NO

DATE 01 04 20

Algebra Superior 2

Retomemos el ejemplo $2x \equiv 6 \pmod{12}$. Tanto 3 como 9 son soluciones y por tanto cualquier elemento en las clases de congruencia X_3 o X_9 es solución.

Esto sugiere la siguiente generalización:

Una congruencia lineal $ax \equiv b \pmod{m}$ se resuelve, o podemos decir que está resuelta, cuando se tiene un conjunto representativo de soluciones

$$\{r_1, r_2, \dots, r_k\} \quad \text{que podría ser vacío}$$

con $0 \leq r_i \leq m-1$ y $r_i \not\equiv r_j$ si $i \neq j$,

Esto garantiza que las r_i's pertenezcan a clases distintas.

de manera que cada solución de $ax \equiv b \pmod{m}$ es elemento de alguna clase de congruencia de algún r_i.

Def. Si $ax \equiv b \pmod{m}$ tiene un conjunto representativo de soluciones $\{r_1, r_2, \dots, r_k\}$ decimos que la congruencia tiene exactamente k soluciones no congruentes módulo m.
Si $k = 1$, decimos que la congruencia tiene solución única módulo m.

Teo. Si $(a,m) = 1$, entonces $ax \equiv b \pmod{m}$ tiene una única solución módulo m.

Dem. Sabemos que existen $u, v \in \mathbb{Z}$ tales que

$ua + vm = 1$, si multiplicamos por b:

$bua + bvm = b$ y $\therefore \; a(bu) - b = (-bv)m$.

De la definición de congruencia lineal se sigue que

$$a(bu) \equiv b \pmod{m}$$

y por tanto $x = bu$ es solución.

Supongamos ahora que r es solución de $ax \equiv b \pmod{m}$, entonces $ar \equiv b \equiv a(bu) \pmod{m}$.

Notación: $a \equiv b = c \equiv d = e \pmod{m}$ abrevia $\begin{cases} a \equiv b \pmod{m} \\ b = c \\ c \equiv d \pmod{m} \\ d = e. \end{cases}$

Como $(a, m) = 1$ podemos usar el teorema de las notas del 27·03·20 (¿cuál?) y se sigue que

$$r \equiv bu \pmod{m}.$$

Por tanto cualquier solución de la congruencia original es congruente con bu módulo m.
Es decir, $ax \equiv b \pmod{m}$ tiene una única solución módulo m. ■

Teo. La congruencia $ax \equiv b \pmod{m}$ tiene solución si y solo si (a,m) divide a b.
Y si (a,m) divide a b, la congruencia tiene exactamente (a,m) soluciones no congruentes módulo m.

Dem. Supongamos primero que r es solución de la congruencia dada. Entonces se tiene (por definición) que

$$ar - b = \ell m \quad \text{para algún } \ell \in \mathbb{Z}.$$

Ahora, como (a,m) divide a a y a m, entonces $(a,m) \mid b$.

Conversamente, si (a,m) divide a b, entonces consideremos la siguiente congruencia:

$$\frac{a}{(a,m)} x \equiv \frac{b}{(a,m)} \left(\text{mod } \frac{m}{(a,m)}\right). \quad (*)$$

Como $\frac{a}{(a,m)}$ y $\frac{m}{(a,m)}$ son primos relativos sabemos que la congruencia tiene solución, llamémosla s.

Ahora, nuevamente por el teorema visto el 27 de marzo,

$a s \equiv b \pmod m$ y $\therefore$ s es solución de la congruencia original.

Veamos ahora que si se satisface la condición $(a,m) \mid b$ entonces la congruencia tiene exactamente (a,m) soluciones no congruentes módulo m: (Esta parte de la demostración es un poco técnica)

Como $(a,m) \mid b$, entonces la congruencia $(*)$ tiene una solución s que cumple $0 \leq s < \frac{m}{(a,m)}$.

Para cada entero j entre 0 y $(a,m)-1$,

es decir, $0 \leq j \leq (a,m)-1$

definimos $s_j = s + \frac{jm}{(a,m)}$.

Por definición de congruencia tenemos que

$$s_j \equiv s \left(\text{mod } \frac{m}{(a,m)}\right)$$

y $\therefore$ s_j es solución de $(*)$ (porque s lo era).

Entonces s_j también es solución de $ax \equiv b \pmod{m}$.

Además, como

$$0 \leq s_0 < s_1 < \cdots < s_{(a,m)-1} < m$$

se sigue que si $0 \leq i < j \leq (a,m)-1$

entonces s_i y s_j no son congruentes módulo m.

Veamos ahora que $\{s_0, s_1, \ldots, s_{(a,m)-1}\}$ es un conjunto representativo de soluciones de $ax \equiv b \pmod{m}$.

Es decir, cada entero t que cumpla $at \equiv b \pmod{m}$ será congruente módulo m con algún s_r.

Si t cumple $at \equiv b \pmod{m}$, entonces t es solución de $\circledast$ y $\therefore$ $t \equiv s \pmod{\frac{m}{(a,m)}}$.

Esto es $t = s + l\left(\frac{m}{(a,m)}\right)$ para alguna $l \in \mathbb{Z}$.

Por el algoritmo de la división podemos escribir a l como $l = q(a,m) + r$ con $0 \leq r \leq (a,m)-1$

Ahora,

$$t = s + \frac{rm}{(a,m)} + qm = s_r + qm \equiv s_r \pmod{m}$$ ∎

Teorema chino del residuo. Si $(m,n)=1$, entonces $x \equiv a \pmod{m}$ y $x \equiv b \pmod{n}$ tienen solución común.

Dem. Como $(m,n)=1$, entonces existen $r,s \in \mathbb{Z}$ tq

$$rm + sn = 1.$$

Sea $x = asn + brm$. Afirmamos que x es solución de ambas congruencias:

$$x = asn + brm = a(1-rm) + brm = a - arm + brm$$
$$= a + (b-a)rm$$

$$\therefore \quad x - a = (b-a)rm.$$

Es decir $m \mid x-a$ y $\therefore$ x satisface la 1ª congruencia.

$$x = asn + brm = asn + b(1-sn) = asn + b - bsn$$
$$= b + (a-b)sn$$

$$\therefore \quad x - b = (a-b)sn.$$

Es decir, $n \mid x-b$ y $\therefore$ x satisface la 2ª congruencia. ∎

¿Se les ocurre como generalizar el teorema a más de 2 congruencias?