49. Китайская теорема об остатках

Лемма. *Пусть* $(a, b) = 1$, *тогда* $\exists c : ac \equiv 1 \pmod{b}$

▲. Рассмотрим числа $a, 2a, ..., (b-1)a$. Они образуют приведённую систему вычетов, а значит есть остаток 1. ■

Теорема (Китайская теорема об остатках)**.** *Пусть* $n_1, n_2, ..., n_k \in \mathbb{N}$ *попарно взаимно простые, а* $r_1, r_2, ..., r_k \in \mathbb{Z}$. *Тогда* $\exists! M$ *по модулю* $\prod_{i=1}^{k} n_i$ *решение системы сравнений:*

$$\begin{cases} M \equiv r_1 \pmod{n_1} \\ M \equiv r_2 \pmod{n_2} \\ ... \\ M \equiv r_k \pmod{n_k} \end{cases}$$

▲. Пусть $N = \prod_{i=1}^{k} n_i; N_i = \frac{N}{n_i}; N_i^{-1}$ – обратный к N_i по модулю n_i.
Существование N_i^{-1} можно обосновать по лемме, так как $(N_i, n_i) = 1$.
Покажем, что $M = \sum_{i=1}^{k} r_i N_i N_i^{-1}$ будет решением.
Рассмотрим M по модулю n_1. Все слагаемые, кроме первого, содержат множитель N_i, который делится на n_1. Получается, что $M \equiv r_1 N_1 N_1^{-1} \pmod{n_1} \equiv r_1 \pmod{n_1}$, то есть M является решением первого сравнения.
Аналогично проверяем все k сравнений.
Теперь докажем, что решение единственно по модулю N.
Пусть A и B – различные решения по модулю N. Тогда $A - B \equiv 0 \pmod{n_i}$. Так как n_i взаимно простые, то $A - B \equiv 0 \pmod{N}$. Получается, что A и B – одинаковые решения по модулю N.
Противоречие. ■