

UNA SOLUCIÓN

P2

ÁLGEBRA
24/25

- ① Recordemos el teorema de la ecuación lineal en congruencias:

$$ax \equiv b \pmod{n} \iff \gcd(a, n) \mid b$$

tiene solución

En este caso hay d soluciones distintas en $\mathbb{Z}/n\mathbb{Z}$.

a=2: $2x \equiv 10 \pmod{12}$

$\gcd(2, 12) = 2$ y $2 \mid 10 \Rightarrow 2$ soluciones en $\mathbb{Z}/12\mathbb{Z}$

a=4 $4x \equiv 10 \pmod{12}$

$\gcd(4, 12) = 4$ y $4 \nmid 10 \Rightarrow 0$ " "

a=5 $5x \equiv 10 \pmod{12}$

$\gcd(5, 12) = 1$ y $1 \mid 10 \Rightarrow 1$ solución " "

- ② Recordemos

$\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ es invertible $\iff \gcd(a, n) = 1$

En este caso el inverso es único.

a=2: $\gcd(2, 18) = 2 \neq 1 \Rightarrow \bar{2}$ no es invertible en $\mathbb{Z}/18\mathbb{Z}$
 $\Rightarrow$ Hay 0 inversos de $\bar{2}$ " "

a=4: $\gcd(4, 18) = 2 \neq 1 \Rightarrow \bar{4}$ " " " " "
 $\Rightarrow$ " " " " " "

a=5 $\gcd(5, 18) = 1 \Rightarrow \bar{5}$ sí " " " "
 $\Rightarrow$ Hay 1 inverso de $\bar{5}$ en $\mathbb{Z}/18\mathbb{Z}$

$$(3) \gcd(5^{454}, 5^{10} + 3) = 1$$

Demo:

Supongamos el $\neq 1$. Sea $p \mid \gcd(5^{454}, 5^{10} + 3)$ un primo

$$\Rightarrow \left\{ \begin{array}{l} p \mid 5^{454} \Rightarrow p \mid 5 \Rightarrow p = 5 \\ p \mid 5^{10} + 3 \end{array} \right\} \Rightarrow$$

$$\Rightarrow 5 \mid (5^{10} + 3) - 5^{10} = 3 \Rightarrow 5 \mid 3 \text{ ¡Contradicción!} \quad \#$$

$$(4) \text{ Si } a \in \mathbb{Z} \text{ no es múltiplo de } 3$$

$$\Leftrightarrow \bar{a} \neq \bar{0} \text{ en } \mathbb{Z}/3\mathbb{Z} \Leftrightarrow \bar{a} \in \{\bar{1}, \bar{2}\}$$

$$\Leftrightarrow \bar{a}^2 \in \{\bar{1}, \underbrace{(\bar{2})^2}_{\bar{1}}\} = \{\bar{1}\} \Leftrightarrow a^2 + 2 \equiv 3 \equiv 0 \pmod{3}$$

$$\Leftrightarrow 3 \mid a^2 + 2 \Leftrightarrow a^2 + 2 \text{ es múltiplo de } 3.$$

$$(5) 93^{2226} \pmod{44}$$

$$\varphi(44) = \varphi(2^2 \cdot 11) = \varphi(2^2) \cdot \varphi(11) = (2^2 - 2)(11 - 1) = 20$$

$$\left. \begin{array}{l} 2226 = 111 \cdot 20 + 6 \\ 93 = 44 \cdot 2 + 5 \end{array} \right\} \Rightarrow 93^{2226}$$

Entonces:

$$93^{2226} \equiv (5^{20})^{111} \cdot 5^6 \equiv 5^6 \pmod{44}$$

$$\boxed{\begin{array}{l} \text{Tema} \\ \text{Euler-Fermat} \end{array}} \rightarrow 1^{111} \pmod{44}$$

$$5^6 \equiv (5^3)^2 \equiv (37)^2 \equiv (-7)^2 \equiv 49 \equiv 5 \pmod{44}$$

$$\Rightarrow 5 \text{ es el resto de dividir } 93^{2226} \text{ por } 44$$

⑥ Recordemos el teorema de ecuación diofántica lineal.

$$ax + by = c$$

tiene solución en $\mathbb{Z}^2 \iff d \mid c$
donde $d = \text{mcd}(a, b)$

Una solución particular:

① $ar + bs = d$ (Identidad de Bezout)

② $a \underbrace{(nr)}_{x_0} + b \underbrace{(ns)}_{y_0} = nd = c$

Así todas las soluciones enteras son de

la forma:

$$\begin{cases} x = x_0 + \frac{b}{d} t \\ y = y_0 - \frac{a}{d} t \end{cases}, t \in \mathbb{Z}$$

Vamos a aplicarlo a la ecuación:

$$40x + 436y = 8$$

Calculamos el $\text{mcd}(40, 436)$ con el algoritmo de

Euclides:

$$436 = 40 \cdot 10 + 36 \rightarrow 36 = 436 - 40 \cdot 10$$

$$40 = 36 \cdot 1 + \boxed{4} \rightarrow 4 = 40 - 36 = 40 - (436 - 4 \cdot 10)$$

$$36 = 4 \cdot 9 + 0$$

$$\boxed{4 = 11 \cdot 40 - 436}$$

$$\Rightarrow \text{mcd}(40, 436) = 4$$



$$8 = (2 \cdot 11) 40 - 2 \cdot 436$$

$$\Rightarrow (x_0, y_0) = (22, -2) \text{ solución particular.}$$

la solución general es:

$$\begin{cases} X = 22 + \frac{436}{4}t = 22 + 109t \\ Y = -2 - \frac{40}{4}t = -2 - 10t \end{cases}, t \in \mathbb{Z}$$

Respondemos a los apartados:

(c) $\begin{cases} X = 22 + 109t \\ Y = -2 - 10t \end{cases}, t \in \mathbb{Z}$

(b) Pasamos la ecuación $40x + 436y = 8$ módulo 436

$$\Rightarrow 40x \equiv 8 \pmod{436}$$

$$\Rightarrow x = 22 + 109t, t \in \mathbb{Z}$$

El ~~T~~ ecuación lineal en congruencias nos dice que tiene 4 soluciones ($4 = \gcd(40, 436)$)

que son:

$$\left\{ \overline{22 + 109t} : t \in \{0, 1, 2, 3\} \right\} = \{ \overline{22}, \overline{131}, \overline{240}, \overline{349} \}$$

(a) Hemos demostrado: $4 = 11 \cdot 40 - 436 \cdot 4$

Dividiendo por 4 obtenemos:

$$11 \cdot 10 - 109 = 1$$

Módulo 109:

$$11 \cdot 10 \equiv 1 \pmod{109}$$

$\Rightarrow$ El inverso de 10 en $\mathbb{Z}/109\mathbb{Z}$ es $\overline{11}$

Obs: Podíamos haber calculado $\gcd(109, 10)$ con el algoritmo de Euclides y llegar a lo mismo.

⑥ (a) Inverso de 10 en $\mathbb{Z}/109\mathbb{Z}$ o utilizando el

Es fácil ver que $10 \cdot 11 = 110$ | algoritmo de Euclides

$\Rightarrow$ El inverso es $\overline{11}$.

⑥ (b) $40x \equiv 8 \pmod{436}$

Dividiendo por 4:

$$10x \equiv 2 \pmod{109}$$

$$\Rightarrow x \equiv 2 \cdot 11 \pmod{109} \Rightarrow x = 22 + 109t, t \in \mathbb{Z}$$

Como $436 = 4 \cdot 109$ vemos que $109(t+4) \equiv 109t \pmod{436}$
con $t \in \{0, 1, 2, 3\}$

$$\Rightarrow \{ \overline{22 + 109t} : t \in \{0, 1, 2, 3\} \} = \{ \overline{22}, \overline{131}, \overline{240}, \overline{349} \}$$

son las soluciones de $40x \equiv 8 \pmod{436}$

en $\mathbb{Z}/436\mathbb{Z}$

⑥ (c) $40x + 436y = 8$ módulo 436 se convierte

en $40x \equiv 8 \pmod{436}$. $\xrightarrow{\text{⑥(b)}} x = 22 + 109t, t \in \mathbb{Z}$

Sustituyendo en la ecuación:

$$40(22 + 109t) + 436y = 8$$

despejamos y obteniendo: $y = -2 - 10t, t \in \mathbb{Z}$

$$\Rightarrow \text{Solución general } \begin{cases} x = 22 + 109t, t \in \mathbb{Z} \\ y = -2 - 10t \end{cases}$$