3 - Chińskie Twierdzenie o Resztach

Wednesday, 19 June 2024 16:04

Mając układ kongruencji:

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

Jeśli $m_1, \dots, m_n$ są parami względnie pierwsze to istnieje dokładnie $1 \pmod{\prod_i m_i}$ rozwiązanie.

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

Niech $c_1 = m_1^{-1} \pmod{m_2}$, $c_2 = m_2^{-1} \pmod{m_1}$

Wtedy $x = a_1 c_2 m_2 + a_2 c_1 m_1 \pmod{m_1 m_2}$