RESOLUCIÓ CONGRUÈNCIES TIPUS $ax \equiv b \pmod{m}$

PAS 1) ÉS RECOMANABLE "REDUIR" COEFICIENTS

EX: $21x \equiv 24 \pmod{15}$

COM $21 \equiv 6 \pmod{15}$

$24 \equiv 9 \pmod{15}$

TENIM $6x \equiv 9 \pmod{15}$

PAS 2) SIMPLIFICAR (SI ES POT)

a) PODEM USAR $ka \equiv kb \bmod (km) \overset{\boxed{\text{SI } k>0}}{\Longleftrightarrow} a \equiv b \pmod{m}$

EX: $6x \equiv 9 \pmod{15} \underset{\div 3>0}{\Longleftrightarrow} 2x \equiv 3 \pmod{5}$

b) PODEM USAR $ka \equiv kb \pmod{m} \underset{\boxed{\text{SI } mcd(k,m)=1}}{\Longleftrightarrow} a \equiv b \pmod{m}$

EX: $6x \equiv 4 \pmod{7} \underset{\boxed{mcd(6,7)=1}}{\Longleftrightarrow} 3x \equiv 2 \pmod{7}$

PAS 3) SUPOSEM QUE APLICADA MÀXIMA SIMPLIFICACIÓ TENIM

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

ALESHORES (SI $\bar{a} \neq \bar{0}$)

$mcd(a,m) = 1 \Longleftrightarrow \exists$ 1 SOLUCIÓ MÒD. m

$mcd(a,m) \neq 1 \Longleftrightarrow$ NO $\exists$ SOLUCIÓ.

DUES MANERES DE TROBAR LA SOLUCIÓ:

EXEMPLE: $2X \equiv 3 \pmod 5$

NO ES POT SIMPLIFICAR i $mcd(2,5)=1 \Rightarrow$ EXISTEIX SOLUCIÓ ÚNICA (MÒDUL 5)

MÈTODE 1 / BUSQUEM INVERS DE $\bar{2}$ (MÒD 5) (ANOMENEM $\underline{a}$ A L'INVERS DE $\bar{2}$)

$$2 \cdot a + 5K = 1$$

(OBS: SI TROBEM $\underline{a}$ QUE SATISFÀ AQUESTA EQ. DIOF. ALESHORES $\underline{a}$ SERÀ L'INVERS MODULAR DE $\bar{2}$ JA QUE $\overline{5K} = \bar{0} \rightarrow \bar{2} \cdot \bar{a} + \bar{0} = \bar{1} \rightarrow \bar{2}\bar{a} = \bar{1}$)

RESOLEM L'EQUACIÓ AMB ALGORISME ESTÈS EUCLIDES i TENIM $\underline{a=-2}$ (NO CAL TROBAR K), PER TANT

$\overline{-2}$ ÉS L'INVERS MODULAR DE $\bar{2}$. $(\overline{-2} \cdot \bar{2} = \bar{1})$

ARA MULTIPLIQUEM $\overline{2X} = \bar{3}$ PER $\overline{-2}$

$$\overline{-2}\,\overline{2X} = \bar{3} \cdot \overline{-2} \Leftrightarrow \underbrace{\overline{-2}\,\bar{2}}_{\bar{1}}\,\bar{X} = \overline{3 \cdot -2} \Leftrightarrow \bar{X} = \overline{-6}$$

PER TANT $\boxed{X \equiv -6 \pmod 5}$

* TAMBÉ PODEM ESCRIURE $\boxed{X \equiv 4 \pmod 5}$

O BÉ $\boxed{X = 4 + K \cdot 5 \quad (K \in \mathbb{Z})}$

MÈTODE 2 / $2X \equiv 3 \pmod 5 \Leftrightarrow 2X = 3 + 5Y$

$\Leftrightarrow 2X - 5Y = 3$

RESOLEM EQ. DIOFÀNTICA $\rightarrow \boxed{X = 9 + 5t}\; t \in \mathbb{Z}$

PER TANT $\boxed{X \equiv 9 \pmod 5}$ O BÉ $\boxed{X \equiv 4 \pmod 5}$

RESOLUCIÓ SISTEMES CONGRUÈNCIES

TIPUS $\begin{array}{l} X \equiv a_1 \pmod{m_1} \\ X \equiv a_2 \pmod{m_2} \end{array}$

$$\begin{array}{l} X \equiv a_1 \pmod{m_1} \Leftrightarrow \\ X \equiv a_2 \pmod{m_2} \Leftrightarrow \end{array} \left.\begin{array}{l} X = a_1 + m_1 Y \\ X = a_2 + m_2 Z. \end{array}\right\} \Leftrightarrow \underbrace{m_1 Y - m_2 Z = a_2 - a_1}_{\text{EQ. DIOF.}}$$

* SI L'EQUACIÓ (DIOFÀNTICA) TÉ SOLUCIÓ, ALESHORES

$$\boxed{X = a_1 + m_1 Y \pmod{\text{MCM}(m_1, m_2)}}$$

* SI L'EQUACIÓ (DIOFÀNTICA) NO TÉ SOLUCIÓ, NO HI HA SOLUCIÓ.

EXEMPLE 1:

$$\left.\begin{array}{l} X \equiv 2 \pmod 4 \\ X \equiv 1 \pmod 6 \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} X = 2 + 4Y \\ X = 1 + 6Z \end{array}\right\} \Leftrightarrow 4Y - 6Z = 1 - 2$$

$\Leftrightarrow 4Y - 6Z = -1$ NO TÉ SOLUCIÓ PQ $\text{mcd}(4, -6) = 2 \nmid 1$

EXEMPLE 2:

$$\left.\begin{array}{l} X \equiv 4 \pmod 5 \\ X \equiv 5 \pmod 6 \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} X = 4 + 5Y \\ X = 5 + 6Z \end{array}\right\} \Leftrightarrow 5Y - 6Z = 5 - 4$$

$\Leftrightarrow 5Y - 6Z = 1$ $\quad \text{mcd}(5, -6) = 1 \wedge 1 \mid 1$ PER TANT

EL SISTEMA TÉ SOL. ÚNICA MÒDUL $\text{MCM}(5, 6) = 30$

→ AMB ALGORITME ESTÈS EUC. TROBEM $Y = -1$, PER TANT

$X = 4 + 5Y = 4 + 5 \cdot -1 = -1$, PER TANT $\boxed{X \equiv -1 \pmod{30}}$

O BÉ PODEM ESCRIURE $\boxed{X \equiv 29 \pmod{30}} \simeq \boxed{X = 29 + 30K}$ $K \in \mathbb{Z}$

SI TENIM

$$\left.\begin{array}{l} X \equiv a_1 \pmod{m_1} \\ X \equiv a_2 \pmod{m_2} \\ X \equiv a_3 \pmod{m_3} \\ \vdots \end{array}\right\}$$

RESOLEM LES DOS PRIMERES PER REDUIR EL SISTEMA EN UNA EQUACIÓ, AIXÍ SUCCESSIVAMENT FINS TROBAR LA SOLUCIÓ, O DETERMINAR QUE NO HI HA SOLUCIÓ.

RESOLUCIÓ SISTEMES 2 EQ. 2 INCÒGNITES

EXEMPLE:

$$\left.\begin{array}{ll} \bar{3}\bar{x} + \bar{5}\bar{y} = \bar{4} & (\text{EQ. 1}) \\ \bar{4}\bar{x} - \bar{2}\bar{y} = \bar{2} & (\text{EQ. 2}) \end{array}\right\} \mathbb{Z}_{11}$$

FEM

$$\begin{array}{lll} \text{EQ. 1} \cdot 2 & \rightarrow & \bar{6}\bar{x} + \overline{10}\bar{y} = \bar{8} \\ \text{EQ. 2} \cdot 5 & \rightarrow & \overline{20}\bar{x} - \overline{10}\bar{y} = \overline{10} \\ \hline & & \overline{26}\bar{x} \quad = \overline{18} \end{array}$$

PER TANT $26x \equiv 18 \pmod{11} \Leftrightarrow 4x \equiv 7 \pmod{11}$

$(\uparrow 26 \equiv 4,\ 18 \equiv 7)\ \mathbb{Z}_{11}$

LA SOLUCIÓ ÉS $\bar{x} = \overline{10}$. SUBSTITUÏM A EQ. 1

$$\bar{3}\,\overline{10} + \bar{5}\bar{y} = \bar{4} \rightarrow \bar{5}\bar{y} = -\overline{26} \underset{\uparrow}{\rightarrow} \bar{5}\bar{y} = \bar{7}$$

$(-26 \equiv 7 \pmod{11})$

LA SOLUCIÓ ÉS $\bar{y} = \bar{8}$. PER TANT:

$$\boxed{\begin{array}{l} x \equiv 10 \pmod{11} \\ y \equiv 8 \pmod{11} \end{array}}$$

POTÈNCIES

$$\left(\begin{array}{l} \text{T}^{\text{ma}} \text{ PETIT} \\ \text{FERMAT} \end{array} : \left.\begin{array}{l} p \text{ PRIMER} \\ p \nmid a \end{array}\right\} \Rightarrow a^{p-1} \equiv 1 \pmod{p} \right)$$

EXEMPLE: CALCULAR $34773^{4969} \pmod{151}$

* PRIMER OBSERVEM $34773 \equiv 43 \pmod{151}$, PER TANT

$$34773^{4969} \pmod{151} \equiv 43^{4969} \pmod{151}$$

* T$^{\text{ma}}$ PETIT FERMAT AMB $p = 151$, $a = 43$ $\Rightarrow 43^{150} \equiv 1 \pmod{151}$

* $43^{4969} = (43^{150})^{33} \cdot 43^{19} \Rightarrow 43^{4969} \equiv \underbrace{(43^{150})}_{\substack{\equiv \\ 1}\ \leftarrow \text{ FERMAT}}{}^{33} \cdot 43^{19}$

$$\equiv 1^{33} \cdot 43^{19} \equiv 43^{19} \pmod{151}$$

* ARA REDUÏM (PIC i PALA !!)

$$43^{19} \equiv (43^2)^9 \cdot 43 \underset{\substack{\uparrow \\ 43^2 \equiv 37}}{\equiv} 37^9 \cdot 43 \equiv (37^2)^4 \cdot 37 \cdot 43 \underset{\substack{\uparrow \\ 37^2 \equiv 10}}{\equiv} 10^4 \cdot 37 \cdot 43 \equiv \boxed{36 \pmod{151}}$$