CHIńSKIE TWIERDZENIE O RESZTACH

Dla ustalonej dodatniej liczby naturalnej n i całkowitej liczby x przez $(x)_n$ zonaczamy resztę z dzielenia liczby x przez n. Jeśli dodatkowo y jest liczbą całkowitą, to definiujemy relację

$$x \equiv y \mod n \longleftrightarrow n|(x-y).$$

Zauważmy, że

$$x \equiv y \mod n \longleftrightarrow (x)_n = (y)_n.$$

Twierdzenie 1 (Chińskie twierdzenie o resztach)**.** *Jeżeli $\{n_1, \ldots, n_m\}$ jest zbiorem dodatnich liczb naturalnych parami względnie pierwszych, $\{a_1, \ldots, a_m\} \subseteq \mathbb{Z}$, to istnieje $x \in \mathbb{Z}$ takie, że*

$$\forall i \in \{1, \ldots, m\} \;\; a_i \equiv x \mod n_i.$$

Ponadto, jesli x, y są dwoma rozwiazaniami powyższego układu kongruencjii, to

$$y \equiv x \mod n_1 \cdot \ldots \cdot n_m.$$

Dowód. Niech $N = n_1 \cdot \ldots \cdot n_m$ oraz $N_i = N/n_i$ dla $i \in \{1, \ldots, m\}$. Zauważmy, że dla każdego $i \in i \in \{1, \ldots, m\}$ $nwd(n_i, N_1) = 1$, więc

$$\forall i \in i \in \{1, \ldots, m\} \; \exists u_i, v_i \in \mathbb{Z} \;\; u_i n_i + v_i N_i = 1.$$

Więc mnożąc i-tą równość stronami przez a_i otrzymujemy:

$$\forall i \in i \in \{1, \ldots, m\} \; \exists u_i, v_i \in \mathbb{Z} \;\; a_i u_i n_i + a_i v_i N_i = a_i.$$

Niech $x = \sum_{j=1}^{m} a_j v_j N_j$, wtedy dla każdego $i \in \{1, \ldots, m\}$ mamy

$$\begin{aligned}(x)_{n_i} =& (\sum_{j=1}^{m} a_j v_j N_j)_{n_i} = (\sum_{j=1}^{m} a_j v_j (N_j)_{n_i})_{n_i} \\ =& (a_i v_i N_i)_{n_i} = (a_i - a_i u_i n_i)_{n_i} = (a_i)_{n_i}.\end{aligned}$$

Skorzystaliśmy z faktu, że jesli $i \neq j$ to $n_i | N_J$.

Niech $x, y \in \mathbb{Z}$ będą rozwiązaniami układu kongruencji, tj.

$$\forall i \in \{1, \ldots, m\} \;\; a_i \equiv x \mod n_i$$

oraz

$$\forall i \in \{1, \ldots, m\} \;\; a_i \equiv y \mod n_i.$$

odejmując stronami, mamy $x \equiv y \mod n_i$ dla wszystkich $i \in \{1, \ldots, m\}$. Ponieważ n_i jest względnie pierwsze z n_j dla różnych i, j, więc $N|(x-y)$. Istnieje $k \in \mathbb{Z}$ takie, że $y = x + k \cdot N$. Łatwo sprawdzamy, że jesli x jest rozwiązaniem naszego układu kongruencji, to dla każdego $k \in \mathbb{Z}$, $y = x + k \cdot N$ również jest rozwiązaniem wspomnianego układu kongruencji. $\square$