中国剩余定理(孙子定理)

$a, b \in N^+$, 对 $\forall 0 \le x < a$, $\forall 0 \le y < b$ 是否存在 S, s.t.

$$\begin{cases} S \equiv x \mod a \\ S \equiv y \mod b \end{cases}$$

不一定成立. 反例: $a=b$, $x \neq y$

{ gcd: greatest common devisor
lcm: least common multiple

attempt 1: a, b 互素, 即 $\gcd(a,b)=1$.

(x,y) 有 $a \times b$ 种可能:

$$(x,y) \in \begin{cases} (0,0) & \cdots & (0,b) \\ \vdots & & \\ (a,0) & \cdots & (a,b) \end{cases}$$

余数对抽屉有 ab 个.

S 有无穷多个. 但 $S+ab \equiv S \mod a$ or b or ab

在模 ab 的意义下. 不妨取 $S \in \{0, 1, \cdots, ab-1\}$ → 现希望每个位置均有一个 S

则 ab 个 S in ab 个抽屉.

同上策 希望建立 一一映射

证 $\forall S_1, S_2 \in [ab-1]$ 有 $(S_1 \% a, S_1 \% b) \neq (S_2 \% a, S_2 \% b)$

反证: 设存在 $S_1, S_2 \in [ab-1]$, 不妨设 $S_1 < S_2$, s.t. $\begin{cases} S_1 \equiv S_2 \mod a \\ S_1 \equiv S_2 \mod b \end{cases}$ (*)

(*) $\Rightarrow \begin{cases} a \mid (S_2 - S_1) \\ b \mid (S_2 - S_1) \end{cases}$ 这一步用 ab 互素 $\Rightarrow ab \mid (S_2 - S_1)$ 得证

$$\mathrm{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$ 得证

设为: $\gcd(a,b)=d$. $S+\frac{ab}{d} \equiv S \mod a$ or b

此时有 $0, \cdots \frac{ab}{d}-1$ 共 $L=\frac{ab}{d}$ 个抽屉

整除：$\begin{cases} a|b : \exists k \in N^+ \text{ s.t } b = k\cdot a \\ \gcd(a,b): a,b\text{的最大公约数 greatest common devisor} \end{cases}$

↓

性质：$a\neq 1$，$a|b\cdot c$ 且 $(a,b)=1 \Rightarrow a|c$

分析 $(a,b)=1$ 将"( )"去掉转为普通的加减乘除

$\exists t$，$bc = at$，$b = qa+r$ 其中 $0\le r<a-1$

$\Rightarrow at = bc = (qa+r)c \Rightarrow c = \frac{t-qc}{r}a$ → integer?

目前：$r=1$ → 不一定 $\Rightarrow$ 用 $mb = qa+r$

则 $at = (qa+r)c \Rightarrow mat = (qa+r)c \Rightarrow (mt-qc)a = rc$

希望 $r=1$?

能否找到 m s.t $mb = qa+r$，其中 $r=1$?

已知 $(a,b)=1$，则 $\exists m,n$ s.t. $ma+nb=1$（可能线性相除），

更一般的：$(a,b)=d$ 则 $\exists m,n$ s.t. $ma+nb=d$ } 裴蜀公式

证：考虑集合 $\{ma+nb \mid m,n\in N\}$ 取其中最小的正整数 r

先证 $\forall c\in Z_{(a,b)}$，$r|c$：

取 $c = qr+r'$，$0\le r'<c$ 有 $\begin{cases} c = xa+yb \\ r = ta+sb \end{cases}$

$\Rightarrow r' = c-qr = (x-qt)a+(y-qs)b \in Z_{(a,b)}$

则 r 只能为 0，否则与 r 是 $Z_{(a,b)}$ 中最小正整数矛盾。

再：取 $\begin{cases} (m,n)=(1,0) \text{ 有 } r|a \\ (m,n)=(0,1) \text{ 有 } r|b \end{cases} \Rightarrow r$ 是 a,b 公约数 $r\le d$

再 $d|a$，$d|b$，$\exists m_0,n_0$ s.t $r = m_0a+n_0b = (m_0\frac{a}{d}+n_0\frac{b}{d})d$

$\Rightarrow d\le r$

故 $d=r$，即集合 $\{ma+nb\}$ 中最小的正整数是 $\gcd(a,b)$