12/09

Ejercicio 12. Resolver cada una de las congruencias siguientes:

a. $3x \equiv 7 \pmod{16}$.
b. $2x + 8 \equiv 5 \pmod{33}$.
c. $3x+9 \equiv 8x+61 \pmod{64}$.
d. $6x - 1 \equiv 5 \pmod{12}$.
e. $9x + 3 \equiv 5 \pmod{18}$.

→ Ppdes. cancelativas: 1. $mcd(c,n)=1$

$ca \equiv cb \pmod n \Rightarrow a \equiv b \pmod n$

2. $c|n$ y $ca \equiv cb \pmod n \Rightarrow a \equiv b \pmod{\frac{n}{c}}$

3. $ca \equiv cb \Rightarrow a \equiv b \mod \left(\frac{n}{mcd(c,n)}\right)$

→ $p(a) \equiv p(b) \pmod n$

→ Ecuaciones con congruencias: $ax \equiv b \pmod n$

tiene sól. si y sólo si $mcd(a,n)|b$, si tiene una sol. ⇒ tiene exactamente $mcd(a,n)$ soluciones módulo n.

→ Vimos como resolver $2x \equiv \pm 1 \pmod n$

(a) $3x \equiv 7 \pmod{16}$

Tiene sol si y sólo si $mcd(3,16) | 7$, $1|7$ ✓

Tenemos que hallar x, y tales que $3x = 7 + 16y$,

$3x - 16y = 7$) AEE

$x = -3$ $y = -1$

$\boxed{-9 + 16 = 7}$ ✓

$x \equiv -3 \pmod{16}$

$x \equiv 13 \pmod{16}$, la sol. es única mod 16 ⇒ estas son todas.

(d) $6x - 1 \equiv 5 \pmod{12}$

$6x \equiv 6 \pmod{12}$

¿Tiene sol? ¿cuántas?

↳ Si, porque $mcd(6,12) = 6 | 6$. Hay exactamente 6 sols. módulo 12.

Por ppd. cancelativa si $6x \equiv 6 \pmod{12} \Rightarrow x \equiv 1 \pmod{\frac{12}{6}}$

$\boxed{x \equiv 1 \pmod 2}$ y $6x \equiv 6 \pmod{12}$

$x \equiv 1, 3, 5, 7, 9, 11 \pmod{12}$

(e) $9x + 3 \equiv 5 \pmod{18} \iff 9x \equiv 2 \pmod{18}$

¿Tiene sol? ¿Cuántas?

↳ Si y sólo si $\text{mcd}(9,18) \mid 2 \iff 9 \mid 2$.

No tiene solución.

Ejercicio 14. Sea $p(x)$ un polinomio con coeficientes enteros tal que $p(0) = 1, p(1) = 2$ y $p(2) = 5$. Probar que $p(x)$ no tiene raices enteras.

$p(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_n x^n$.

$p(0) = 1 \Rightarrow a_0 = 1$

$p(1) = 2 \Rightarrow a_0 + \underbrace{a_1 + \dots + a_n}_{} = 2$

$p(2) = 5 \Rightarrow a_0 + 2a_1 + 2^2 a_2 + \dots + 2^n a_n = 5$.

Supongamos que $p(a) = 0$ con $a \in \mathbb{Z}$.

$x \neq a$: $\boxed{(x-a) \mid p(x) - p(a)}$

$p(x) - p(a) = a_1 \cdot x - a_1 \cdot a + a_2 \cdot x^2 - a_2 a^2 + \dots + a_n x^n - a_n a^n$.

$= (x-a)(a_1) + x^2 - a^2 (a_2) + \dots + (x^n - a^n)(a_n)$

$= (x-a) \cdot (a_1$ $\quad (x-a)(x+a) \quad$ calcular $(x-a) \sum_{k=0}^{n-1} x^k a^{n-k-1}$ ...

$x=0$: $-a \mid p(0) - p(a) = 1 - 0 = 1$

$\boxed{-a \mid 1}$ $\quad \boxed{a \in \{\pm 1\}}$

Si a existe,

$\Rightarrow a \in \{\pm 1\} \cap \{-1, 0, 2, 3\}$

$\boxed{a = -1}$

$x=1$: $(1-a) \mid p(1) - p(a) = 2 - 0 = 2$

$(1-a) \in \{\pm 1, \pm 2\} \Rightarrow \boxed{a \in \{0, 2, -1, 3\}}$

$x=2$: $(2-a) \mid p(2) - p(a) = 5 - 0 = 5$

$(2-a) \in \{\pm 1, \pm 5\}$ $\quad (a \in \{1, -3, 3, 7\})$

Si tomamos $a = -1 \Rightarrow 2 - a = 3 \notin \{\pm 1, \pm 5\}$. ↯

Ejercicio 1. Resolver los siguientes sistemas de módulos coprimos de dos formas: por substitución y utilizando la solución particular vista en teórico.

a. $\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{13} \end{cases}$ **b.** $\begin{cases} x \equiv 3 \pmod{14} \\ 2x \equiv 3 \pmod{11} \end{cases}$ ~~**c.**~~ $\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{12} \end{cases}$

(a) $* \begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod{13} \end{cases} \iff \begin{cases} 7 \mid x-3 \\ 13 \mid x-5 \end{cases} \iff \begin{cases} \exists s: & x-3 = 7\cdot s \\ \exists t: & x-5 = 13\cdot t \end{cases}$

Resolver $*$ es equivalente a hallar s, t. tales que $7s+3 = 13t+5$ y tomar $x = 7s+3 = 13t+5$.

$$\boxed{7s - 13t = 2}$$

¿Tiene sol.? Si, porque $\operatorname{mcd}(7,13) = 1 \mid 2$.

AEE nos da: $7\cdot 2 - 13\cdot 1 = 1$

$\Rightarrow 7\cdot 4 - 13\cdot 2 = 2$

$\Rightarrow s = 4 \quad t = 2$

$\Rightarrow x = 7\cdot 4 + 3 = 31$ es sol. particular.

Teorema Chino de los Restos: $a_1, \dots, a_n \in \mathbb{Z}$ y $m_1, \dots, m_n$ enteros coprimos 2 a 2.

$\Rightarrow \begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$

tiene sol. y es única modulo $m_1 \cdots m_n$.

Por el T.C.R. todas las sols. son $\boxed{x \equiv 31 \pmod{7\cdot 13}}$

$x = 31$

$31 + 7\cdot 13$

$31 + 7\cdot 13\cdot 2 \dots$

Ejemplo: $\begin{cases} x \equiv a \pmod p \\ x \equiv a \pmod q \end{cases}$ con p y q coprimos.

Por el T.C.R. $x = a$ es sol. particular y todas son $x \equiv a \pmod{pq}$

$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \end{cases} \iff x \equiv 1 \pmod 6$

$$\begin{cases} x \equiv 1 \ (4) \\ x \equiv 1 \ (6) \end{cases}$$

no tiene sol. única mod 24.

(1 y 13 son sol.)

Falla: 4 y 6 no son coprimos.