定义

中国剩余定理 (Chinese Remainder Theorem, CRT) 可求解如下形式的一元线性同余方程组（其中 $n_1, n_2, \cdots, n_k$ 两两互质）：

$$\begin{cases} x & \equiv a_1 \pmod{n_1} \\ x & \equiv a_2 \pmod{n_2} \\ & \vdots \\ x & \equiv a_k \pmod{n_k} \end{cases}$$

上面的「物不知数」问题就是一元线性同余方程组的一个实例。

过程 ¶

1. 计算所有模数的积 n；
2. 对于第 i 个方程：
    a. 计算 $m_i = \frac{n}{n_i}$；
    b. 计算 m_i 在模 n_i 意义下的 逆元 m_i^{-1}；
    c. 计算 $c_i = m_i m_i^{-1}$（**不要对 n_i 取模**）。
3. 方程组在模 n 意义下的唯一解为：$x = \sum_{i=1}^{k} a_i c_i \pmod{n}$。