Sistemas de congruencias

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_1 \bmod m_2$$
$$\vdots$$
$$x \equiv a_n \bmod m_n$$

1) $m = m_1 * m_2 * \cdots * m_n$

$M_1 = m / m_1$

$M_2 = m / m_2$

$\vdots$

$M_n = m / m_n$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots a_n M_n y_n$$

y_i Inverso $M_i \bmod m_i$

y_2 Inverso $M_1 \bmod m_1$

$x \equiv 2 \bmod 3$ $\quad a_1 = 2$ $\quad m_1 = 3$

$x \equiv 3 \bmod 5$ $\quad a_2 = 3$ $\quad m_2 = 5$

$x \equiv 2 \bmod 7$ $\quad a_3 = 2$ $\quad m_3 = 7$

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

2) $M_1 = 105/3 = 35$ $\quad M_2 = 105/5 = 21$ $\quad M_3 = 105/7 = 15$

$y_1 \equiv -1$ $\quad M_1 \bmod m_1$

$35 \bmod 3$

(35 = a, 3 = b)

Inverso

$35(s) + 3(t) = 1$

1) $mcd(35, 3) = 1$

$35 \bmod 3 = 2$

$3 \bmod 2 = 1$

$2 \bmod 1 = 0$

$2 = 35 - 3(11)$

$1 = 3 - 2$

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

$\equiv (1 + 11)3 - 35$

$1 = (12)3 - 35$

$1 = 3 - 2$

$s \quad t$

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

$y_2 = 1 \quad M_2 \bmod m_2 \qquad 21 \bmod 5$

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

$1 = 21(1) + 5(-4)$

$s \qquad t$

$y_3 \Rightarrow 1 \quad M_3 \bmod m_3 \qquad 15 \bmod 7 = 1$

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

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

$x = 2 \times 35 \times (-1) + 3 \times 21 \times 1 + 2 \times 15 \times 1$

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

Comprobar

$23 = 2 \bmod 3$

$23 = 3 \bmod 5$

$23 = 2 \bmod 7$

$a = b \bmod m \qquad (a - b) \bmod m = 0$

$21 \bmod 3 = 0 \checkmark$

$20 \bmod 5 = 0 \checkmark$

$21 \bmod 7 = 0 \checkmark$

QED!