同余基本性质：$\forall a,b\in\mathbb{Z}^+$, $a\equiv b \bmod m \Rightarrow m\mid(a-b)$

共伴：1 自反性 $a\equiv a \bmod m$

2 对称性 $a\equiv b \bmod m$. $b\equiv a \bmod m$

3 传递性 $a\equiv b$, $b\equiv c \bmod m \Rightarrow a\equiv c \bmod m$

4 可加/乘：$a\equiv b \bmod m$ $c\equiv d \bmod m$

$m\mid(a-b)$ $m\mid(c-d)$

$\Rightarrow m\mid(a-b)\pm(c-d)=(a\pm c)-(b\pm d)$

$m\mid(a-b)c+(c-d)b=ac-bd$

例：$a\pm c\equiv b\pm d \bmod m$

$ac\equiv bd \bmod m$

$a^k\equiv b^k \bmod m$

5 $d\in\mathbb{N}^+$. $d\mid m$, $a\equiv b \bmod m \Rightarrow a\equiv b \bmod d$ $d\mid m\mid b-a$.

6. $d\in\mathbb{N}^+$, $a\equiv b \bmod m$, $\Rightarrow da\equiv db \bmod m$ $m\mid(b-a)\mid d(a-b)$

7. $(d,m)=1$, $a\equiv b \bmod m \Leftrightarrow da\equiv db \bmod m$ $(m,d)=1:m\mid(b-a)\Leftrightarrow m\mid d(b-a)$

一次同余方程：$ax\equiv b \bmod m$

存在性：是否总有解：不一定有解. 有解 $\Leftrightarrow (a,m)\mid b$

有解 $\Leftrightarrow m\mid(ax-b)$

$\Leftrightarrow \exists k$ s.t. $ax-b=km$

$\Leftrightarrow b=ax-km\in\{sa+tm \mid s,t\in\mathbb{Z}\}$ ↖裴蜀公式

$\Leftrightarrow (a,m)\mid b$

唯一性：解的个数：

先限制在$\{0,1,\cdots m-1\}$中. 因为若x是解. $x+m$仍是解.

$\#x:(ax\equiv b \bmod m)=\#x:(b=ax+my)$ $\#x$表示x的个数

解的个数有 $d=\gcd(a,m)$个解 (往前看)

(x,y), $(x-\frac{m}{d}, y+\frac{a}{d})\cdots$

不从裴蜀看：求通解：设 $\begin{cases}ax_0\equiv b \bmod m\\ ax\equiv b \bmod m\end{cases}\Rightarrow a(x-x_0)\equiv 0 \bmod m$

$m\mid a\Delta x\Rightarrow \frac{m}{(a,m)}\mid\frac{a}{(a,m)}\Delta x$ 而 $(\frac{m}{(a,m)},\frac{a}{(a,m)})=1\Rightarrow \frac{m}{(a,m)}=\Delta x$

$x=k\cdot\frac{m}{(a,m)}+x_0$, 在$\{1,2,\cdots m-1\}$中有 $d=(a,m)$个解.

特：若$(m,a)=1$. 则 $1,\cdots,m$中只有一个解.

回顾：中国剩余定理 $\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{cases}$ 何时有解：

$\forall (a_1, a_2)$ 均有解 $\Leftrightarrow (m_1, m_2) = 1$.

更一般的：$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_k \mod m_k \end{cases}$ 取 $M = m_1 \cdots m_k$，按 $\{0, 1 \cdots M-1\}$ 内问解.

$\forall (a_1, \cdots a_k)$ 有解 $\Leftrightarrow (m_i, m_j) = 1 \ \forall i, j$.

将此个问题分解成 k 个子问题

$$\begin{cases} x_1 \equiv a_1 \mod m_1 \\ x_1 \equiv 0 \mod m_2 \\ \vdots \\ x_1 \equiv 0 \mod m_k \end{cases} \quad \begin{cases} x_2 \equiv 0 \mod m_1 \\ x_2 \equiv a_2 \mod m_2 \\ \vdots \\ x_2 \equiv 0 \mod m_k \end{cases} \quad \cdots \quad \begin{cases} x_k \equiv 0 \mod m_1 \\ x_k \equiv 0 \mod m_2 \\ \vdots \\ x_k \equiv a_k \mod m_k \end{cases}$$

分别求解后直接求和. $x_1 + \cdots + x_k \equiv a_1 + 0 + \cdots + 0 \mod m_1$

$\vdots$

对问题 i 有解：$\begin{cases} x_i \equiv a_i \mod m_i \\ x_i \equiv 0 \mod \frac{M}{m_i} \end{cases} \Leftrightarrow (m_i, \frac{M}{m_i}) = 1$.

原问题总有解 $\Leftrightarrow$ 须 $(m_i, m_j) = 1 \ \forall i, j$