Ejercicio 4. Investigar si los siguientes sistemas tienen solución, y en caso de que así sea, hallarlas todas (observar que cuando existen soluciones, son únicas módulo el m.c.m. de los módulos de cada ecuación).

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

a) $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 6 \pmod{21} \\ x \equiv 11 \pmod{15} \end{cases} \Longleftrightarrow \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 6 \pmod{3} \\ x \equiv 6 \pmod{7} \\ x \equiv 11 \pmod{15} \end{cases}$ incompatible

los modulos no son coprimos

no tiene solución

$* \; x \equiv 6 \pmod{21} \Rightarrow 21 \mid x-6 \Rightarrow \begin{cases} 3 \mid x-6 \\ 7 \mid x-6 \end{cases} \Rightarrow \begin{cases} x \equiv 6 \pmod{3} \\ x \equiv 6 \pmod{7} \end{cases}$

$21 = 3 \cdot 7$

$$x \equiv 6 \pmod{21} \overset{TCR}{\Longleftrightarrow} \begin{cases} x \equiv 6 \pmod{3} \\ x \equiv 6 \pmod{7} \end{cases}$$

3 y 7 son coprimos

c) $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 15 \pmod{18} \end{cases}$

$* \; x \equiv 6 \pmod{15} \overset{TCR}{\Longleftrightarrow} \begin{cases} x \equiv 6 \pmod{3} \\ x \equiv 6 \pmod{5} \end{cases} \Longleftrightarrow \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$

$15 = 3 \cdot 5$

$\Rightarrow$ porque $3 \mid 15$ y $5 \mid 15$

$* \; x \equiv 15 \pmod{18} \overset{TCR}{\Longleftrightarrow} \begin{cases} x \equiv 15 \pmod{\overbrace{3^2}^{9}} \\ x \equiv 15 \pmod{2} \end{cases} \Longleftrightarrow \begin{cases} x \equiv 6 \pmod{9} \\ x \equiv 1 \pmod{2} \end{cases}$

$18 = 3^2 \cdot 2$

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 15 \pmod{18} \end{cases} \iff \begin{cases} x \equiv 3 \pmod{4} \\ \cancel{x \equiv 0 \pmod{3}} \\ x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{9} \\ \cancel{x \equiv 1 \pmod{2}} \end{cases}$$

$\Rightarrow x \equiv 3 \pmod{2}$
$\Rightarrow x \equiv 1 \pmod{2}$

$\Rightarrow x \equiv 6 \pmod{3}$
$\Rightarrow x \equiv 0 \pmod{3}$

$$\iff \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{9} \end{cases}$$

$\left.\begin{matrix} x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{9} \end{matrix}\right\}$ solución particular 6

$$\overset{TCR}{\iff} \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{45} \end{cases} \rightarrow 6 \xrightarrow{+45} 51$$

6 ✗ 51 ✓

$$\overset{TCR}{\iff} x \equiv 51 \pmod{180}$$

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{9} \end{cases} \rightarrow 6$$

✓

TEOREMA DE EULER

* función de Euler

$$\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$

$$\varphi(n) = \#\{a \in \{1, \dots, n\} : \text{mcd}(a,n) = 1\}$$

= cantidad de naturales menores que n que son coprimos con n

si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

ej: $18 = 3^2 2$

$$\varphi(18) = 18\left(1-\frac{1}{3}\right)\left(1-\frac{1}{2}\right) = 18\,\frac{2}{3}\cdot\frac{1}{2} = \frac{18\cdot 2}{6} = \frac{3\cdot 6\cdot 2}{6} = 6$$

ej: p primo

$$\varphi(p) = p-1$$

* teorema de Euler:

Sean $n, a \in \mathbb{Z}$ tales que n y a son $\boxed{\text{COPRIMOS}}$

entonces $$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Ejercicio 5

a) buscamos los últimos dos dígitos de 7^{42}

$$7^{42} \equiv r \pmod{100} \quad \text{con} \quad 0 \le r \le 99$$

7 y 100 son coprimos $\Rightarrow$ podemos aplicar el teorema de Euler

$$100 = 4\cdot 25 = 2^2\cdot 5^2$$

$$\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100\cdot\frac{1}{2}\cdot\frac{4}{5} = \frac{100\cdot 4}{10} = 40$$

entonces por el teorema de Euler:

$$7^{40} \equiv 1 \pmod{100}$$

$$7^{42} \equiv 7^{40+2} \pmod{100}$$
$$\equiv \underbrace{7^{40}}_{\equiv 1 \pmod{100}} \cdot 7^2 \pmod{100}$$
$$\equiv 7^2 \pmod{100}$$
$$\equiv 49 \pmod{100}$$

$$7^{40} \equiv 1 \pmod{100}$$
$$7^{40} \cdot 7^2 \equiv 7^2 \pmod{100}$$
$$7^{42} \equiv 49 \pmod{100}$$

los últimos dos dígitos de 7^{42} son 49

d. 123^{253} (mód 490).

$123^{253} \equiv r \pmod{490}$ con $0 \leq r \leq 489$

$490 = 49 \cdot 10 = 2 \cdot 5 \cdot 7^2$

123 y 490 son coprimos $\Rightarrow$ podemos aplicar el teorema de Euler

$\varphi(490) = 490(1-\frac{1}{2})(1-\frac{1}{5})(1-\frac{1}{7}) = 490 \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 168$

Euler: $123^{168} \equiv 1 \pmod{490}$

$$123^{253} \equiv 123^{168+85} \pmod{490}$$
$$\equiv 123^{85} \pmod{490}$$

$$r \equiv 123^{253} \pmod{490} \overset{TCR}{\Longleftrightarrow} \begin{cases} r \equiv 123^{253} \pmod{2} \\ r \equiv 123^{253} \pmod{5} \\ r \equiv 123^{253} \pmod{49} \end{cases}$$

$490 = 2 \cdot 5 \cdot 7^2$

* $r \equiv 123^{253} \pmod{2} \iff r \equiv 1^{253} \pmod{2}$

$\iff \boxed{r \equiv 1 \pmod{2}}$

* $r \equiv 123^{253} \pmod{5} \iff r \equiv 3^{253} \pmod{5}$

3 y 5 son coprimos $\Rightarrow$ podemos aplicar el teorema de Euler

$\varphi(5) = 4$

entonces por el teorema de Euler: $3^4 \equiv 1 \pmod{5}$

$253 = 63 \cdot 4 + 1$

$$3^{253} \equiv 3^{63\cdot 4+1} \pmod 5$$
$$\equiv (3^4)^{63} \cdot 3^1 \pmod 5$$
$$\equiv 1^{63} \cdot 3 \pmod 5$$
$$\equiv 3 \pmod 5$$

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

* $r \equiv 123^{253} \pmod{49} \iff r \equiv 25^{253} \pmod{49}$

25 y 49 son coprimos, entonces podemos aplicar el teorema de Euler

$49 = 7^2$

$\varphi(49) = 49(1-\frac{1}{7}) = 49 \cdot \frac{6}{7} = 7\cdot 6 = 42$

entonces por el teorema de Euler: $25^{42} \equiv 1 \pmod{49}$

$253 = 42\cdot 6 + 1$

$$25^{253} \equiv 25^{42\cdot 6+1} \pmod{49}$$
$$\equiv (25^{42})^6 \, 25^1 \pmod{49}$$
$$\equiv 1^6 \cdot 25 \pmod{49}$$
$$\equiv 25 \pmod{49}$$

$$\boxed{r \equiv 25 \pmod{49}}$$

$$r \equiv 123^{253} \pmod{490} \overset{TCR}{\iff} \begin{cases} r \equiv 123^{253} \pmod 2 \\ r \equiv 123^{253} \pmod 5 \\ r \equiv 123^{253} \pmod{49} \end{cases}$$

$$\iff \begin{cases} r \equiv 1 \pmod 2 \\ r \equiv 3 \pmod 5 \\ r \equiv 25 \pmod{49} \end{cases}$$

solución particular: 3

$$\overset{TCR}{\iff} \begin{cases} r \equiv 3 \pmod{10} \\ r \equiv 25 \pmod{49} \end{cases} \to 25 \xrightarrow{+49} 74 \xrightarrow{+49} 123$$

25 ✗ 74 ✗ 123 ✓

$$\overset{TCR}{\iff} r \equiv 123 \pmod{490}$$

entonces el resto de dividir 123^{253} entre 490 es 123

$\varphi(p^k) = ?$

$$\varphi(p^k) = \#\{a \in \{1,2,\dots,p^k\} : mcd(a,p^k) = 1\}$$

$$= \#\{1,2,\dots,p^k\} - \#\{a \in \{1,2,\dots,p^k\} : mcd(a,p^k) \neq 1\}$$

$$= p^k - p^{k-1}$$

$$= p^k\left(1 - \frac{1}{p}\right) = p^{k-1}(p-1)$$

cardinal de $\{a \in \{1,2,\dots,p^k\} : \underbrace{mcd(a,p^k) \neq 1}_{\Rightarrow\, a = pq}\}$

$$\left.\begin{array}{l} a \in \{1,2,\dots,p^k\} \\ a = pq \end{array}\right\} \Rightarrow q \in \{1,2,\dots,p^{k-1}\}$$