Teorema Chino del resto

Sean $m_1, m_2, \dots, m_k$ enteros coprimos dos a dos y $a_1, a_2, \dots, a_k \in \mathbb{Z}$

Entonces el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

tiene solución y hay una unica solución modulo $m_1 m_2 \cdots m_k$

es decir si x_0 es una solución particular entonces todas las soluciones son

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$$

Ejercicio 1

a) $\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{13} \end{cases}$

como 7 y 13 son coprimos, el sistema tiene solución y la solución es unica modulo $7 \cdot 13$

método de resolución con diofánticas:

$x \equiv 3 \pmod{7} \Rightarrow 7 \mid x-3 \Rightarrow x-3 = 7y \Rightarrow x = 7y+3$

$x \equiv 5 \pmod{13} \Rightarrow 13 \mid x-5 \Rightarrow x-5 = 13z \Rightarrow x = 13z+5$

entonces $7y+3 = 13z+5$

$$\Rightarrow \boxed{7y - 13z = 2}$$

* solución particular ?

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

$$y_0 = 4, \quad z_0 = 2$$

* conjunto de soluciones?

$$7(4+13k)-13(2+7k)=2$$

$y=4+13k$
con $k\in\mathbb{Z}$
$z=2+7k$

* volvemos al sistema original

$$x=7y+3=7(4+13k)+3=31+\overbrace{7\cdot 13}^{91}k$$

$x=31+91k \Rightarrow x-31=91k$

$\Rightarrow 91 \mid x-31$

$\Rightarrow x\equiv 31 \pmod{91}$

Otra forma:

$$\begin{cases} x\equiv 3 \pmod 7 \\ x\equiv 5 \pmod{13} \end{cases}$$

7 y 13 son coprimos $\Rightarrow$ hay una única solución módulo 91

nos alcanza con encontrar una solución particular

$x\equiv 3 \pmod 7 \iff x=7y+3$

$x\equiv 5 \pmod{13} \iff x=13z+5$

entonces $7y+3=13z+5$

$\Rightarrow 7y-13z=2$

solución particular: $\begin{cases} y_0=4 \\ z_0=2 \end{cases}$

entonces $x_0=7\cdot 4+3=31$ es solución particular del sistema

$\Rightarrow$ por el teorema chino del resto, todas las soluciones son

$$x\equiv 31 \pmod{91}$$

b) $\begin{cases} x \equiv 3 \pmod{14} \\ 2x \equiv 3 \pmod{11} \end{cases}$

$* \quad 2x \equiv 3 \pmod{11} \iff 2x \equiv \overbrace{3+11}^{14} \pmod{11}$

$\iff x \equiv 7 \pmod{11}$

2 y 11 son coprimos

otra forma

$2 \cdot 6 \equiv 1 \pmod{11}$

6 y 11 coprimos

entonces $2x \equiv 3 \pmod{11} \iff 6 \cdot 2 \cdot x \equiv 6 \cdot 3 \pmod{11}$

$\iff x \equiv 7 \pmod{11}$

$\begin{cases} x \equiv 3 \pmod{14} \\ 2x \equiv 3 \pmod{11} \end{cases} \iff \begin{cases} x \equiv 3 \pmod{14} \\ x \equiv 7 \pmod{11} \end{cases}$

como 14 y 11 son coprimos, por el TCR, el sistema tiene solución

método de resolución por sustitución

$x \equiv 3 \pmod{14} \implies x = 14q + 3$

reemplazamos en la segunda

$14q + 3 \equiv 7 \pmod{11}$

$\implies 14q \equiv 4 \pmod{11}$

inverso de 14 modulo 11? $\quad 14 \, \square \equiv 1 \pmod{11}$

vamos a escribir la identidad de Bezout para 14 y 11

$14 = 11 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 2 + 1$

$1 = 3 - 2$

$= 3 - (11 - 3 \cdot 3)$

$= -11 + 4 \cdot 3$

$= -11 + 4(14 - 11)$

$= 4 \cdot 14 - 5 \cdot 11$

$\boxed{4 \cdot 14 - 5 \cdot 11 = 1}$

$4 \cdot 14 - 5 \cdot 11 \equiv 1 \pmod{11}$

$\underset{\substack{\uparrow \\ \text{inverso de 14 modulo 11}}}{4} \cdot 14 \equiv 1 \pmod{11}$

entonces $14q \equiv 4 \pmod{11}$

$\Rightarrow 4 \cdot 14 q \equiv 4 \cdot 4 \pmod{11}$

$\Rightarrow q \equiv 5 \pmod{11}$

$\Rightarrow q = 11k + 5$

entonces:

$x = 14q + 3 = 14(11k+5) + 3 = 73 + \overbrace{14 \cdot 11}^{154} k$

$\Rightarrow \boxed{x \equiv 73 \pmod{154}}$

Ejercicio 2.

a. Hallar el menor natural que dividido 3 da resto 1, divido 4 da resto 3 y dividido 7 da resto 5.

b. Hallar el menor par $x > 199$ que cumpla $2x + 3 \equiv 4 \pmod{5}$ y $3x + 4 \equiv 3 \pmod{7}$.

c. Una banda de 13 piratas obtuvo un cofre con monedas de oro, que trataron de distribuir entre sí equitativamente, pero les sobraban 8 monedas. Dos de ellos fueron expulsados de la banda por intentar robarse todo el botín. Al volver a intentar el reparto, sobraban 3 monedas. Luego se ahogaron tres de ellos, y al intentar distribuir las monedas sobraban 5. ¿Cuántas monedas había en el botín?

d. Encontrar el menor natural n que dividido 2 da resto 1, dividido 3 da resto 2, dividido 4 da resto 3, dividido 5 da resto 4, dividido 6 da resto 5, dividido 7 da resto 6, dividido 8 da resto 7 y dividido 9 da resto 8. Sugerencia: considerar $n + 1$.

a) buscamos el menor n natural tal que

$$\begin{cases} n \equiv 1 \pmod{3} \\ n \equiv 3 \pmod{4} \\ n \equiv 5 \pmod{7} \end{cases}$$

$\left.\begin{matrix} n \equiv 1 \pmod{3} \\ n \equiv 3 \pmod{4} \end{matrix}\right\} \iff n \equiv \quad \pmod{3 \cdot 4}$

3, 4 y 7 son coprimos dos a dos entonces por el TCR hay solución y es única módulo $3 \cdot 4 \cdot 7$

$$\begin{cases} n \equiv 1 \pmod{3} \\ n \equiv 3 \pmod{4} \\ n \equiv 5 \pmod{7} \end{cases}$$

$n \equiv 5 \pmod{7} \longrightarrow \underset{\times}{5} \xrightarrow{+7} \underset{\times}{12} \xrightarrow{+7} \underset{\checkmark}{19}$

$$\begin{cases} 19 \equiv 1 \pmod 3 \\ 19 \equiv 3 \pmod 4 \\ 19 \equiv 5 \pmod 7 \end{cases}$$

$\Rightarrow$ 19 es solución particular

entonces por el TCR

$$\begin{cases} n \equiv 1 \pmod 3 \\ n \equiv 3 \pmod 4 \\ n \equiv 5 \pmod 7 \end{cases} \iff n \equiv 19 \pmod{84}$$

$\rightsquigarrow$ el menor natural que verifica es 19

d. Encontrar el menor natural n que dividido 2 da resto 1, dividido 3 da resto 2, dividido 4 da resto 3, dividido 5 da resto 4, dividido 6 da resto 5, dividido 7 da resto 6, dividido 8 da resto 7 y dividido 9 da resto 8. Sugerencia: considerar $n+1$.

buscamos el menor natural n tal que:

$n+1 \equiv \overbrace{1+1}^{=0} \pmod 2$

$$(*)\begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 2 \pmod 3 \\ n \equiv 3 \pmod 4 \\ n \equiv 4 \pmod 5 \\ n \equiv 5 \pmod 6 \\ n \equiv 6 \pmod 7 \\ n \equiv 7 \pmod 8 \\ n \equiv 8 \pmod 9 \end{cases} \iff \begin{cases} \cancel{n \equiv -1 \pmod 2} \\ \cancel{n \equiv -1 \pmod 3} \\ \cancel{n \equiv -1 \pmod 4} \Rightarrow n \equiv -1 \pmod 2 \\ n \equiv -1 \pmod 5 \\ \cancel{n \equiv -1 \pmod 6} \iff \begin{matrix} n \equiv -1 \pmod 2 \\ n \equiv -1 \pmod 3 \end{matrix} \\ n \equiv -1 \pmod 7 \\ n \equiv -1 \pmod 8 \Rightarrow n \equiv -1 \pmod 4 \Rightarrow \underline{n \equiv -1 \pmod 2} \\ n \equiv -1 \pmod 9 \Rightarrow \underline{n \equiv -1 \pmod 3} \end{cases}$$

$*$ $n \equiv -1 \pmod 4 \Rightarrow 4 \mid n+1 \Rightarrow 2 \mid n+1 \Rightarrow n \equiv -1 \pmod 2$

$*$ $n \equiv -1 \pmod 8 \Rightarrow 8 \mid n+1 \Rightarrow 4 \mid n+1 \Rightarrow n \equiv -1 \pmod 4$

$*$ $n \equiv -1 \pmod 9 \Rightarrow 9 \mid n+1 \Rightarrow 3 \mid n+1 \Rightarrow n \equiv -1 \pmod 3$

$*$ $n \equiv -1 \pmod 6 \Rightarrow 6 \mid n+1 \Rightarrow \begin{cases} 2 \mid n+1 \\ 3 \mid n+1 \end{cases} \Rightarrow \begin{matrix} n \equiv -1 \pmod 2 \\ n \equiv -1 \pmod 3 \end{matrix}$

$$n \equiv -1 \pmod 6 \overset{\text{TCR}}{\underset{2|6 \text{ y } 3|6}{\iff}} \begin{cases} n \equiv -1 \pmod 2 \\ n \equiv -1 \pmod 3 \end{cases}$$

$$\ast \iff \begin{cases} n \equiv -1 \pmod 5 \\ n \equiv -1 \pmod 7 \\ n \equiv -1 \pmod 8 \\ n \equiv -1 \pmod 9 \end{cases} \overset{\text{TCR}}{\iff} n \equiv -1 \ (\text{mod } \underbrace{5 \cdot 7 \cdot 8 \cdot 9}_{2520})$$

los módulos son coprimos dos a dos

el menor natural que verifica es $-1 + 2520 = 2519$