14/04

Práctico 6: TCR - Teoremas de Fermat y Euler.

$$(*)\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

TCR: Si los m_i son coprimos dos a dos $\Rightarrow$ $*$ tiene sol. única módulo $m_1 \dots m_n$.

En gral $*$ tiene sol. única módulo $\text{mcm}(m_i)$.

Ejemplo: ① $\begin{cases} x \equiv a^1 \pmod{m_1^2} \\ x \equiv a^1 \pmod{m_2^3} \end{cases}$ con m_1 y m_2 coprimos.

Una sol. particular es $x=1$, por el T.C. todas las sols. son $x \equiv 1 \pmod 6$

② $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 6 \end{cases}$

Una sol. es $x=1$. ¿Todas las sols. son $x \equiv 1 \pmod{24}$?

Otra sol. es $x=13$. $\Rightarrow$ No.

$\Rightarrow$ La sol. es $\boxed{x \equiv 1 \pmod{12}}$. (Las sol. son $x=1, 1+12, 1+12\cdot 2, \dots, 1+12\cdot k$)

$\cdot\, x \equiv 1 \pmod{24}$

$\cdot\, x \equiv 13 \pmod{24}$

③ Cambios de variable.

$*\begin{cases} x \equiv 2 \pmod{13} \\ x \equiv 15 \pmod{17} \end{cases}$ C.V: $x' = x \pm A$, $x' = x - 15$ $\quad \begin{cases} x' = a \pmod{13} \\ x' = a \pmod{17}. \end{cases}$

$**\begin{cases} x' \equiv -13 \equiv 0 \pmod{13} \\ x' \equiv 0 \pmod{17} \end{cases}$

$**$ tiene sol. trivial $0 \bmod (13 \cdot 17)$

Deshacemos el cv: $x = x' + 15 = 15 \pmod{13 \cdot 17}$

Ej 1. (b) $\begin{cases} x \equiv 3 \pmod{14} \\ 2x \equiv 3 \pmod{11} \end{cases}$ (c) $\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod 7 \\ x \equiv 10 \pmod{12} \end{cases}$

Resolver $\leftarrow$ por sust.

usando la sol. particular.

Sust. (6) $\begin{cases} x \equiv 3 \ (14) \\ 2^{-1} 2x \equiv 3 \ (11) \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \ (14) \\ 6 \cdot 2x \equiv 6 \cdot 3 \ (11) \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \ (14) \\ x \equiv 7 \ (11) \end{cases}$

Recordar: $2^{-1} = \text{coc}(11,2) + 1 = 5 + 1 = 6$.

$x \equiv 3 \mod 14 \Leftrightarrow \exists s$ tq $14s + 3 = x$

$\Leftrightarrow \exists s,t \begin{cases} x = 3 + 14s \\ x = 7 + 11t \end{cases}$

$x = 3 + 14s = 7 + 11t$

$\exists s,t \cdot \quad 14s - 11t = 4$ — AEE.

$s = 16 \quad t = 20$

Sol. part: $x = 3 + 14 \cdot 16 = 7 + 11 \cdot 20 = \boxed{227}$.

Todas las sols. son $x \equiv 227 \pmod{14 \cdot 11}$

Sol particular $\forall$ m_i coprimos

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

$$x_0 = a_1 M_1 M_1' + a_2 M_2 M_2' + \ldots + a_n M_n M_n'$$

$M = m_1 \cdots m_n$

$M_i = M / m_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_n$

M_i' el inverso de M_i modulo m_i. $(M_i M_i' \equiv 1 \ (m_i))$

$\begin{cases} x \equiv 3 \ (14) \\ x \equiv 7 \ (11) \end{cases}$

$a_1 = 3 \qquad M_1 = m_2 = 11$

$a_2 = 7 \qquad M_2 = m_1 = 14$

Tenemos que hallar $M_1' \equiv 1^{-1} \mod 14$ y $M_2' \equiv 14^{-1} \pmod{11}$

$M_2' \equiv 3^{-1} \pmod{11}$

$M_1' \equiv 11^{-1} \pmod{14}$, $11^{-1} = x$ tq $11 \cdot x \equiv 1 \mod 14$.

Necesitamos x, y tq $11x - 14y = 1$

$\boxed{x = -5}$ $y = -4$

$11 \cdot -5 + 14 \cdot 4 = -55 + 56 = 1$.

$M_1' \equiv -5 \pmod{14}$

$\equiv 9 \pmod{14}$

$M_2' \equiv ? \pmod{11}$ AEE

$$X_0 \equiv a_1 M_1 M_1' + a_2 M_2 M_2' \equiv 3 \cdot 11 \cdot 9 + 7 \cdot 14 \cdot ? \pmod{m_1 m_2}$$

Ejercicio 2: Hallar el menor n tq.

$$*\begin{cases} n \equiv 1 \ (2) \\ n \equiv 2 \ (3) \\ n \equiv 3 \ (4) \\ n \equiv 4 \ (5) \\ n \equiv 5 \ (6) \\ n \equiv 6 \ (7) \\ n \equiv 7 \ (8) \\ n \equiv 8 \ (9) \end{cases}$$

$\cdot n \equiv a \pmod 6$

$\cdot n \equiv 3 \ (4)$

Sugerencia: Pensemos $n' = n + C$ tq

$$\begin{cases} n' \equiv a \ (2) \\ n' \equiv a \ (3) \\ \vdots \\ n' \equiv a \ (9) \end{cases}$$

$n' = n + 1$:

$$\begin{cases} n' = n+1 \equiv 0 \ (2) \\ n' = n+1 \equiv 0 \ (3) \\ \vdots \\ n' = n+1 \equiv 0 \ (9) \end{cases}$$

$\Rightarrow n' \equiv 0 \mod (\text{mcm}(2, 3, 4, \dots, 9))$

$\mod (8 \cdot 9 \cdot 5 \cdot 7)$

$n \equiv n' - 1 \equiv -1 \pmod{\text{mcm}}$.

(d) $x>0$ t.q. $\star \begin{cases} x \equiv 8 \ (13) \\ x \equiv 3 \ (11) \\ x \equiv 5 \ (8) \end{cases}$.

Hay una sol. a $\star$ mod $8 \cdot 11 \cdot 13$.

Las sol. van a ser $x : \{x>0 \quad x \equiv a \pmod{8 \cdot 11 \cdot 13}\}$

$a_1 = 8 \qquad a_2 = 3 \qquad a_3 = 5$

$M = 8 \cdot 11 \cdot 13$

$M_1 = 11 \cdot 8 \qquad M_2 = 13 \cdot 8 \qquad M_3 = 11 \cdot 13$

$M_1' \equiv 1 \ (13) \qquad M_2' \equiv 1 \ (11) \qquad M_3' \equiv 5 \ (8)$

$x_0 \equiv 8 \cdot 11 \cdot 8 \cdot 1 + 3 \cdot 13 \cdot 8 \cdot 1 + 5 \cdot 11 \cdot 13 \cdot 5 \pmod{8 \cdot 11 \cdot 13}$