Ejemplo

Resolver el sistema

$$\begin{cases} 5x \equiv 4 \pmod 7 \\ 3x \equiv 5 \pmod 8 \\ x \equiv 9 \pmod{13} \end{cases}$$

Primero: las congruencias deben estar despejadas y tener solución de manera individual.

Para despejar debemos multiplicar cada congruencia por el inverso del coeficiente de x.

- $5x \equiv 4 \pmod 7 \overset{\cdot 3}{\iff} 15x \equiv 12 \pmod 7$ (donde $5 \cdot a \equiv 1 \pmod 7 \to a = 3$)
$$\iff x \equiv 5 \pmod 7$$
- $3x \equiv 5 \pmod 8 \overset{\cdot 3}{\iff} 9x \equiv 15 \pmod 8$ (donde $3 \cdot a \equiv 1 \pmod 8 \to a = 3$)
$$\iff x \equiv 7 \pmod 8$$

Consideramos el sistema equivalente

$$\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod 8 \\ x \equiv 9 \pmod{13} \end{cases}$$

Segundo: Comprobar si todos los módulos son primos entre sí, es decir, $\text{mcd}(7,8) = 1$

$\text{mcd}(7,13)=1$ y $\text{mcd}(8,13)=1$. Si es el caso entonces podremos siempre afirmar que el sistema tiene solución.
En nuestro todos los módulos son primos entre sí y por tanto tiene solución:

Tercero: Resolvemos por sustitución. La solución siempre estará en módulo el M.C.M de todos los módulos.

- $x \equiv 5 \pmod 7 \iff \boxed{x = 5 + 7\cdot\alpha}$

sustituimos en:

- $x \equiv 7 \pmod 8 \longrightarrow 5 + 7\alpha \equiv 7 \pmod 8$

$\iff 7\alpha \equiv 2 \pmod 8$

$\iff -\alpha \equiv 2 \pmod 8$

$\Rightarrow \alpha = -2 + 8\beta$

Entonces: $x = 5 + 7(-2+8\beta) = 5 - 14 + 56\beta = -9 + 56\beta$

$[x]_{56} = [-9]_{56} = [47]_{56} \iff x \equiv 47 \pmod{56}$

Hemos obtenido que $x \equiv 47 \pmod{56}$ es solución de $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod 8 \end{cases}$

Por tanto $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod 8 \\ x \equiv 9 \pmod{13} \end{cases} \iff \begin{cases} x \equiv 47 \pmod{56} \\ x \equiv 9 \pmod{13} \end{cases}$

Volvemos a repetir la jugada:

$x \equiv 47 \pmod{56} \iff \boxed{x = 47 + 56\alpha}$

Sustituimos

$$x \equiv 9 \pmod{13} \iff 47 + 56\alpha \equiv 9 \pmod{13}$$
$$\iff 8 + 4\alpha \equiv 9 \pmod{13}$$
$$\iff 4\alpha \equiv 1 \pmod{13}$$
$$\iff \alpha \equiv 10 \pmod{13}$$
$$\implies \alpha = 10 + 13\cdot\beta$$

Entonces $x = 47 + 56\cdot(10 + 13\cdot\beta) = 47 + 560 + 728\beta$

$= 607 + 728\beta$

Es decir, la solución es: $[x]_{728} = [607]_{728}$

Ejemplo.

Resolver: $\begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 12 \pmod{14} \end{cases}$

Observamos que $\text{mcd}(7,14) = 7 \neq 1$. Por tanto aún no sabemos si tiene solución. Vamos a intentar resolverlo:

$$x \equiv 6 \pmod{7} \iff \boxed{x = 6 + 7\alpha}$$

Sustituimos:

$$x \equiv 12 \pmod{14} \iff 6 + 7\alpha \equiv 12 \pmod{14}$$
$$\iff 7\alpha \equiv 12 - 6 = 6 \pmod{14}$$

Esta congruencia no tiene solución ya que $\text{mcd}(7,14) = 7$ no divide a 6.

Por tanto el sistema no tiene solución

Ejemplo

Resolver $\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 12 \pmod{14} \end{cases}$

Al igual que antes $\text{mcd}(7,14) = 7 \neq 1$. No sabemos si tiene solución:

$$x \equiv 5 \pmod 7 \iff \boxed{x = 5 + 7\alpha}$$

Sustituyendo

$$x \equiv 12 \pmod{14} \iff 5 + 7\alpha \equiv 12 \pmod{14}$$
$$\iff 7\alpha \equiv 7 \pmod{14}$$

Para resolver una congruencia donde $\text{mcd}(7,14) = 7 \neq 1$ debemos pasar por la congruencia auxiliar

$$\alpha \equiv 1 \pmod 2 \quad \text{(Resultante de dividir la anterior por mcd(7,14)=7)}$$
$$\iff \alpha = 1 + 2\cdot\beta$$

Entonces $x = 5 + 7(1 + 2\beta) = 5 + 7 \cdot 14 \cdot \beta = 12 + 14\beta$.

Luego $[x]_{14} = [12]_{14}$ es la solución al sistema.

Ejercicio

¿Cuándo podemos afirmar que $\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$

tiene solución? (Pensar que $\text{mcd}(m_1, m_2) \neq 1$)

Ejemplo.

Calcular el primer número de cuatro cifras múltiplo de 9 cuyos dos últimos dígitos sean 21.

$$\begin{cases} x \equiv 0 \pmod 9 \\ x \equiv 21 \pmod{100} \end{cases}$$

Este sistema tiene solución ya que $\text{mcd}(9,100) = 1$

$$x \equiv 21 \pmod{100} \iff x = 21 + 100\alpha.$$

Sustituyendo:

$$x \equiv 0 \pmod 9 \iff 21 + 100\alpha \equiv 0 \pmod 9$$
$$\iff 3 + \alpha \equiv 0 \pmod 9$$
$$\iff \alpha \equiv -3 \equiv 6 \pmod 9$$
$$\Rightarrow \alpha = 6 + 9\cdot\beta$$

Entonces $x = 21 + 100\cdot(6+9\beta) = 21 + 600 + 900\beta$

$$= 621 + 900\beta$$

Luego $[x]_{900} = [621]_{900} = [1521]_{900}$

Por tanto el primer número múltiplo de 9 cuyas dos últimas cifras es 21 es 1521.

Ejercicio: Calcular el primer nº de 5 cifras múltiplo de 13 y cuyas dos últimas cifras es 21.

Ejemplo.

Demostrar el criterio de divisibilidad del 3.

Vamos a expresar

$$X = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$1521 = 1 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10 + 1$

Entonces

$X \equiv 0 \pmod 3 \iff a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \pmod 3$

Pero

$$[10]_3 = [1]_3 \quad , \quad [10^2]_3 = [10]_3 \cdot [10]_3 = [1]_3 \cdot [1]_3 = [1]_3$$

$$[10^3]_3 = [10^2]_3 \cdot [10]_3 = [1]_3 \cdot [1]_3 = [1]_3$$

En general $[10^k]_3 = [1]_3$ para todo $k \in \mathbb{N}$.

Entonces

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \pmod 3$$

$$\iff a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \equiv 0 \pmod 3$$

Es decir, que la suma de sus cifras sean múltiplo de 3

Ejercicio. Tratar de dar un criterio de divisibilidad para el 7.

Ejercicio: Hallar el valor de "a" para que $6543a2$ sea múltiplo de 7.

Función φ de Euler

Se define la función φ de Euler: $\varphi : \mathbb{N} \to \mathbb{N}$

$$\varphi(n) = \text{Card}(\{a \in \mathbb{N} / a \leq n \text{ y } \text{mcd}(a,n)=1\})$$

$\equiv$ Contar cuantos primos entre sí con n hay menores que él.

Ejemplo:

- $\varphi(6) = \text{Card}(\{a \in \mathbb{N} / a \leq 6, \text{mcd}(a,6)=1\})$
  $= \text{Card}(\{1,5\}) = 2$
- $\varphi(p) = p-1$ con p primo.
- $\varphi(7) = \text{Card}(\{1,2,3,4,5,6\}) = 6$

Propiedades:

- Si $\text{mcd}(n,m)=1$ entonces $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

- Th. de Euler: $a^{\varphi(m)} \equiv 1 \pmod{m}$ si $\text{mcd}(a,m)=1$.
- Th. de Fermat: $a^p \equiv a \pmod{m}$ con p primo
- Th. de Wilson: $(p-1)! + 1 \equiv 0 \pmod{p}$ con p primo.

Ejemplo.

Calcular el resto de dividir 4^{30} por 9.

Queremos calcular

$$x \equiv 4^{30} \pmod{9}$$

Vamos a aplicar el Th. de Euler:

$a=4$ y $m=9$ entonces, $\text{mcd}(4,9)=1$

Th Euler: $4^{\varphi(9)} \equiv 1 \pmod{9}$

$\varphi(9) = \text{Card}(\{1,2,4,5,7,8\}) = 6$

$$4^6 \equiv 1 \pmod 9$$

Pero: $4^{12} = 4^6 4^6 \equiv 1 \cdot 1 = 1 \pmod 9$

En particular $4^{30} = (4^6)^5 \equiv_9 (1)^5 = 1 \pmod 9$

Por tanto $x \equiv 4^{30} \equiv 1 \pmod 9$

Ejercicio Calcular el resto de dividir 7^{208} entre 17.