

Recordar

$$ax \equiv c \pmod{m}$$

tiene solución si y solo si $(a:m) \mid c$

En cuyo caso la ecuación es equivalente a

$$\frac{a}{(a:m)} x \equiv \frac{c}{(a:m)} \pmod{\frac{m}{a:m}}$$

y lo escribiremos con: $a' = \frac{a}{(a:m)}$ $c' = \frac{c}{(a:m)}$ $m' = \frac{m}{(a:m)}$

ecuación reducida: $a'x \equiv c' \pmod{m'}$

Además todas las soluciones son de la forma $x_0 + k m'$, $k \in \mathbb{Z}$

x_0 es una solución particular (con algoritmo de Euclides entre a' y m')

Por ejemplo $(a' : m') = 1$

$$1 = a' h + m' p \implies$$

$$\implies c' = a' \cdot h \cdot c' + m' \cdot p \cdot c'$$

Entonces una solución de $a'x \equiv c' \pmod{m'}$ es $\boxed{x = h \cdot c'}$

* Funciona también para números no coprimos reemplazando 1 por d

Además $\exists!$ x_1 solución del sistema con $0 \leq x_1 < m'$

$$\text{Ej)} \quad 4x \equiv 3 \pmod{13}$$

tiene solución porque 13 es primo, entonces $(4:13) = 1$

Entonces $1 = 4 \cdot k + 13 \cdot p$ con $k = -3$ y $p = 1$ se verifica la ecuación.

$$1 = 4(-3) + 13 \cdot (1)$$

mult. plica 3 m.a.m

$$3 = 4(-3) \cdot 3 + 13 \cdot (1) \cdot 3$$

tomando congruencia mod 13

$$3 \equiv 4(-9) \pmod{13}$$

$$\Rightarrow \text{Rta: } x_0 = -3 \cdot 3 = -9$$

$$-9 \equiv 4 \pmod{13}$$

Entonces $x_1 = 4$ es la única solución que verifica $0 \leq x_1 < 13$

Todas las soluciones son de la forma $4 + 13k$, $k \in \mathbb{Z}$

$$\text{Ej)} \quad 3x \equiv 4 \pmod{15}$$

$$(15:3) = 3 \quad \text{y} \quad 3 \nmid 4$$

$\Rightarrow$ no existe solución

$$\text{Ej)} \quad 5x \equiv 3 \pmod{17}$$

$$(5:17) = 1 \Rightarrow \exists \text{ sol.}$$

$$\text{Si } x = 1$$

$$5 \cdot 1 \equiv 5 \pmod{17}$$

$$\text{Si } x = 2$$

$$5 \cdot 2 \equiv 10 \pmod{17}$$

$\vdots$

$$\text{Si } x = 9$$

$$5 \cdot 9 \equiv 3 \pmod{17}$$

Entonces $x_0 = 9$ es solución

Ej) $5x \equiv 9 \pmod{17}$

$5 \cdot 3 \equiv -2 \pmod{17}$

$\Rightarrow 5 \cdot (3+3) \equiv -9 \pmod{17} \Rightarrow 5(-6) \equiv 9 \pmod{17}$

Rta: $x_0 = -6$ y $\boxed{x_1 = 11}$

Lema: Sean $m_1, m_2 \in \mathbb{Z}$

$(m_1, m_2) = 1$

Entonces la ecuación $ax \equiv c \pmod{m_1 \cdot m_2}$ es equivalente a

System 2: $\begin{cases} ax \equiv c \pmod{m_1} \\ ax \equiv c \pmod{m_2} \end{cases}$ (desacoplado)

Dem: Sea x_1 solución de $ax_1 \equiv c \pmod{m_1 \cdot m_2} \Leftrightarrow$

$\Leftrightarrow m_1 \cdot m_2 \mid ax_1 - c$

Entonces $\Leftrightarrow m_1 \mid ax_1 - c$

$\Leftrightarrow m_2 \mid ax_1 - c \Leftrightarrow \begin{cases} ax_1 \equiv c \pmod{m_1} \\ ax_1 \equiv c \pmod{m_2} \end{cases} \Leftrightarrow x_1 \text{ es solución}$

la vuelta vale si $(m_1, m_2) = 1$ ya que:

$(m_1, m_2) = 1 \Rightarrow m_1 \cdot m_2 \mid ax_1 - c$ (Prop de congruencia)

Teorema chino del resto.

objetivo: resolver sistemas de ecuaciones de congruencia lineal

$$\begin{cases} a_1 x \equiv c_1 (m_1) \\ a_2 x \equiv c_2 (m_2) \\ \vdots \\ a_n x \equiv c_n (m_n) \end{cases}$$

T.C.R.

El sistema

$$\begin{cases} x \equiv c_1 (m_1) \\ x \equiv c_2 (m_2) \\ \vdots \\ x \equiv c_n (m_n) \end{cases}$$

$m_1, m_2, \dots, m_n$ coprimos
dos a dos

$$\Rightarrow \exists! \text{ sol } / \text{ tal } 0 \leq x_0 < M = \prod_{i=1}^n m_i$$

Solución general: $x = x_0 + kM, k \in \mathbb{Z}$

Dem: unicidad

Sean x_0 y x_1 dos soluciones $0 \leq x_0 < x_1 < M$

Por ser solución debe ser

$$x_0 \equiv c_i (m_i)$$

$$x_1 \equiv c_i (m_i)$$

por transitividad $\Rightarrow$

Entonces $x_0 \equiv x_1 (m_i) \quad \forall 1 \leq i \leq n$

Entonces $m_i \mid x_1 - x_0$

Como los m_i son coprimos dos a dos, entonces $\prod_{i=1}^n m_i \mid x_1 - x_0$

i.e. $M \mid x_1 - x_0$

Como $0 \leq x_1 - x_0 < M$ entonces $x_1 - x_0 = 0$

Existencia:

- Si $n = 1$ (una sola solución)

Ya este resuelto $x = c_1$ es sol y $c_1 + m_1 \cdot k$, $k \in \mathbb{Z}$

- Si $n = 2$ $\begin{cases} x \equiv c_1 (m_1) \\ x \equiv c_2 (m_2) \end{cases}$

$$\text{Como } (m_1 : m_2) = 1 = m_1 k_1 + m_2 k_2$$

Entonces el número $x = m_1 k_1 c_2 + m_2 k_2 c_1$

verifica que $\rightarrow x \equiv m_2 k_2 c_1 (m_1)$

$$x \equiv 1 \cdot c_1 (m_1)$$

$$\boxed{x \equiv c_1 (m_1)}$$

$$x \equiv m_1 k_1 \cdot c_2 (m_2)$$

$$x \equiv 1 \cdot c_2 (m_2)$$

$$\boxed{x \equiv c_2 (m_2)}$$

En definitiva hallamos una solución particular $x_0 = m_1 k_1 c_2 + m_2 k_2 \cdot c_1$

Solución general: $x = x_0 + k \cdot m_1 \cdot m_2$, $k \in \mathbb{Z}$

Obs: Lo que también demostramos es que el sistema $\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases}$ con $(m_1 : m_2) = 1$

es equivalente a la ecuación: $x \equiv x_0 (m_1 \cdot m_2)$

→ Para $n \geq 3$ se amplían las ecuaciones reduciendo de contados hasta

llegar a dos y resolver como el caso $n=2$ ya que $(m_1 \cdot m_2 : m_3) = 1$

Otra forma técnica de resolver el sistema

$$x \equiv c_1 (m_1)$$

$$x \equiv c_2 (m_2)$$

$\vdots$

$$x \equiv c_n (m_n)$$

con m_i coprimos dos a dos

$$\text{Sea } M = \prod_{j=1}^n m_j \quad \text{y sea } M_i = \frac{M}{m_i} \in \mathbb{Z}$$

$$\text{Vale } (m_i : M_i) = 1$$

$$\text{Entonces } 1 = m_i k_i + M_i p_i$$

$$\text{Vale pues } \begin{cases} M_i p_i \equiv 1 (m_i) \\ M_i p_i \equiv 0 (m_j) \quad j \neq i \end{cases}$$

$$\text{Entonces } \begin{cases} c_i M_i p_i \equiv c_i (m_i) \\ c_i M_i p_i \equiv 0 (m_j) \end{cases}$$

$$\text{Sea } x = \sum_{i=1}^n c_i M_i p_i \text{ es solución del sistema.}$$

$$\text{Se tiene } x \equiv c_j M_j p_j \equiv c_j (m_j)$$

$$\text{Ej.) } \begin{cases} x \equiv 4 (8) \\ x \equiv 12 (33) \\ x \equiv 4 (5) \end{cases} \quad \text{Hay que ver si } 8, 33 \text{ y } 5 \text{ son coprimos dos a dos}$$

$(8 : 33) = 1 \quad (8 : 5) = 1 \quad (33 : 5) = 1$

Cumplir las hipótesis del teorema chino del resto.

$$\text{resolver } \begin{cases} x \equiv 4 (8) \\ x \equiv 12 (33) \end{cases}$$

$$(8:33) = 1 \quad \text{con Euclides}$$

$$1 = 8 \cdot (-9) + 33 \cdot (1)$$

Entonces $x_0 = 8 \cdot (-9) \cdot 12 + 33 \cdot 4$ es solución

$$x_0 \equiv -252 \pmod{(8 \cdot 33)}$$

$$x_0 \equiv 12 \pmod{(264)}$$

Ahora resolvemos

$$\begin{cases} x_0 \equiv 12 \pmod{(264)} \\ x \equiv 9 \pmod{(5)} \end{cases}$$

$$\begin{array}{r} 264 \overline{) 5} \\ \underline{14} \\ 53 \\ \underline{-1} \\ 8 \end{array}$$

Solamos que $(264:5) = 1$

$$1 = 5 \cdot 53 + 264 \cdot (-1)$$

Entonces $x_0 = 5 \cdot 53 \cdot 12 + 264 \cdot (-1) \cdot 4$

$$x_0 = 2129 \quad \text{es solución}$$

Como $\begin{array}{r} 264 \\ \times 5 \\ \hline 1320 \end{array}$ todo sol es de la forma $2129 + 1320 \cdot k$, $k \in \mathbb{Z}$

y la solución positiva menor es $\boxed{x_1 = 809}$ $0 \leq x_1 < 1320$

y el sistema original tiene toda solución de la forma

$$x \equiv 809 \pmod{(1320)}$$

Otra forma

$$x \equiv 4 (8) \quad x = 4 + k \cdot 8, \quad k \in \mathbb{Z}$$

reemplazado en la segunda ecuación: $4 + k \cdot 8 \equiv 12 (33)$

$$\text{con } k = 1 \quad 4 + 1 \cdot 8 \equiv 12 (33) \quad \checkmark \text{ sí cumple}$$

Entonces $k = 1$ es solución

Entonces las soluciones del resto de las dos primeras ecuaciones son de la forma $x = 12 + k \cdot 33 \cdot 8$

Reemplazado en la tercera ecuación obtenemos:

$$12 + k \cdot 33 \cdot 8 \equiv 4 (5)$$

$$2 + k \cdot 4 \equiv 4 (5)$$

$k = 3$ es solución

Entonces $12 + 33 \cdot 3 \cdot 8$ es solución

804 es solución

Finalmente toda solución es de la forma

$$\boxed{804 + k \cdot 8 \cdot 33 \cdot 5}$$