Китайская теорема об остатках

1 КТО ~~затехает это за ме...~~

Теорема 1.1. *Пусть $a_1, a_2, \ldots, a_n$ – попарно взаимно простые целые числа, $r_1, r_2, \ldots, r_n$ – некоторые целые числа. Для простоты считаем, что $0 \leq r_i < |a_i|$ $\forall i \in \{1, 2, \ldots, n\}$. Тогда:*

$$\exists N \in \mathbb{N} : N \equiv r_i \ (mod\ a_i) \quad \forall i \in \{1, 2, \ldots, n\}$$

Более того, если N_1 и N_2 – решения системы сравнений, то:

$$N_1 \equiv N_2 \ (mod\ a_1 a_2 \ldots a_n)$$

Доказательство. Покажем требуемое индукцией по n.
База. При $n = 1$ тривиально существование требуемого решения системы сравнений. К тому же очевидно, что если $N_1 \equiv r_1 \ (mod\ a_1)$ и $N_2 \equiv r_1 \ (mod\ a_1)$, то $N_1 \equiv N_2 \ (mod\ a_1)$.
Шаг. Пусть утверждение верно при $n = k$. Рассмотрим $n = k + 1$:

$$\begin{cases} x \equiv r_1 \ (mod\ a_1) \\ x \equiv r_2 \ (mod\ a_2) \\ \ldots \\ x \equiv r_k \ (mod\ a_k) \\ x \equiv r_{k+1} \ (mod\ a_{k+1}) \end{cases}$$

По предположению индукции у подсистемы

$$\begin{cases} x \equiv r_1 \ (mod\ a_1) \\ x \equiv r_2 \ (mod\ a_2) \\ \ldots \\ x \equiv r_k \ (mod\ a_k) \end{cases}$$

существует решение N. Положим $d = a_1 a_2 \ldots a_k$. По условию выполнено, что НОД$(d, a_{k+1}) = 1$. Теперь рассмотрим следующий набор чисел:

$$N, N + d, N + 2d, \ldots, N + (a_{k+1} - 1)d$$

Заметим, что все числа из этого набора попарно несравнимы по модулю a_{k+1}. В самом деле, если бы от противного

$$\exists i, j \in \{0, \ldots, a_{k+1} - 1\} : N + id \equiv N + jd \ (mod\ a_{k+1}),$$

то:

$$(N + id) - (N + jd) = d(i - j) \equiv 0 \ (mod\ a_{k+1}),$$

откуда получаем противоречие. Значит в рассматриваемом наборе есть все остатки по модулю a_{k+1}, в том числе r_{k+1}. Пусть тогда $j \in \{0, \ldots a_{k+1-1}\}$ такое, что $N + jd \equiv r_{k+1} \ (mod\ a_{k+1})$. Легко видеть, что в таком случае

$$N + jd \equiv r_i \ (mod\ a_i) \quad \forall i \in \{1, \ldots, k + 1\}$$

Значит $N + jd$ – искомое решение всей исходной системы сравнений. Более того, если N_1 и N_2 – решения исходной системы сравнений, то по предположению индукции $(N_1 - N_2) \vdots d$, а из того, что эти числа суть решения всей системы сравнений, получим $(N_1 - N_2) \vdots a_{k+1}$. Так как НОД$(d, a_{k+1}) = 1$, то немедленно получаем:

$$(N_1 - N_2) \vdots da_{k+1} \iff N_1 \equiv N_2 \ (mod\ da_{k+1}),$$

что и требовалось. □