如果 $a \equiv b(\operatorname{mod} m)$ ，我們會說 a, b 在模 m 下同餘。

以下為性質：

- 整除性： $a \equiv b \pmod m \Rightarrow c \cdot m = a - b, c \in \mathbb{Z}$
  $\Rightarrow a \equiv b \pmod m \Rightarrow m \mid a - b$
- 遞移性：若 $a \equiv b \pmod c, b \equiv d \pmod c$
  則 $a \equiv d(\operatorname{mod} c)$
- 保持基本運算：

$$\begin{cases} a \equiv b(\operatorname{mod} m) \\ c \equiv d(\operatorname{mod} m) \end{cases} \Rightarrow \begin{cases} a \pm c \equiv b \pm d(\operatorname{mod} m) \\ a \cdot c \equiv b \cdot d(\operatorname{mod} m) \end{cases}$$

- 放大縮小模數：

$$k \in \mathbb{Z}^+, a \equiv b \pmod m \Leftrightarrow k \cdot a \equiv k \cdot b \pmod{k \cdot m}$$

模逆元是取模下的反元素，即為找到 a^{-1} 使得 $aa^{-1} \equiv\ 1 \operatorname{mod} c$ 。

整數 a 在 $\operatorname{mod} c$ 下要有模反元素的充分必要條件為 a, c 互質。

模逆元如果存在會有無限個，任意兩相鄰模逆元相差 c 。

費馬小定理

給定一個質數 p 及一個整數 a ，那麼： $a^p \equiv a(\mod p)$ 如果 $gcd(a, p) = 1$ ，則：
$a^{p-1} \equiv 1(\mod p)$

歐拉定理

歐拉定理是比較 general 版本的費馬小定理。給定兩個整數 n 和 a ，如果 $gcd(a, n) = 1$ ，貝
$a^{\Phi(n)} \equiv 1(\mod n)$ 如果 n 是質數， $\Phi(n) = n - 1$ ，也就是費馬小定理。

Wilson's theorem

給定一個質數 p ，則： $(p-1)! \equiv -1(\mod p)$