同餘(一)

這一章是在其他後面幾個章節完成後才補上的，原想主線是討論質數的一些有趣性質，但是有關整除性，帶餘除法的討論總不能擺脫同餘的概念，同餘的概念充斥於數論的每一個角落，在左閃右避的情況下，不若補回介紹同餘概念的這一節。

一些用詞

「同餘」是指有相同的餘數。

例一:

8 被 6 除，餘 2；
50 被 6 除，餘 2；
52 被 6 除，餘 4；

所以，8 與 50 被 6 除有相同的餘數，8 與 50 同餘；8 與 52、50 與 52 不同餘。

例二:

8 被 7 除，餘 1；
50 被 7 除，餘 1；
52 被 7 除，餘 3；

所以，8 與 50 同餘。

然則我們就可以簡單地說 8 與 50 同餘嗎？

例三:8 被 8 除，餘 0；50 被 8 除，餘 2；這時候，8 與 50 不同餘。

爲什麼？8 與 50 有時是「同餘」的，有時是「不同餘」的？關鍵是除數的不同。是以用「同餘」一詞作描述時，必需一併說出這個除數。以剛才的例子爲例：

8 同餘於 50 模 6，記作 $8 \equiv 50 (\mathrm{mod} 6)$

8 同餘於 50 模 7，記作 $8 \equiv 50 (\mathrm{mod} 7)$

8 不同餘於 50 模 8，記作 $8 \not\equiv 50 (\mathrm{mod} 8)$

模算術的出現

研究有關餘數的問題,我國的《孫子算經》(約公元 300-400 年)下卷中的"物不知數"問題，就是一道一次同餘式問題:

今有物，不知其數。三三數之，賸二；五五數之，賸三；七七數之，賸二。問物幾何？
答曰：二十三。

術曰：三三數之，賸二，置一百四十；五五數之，賸三，置六十三；七七數之，賸二，置三十。并之，得二百三十三，以二百一十減之，即得。凡三三數之，賸一，則置七十五；五五數之，賸一，則置二十一；七七數之，賸一，則置十五。一百六以上，以一百五減之，即得。

在歐洲,有關餘數的研究則是由不定方程開始,經歷過很多數學家的參與,由 Claude Gaspard Bachet de Méziriac (1624), Christlieb von Clausberg (1732), Leonhard Euler (1734), Joseph Louis Lagrange (1736-1813), Abraham Kästner, Carl Friedrich Hindenburg 直至 Carl Friedrich Gauss 高斯 在他的巨著 Disquisitiones Arithmeticae 算術探究 (1801)模算術 的架構基本上完成。

而 "模"及其他術語則首見於 Disquisitiones Arithmeticae 算術探究:

(拉丁文原文):
Definitiones. Si numerus aliquis, quem moduli nomine denotabimus, duorum numerorum differentiam metitur, hi secundum illum congrui dicentur, sin minus, incongrui. Priori casu alteruter numerorum alterius residuum vocatur, posteriori non-residuum. Ita numeri 32, 11 congrui dicentur secundum modulum 7, quippe quorum differentia 21 per 7 dividitur.

Maiorem utilitatem afferret ad calculos contrahendo numeros congruos signo denotare: ad quod ob insignam inter eos et quantitates aequales analogiam hoc utemur $\equiv$, modulo quando ad ambiguitatem evitandam necessarium videbitur clausulis apposito. Exempla §.1.igitur tali modo exhibentur $32 \equiv 11(mod.7); -19 \equiv +1(mod.5)$.

(英譯):
Definitions. If a certain number, which we will call the modulus, measures the difference of two numbers, we will call these numbers congruent to the modulus, if not, incongruent. In the first case one of the two numbers will be called the residue of the other, in the second case, a non-residue. E.g. 32 and 11 will be called congruent to the modulus 7, because the difference of these numbers, 21, is divisible by 7. Denoting congruent numbers by a sign is very useful for abbreviating calculations: thus, because of the analogy with equality between numbers, we will use as a sign, this sign $\equiv$, the modulus can be added in brackets to avoid ambiguity if it is considered necessary. For example §.1. can be written in this way as $32 \equiv 11(mod.7); -19 \equiv +1(mod.5)$.

(中譯):
定義. 若一給定的數，我們稱之爲模，除盡兩個數的差，我們稱這兩個數 對於這模同餘，否則，不同餘。若屬第一種情況，其中的一個數稱爲另一個數的剩餘；若是第二種情況，稱爲非剩餘。例如，32 和 11 爲模 7 同餘，因爲這兩數的差 21 被 7 整除。以一個符號表示同餘對於簡化計算是非常有用的：爲此，由於與兩個數字的相等類似，我們用符號 $\equiv$ 來表示，爲免含糊，如需要，可加入括上的模。例如，§.1.可以寫成 $32 \equiv 11(mod.7); -19 \equiv +1(mod.5)$.

定義：同餘

設 $m \neq 0$，若 $m \mid a-b$，即 m 整除 $a-b$，或 $a-b=km$ (其中 k 爲整數，k 爲 0，正整數或負整數)，則稱:

1. a 同餘於 b 模 m
2. b 是 a 對模 m 的剩餘
3. 記作 $a \equiv b(\text{mod } m)$

若 a 同餘於 b 模 m，亦會有 b 同餘於 a 模 m，所以簡單地稱 a 與 b 對於模 m 同餘。

若 $a \equiv b(\text{mod } m)$，可以證明 $a \equiv b(\text{mod} - m)$：

1. $a - b = km$
2. $a - b = (-k) \times (-m)$
3. $\therefore a \equiv b(\text{mod} - m)$

所以，除特別原因外，討論同餘的時候，一般假定模爲正整數。

定義：最小剩餘

若 $a \equiv b(\text{mod } m)$，

1. 若 $0 \leq b < m$，則稱 b 是 a 對模 m 的最小非負剩餘；
2. 若 $0 < b < m$，則稱 b 是 a 對模 m 的最小正剩餘；
3. 若 $-\frac{m}{2} < b \leq \frac{m}{2}$，或 $-\frac{m}{2} \leq b < \frac{m}{2}$ 則稱 b 是 a 對模 m 的絕對最小剩餘。

等價關係

高斯在引入同餘的時候，指出「由於與兩個數字的相等類似，我們用符號 $\equiv$ 來表示”」。他所指的「類似」是指甚麼?其實，他是指「相等 ”=” 和同餘 ”≡” 都是等價關係」。

一種關係relation稱爲等價關係equivalence relation，必須具備以下三個性質:

1. 這關係是自反的reflexive
2. 這關係是對稱的symmetric
3. 這關係是傳遞的transitive

1. 在討論中的事物中，若任何其中的事物 A，必與其自身有這種關係，則稱這種關係爲「自反關係」，例如：
   (a) 對於任何一個某甲,某甲都與自己是”同齡”的,所以”同齡”是一個自反關係。
   (b) 對於整數,任何一個數 A 總不”大於” A，所以”大於”不是自反的。
2. 在討論的事物中，對於任意的 A 與 B，若 A 與 B 存在這種關係，則 B 與 A 都有這種關係，則稱這種關係爲「對稱關係」，例如：
   (a) 對於任意的兩個三角形 A 與 B，A 與 B 相似，則一定有 B 與 A 相似，所以三角形的相似關係是一種「對稱關係」。
   (b) 對於兩個人 A 與 B，A 是 B 的父親，則 B 必定不是 A 的父親。對於人類來說，「X 是 Y 的父親」不是一種「對稱關係」。
3. 在討論的事物中，對於任意的 A，B 與 C，若 A 與 B，且 B 與 C 都存在這種關係，則 A 與 C 都有這種關係，則稱這種關係爲「傳遞關係」，例如：

(a) 對於任意的三角形 A，B 與 C，若 A 全等於 B，且 B 全等於 C，則必定有 A 全等於 C，所以三角形的全等是一種「傳遞關係」。

(b) 對於任意的三個整數 A，B 與 C，若 $A > B$，$B > C$，則有 $A > C$，所以「$>$」是傳遞的。

(c) 對於任何三個人甲，乙與丙，若甲與乙認識，乙與丙認識，不一定有甲與丙認識，所以「認識」不是傳遞的。

在以上的示例中:

關係	自反的	對稱的	傳遞的
同齡	√	√	√
大於	×	×	√
三角形的相似	√	√	√
X 是 Y 的父親	×	×	×
三角形的全等	√	√	√
認識	√	√	×
相等	√	√	√

在以上的示例中，「同齡」、「三角形的相似」、「三角形的全等」及「相等」都是等價關係。

同餘是一種等價關係

對於任何整數 a, b, c 及模 m，

(A). 同餘是自反的：
$m \mid (a - a) = 0$
所以 $a \equiv a (\text{mod } m)$
所以同餘是自反的。

(B). 同餘是對稱的：
若 $a \equiv b (\text{mod } m)$，有 $a - b = km$；
所以 $b - a = (-k)m, \quad b \equiv a (\text{mod } m)$
所以同餘是對稱的。

(C). 同餘是傳遞的：
若 $a \equiv b (\text{mod } m), b \equiv c (\text{mod } m)$
$a - b = km, b - c = hm$
$a - c = a - b + b - c = km + hm = (k + h)m$
所以 $a \equiv c (\text{mod } m)$
所以同餘是傳遞的。

由 (A)，(B)，(C)，可以得知同餘是一種等價關係。

同餘式的相加

若 (i) $x \equiv a (\text{mod } m)$、
(ii) $y \equiv b (\text{mod } m)$，則

$$x + y \equiv a + b (\text{mod } m)$$

1. 由 $x \equiv a (\text{mod } m)$， 有 $x - a = hm$
2. $x = a + hm$
3. 由 $y \equiv b (\text{mod } m)$， 有 $y - b = km$
4. $y = b + km$
5. $x + y = a + b + (h + k)m$
6. $(x + y) - (a + b) = (h + k)m$
7. 所以 $x + y \equiv a + b (\text{mod } m)$

如一般的方程一樣，在同餘式的兩邊同時加上同一個數，同餘式仍然維持不變。

若 $x \equiv a(\text{mod } m)$，則

$$x + b \equiv a + b(\text{mod } m)$$

因爲 $b \equiv b(\text{mod } m)$

$x \equiv a(\text{mod } m)$

所以 $x + b \equiv a + b(\text{mod } m)$

若 $x \equiv a(\text{mod } m)$，則

$$nx \equiv na(\text{mod } m)$$

$$\underbrace{x + x + \cdots + x}_{n\text{ 項}} \equiv \underbrace{a + a + \cdots + a}_{n\text{ 項}}(\text{mod } m)$$

$$nx \equiv na(\text{mod } m)$$

例一: $10 \equiv 3(\text{mod } 7)$

$1000 \equiv 100 \times 3 \equiv 300(\text{mod } 7)$

$300 \equiv 6(\text{mod } 7)$

$\therefore \quad 1000 \equiv 6(\text{mod } 7)$

例:二 $365 \equiv 1(\text{mod } 7)$

$3650 \equiv 10 \equiv 3(\text{mod } 7)$

例三: 2012 年 12 月 17 日是星期一

2022 年 12 月 17 日 是由今天起再加 3650+2 日 (2016年，2020年爲閏年)

所以， 2022 年 12 月 17 日 是星期六 (星期一再加$3 + 2$ 日)

同餘式的相減

若 (i) $x \equiv a(\text{mod } m)$

(ii) $y \equiv b(\text{mod } m)$，則

$$x - y \equiv a - b(\text{mod } m)$$

1. 由 $x \equiv a(\text{mod } m)$，
   有 $x - a = hm$，$x = a + hm$
2. 由 $y \equiv b(\text{mod } m)$，
   有 $y - b = km$，$y = b + km$
3. $x - y = a - b + (h - k)m$，
   $(x - y) - (a - b) = (h - k)m$
4. 所以 $x - y \equiv a - b(\text{mod } m)$

如加法一樣，在同餘式的兩邊減去同一個數，同餘式仍然維持不變， 若 $x \equiv a(\text{mod } m)$，則

$$x - b \equiv a - b(\text{mod } m)$$

同餘式的相乘

若 (i) $x \equiv a(\text{mod } m)$

(ii) $y \equiv b(\text{mod } m)$，則

$$xy \equiv ab(\text{mod } m)$$

1. 由 $x \equiv a(\text{mod } m)$，
   有 $x - a = hm$，$x = a + hm$
2. 由 $y \equiv b(\text{mod } m)$，
   有 $y - b = km$，$y = b + km$
3. $xy = ab + (ak + bh + hkm)m$，$xy - ab = (ak + bh + hkm)m$
4. 所以 $xy \equiv ab(\text{mod } m)$

如加法一樣，在同餘式的兩邊乘同一個數，同餘式仍然維持不變， 若 $x \equiv a(\text{mod } m)$，則

$$bx \equiv ab(\text{mod } m)$$

同時，亦可以得到同餘式的連乘，若 $x \equiv a(\text{mod } m)$，有

$$\underbrace{x \times x \times \cdots \times x}_{n\text{ 項}} \equiv \underbrace{a \times a \times \cdots \times a}_{n\text{ 項}}(\text{mod } m) \quad \text{即} x^n \equiv a^n(\text{mod } m)$$

模的約簡

若 (i) $x \equiv a(\text{mod } m)$
(ii) $d \mid m$，即 d 整除 m，則

$$x \equiv a(\text{mod } d)$$

1. 由 $x \equiv a(\text{mod } m)$，有 $x - a = km$；
2. $d \mid m$，有 $m = qd$；
3. $x - a = km = (kq)d$
4. 所以，$x \equiv a(\text{mod } d)$

同餘式的約簡

不一定可以約簡同餘式。如: $18 \equiv 48 \equiv 8(\text{mod } 10)$，$6 \times 3 \equiv 6 \times 8(\text{mod } 10)$，惟 $3 \not\equiv 8(\text{mod } 10)$

若 $ca \equiv cb(\text{mod } m)$，則

$$a \equiv b(\text{mod } \frac{m}{(c,m)})$$

其中 (c,m) 爲 c 與 m 的最大公約數。

1. $ca \equiv cb(\text{mod } m)$，$ca - cb = km$；
2. $\frac{c}{(c,m)}(a-b) = k\frac{m}{(c,m)}$
3. 因爲 $\frac{c}{(c,m)}$ 和 $k\frac{m}{(c,m)}$ 再沒有其他公因數，他們互質，
4. 又 $\frac{m}{(c,m)} \mid \frac{c}{(c,m)}(a-b)$，
   所以 $\frac{m}{(c,m)} \mid (a-b)$，
5. 故 $a \equiv b(\text{ mod } \frac{m}{(c,m)})$。

若 $(c,m) = 1$、 $ca \equiv cb(\text{mod } m)$則，

$$a \equiv b(\text{mod } m)$$

例一：

$$\begin{aligned} 18 &\equiv 48(\text{ mod } 10) \\ (2,10) &= 2 \\ \frac{18}{2} &\equiv \frac{48}{2}(\text{ mod } \frac{10}{2}) \\ 9 &\equiv 24(\text{ mod } 5) \end{aligned}$$

例二：

$$\begin{aligned} 18 &\equiv 51(\text{ mod } 11) \\ (3,11) &= 1 \\ \frac{18}{3} &\equiv \frac{51}{3}(\text{ mod } \frac{11}{1}) \\ 6 &\equiv 17(\text{ mod } 11) \end{aligned}$$

例三：常見的 3、9、11 的整除性檢定方法，可以如下證明:

1. 以檢定 31415926 能否被 3 整除爲例，因爲 $10 \equiv 1(\text{mod } 3)$、$10^n \equiv 1^n \equiv 1(\text{mod } 3)$
$$\begin{aligned} 31415926 &= 3 \times 10^7 + 1 \times 10^6 + 4 \times 10^5 + 1 \times 10^4 + 5 \times 10^3 + 9 \times 10^2 + 2 \times 10^1 + 6 \\ &\equiv 3 \times 1 + 1 \times 1 + 4 \times 1 + 1 \times 1 + 5 \times 1 + 9 \times 1 + 2 \times 1 + 6(\text{mod } 3) \\ &\equiv 3 + 1 + 4 + 1 + 5 + 9 + 2 + 6 \equiv 31 \not\equiv 0(\text{mod } 3) \end{aligned}$$
由 $3 + 1 + 4 + 1 + 5 + 9 + 2 + 6 = 31$ 不能被 3 整除，可以得知 31415926 不能被 3 整除。

2. 以檢定 31415926 能否被 9 整除爲例，因爲 $10 \equiv 1 \pmod 9$、$10^n \equiv 1^n \equiv 1 \pmod 9$
$$\begin{aligned} 31415926 &= 3\times 10^7 + 1\times 10^6 + 4\times 10^5 + 1\times 10^4 + 5\times 10^3 + 9\times 10^2 + 2\times 10^1 + 6 \\ &\equiv 3\times 1 + 1\times 1 + 4\times 1 + 1\times 1 + 5\times 1 + 9\times 1 + 2\times 1 + 6 \pmod 9 \\ &\equiv 3+1+4+1+5+9+2+6 \equiv 31 \not\equiv 0 \pmod 9 \end{aligned}$$
因 $3+1+4+1+5+9+2+6 = 31$ 不能被 9 整除，故 31415926 不能被 9 整除。

3. 以檢定 31415926 能否被 11 整除爲例，因爲 $10 \equiv -1 \pmod{11}$，$10^n \equiv (-1)^n \pmod{11}$
$10^1 \equiv -1 \pmod{11}$、$10^2 \equiv 1 \pmod{11}$、$10^3 \equiv -1 \pmod{11}$、$\cdots$
$$\begin{aligned} 31415926 &= 3\times 10^7 + 1\times 10^6 + 4\times 10^5 + 1\times 10^4 + 5\times 10^3 + 9\times 10^2 + 2\times 10^1 + 6 \\ &\equiv 3\times(-10) + 1\times 1 + 4\times(-1) + 1\times 1 + 5\times(-1) + 9\times 1 + 2\times(-1) + 6 \pmod{11} \\ &\equiv -3+1-4+1-5+9-2+6 \equiv 3 \not\equiv 0 \pmod{11} \end{aligned}$$
由 $-3+1-4+1-5+9-2+6 = 3$ 不能被 11 整除，得知 31415926 不能被 11 整除。

例四：證明 $x^2 + y^2 = 403$ 沒有整數解：

1. 若 x爲奇數，$x = 2m+1$，
$x^2 = 4m^2 + 4m + 1 \equiv 1 \pmod 4$；
2. 若 x爲偶數，$x = 2n$，
$x^2 = 4n^2 \equiv 0 \pmod 4$；
3. $x \equiv 0 \pmod 4$ 或 $x \equiv 1 \pmod 4$；
4. 同理，$y \equiv 0 \pmod 4$ 或 $y \equiv 1 \pmod 4$；
5. 由此, 對於模 4, $x^2 + y^2$ 只能與 0、1 或 2 同餘。
6. 因爲 $403 \equiv 3 \pmod 4$，所以 $x^2 + y^2 = 403$ 沒有整數解。
7. 亦可如上概推 $x^2 + y^2 = 4m + 3$ 沒有整數解。

加法恆等元

對於任何整數 a，總存在整數 x 使得
$$a + x \equiv x + a \equiv a \pmod m$$
整數 x 爲對於模 m 的加法恆等元additive identity，對於任何模 m，0 都是加法恆等元。

1. 對於任何模 m，$a + km \equiv km + a \equiv a \pmod m$，所以 km 都是模 m 的加法恆等元。
2. 例如，對於模 5，加法恆等元是 $\cdots$、0、5、10、15、$\cdots$；
3. 惟在對模 m 的最小非負剩餘中，即 0、1、2、$\cdots$、$m-1$ 中，只有 0 是加法恆等元。

加法逆元

對於任何整數 a，總存在整數 x 使得
$$a + x \equiv x + a \equiv 0 \pmod m$$
整數 x 稱爲 a 對於模 m 的 加法逆元additive inverse。顯然，$-a$ 是 a 的加法逆元。

對於模 m，加法逆元不是唯一的，因爲 $a + (km - a) \equiv (km - a) + a \equiv 0 \pmod m$，所以 $(km - a)$ 都是 a 對於模 m 的加法逆元。

例如:

a) $2+3 \equiv 0 \pmod 5$

b) $2+8 \equiv 0 \pmod 5$

c) $2+13 \equiv 0 \pmod 5$

d) $2+18 \equiv 0 \pmod 5$

對於模 5，3、8、13、18 都是 2 的加法逆元。

惟在對模 m 的最小非負剩餘中，即 0、1、2、$\cdots$、$m-1$，a 的加法逆元只有一個。在模 5 的最小非負剩餘中，只有 3 是 2 的加法逆元。

若只考慮最小非負剩餘，

a) $2+3 \equiv 0 \pmod 5$
對於模 5，2 的加法逆元是 3。

b) $2+4 \equiv 0 \pmod 6$
對於模 6，2 的加法逆元是 4。

c) $2+5 \equiv 0 \pmod 7$
對於模 7，2 的加法逆元是 5。

d) $2+6 \equiv 0 \pmod 8$
對於模 8，2 的加法逆元是 6。

由以上例子可以得知，對於不同的模，一個數的加法逆元會不同。

乘法恆等元

對於整數 a，總存在一個整數 x 使得

$$ax \equiv xa \equiv a \pmod m$$

整數 x 稱爲乘法恆等元multiplicative identity。顯然，對於任何模 m，1 是乘法恆等元。

因爲 $a(km+1) \equiv (km+1)a \equiv a \pmod m$，所以 $(km+1)$ 都是模 m 的乘法恆等元，例如:

a) $2 \times 1 \equiv 2 \pmod 5$

b) $2 \times 6 \equiv 2 \pmod 5$

c) $2 \times 11 \equiv 2 \pmod 5$

d) $2+16 \equiv 2 \pmod 5$

對於模 5，1、6、11、16 都是 2 的乘法恆等元。

惟在對模 m 的最小非負剩餘中，即 0、1、2、$\cdots$、$m-1$，只有 1 是乘法恆等元。

乘法逆元

對於一個整數 a, 若存在一個整數 x 使得

$$ax \equiv xa \equiv 1 \pmod m$$

則稱整數 x 爲 a 對於模 m 的乘法逆元multiplicative inverse，並記作 a^{-1}

在模算術中，對於一個給定的模，不是每一個數都必定有乘法逆元的。

顯然，$0 \times a \equiv 0 \not\equiv 1 \pmod m$，0 沒有乘法逆元。

以模 10 爲例，右表爲模 10 的最小非負剩餘乘法表，可以見到 0、2、4、5、6、8 都沒有乘法逆元，而

1. $1 \times 1 \equiv 1 (\text{mod } 10)$，$1^{-1} \equiv 1 (\text{mod } 10)$
2. $3 \times 7 \equiv 1 (\text{mod } 10)$，$3^{-1} \equiv 7 (\text{mod } 10)$
3. $7 \times 3 \equiv 1 (\text{mod } 10)$，$7^{-1} \equiv 3 (\text{mod } 10)$
4. $9 \times 9 \equiv 1 (\text{mod } 10)$，$9^{-1} \equiv 9 (\text{mod } 10)$

×	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

右圖爲模 5 的最小非負剩餘乘法表，除 0 以外，每一個數都有乘法逆元。

1. $1 \times 1 \equiv 1 (\text{mod } 5)$，$1^{-1} \equiv 1 (\text{mod } 5)$
2. $2 \times 3 \equiv 1 (\text{mod } 5)$，$2^{-1} \equiv 3 (\text{mod } 5)$
3. $3 \times 2 \equiv 1 (\text{mod } 5)$，$3^{-1} \equiv 2 (\text{mod } 5)$
4. $4 \times 4 \equiv 1 (\text{mod } 5)$，$4^{-1} \equiv 4 (\text{mod } 5)$

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

因爲在模算術中，除法並不是封閉的(即整數除整數並不一定是整數)，在需要進行類似「除法」的運算時，乘法逆元便擔當著非常重要的角式。

> 若 a 與 m 互質(即 $(a, m) = 1$)，a 必定有乘法逆元。

1. 因爲 $(a, m) = 1$，由「裴蜀定理」，
   存在整數 h、k 使得 $ah + mk = 1$
   故 $ah + mk \equiv 1 (\text{mod } m)$，$ah \equiv 1 (\text{mod } m)$
2. h 便是 a 的乘法逆元。

同餘的應用：次冪與連續平方法

質數的討論，過往多限於有關純數學的討論，可是在現今數字化的年代，質數卻又變得非常有用和重要，在私人信息，密函傳送方面，質數與及同餘的計算更大派用場，是以在這先討論一些有關同餘的計算。

在密碼學中，很多時候需要求一個大數的高次冪對於以另一個大數爲模的同餘，例如：計算 $12153688313^{7814} (\text{mod } 19919)$，$12153688313^{7814}$ 約有 10 萬個位，求被 19919 除所得的餘數，其繁複程度可想而知。可是，在日常的應用，尤其是商業上，甚或軍事上的應用，上述使用的數字根本談不上，何解？因爲，這數字是太小了，計算亦太簡單!!!

爲展示求一個數的高次冪對於另一個數爲模的同餘，先以幾個簡單的數字作爲示例：

例： 求 2^{277} 對模 13 的最小非負剩餘。

1. 先化 277 爲 2 進數，$277 = 100010101_2$，
   並迭次將 2 連續平方，有
   $2^1 \equiv 2 (\text{mod } 13)$
   $2^2 \equiv 4 (\text{mod } 13)$
   $2^4 \equiv 16 \equiv 3 (\text{mod } 13)$
   $2^8 \equiv 9 (\text{mod } 13)$
   $2^{16} \equiv 81 \equiv 3 (\text{mod } 13)$
   $2^{32} \equiv 9 (\text{mod } 13)$
   $2^{64} \equiv 81 \equiv 3 (\text{mod } 13)$
   $2^{128} \equiv 9 (\text{mod } 13)$
   $2^{256} \equiv 81 \equiv 3 (\text{mod } 13)$

2. 因 $2^{277} \equiv 2^{1+4+16+256} (\text{mod } 13)$，所以

$$\begin{aligned} 2^{277} &\equiv 2^1 \times 2^4 \times 2^{16} \times 2^{256} (\text{mod } 13) \\ &\equiv 2 \times 3 \times 3 \times 3 (\text{mod } 13) \\ &\equiv 18 \times 3 (\text{mod } 13) \\ &\equiv 5 \times 3 (\text{mod } 13) \\ &\equiv 15 \equiv 2 (\text{mod } 13) \end{aligned}$$

3. 所以 2^{277} 被 13 除餘 2。