar.

   c. Probar que n posee al menos tres factores primos distintos.