同餘算數(Modular Arithmetic) – 模數

- 模數 (Modulo)
  - 取餘數的運算

    令一個正整數 n 與整數 a，並 a 除以 n 得到商為 q，與餘數 b，如下：

    $a = qn + b \quad 0 \leqq b < n$；$q = \lceil a/n \rfloor$

    可定義模數運算如下：

    $b \equiv a \bmod n$
  - modulo 2 (二進位運算)、modulo 8、modulo 16、modulo 24
  - 譬如：

    $16 \bmod 8 \equiv 0 \quad (0 \sim 7) \quad n=8$

    $16 \bmod 10 \equiv 6 \quad (0 \sim 9) \quad n=10$

    $54 \bmod 24 \equiv 6 \quad (0 \sim 23) \quad n=24$
  - n 越大安全性越高。

同餘算數(Modular Arithmetic)－模數

- 模數的特性：
  - 反向性：a ≡ a mod n。(0<= a < n)

    (驗證： 5 ≡ 5 mod 10
  - 對稱性：若 a ≡ b mod n，則 b ≡ a mod n。

    (驗證：5 ≡ 15 mod 10 則15 ≡ 5 mod 10 ≡ 5 = a)
  - 遞移性：若 a ≡ b mod n 且b ≡ c mod n，則 a ≡ c mod n。

    (驗證：5 ≡ 15 mod 10 且15 ≡ 25 mod 10，則 5 ≡ 25 mod 10≡ 5 = a)
  - 若 (a mod n) = (b mod n)，可推論出 a ≡ b mod n。

    (驗證：(15 mod 10) = (25 mod 10)，則 15 ≡ 25 mod 10≡ 5 = a)