

Sistema congruencia lineal

$$\left. \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{array} \right\}$$

$$\left. \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{array} \right\}$$

1) $m = m_1 \times m_2 \times \dots \times m_n$

2) $M_1 = m/m_1 \quad M_2 = m/m_2 \quad \dots \quad M_n = m/m_n$

3) $x = \underline{a_1 M_1} y_1 + \underline{a_2 M_2} y_2 + \dots + \underline{a_n M_n} y_n$

4) $M_k y_k \equiv 1 \pmod{m_k} \quad \text{Inverso}$

$$M_k a_k \text{ (circled)} \equiv a_k \pmod{m_k}$$

$$\text{Inverso } \underline{M_k \pmod{m_k}} = \text{(circled)} y_k$$

$$\begin{array}{l} a_1 \\ x \equiv 2 \pmod{3} \end{array} \quad \begin{array}{l} m_1 \\ \end{array}$$

$$\begin{array}{l} a_2 \\ x \equiv 3 \pmod{5} \end{array} \quad \begin{array}{l} m_2 \\ \end{array}$$

$$\begin{array}{l} a_3 \\ x \equiv 2 \pmod{7} \end{array} \quad \begin{array}{l} m_3 \\ \end{array}$$

$$m = 3 \times 5 \times 7 = 105$$

1) $M_1 = \frac{105}{3} = 35 \quad M_2 = \frac{105}{5} = 21$

$$M_3 = \frac{105}{7} = 15$$

$y_1 = -1$

$$\begin{array}{l} 35 \pmod{3} \\ M_1 \pmod{m_1} \end{array}$$

$$\begin{array}{l} a \\ \downarrow \\ 1) \gcd(35, 3) = 1 \quad \checkmark \\ 35 \pmod{3} = 2 \quad 2 = 35 - (11)3 \\ \swarrow \quad \searrow \\ 3 \pmod{2} = 1 \quad 1 = 3 - 2 \\ \swarrow \quad \searrow \\ 3 \pmod{1} = 0 \end{array}$$

$$1 = a s + b t$$

$$1 = 3 - 2$$

$$1 = 3 - (35 - 11(3))$$

$$1 = (12)3 - 35$$

$$1 = \underset{\substack{\uparrow \\ s}}{35}(-1) + \underset{\substack{\uparrow \\ t}}{(12)}3$$

$$y_2 = 1$$

$$M_2 \bmod m_2$$

$$21 \bmod 5$$

$$2) \text{ mcd} \left(\overset{a}{21}, \overset{b}{5} \right) = 1$$

$$21 \bmod 5 = 1 \quad 1 = 21 - 5(4)$$

$$1 = \underset{\substack{\uparrow \\ s}}{21}(\underset{\substack{\uparrow \\ t}}{1}) + 5(-4)$$

$$y_3 = 1$$

$$M_3 \bmod m_3$$

$$15 \bmod 7$$

$$\text{mcd}(15, 7) = 1$$

$$15 \bmod 7 = 1 \quad 1 = 15 - 7(2)$$

$$1 = 15(1) + 7(-2)$$

$$X = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$

$$X = (2)(35)(1) + (3)(21)(1) + (2)(15)(1)$$

$$X = -70 + 63 + 30 = 23$$

$$\rightarrow 23 \equiv 2 \bmod 3 \quad \checkmark$$

$$\rightarrow 23 \equiv 3 \bmod 5$$

$$\rightarrow 23 \equiv 2 \bmod 7$$