# Ecuaciones con congruencias

## Inversos modulares

Dado un número entero, por ejemplo $2 \in \mathbb{Z}$, sabemos que en $\mathbb{Z}$ la ecuación lineal

$$2x = 1$$

no tiene solución. En otras palabras, en $\mathbb{Z}$ el número 2 no tiene inverso multiplicativo.

Si consideramos enteros módulo $n$, lo anterior cambia. Por ejemplo, consideremos los enteros módulo 3.

¿Existe $x \in \mathbb{Z}$ tal que $2x \equiv 1 \pmod 3$?

La respuesta es sí. Por ejemplo, $x = 2$ es solución de la ecuación lineal modular de una variable

$$2x \equiv 1 \pmod 3.$$

En otras palabras, 2 es inverso multiplicativo de sí mismo módulo 3.

**Definición:** Sean $a, b, n \in \mathbb{Z}$ con $n$ fijo. Decimos que $b$ es inverso de $a$ módulo $n$ si $a \cdot b \equiv 1 \pmod n$.

Recordemos que para cada $n \in \mathbb{Z}^+$, el conjunto $\mathbb{Z}$ se escribe como unión disjunta

$$\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n,$$

donde $[k]_n$ es la clase de congruencia de $k$ módulo $n$.

**Definición**: El **conjunto de enteros módulo $n$** es el conjunto dado por

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

Cuando el $n$ está sobreentendido, escribimos el conjunto anterior como

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}.$$

**Observación**: En $\mathbb{Z}_n$,

① $\bar{a} = \bar{b}$ si y solamente si $a \equiv b \pmod{n}$.

② Podemos definir operaciones de suma y multiplicación como sigue:

$$\bar{a} + \bar{b} := \overline{a+b} \quad \text{y} \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

Estas operaciones están bien definidas y dan a $\mathbb{Z}_n$ cierto tipo de estructura (veremos esto más adelante).

Por ejemplo, para $n = 3$,

$\bar{1} + \bar{2} = \overline{1+2} = \bar{3} = \bar{0}$.

$\bar{2} \cdot \bar{2} = \overline{2 \cdot 2} = \bar{4} = \bar{1}$.

③ $ax \equiv 1 \pmod{n}$ ($x$ es inverso de $a$ módulo $n$) si y solamente si $\bar{x}$ es inverso multiplicativo de $\bar{a}$ en $\mathbb{Z}_n$.

Ejemplo:

① $\mathbb{Z}_3$:

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

| $\cdot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

Note que em $\mathbb{Z}_3$, todo $\bar{a} \in \mathbb{Z}_3$ com $a \not\equiv 0 \pmod{3}$ tiene inverso multiplicativo.

② $\mathbb{Z}_4$:

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

| $\cdot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Vemos que $\bar{2} \in \mathbb{Z}_4$ no tiene inverso multiplicativo en $\mathbb{Z}_4$.

Observación: A causa de los ejemplos anteriones, podemos llegan a pensan que si $p$ es primo, entonces todo elemento no nulo en $\mathbb{Z}_p$ tiene inverso multiplicativo. Esto es de hecho cierto, y será consecuencia de un resultado conocido como el pequeño teorema de Fermat.

# El pequeño teorema de Fermat

Cuando $p$ es primo, los enteros módulo $p$ tienen la siguiente propiedad "cíclica".

**Teorema (Fermat):** Sea $a \in \mathbb{N}$ y $p$ primo. Entonces,

$$a^p \equiv a \pmod{p}.$$

- **Demostración:** Usaremos inducción sobre $a$.
- Paso inicial: Es claro que $0^p \equiv 0 \pmod{p}$.
- Paso inductivo: Supongamos que $a^p \equiv a \pmod{p}$ (hipótesis inductiva). Queremos probar que

$$(a+1)^p \equiv a+1 \pmod{p} \quad \text{(tesis inductiva)}.$$

Utilizamos el binomio de Newton para desarrollar $(a+1)^p$:

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1$$

$$(a+1)^p - (a+1) = (a^p - a) + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$$

$$= (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}.$$

$a^p - a$ es divisible por $p$, por la hipótesis inductiva. Entonces, la prueba se reduce a demostrar que $p$ divide a $\sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}$, para lo cual basta ver que $p$ divide a cada coeficiente binomial $\binom{p}{k}$.

Recordemos que $\binom{p}{k} = \frac{p!}{(p-k)!\,k!} = p \cdot \frac{(p-1)!}{(p-k)!\,k!}$.

Como $p$ es primo, ninguno de los factores de $(p-k)!$ y de $k!$ (distintos de 1) divide a $p$. Por lo tanto, $p$ divide a $\binom{p}{k}$.

Así, $(a+1)^p - (a+1)$ es divisible por $p$, es decir,

$$(a+1)^p \equiv a+1 \pmod{p}.$$ ■

Como consecuencia, tenemos lo siguiente:

<u>Corolario</u>: Si $p$ es primo y $a$ es coprimo con $p$, entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

<u>Observación</u>: Si $a < p$, es claro que $a$ es coprimo con $p$. Entonces para $\bar{a} \in \mathbb{Z}_p$, $a \not\equiv 0 \pmod{p}$, se tiene que $\overline{a^{p-2}}$ es el inverso multiplicativo de $\bar{a}$ en $\mathbb{Z}_p$.

· <u>Demostración del corolario</u>: Por el pequeño teorema de Fermat, se tiene que $a^p \equiv a \pmod{p}$, es decir, $p \mid a(a^{p-1}-1)$. Como $\mathrm{mcd}(a, p) = 1$, se tiene por el Lema de Euclides que $p \mid (a^{p-1}-1)$, es decir, $a^{p-1} \equiv 1 \pmod{p}$. ■

# Ecuaciones lineales con congruencia de una variable

Anteriormente resolvimos el problema de hallar $x \in \mathbb{Z}$ tal que

$$ax \equiv 1 \pmod{n}.$$

Sabemos que no siempre hay solución, como es el caso de

$$2x \equiv 1 \pmod{4}.$$

Podemos generalizar el problema de la siguiente forma: dados $a, b \in \mathbb{Z}$, y $n \in \mathbb{Z}$ fijo, queremos hallar todos los $x \in \mathbb{Z}$ tales que

$$ax \equiv b \pmod{n},$$

dentro del caso en el cual tales $x$ existen.

Para tal fin, ayuda un poco recordar la teoría de ecuaciones diofánticas. Lo haremos mediante un ejemplo.

**Ejemplo:** Determine si $9x \equiv 1 \pmod{3}$ tiene solución. De ser el caso, encuéntrelas.

$9x \equiv 1 \pmod{3} \iff 9x - 1 = 3y$ para algún $y \in \mathbb{Z}$

Es decir, $9x \equiv 1 \pmod{3}$ tiene solución si la ecuación diofántica $9x - 3y = 1$ tiene solución. Como $\text{mcd}(9, 3) = 3 \neq 1$, tenemos que $9x - 3y = 1$ no tiene solución. Por lo tanto, $9x \equiv 1 \pmod{3}$ no tiene solución.

- Determine si $9x \equiv 1 \pmod{10}$ tiene solución. En caso afirmativo, encuéntrelas.

$9x \equiv 1 \pmod{10} \iff$ Existen $x, y \in \mathbb{Z}$ tales que

$$9x - 10y = 1$$

$$\iff \text{mcd}(9, 10) = 1 \mid 1.$$

Tenemos entonces que $9x \equiv 1 \pmod{10}$ tiene solución como

$$9(-1) - 10(-1) = 1,$$

tenemos que todas las soluciones de $9x \equiv 1 \pmod{10}$ son de la forma

$$x = -1 + k \cdot \frac{(-10)}{\text{mcd}(9, 10)}$$

$$x = -1 - 10k, \text{ con } k \in \mathbb{Z}.$$

Como dato adicional, vemos que si $-1 - 10k_1$ y $-1 - 10k_2$ son soluciones de $9x \equiv 1 \pmod{10}$, entonces $-1 - 10k_1 \equiv -1 - 10k_2 \pmod{10}$.

Formalicemos las observaciones de los ejemplos anteriores en resultados. Básicamente, lo que va a ocurrir es una reescritura de los resultados de la teoría de ecuaciones diofánticas en la notación de congruencias modulares.

**Proposición (existencia de soluciones de una ecuación lineal de congruencia):** Dados $a, b, n \in \mathbb{Z}$, la ecuación

$$ax \equiv b \pmod{n}$$

tiene solución si y solamente si $\text{mcd}(a,n) \mid b$.

- **Demostración:** Supongamos primero que $ax \equiv b \pmod{n}$ tiene solución $x_0 \in \mathbb{Z}$. Luego, $n \mid (ax_0 - b)$, es decir, existe $y_0 \in \mathbb{Z}$ tal que

$$ax_0 - b = ny_0$$
$$ax_0 - ny_0 = b.$$

Si $d = \text{mcd}(a,n)$, entonces $d \mid (ax_0 - ny_0)$ ya que $d \mid a$ y $d \mid n$. Por lo tanto, $d \mid b$.

Ahora supongamos que $d \mid b$. Para empezar, por el teorema de Bézout sabemos que existen $x_1$ e $y_1$ en $\mathbb{Z}$ tales que

$$d = ax_1 + ny_1.$$

Por otro lado, $b = qd$ para algún $q \in \mathbb{Z}$, ya que $d \mid b$. Luego,

$$b = a(qx_1) + n(qy_1).$$

Se sigue entonces que $n \mid (a(qx_1) - b)$, es decir, $qx_1$ es solución de $ax \equiv b \pmod{n}$. ∎

**Proposición (congruencia entre soluciones):**

Si $x_0 \in \mathbb{Z}$ es una solución de $ax \equiv b \pmod{m}$, entonces $x_1$ también es solución de $ax \equiv b \pmod{m}$ para todo $x_1 \in \overline{x_0}$

· **Demostración:** Sea $x_1 \in \overline{x_0}$. Se tiene que

$$x_1 \equiv x_0 \pmod{m}$$

Luego, $$ax_1 \equiv ax_0 \pmod{m}.$$

Como $ax_0 \equiv b \pmod{m}$, se tiene por la propiedad de transitividad que

$$ax_1 \equiv b \pmod{m}. \blacksquare$$

**Observación:**

1) El Recíproco de la proposición anterior no es cierto en general. Es decir, si $x_0$ y $x_1$ son soluciones de $ax \equiv b \pmod{m}$, no necesariamente ocurre que $x_1 \equiv x_0 \pmod{m}$.

Por ejemplo, 1 y 3 son soluciones de la ecuación $2x \equiv 2 \pmod{4}$, pero $3 \not\equiv 1 \pmod{4}$.

2) Sin embargo, si $ax_0 \equiv b \pmod{m}$, $ax_1 \equiv b \pmod{m}$ y $mcd(a, m) = 1$, entonces $x_1 \equiv x_0 \pmod{m}$. Note que esto es consecuencia del Lema de Euclides.

Vemos de las observaciones anteriores que la ecuación $ax \equiv b \pmod{m}$, en caso de tener solución, no necesariamente es única módulo $m$. ¿Se puede determinar la cantidad total de soluciones de $ax \equiv b \pmod{m}$ módulo $m$? La respuesta la da el siguiente resultado.

Teorema (descripción y cantidad de soluciones):
Considere la ecuación

$$ax \equiv b \pmod{m},$$

con $m > 1$, donde $\text{mcd}(a,m) \mid b$. Entonces, existen $\text{mcd}(a,m)$ soluciones distintas módulo $m$.

· Demostración: Como $\text{mcd}(a,m) \mid b$, la ecuación $ax \equiv b \pmod{m}$ tiene solución. Equivalentemente, existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$ax_0 - my_0 = b.$$

Por otro lado, todas las soluciones de la ecuación diofántica $ax - my = b$ vienen dadas por

$$x = x_0 - k\frac{m}{\text{mcd}(a,m)} \quad \text{e} \quad y = y_0 - k\frac{a}{\text{mcd}(a,m)},$$

donde $k \in \mathbb{Z}$.

Luego, todas las soluciones de $ax \equiv b \pmod{n}$ vienen dadas por

$$x = x_0 - k n^*,$$

con $k \in \mathbb{Z}$ y donde $n^* = n/\text{mcd}(a,n)$.

Observamos entonces que

$$\{ x_0, x_0 - n^*, x_0 - 2n^*, \ldots, x_0 - (\text{mcd}(a,n)-1)n^* \}$$

es el conjunto de soluciones distintas módulo $n$.

En efecto,

$$x_0 \equiv x_0 - \underbrace{d\, n^*}_{=n} \pmod{n}$$

$$x_0 - n^* \equiv x_0 - (d+1) n^* \pmod{n}$$

$$\vdots \text{ y así sucesivamente.} \quad \blacksquare$$

<u>Ejemplo</u>: Encuentre el conjunto de soluciones de

$$362x \equiv 236 \pmod{24} \quad \text{y} \quad 131x \equiv 21 \pmod{77}.$$

- Para la primera ecuación, $\text{mcd}(362,24) = 2 \mid 236$.

Entonces, existen soluciones. Lo primero es hallar las soluciones a la ecuación diofántica

$$362x - 24y = 236.$$

Lo primero es notar que

$$2 = 362 \cdot 1 - 24 \cdot 15$$

Luego, $236 = 118 \cdot 2 = 362 \cdot 118 - 24 \cdot 1770$

$236 = 362 \cdot 118 - 24 \cdot 1770.$

Las soluciones de $362X \equiv 236 \pmod{24}$

vienen dadas por

$$X = 118 + K \cdot \frac{(-24)}{2}$$

$$X = 118 - 12K, \quad K \in \mathbb{Z},$$

de las cuales solo

$$X_0 = 118 \quad \text{y} \quad X_1 = 118 - 12 \cdot 1 = 106$$

son diferentes módulo 24.

- Para la ecuación $131X \equiv 21 \pmod{77}$ procedemos de la misma forma. En este caso, $\text{mcd}(131, 77) = 1$.

$131 = 1 \cdot 77 + 54$
$77 = 1 \cdot 54 + 23$
$54 = 2 \cdot 23 + 8$
$23 = 2 \cdot 8 + 7$
$8 = 1 \cdot 7 + 1$

$1 = 8 - 1 \cdot 7 = 8 - 1 \cdot (23 - 2 \cdot 8)$
$1 = 3 \cdot 8 - 23 = 3(54 - 2 \cdot 23) - 23$
$1 = 3 \cdot 54 - 7 \cdot 23$
$1 = 3 \cdot 54 - 7 \cdot (77 - 1 \cdot 54)$
$1 = -7 \cdot 77 + 10 \cdot 54$
$1 = 10(131 - 77) - 7 \cdot 77$
$1 = 131 \cdot 10 - 77 \cdot 17$

$$X = 21 \cdot 10 + K\frac{(-77)}{1} = 210 - 77K, \quad K \in \mathbb{Z}.$$

$X_0 = 210$ es la única solución módulo 77.

# - Teorema chino del resto -

Hay ocasiones donde el procedimiento para resolver una ecuación de congruencia se ve alargado porque el módulo de dicha ecuación es muy grande. Por ejemplo, supongamos que queremos resolver la ecuación dada por:

$$7x \equiv 6 \pmod{100}.$$

Como $\text{mcd}(7, 100) = 1 \mid 6$, la ecuación tiene solución única módulo 100. Para hallar tal solución, primero debemos resolver

$$1 = 7x - 100y$$

mediante el algoritmo extendido de Euclides, y esto puede llevar su tiempo.

Otra manera de resolver la ecuación consiste en descomponerla en ecuaciones equivalentes.

Tenemos que $100 \mid (7x - 6)$ y que $100 = 4 \cdot 25$, por lo cual $4 \mid (7x - 6)$ y $25 \mid (7x - 6)$, es decir,

$$7x \equiv 6 \pmod{100} \implies 7x \equiv 6 \pmod{4} \text{ y } 7x \equiv 6 \pmod{25}.$$

Por otro lado, si suponemos que $7x \equiv 6 \pmod{4}$ y que $7x \equiv 6 \pmod{25}$, tenemos que $7x - 6$ es múltiplo común de 4 y 25, por lo cual

$$\text{mcm}(4, 25) \mid (7x - 6)$$

Pero como 4 y 25 son coprimos, se tiene que

$$mcm(4, 25) = 4 \cdot 25 = 100,$$

de donde $100 \mid (7x - 6)$. Entonces,

$$\left.\begin{array}{l} 7x \equiv 6 \pmod 4 \\ 7x \equiv 6 \pmod{25} \end{array}\right\} \Longrightarrow 7x \equiv 6 \pmod{100}.$$

Por lo tanto,

$$7x \equiv 6 \pmod{100} \iff \begin{cases} 7x \equiv 6 \pmod 4 \\ 7x \equiv 6 \pmod{25} \end{cases} \text{ y}$$

Resolvamos entonces las ecuaciones de la derecha, y luego buscamos la solución común módulo 100 (que sabemos que es única).

- $7x \equiv 6 \pmod 4$

  $7x - 4y = 6$ (ecuación diofántica asociada).

  Como $1 = mcd(7, 4)$, tenemos que

  $$1 = 7 \cdot (-1) - 4 \cdot (-2).$$

  Así,
  $$6 = 7 \cdot (-6) - 4(-12),$$

  por lo cual $x \equiv -6 \pmod 4$

  $$x \equiv 2 \pmod 4$$

Las soluciones menores que 100 son:

$x = 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, 66, 70, 74, 78, 82, 86, 90, 94, 98.$

• $7x \equiv 6 \pmod{25}$

$7x - 25y = 6$ (ecuación diofántica asociada)

Vemos que $7 \cdot 4 - 25 \cdot 1 = 3$, de donde

$$7 \cdot 8 - 25 \cdot 2 = 6.$$

Entonces, $x \equiv 8 \pmod{25}$.

Las soluciones menores que 100 son:

$x = 8, 33, 58, 83.$

La única solución común módulo 100 a $7x \equiv 6 \pmod{4}$ y a $7x \equiv 6 \pmod{25}$ es $x \equiv 58 \pmod{100}$. Por lo tanto, la solución de $7x \equiv 6 \pmod{100}$ es

$$x \equiv 58 \pmod{100}.$$

Generalicemos lo observado en este ejemplo en el siguiente resultado:

<u>Proposición</u>: Sean $m_1, m_2, \ldots, m_n \in \mathbb{Z}^+$. Entonces, el sistema

$$\begin{cases} ax \equiv b \pmod{m_1} \\ ax \equiv b \pmod{m_2} \\ \vdots \\ ax \equiv b \pmod{m_n} \end{cases}$$

es equivalente a la ecuación

$$ax \equiv b \pmod{\text{mcm}(m_1, m_2, \ldots, m_n)}.$$

El símbolo $\text{mcm}(m_1, m_2, \ldots, m_n)$ denota el mínimo común múltiplo de $m_1, m_2, \ldots, m_n$. Se define de manera similar al mínimo común múltiplo de dos enteros. Es decir, si $m_1, m_2, \ldots, m_n$ son enteros no nulos y

$$m = \text{mcm}(m_1, m_2, \ldots, m_n),$$

entonces $m$ es el menor entero positivo tal que $m$ es múltiplo común de $m_i$ para todo $i \in \{1, \ldots, n\}$. Equivalentemente, $m = \text{mcm}(m_1, m_2, \ldots, m_n)$ si:

1) $m_i \mid m$ para todo $i \in \{1, 2, \ldots, n\}$.

2) $m \mid c$ para todo $c$ múltiplo común de $m_1, m_2, \ldots, m_n$.

Como propiedad, mencionamos que si los $m_1, \ldots, m_n$ son coprimos dos a dos, es decir,

$$\text{mcd}(m_i, m_j) = 1 \quad \text{si} \quad i \neq j,$$

entonces

$$\boxed{\text{mcm}(m_1, m_2, \ldots, m_n) = m_1 \cdot m_2 \cdots m_n.}$$

· Demostración de la proposición: Supongamos primero que el sistema no tiene solución, es decir, para todo $x \in \mathbb{Z}$ existe $i \in \{1, 2, \ldots, n\}$ tal que $m_i \nmid (ax - b)$. Por otro lado, si $m = \text{mcm}(m_1, m_2, \ldots, m_n)$ y la ecuación $ax \equiv b \pmod{m}$ tiene solución, entonces $m_i \mid (ax - b)$ para algún $x \in \mathbb{Z}$ y para todo $i \in \{1, 2, \ldots, n\}$, lo cual es una contradicción. Por lo tanto, $ax \equiv b \pmod{m}$ no tiene solución.

Recíprocamente, si $ax \equiv b \pmod{m}$ no tiene solución, el sistema tampoco. En caso contrario, existiría $x \in \mathbb{Z}$ tal que

$$m_i \mid (ax-b) \quad \forall i \in \{1,2,\dots,n\}.$$

Luego, al ser $ax-b$ múltiplo común de $m_1, m_2, \dots, m_n$, nos queda que

$$m \mid (ax-b),$$

es decir que $x$ es solución de $ax \equiv b \pmod{m}$, lo cual es una contradicción.

De manera similar, se puede probar que el sistema tiene solución si y solamente si la ecuación $ax \equiv b \pmod{m}$ tiene solución. ∎

Como aplicación particular, tenemos lo siguiente.

Corolario: Sea $m \in \mathbb{Z}^+$ con $m > 1$ y con descomposición única

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

donde $p_1 < p_2 < \cdots < p_n$ son primos y $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}^+$. Entonces, $ax \equiv b \pmod{m}$ tiene solución si y solamente si el sistema

$$\begin{cases} ax \equiv b \pmod{p_1^{\alpha_1}} \\ ax \equiv b \pmod{p_2^{\alpha_2}} \\ \quad \vdots \\ ax \equiv b \pmod{p_n^{\alpha_n}} \end{cases}$$

tiene solución.

Hasta ahona hemos amalizado sistemas cuyas ecuaciones tienem em comúm la parte $ax \equiv b$, peno difienem de módulo. ¿Cómo podemos amalizar um sistema cuando también las pantes $ax \equiv b$ difienem? Emcanemos pnimeno um ejemplo.

Resolvamos el siguiente sistema:

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{19} \end{cases}$$

Pana empezan, notamos que pon sepanado cada ecuación tieme solución. ¿Habná solución comúm a las tnes?

Resolvamos pnimeno el sistema que connesponde a las pnimenas dos ecuaciones:

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 6 \pmod{15}. \end{cases}$$

Podemos pnoceden de dos mamenas:

1) $x \equiv 5 \pmod{11}$ es equivalente a la ecuación diofántica $x - 11y = 5$, así como $x \equiv 6 \pmod{15}$ es equivalente a $x - 15y' = 6$. Luego,

$$11y + 5 = x = 15y' + 6$$

$$11y - 15y' = 1.$$

Vemos así que el sistema $\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 6 \pmod{15} \end{cases}$ tieme solución si y solamente si la ecuación diofántica $11y - 15y' = 1$ tieme solución.

Note que $11 \cdot (-4) - 15 \cdot (-3) = 1$.

($y_0 = -4$ e $y_0' = -3$ es uma solução particular)

Solução general: $y = -4 - 15k$, $k \in \mathbb{Z}$.

$y' = -3 - 11k$

Luego, $x = 11y + 5 = 11(-4 - 15k) + 5 = -44 - 165k + 5$

$x = -39 - 165k$

$x \equiv -39 \pmod{165}$

Es decir, $x \equiv 126 \pmod{165}$.

Por lo tanto, notamos que

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 6 \pmod{15} \end{cases} \iff x \equiv 126 \pmod{11 \cdot 15}.$$

2) Si $x \equiv 5 \pmod{11}$, entonces $x = 5 + 11y$. Al sustituir en la segunda ecuación, obtenemos

$$5 + 11y \equiv 6 \pmod{15}$$
$$11y \equiv 1 \pmod{15},$$

lo cual equivale a resolver $11y - 15y' = 1$.

Ya sea de 1) o de 2), notamos que Resolver el sistema original equivale a Resolver

$$\begin{cases} x \equiv 126 \pmod{165} \\ x \equiv 7 \pmod{19} \end{cases}$$

$x \equiv 126 \pmod{165} \iff x = 126 + 165z$, para algún $z \in \mathbb{Z}$. (8)

Luego, $126 + 165z \equiv 7 \pmod{19}$

$165z \equiv -119 \pmod{19}$, $\quad 119 = 19 \cdot 6 + 5$

$165z \equiv -19 \cdot 6 - 5 \pmod{19}$

$165z \equiv -5 \pmod{19}$

$165z \equiv 14 \pmod{19}$

$\text{mcd}(165, 19) = 1 \Rightarrow$ la ecuación anterior tiene solución única módulo 19.

Ahora hay que resolver

$$165z - 19t = 14.$$

$165 = 8 \cdot 19 + 13$
$19 = 1 \cdot 13 + 6$
$13 = 2 \cdot 6 + 1$

$1 = 13 - 2 \cdot 6$
$1 = 13 - 2(19 - 1 \cdot 13)$
$1 = 3 \cdot 13 - 2 \cdot 19$
$1 = 3(165 - 8 \cdot 19) - 2 \cdot 19$
$1 = 3 \cdot 165 - 10 \cdot 19$

Luego, $165 \cdot (14 \cdot 3) - 19 \cdot (14 \cdot 10) = 14$

$z_0 = 42$ y $t_0 = 140$ (solución particular)

Solución general: $z = 42 - 19h$, $h \in \mathbb{Z}$.
$t = 140 - 165h$

Al sustituir, obtenemos

$x = 126 + 165(42 - 19h) = 126 + 6930 - 165 \cdot 19h$

$x = 7056 - 3135h$

$x \equiv 7056 \pmod{3135}$

$x \equiv 786 \pmod{3135}$, donde $3135 = 11 \cdot 15 \cdot 19$.

Por lo tanto, vemos que el sistema

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{19} \end{cases}$$

es equivalente a la ecuación

$$x \equiv 786 \pmod{3135}.$$

El procedimiento mostrado anteriormente puede aplicarse, dentro de ciertas hipótesis, a cualquier sistema de congruencias. El resultado que describe y demuestra la situación general se conoce como el teorema chino del resto.

Teorema chino del resto: Sea

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases}$$

un sistema de congruencias que satisface las siguientes condiciones:

1) $mcd(a_i, m_i) = 1$ para todo $i \in \{1, 2, \dots, n\}$. Es decir, cada ecuación de congruencia tiene solución única (módulo $m_i$)

2) $mcd(m_i, m_j) = 1$ si $i \neq j$. Es decir, los módulos son coprimos dos a dos.

Entonces, el sistema tiene solución única módulo $m_1 m_2 \cdots m_n$.

· **Demostración**: Usaremos inducción sobre el número de ecuaciones.

- Caso $n = 1$: $a_1 x \equiv b_1 \pmod{m_1}$ tiene solución única ya que $\text{mcd}(a_1, m_1) = 1 \mid b_1$.

- Supongamos que vale el teorema para las primeras $n-1$ ecuaciones, es decir, el sistema

$$(*) \quad \begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_{n-1} x \equiv b_{n-1} \pmod{m_{n-1}} \end{cases}$$

tiene solución única módulo $m_1 m_2 \cdots m_{n-1}$.

Sea $m = m_1 m_2 \cdots m_{n-1}$, y consideremos el sistema

$$\begin{cases} x \equiv x_1 \pmod{m} \\ a_n x \equiv b_n \pmod{m_n} \end{cases}$$

donde $x_1$ es la solución de $(*)$.

Veamos que $\text{mcd}(m, m_n) = 1$. Sea $d = \text{mcd}(m, m_n)$. Luego, $d \mid m_1 \cdots m_{n-1}$. Si $d_1 = \text{mcd}(d, m_1)$, entonces $d_1 \mid d$, por lo cual $d_1$ es divisor común de $m_1$ y $m_n$. Como $\text{mcd}(m_1, m_n) = 1$, se tiene que $d_1 = 1$.

$\text{mcd}(d, m_1) = 1$

y $d \mid m_1 m_2 \cdots m_{n-1} \implies d \mid m_2 \cdots m_{n-1}$ por el Lema de Euclides.

Procediendo de esta manera llegaremos a que $d \mid m_{m-1}$. Luego, $d$ es divisor común positivo de $m_{m-1}$ y de $m_m$. Como $\text{mcd}(m_{m-1}, m_m) = 1$, tenemos que $d = 1$.

Entonces, el sistema $\begin{cases} x \equiv x_1 \pmod{m} \\ a_m x \equiv b_m \pmod{m_m} \end{cases}$

tiene solución única módulo $m \cdot m_m$. Llamemos a tal solución $x_0$, es decir,

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_m}.$$

Tenemos que $a_m x_0 \equiv b_m \pmod{m_m}$ y

$$x_0 \equiv x_1 \pmod{m}.$$

Como $x_1$ es solución de las primeras $m-1$ ecuaciones y $x_0 \equiv x_1 \pmod{m}$ (de donde $x_0 \equiv x_1 \pmod{m_k}$ para $k = 1, \ldots, m-1$), tenemos que $x_0$ también es solución de las primeras $m-1$ ecuaciones. Por lo tanto, $x_0$ es la solución única módulo $m_1 m_2 \cdots m_m$ del sistema original. ■

<u>Ejemplo</u>: Una banda de 17 piratas se repartió sus doblones de oro en partes iguales, y les sobraron 3 monedas que acordaron dar a su cocinero Wum Tu. Pero 6 de los piratas murieron en una pelea y, al distribuir la fortuna total en partes iguales, esta vez sobraron 4 monedas para Wum Tu. Después de un naufragio solo quedaron 6 de los piratas, las

monedas y el cocimero se salvanom. Al volver a Repartir los doblones em partes iguales, sobranom 5 monedas para Wum Tu. Camsado de la tacañería de sus amos, Wum Tu los envenenó a todos y se quedó com los doblones. ¿Cuál es la cantidad más pequeña de monedas com que pudo habense quedado Wum Tu?

Sea $x$ la cantidad de doblones de ono. A partir de la infonmación del problema, tenemos las siguientes ecuaciones de congruencia

$$\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{6}. \end{cases}$$

Como 17, 11 y 6 son coprimos dos a dos, por el teorema chino del Resto existe una solución única módulo $17 \cdot 11 \cdot 6$.

- Resolvemos las primenas dos ecuaciones:

$$x \equiv 3 \pmod{17} \Rightarrow x = 3 + 17y$$
$$x \equiv 4 \pmod{11} \Rightarrow x = 4 + 11z$$

Luego, $3 + 17y = 4 + 11z$

$$17y - 11z = 1.$$

$y_0 = 2$ y $z_0 = 3$ es una solución particular de la ecuación diofántica anterior, por lo cual su solución general viene dada por

$$y = 2 - 11k \quad \text{y} \quad z = 3 - 17k \qquad k \in \mathbb{Z}.$$

Entonces, $x = 3 + 17y = 3 + 17(2 - 11k) = 37 - 17 \cdot 11k$

$x \equiv 37 \pmod{17 \cdot 11}$

El sistema original se reduce a:

$$\begin{cases} x \equiv 37 \pmod{17 \cdot 11} \\ x \equiv 5 \pmod{6} \end{cases}$$

Luego $37 - 17 \cdot 11k = 5 + 6h$

$32 = 17 \cdot 11k + 6h.$

Como $17 \cdot 11 \cdot (1) + 6 \cdot (-31) = 1$, nos queda

$17 \cdot 11 \cdot (32) + 6 \cdot (-31 \cdot 32) = 32.$

Es decir, $k_0 = 32$ y $h_0 = -31 \cdot 32$ es solución particular de la ecuación diofántica $17 \cdot 11k + 6h = 32$. Su solución general viene dada por

$k = 32 + 6t$ y $h = -31 \cdot 32 - 17 \cdot 11t.$

Por lo tanto, $x = 37 - 17 \cdot 11(32 + 6t)$

$x = (37 - 17 \cdot 11 \cdot 32) - 17 \cdot 11 \cdot 6t$

$x \equiv 37 - 17 \cdot 11 \cdot 32 \pmod{17 \cdot 11 \cdot 6}$

$x \equiv -5947 \pmod{1122}$

$x \equiv 785 \pmod{1122}.$

La menor cantidad de monedas que puede obtener Wun Tu es de 785 doblones.

El teorema chino del resto no abarca la situación en la cual los módulos de las ecuaciones no son coprimos dos a dos. ¿Qué podemos hacer en estos casos? La idea es hallar un sistema equivalente con módulos coprimos dos a dos.

Ejemplo: Resolver el sistema

$$\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 26 \pmod{45} \\ x \equiv 11 \pmod{100} \end{cases}$$

- $6 = 3 \cdot 2$ donde $\text{mcd}(2,3) = 1$. Entonces,

$$x \equiv 5 \pmod 6 \iff \begin{cases} x \equiv 5 \pmod 2 \\ x \equiv 5 \pmod 3 \end{cases}$$

$$\iff \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$$

- $45 = 5 \cdot 9$ donde $\text{mcd}(5,9) = 1$. Entonces,

$$x \equiv 26 \pmod{45} \iff \begin{cases} x \equiv 26 \pmod 5 \\ x \equiv 26 \pmod 9 \end{cases}$$

$$\iff \begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 8 \pmod 9 \end{cases}$$

- $100 = 4 \cdot 25$ donde $\text{mcd}(4,25) = 1$. Entonces,

$$x \equiv 11 \pmod{100} \iff \begin{cases} x \equiv 11 \pmod 4 \\ x \equiv 11 \pmod{25} \end{cases}$$

$$\iff \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 11 \pmod{25} \end{cases}$$

Entonces, el sistema original es equivalente a

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 8 \pmod 9 \\ x \equiv 3 \pmod 4 \\ x \equiv 11 \pmod{25} \end{cases}$$

Observe que $x \equiv 3 \pmod 4 \Rightarrow x \equiv 3 \pmod 2$, $x \equiv 1 \pmod 2$

$x \equiv 8 \pmod 9 \Rightarrow x \equiv 8 \pmod 3$, $x \equiv 2 \pmod 3$

$x \equiv 11 \pmod{25} \Rightarrow x \equiv 11 \pmod 5$, $x \equiv 1 \pmod 3$

Es decir, las últimas 3 ecuaciones implican las primeras 3. Entonces, el sistema a resolver es

$$\begin{cases} x \equiv 8 \pmod 9 \\ x \equiv 3 \pmod 4 \\ x \equiv 11 \pmod{25}. \end{cases}$$

Pasemos a resolver el sistema anterior

$$\begin{cases} x \equiv 8 \pmod 9 \\ x \equiv 3 \pmod 4 \end{cases} \Rightarrow \begin{aligned} 8 + 9y = x &= 3 + 4z \\ 9y - 4z &= -5 \\ 4z - 9y &= 5. \end{aligned}$$

$z_0 = -1$ e $y_0 = -1$ es una solución particular de la ecuación diofántica anterior.

La solución general viene dada por

$$z = -1 - 9k \quad e \quad y = -1 - 4k, \quad k \in \mathbb{Z}.$$

Luego, $x = 3 + 4(-1 - 9k) = -1 - 36k$

$$x \equiv -1 \pmod{36}$$
$$x \equiv 35 \pmod{36}$$

Ahora resolvemos $\begin{cases} x \equiv 35 \pmod{36} \\ x \equiv 11 \pmod{25} \end{cases}$

Vemos que

$$-1 - 36k = x = 11 + 25t$$
$$36k + 25t = -12$$

$k_0 = -2$ y $t_0 = 2$ es solución particular de esta ecuación diofántica. Su solución general viene dada por

$$k = -2 + 25m \quad y \quad t = 2 - 36m, \quad m \in \mathbb{Z}.$$

Así, $x = -1 - 36(-2 + 25m) = 71 - 36 \cdot 25m$

$$x \equiv 71 \pmod{900}.$$

Esta es la solución del sistema original.

Observación: Note que $900 = mcm(6, 45, 100)$.

$$\left.\begin{array}{l} 6 = 2 \cdot 3 \\ 45 = 3^2 \cdot 5 \\ 100 = 2^2 \cdot 5^2 \end{array}\right\} \longrightarrow mcm(6, 45, 100) = 2^2 \cdot 3^2 \cdot 5^2 = (30)^2 = 900.$$

## Connección em la demostnación del teonema chimo del nesto:

La demostnación dada anteniormente solo vale pana $n \geq 3$, pon lo que hay que anneglan el paso base em el angumento de inducción.

- **Paso base ($n = 2$)**: Tenemos el sistema

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \end{cases}.$$

Lo pnimeno que hanemos sená simplifican el sistema.

- Como $a_1$ y $m_1$ son copnimos, existe $x_0 \in \mathbb{Z}$ tal que

$$a_1 x_0 \equiv 1 \pmod{m_1}.$$

En efecto, sabemos pon el Teonema de Bézout que existen $x_0$ e $y_0 \in \mathbb{Z}$ tales que

$$a_1 x_0 + m_1 y_0 = 1,$$

es decin,

$$a_1 x_0 = 1 - m_1 y_0.$$

Luego, $a_1 x_0 \equiv 1 \pmod{m_1}$.

$$a_1 x_0 \equiv 1 \pmod{m_1} \Rightarrow a_1 x_0 x \equiv x \pmod{m_1}$$
$$a_1 x \equiv b_1 \pmod{m_1} \Rightarrow a_1 x_0 x \equiv x_0 b_1 \pmod{m_1}$$

Pon la tnansitividad de la nelación de congnuencia, tenemos que

$$x \equiv x_0 b_1 \pmod{m_1}.$$

De manera similar, existe $x_1 \in \mathbb{Z}$ tal que

$$x \equiv x_1 b_2 \pmod{m_2}.$$

Entonces, el sistema original es equivalente a

$$\begin{cases} x \equiv x_0 b_1 \pmod{m_1} \\ x \equiv x_1 b_2 \pmod{m_2}. \end{cases}$$

Luego, $x_0 b_1 + m_1 y = x = x_1 b_2 + m_2 z$

$$m_1 y - m_2 z = x_1 b_2 - x_0 b_1$$

Como $\text{mcd}(m_1, m_2) = 1$, la ecuación diofántica anterior tiene solución. Si $y_0$ y $z_0$ forman una solución particular, la solución general viene dada por

$$y = y_0 - m_2 k \quad \text{y} \quad z = z_0 - m_1 k, \quad k \in \mathbb{Z}.$$

Por lo tanto, $x = x_0 b_1 + m_1 (y_0 - m_2 k)$

$$x = x_0 b_1 + m_1 y_0 - m_1 m_2 k$$

$$x \equiv x_0 b_1 + m_1 y_0 \pmod{m_1 m_2},$$

es la solución módulo $m_1 m_2$.