

mogły być dowolnymi liczbami rzeczywistymi (a nie tylko całkowitymi).

- 3. [M26] (*Uogólnione chińskie twierdzenie o resztach*.) Niech $m_1, m_2, \dots, m_r$ będą dodatnimi liczbami całkowitymi. Niech m będzie najmniejszą wspólną wielokrotnością $m_1, m_2, \dots, m_r$ i niech $a, u_1, u_2, \dots, u_r$ będą dowolnymi liczbami całkowitymi. Udowodnij, że istnieje dokładnie jedna liczba całkowita u spełniająca warunki

$$a \leq u < a + m, \quad u \equiv u_j \pmod{m_j}, \quad 1 \leq j \leq r,$$

o ile

$$u_i \equiv u_j \pmod{\text{NWD}(m_i, m_j)}, \quad 1 \leq i < j \leq r;$$

oraz że taka liczba u nie istnieje, jeśli ten ostatni warunek nie jest spełniony.

3. Z tego, że $u \equiv u_i \pmod{m_i}$, wynika, że $u \equiv u_i \pmod{\text{NWD}(m_i, m_j)}$, więc warunek $u_i \equiv u_j \pmod{\text{NWD}(m_i, m_j)}$ musi zachodzić, jeśli istnieje rozwiązanie. Dalej, jeśli $u \equiv v \pmod{m_j}$ dla każdego j , to $u - v$ jest wielokrotnością $\text{lcm}(m_1, \dots, m_r) = m$; zatem istnieje co najwyżej jedno rozwiązanie.

Dokończenie dowodu metodą niekonstruktywną polega na obliczeniu, ile jest różnych r -tek $(u_1, \dots, u_r)$ spełniających warunki $0 \leq u_j < m_j$ oraz $u_i \equiv u_j \pmod{\text{NWD}(m_i, m_j)}$. Jeśli ta liczba jest równa m , to musi istnieć rozwiązanie, ponieważ $(u \bmod m_1, \dots, u \bmod m_r)$ przyjmuje m różnych wartości dla u zmieniającego się od a do $a + m - 1$. Załóżmy, że wybraliśmy $u_1, \dots, u_{r-1}$ spełniające zadane warunki; musimy teraz wybrać $u_r \equiv u_j \pmod{\text{NWD}(m_j, m_r)}$ dla $1 \leq j < r$, a z uogólnionego chińskiego twierdzenia o resztach dla $r - 1$ elementów wynika, że można to zrobić na

$$m_r / \text{lcm}(\text{NWD}(m_1, m_r), \dots, \text{NWD}(m_{r-1}, m_r)) = m_r / \text{NWD}(\text{lcm}(m_1, \dots, m_{r-1}), m_r) \\ = \text{lcm}(m_1, \dots, m_r) / \text{lcm}(m_1, \dots, m_{r-1})$$

sposobów. [Ten dowód jest oparty na tożsamościach (10), (11), (12), and (14) z Podrozdziału 4.5.2.]

Dowód konstruktywny [A. S. Fraenkel, *Proc. Amer. Math. Soc.* **14** (1963), 790-791], uogólniający wzór (25), może wyglądać następująco. Niech $M_j = \text{lcm}(m_1, \dots, m_j)$; chcemy znaleźć $u = v_r M_{r-1} + \dots + v_2 M_1 + v_1$, gdzie $0 \leq v_j < M_j / M_{j-1}$. Załóżmy, że $v_1, \dots, v_{j-1}$ zostały już wyznaczone; musimy teraz rozwiązać kongruencję

$$v_j M_{j-1} + v_{j-1} M_{j-2} + \dots + v_1 \equiv u_j \pmod{m_j}.$$

Z założenia mamy tu $v_{j-1} M_{j-2} + \dots + v_1 \equiv u_i \equiv u_j \pmod{\text{NWD}(m_i, m_j)}$ dla $i < j$, więc $c = u_j - (v_{j-1} M_{j-2} + \dots + v_1)$ jest wielokrotnością

$$\text{lcm}(\text{NWD}(m_1, m_j), \dots, \text{NWD}(m_{j-1}, m_j)) = \text{NWD}(M_{j-1}, m_j) = d_j.$$

Musimy zatem rozwiązać kongruencję $v_j M_{j-1} \equiv c \pmod{m_j}$. Algorytmem Euklidesa znajdziemy liczbę c_j taką, że $c_j M_{j-1} \equiv d_j \pmod{m_j}$; możemy zatem wziąć

$$v_j = (c_j c) / d_j \bmod (m_j / d_j).$$

Zauważmy, że, tak jak w dowodzie niekonstruktywnym, mamy $m_j / d_j = M_j / M_{j-1}$.

(W przykładzie 1, gdzie $m_1 = 91 = 7 \cdot 13$ wykorzystaliśmy wszystkie mniejsze niż 100 iloczyny