Китайская теорема об остатках.

Теорема. Если натуральные m и n взаимно просты, то система

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n} \end{cases}$$

имеет решения в целых числах. Все эти решения удовлетворяют одному сравнению $x \equiv C \pmod{mn}$.

Иными словами, множество решений такой системы представляет собой один вычет по модулю mn.

То, что множество решений имеет именно такой вид, если они вообще существуют, более или менее очевидно: если системе удовлетворяет некоторое целое C, то любое $C_1 \equiv C \pmod{mn}$ сравнимо с C по модулям m и n, и, наоборот, если $C_1 \equiv C \pmod{m}$ и $C_1 \equiv C \pmod{n}$, то (так как $(m, n) = 1$) $C_1 \equiv C \pmod{mn}$. Поэтому доказывать нужно только существование решения.

Скучное арифметическое доказательство существования основывается на свойстве полной системы вычетов. Если подействовать на полную систему вычетов 0, 1, 2, ..., $m - 1$ линейной функцией $t \mapsto nt + b$, получится также полная система вычетов b, $n + b$, $2n + b$, ..., $(m - 1)n + b$ по модулю m, содержащая, среди прочих, число, сравнимое по модулю m с a.

Более интересное арифметическое доказательство начинается с решения линейных сравнений $mm_1 \equiv 1 \pmod{n}$ и $nn_1 \equiv 1 \pmod{m}$ (почему решения существуют?) Тогда решением исходной системы будет

$$x \equiv ann_1 + bmm_1 \pmod{mn}$$

(проверьте).

Наконец, **комбинаторное доказательство** получается, если сопоставить каждому вычету $C \bmod mn$ пару вычетов $(a \bmod m, b \bmod n)$ так, что $C \equiv a \pmod{m}$, $C \equiv b \pmod{n}$. Ясно, что разным вычетам $\bmod mn$ сопоставляются разные пары вычетов (a, b). Поскольку вычетов $\bmod mn$ столько же, сколько пар, составленных из вычета $\bmod m$ и вычета $\bmod n$, а именно mn, каждая пара будет сопоставлена какому-нибудь вычету $\bmod mn$.

Если вычеты m_1, m_2, ..., m_k попарно взаимно просты, то при любых целых a_1, a_2, ..., a_k система

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

эквивалентна одному сравнению вида $x \equiv C \pmod{m_1 m_2 \dots m_k}$. Эта, более общая, формулировка китайской теоремы об остатках может быть получена из утверждения о двух сравнениях индукцией по k. С другой стороны, комбинаторное доказательство (как и второе арифметическое) практически не меняется при переходе от двух сравнений к любому количеству.