

Теорема (китайская теорема об остатках)

Пусть числа $m_1, \dots, m_k \in \mathbb{N}$ взаимно просты (т.е. $(m_i, m_j) = 1$ при $i \neq j$).

Тогда для любых $b_1, \dots, b_k \in \mathbb{Z}$

система сравнений

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases} (*)$$

имеет решение.

Док-во. Положим $M = m_1 \cdot \dots \cdot m_k$, $M_i = \frac{M}{m_i}$.

Далее, определяем числа M'_i , $i \in \overline{1, k}$, из условия $M_i \cdot M'_i \equiv 1 \pmod{m_i}$; т.к. $(m_i, M_i) = 1$, такие M'_i существуют (см. следствие из алгор. Евкл.).

Рассм. число
$$x_0 = b_1 M_1 M'_1 + b_2 M_2 M'_2 + \dots + b_k M_k M'_k.$$

Покажем, что $x_0 \equiv b_i \pmod{m_i} \forall i \in \overline{1, k}$. Имеем $x_0 \equiv 0 + 0 + \dots + b_i M_i M'_i + 0 + \dots + 0 \equiv b_i \cdot 1 \equiv b_i \pmod{m_i}$.

Далее, пусть $\tilde{x}$ — какое-либо решение системы сравнений (*). Имеем

$$\tilde{x} \equiv b_i \equiv x_0 \pmod{m_i} \Rightarrow \tilde{x} \equiv x_0 \pmod{m_i} \forall i \in \overline{1, k}$$

Т.о., $m_1 m_2 \dots m_k \mid (\tilde{x} - x_0)$, откуда
$$\tilde{x} \equiv x_0 \pmod{M}$$

— все решения имеют такой вид.

Док-но.