

Chińskie twierdzenie o resztach (w prostszej wersji):

Niech k będzie liczbą całkowitą dodatnią i niech dane będą parami względnie pierwsze liczby całkowite dodatnie $m_1, m_2, m_3, \dots, m_k$. Wówczas dla dowolnych liczb całkowitych $r_1, r_2, r_3, \dots, r_k$ układ kongruencji

$$\begin{cases} n \equiv r_1 \pmod{m_1} \\ n \equiv r_2 \pmod{m_2} \\ n \equiv r_3 \pmod{m_3} \\ \dots \dots \dots \dots \dots \dots \\ n \equiv r_k \pmod{m_k} \end{cases}$$

ma rozwiązanie całkowite n . Co więcej, istnieje dokładnie jedno rozwiązanie nieujemne $n < m_1 m_2 m_3 \dots m_k$, a wszystkie pozostałe rozwiązania całkowite uzyskuje się z niego przez dodanie/odjęcie wielokrotności iloczynu $m_1 m_2 m_3 \dots m_k$.

Bez użycia kongruencji możemy wyrazić to następująco: Jeżeli zażyczymy sobie, że liczba n ma dawać przy dzieleniu przez m_i resztę r_i dla $i = 1, 2, 3, \dots, k$, to takie życzenia daje się zrealizować, jeżeli liczby m_i są parami względnie pierwsze.

Chińskie twierdzenie o resztach (w wersji ogólnej):

Niech k będzie liczbą całkowitą dodatnią i niech dane będą liczby całkowite dodatnie $m_1, m_2, m_3, \dots, m_k$ oraz liczby całkowite $r_1, r_2, r_3, \dots, r_k$ spełniające warunek

$$r_i \equiv r_j \pmod{\text{NWD}(m_i, m_j)} \quad \text{dla } 1 \leq i < j \leq k.$$

Wówczas układ kongruencji

$$\begin{cases} n \equiv r_1 \pmod{m_1} \\ n \equiv r_2 \pmod{m_2} \\ n \equiv r_3 \pmod{m_3} \\ \dots \dots \dots \dots \dots \dots \\ n \equiv r_k \pmod{m_k} \end{cases}$$

ma rozwiązanie całkowite n . Co więcej, istnieje dokładnie jedno rozwiązanie nieujemne $n < \text{NWW}(m_1, m_2, m_3, \dots, m_k)$, a wszystkie pozostałe rozwiązania całkowite uzyskuje się z niego przez dodanie/odjęcie wielokrotności $\text{NWW}(m_1, m_2, m_3, \dots, m_k)$.

Bez użycia kongruencji możemy wyrazić to następująco: Jeżeli zażyczymy sobie, że liczba n ma dawać przy dzieleniu przez m_i resztę r_i dla $i = 1, 2, 3, \dots, k$, to takie życzenia daje się zrealizować, o ile nie stoją one w oczywistej sprzeczności, jak na przykład jednocześnie żądanie, że liczba n ma być parzysta i nieparzysta.