6 中國剩餘定理

“孫子算經”是中國古代一部優秀數學著作，確切的出版年月無從考證。其中有“物不知其數”一問，原文如下：“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？”

這類的問題在中國古代數學史上有不少有趣的名稱。除上所說的“物不知其數”外，還有稱之為“鬼谷算”的，“秦王暗點兵”的，“神奇妙算”的，“大衍求一術”的，…，等等。

這問題是屬於數論中算術數列（等差數列）的範疇。在這節裡，我們將對這樣的問題進行更為一般的探索。值得一提的是，本節所用的同餘符號“≡”是高斯在 1799 年時所引進，發明的。由於同餘符號“≡”的方便好用，後來廣為數學家所使用。可以說是一個家喻戶曉的數學符號。

6.1 等差數列與同餘式

首項是 2，而公差為 5 的等差數列是

$$2,7,12,17,22,\cdots,$$

但被 5 除之，餘數為 2 的同餘數列為

$$\cdots,-18,-13,-8,-3,2,7,12,17,22,\cdots.$$

因此等差數列是同餘數列的一部份。為了方便，將被 5 除之，餘數為 2 的同餘數列

$$\cdots,-18,-13,-8,-3,2,7,12,17,22,\cdots$$

用同餘式

$$x \equiv 2 \pmod{5}$$

表示。因此同餘式

$$x \equiv a \pmod{n}$$

代表所有被 n 除之，餘數為 a 的整數。

6.2 中國剩餘定理

韓信叫兩個人去清點他的士兵，如果他們都用很偷懶的幾個士兵一數的點兵方式，回報給韓信的可能是“士兵m個一數剩a人；n個一數剩b人”這樣的結果。為了解決這樣的“韓信點兵問題”，我們需要判別兩個同餘式（或等差數列）何時有共同的解，而且如何去求它們的共同解。這就是有名的中國剩餘定理（或孫子定理）。

定理 6.1 (中國剩餘定理) 設m,n是互質的正整數，a,b為整數，則同餘式

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

有共同的整數解x_0，且所有共同的整數解x也構成一個同餘式為

$$x \equiv x_0 \pmod{mn}.$$

【証明】因為m,n是互質的正整數，所以可以找到整數x, y使得（根據定理 5.2）

$$mx - ny = b - a.$$

令$x_0 = mx + a = ny + b$，則

$$\begin{cases} x_0 \equiv a \pmod{m}, \\ x_0 \equiv b \pmod{n}. \end{cases}$$

現在令整數x滿足

$$\begin{aligned} \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} &\Rightarrow \begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases} \\ &\Rightarrow x - x_0 \equiv 0 \pmod{mn} \\ &\Rightarrow x \equiv x_0 \pmod{mn}. \end{aligned}$$

因此所有共同的整數解x會滿足同餘式

$$x \equiv x_0 \pmod{mn}.$$

中國剩餘定理告訴我們：兩個公差互質的等差數列的交集亦為一個等差數列（事實上，此新等差數列的公差為前兩個等差數列公差的乘積）。

例題 6.1　解同餘式

$$\begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{7}, \\ x \equiv 4 \pmod{11}. \end{cases}$$

【解】因為同餘式

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases} \Rightarrow x \equiv 17 \pmod{35},$$

所以

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases} \Rightarrow \begin{cases} x \equiv 17 \pmod{35} \\ x \equiv 4 \pmod{11} \end{cases}$$

$$\Rightarrow x \equiv 367 \pmod{385}.$$

最後這步，技巧熟練的話，會比較快找到 367 這個數字。你得出 367 的技巧是好的嗎？

6.3 同餘式的應用

例題 6.2　試求滿足$1+3^y = 2^x$的非負整數x與y。

【解】我們對方程式取模 8 得到

$$1+3^y \equiv 2^x \pmod{8}.$$

根據y的奇、偶性可分為

(1) 當y為偶數時，因為$3^y \equiv 1 \pmod{8}$，所以

$$2^x \equiv 1+3^y \equiv 2 \pmod{8} \Rightarrow x = 1.$$

由此得到$(x, y) = (1, 0)$。

(2) 當y為奇數時，因為$3^y \equiv 3 \pmod{8}$，所以

$$2^x \equiv 1+3^y \equiv 4 \pmod{8} \Rightarrow x = 2.$$

由此得到$(x,\ y)\ =\ (2,\ 1)$。

綜合(1)及(2)得到

$$(x,\ y)\ =\ (1,\ 0)\text{ 或 }(2,\ 1).$$

例題 6.3 證明：被 8 除之，餘數為 7 的正整數n不能表為三個整數的平方和。

【証明】設整數x, y, z滿足

$$x^2+y^2+z^2=n,$$

其中$n\equiv 7 \pmod 8$。因此

$$x^2+y^2+z^2\equiv 7 \pmod 8;$$

但這與同餘式

$$\begin{cases} x^2\equiv 0,1,4 \pmod{8} \\ y^2\equiv 0,1,4 \pmod{8} \\ z^2\equiv 0,1,4 \pmod{8} \end{cases}$$

矛盾。因此被 8 除之，餘數為 7 的正整數n不能表為三個整數的平方和。

例題 6.4 試求$5x^3+11y^3+13z^3=0$的整數解x, y, z。

【解】假設$(x,\ y,\ z)\ \neq\ (0,\ 0,\ 0)$且$(x,\ y,\ z)=\ 1$的整數$x, y, z$滿足

$$5x^3+11y^3+13z^3=0.$$

因此

$$5x^3+11y^3\equiv 0 \pmod{13}.$$

又

$$\begin{cases} x^3 \equiv 0,1,5,8,12 \pmod{13} \\ y^3 \equiv 0,1,5,8,12 \pmod{13} \end{cases}$$
$$\Rightarrow \begin{cases} 5x^3 \equiv 0,1,5,8,12 \pmod{13}, \\ 11y^3 \equiv 0,2,3,10,11 \pmod{13}, \end{cases}$$

所以由上式的各種組合可推得

$$\begin{cases} 5x^3 \equiv 0 \pmod{13} \\ 11y^3 \equiv 0 \pmod{13} \end{cases} \Rightarrow \begin{cases} 13 \mid x \\ 13 \mid y \end{cases} \Rightarrow 13 \mid x, 13 \mid y, 13 \mid z.$$

此與互質的假設矛盾；因此 $x = y = z = 0$ 為唯一的整數解。

習題 6.1　解同餘式

$$\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 3 \pmod{7}, \\ x \equiv 9 \pmod{11}. \end{cases}$$

習題 6.2　如果整數 x, y, z 滿足 $x^3 + y^3 = z^3$，則證明 x, y, z 至少有一個是 7 的倍數。

習題 6.3　試求 $5x^2 + 13y^2 = 7z^2$ 的整數解 x, y, z。

習題 6.4　試求 $x^2 + 3xy - 2y^2 = 122$ 的整數解 x, y。[4]

[4] 配平方之後再取模 17。

習題 6.5　小明將他的三個小孩子(大毛、二毛、三毛)的零用錢存起來，一共有七筆如下(單元：元)：

130,　320,　430,　790,　3500,　3620,　4160.

迷糊的小明早已記不得哪幾筆錢是那個小孩子的。但是小明知道三毛僅有一

筆錢，大毛的錢數是二毛的六倍。聰明的你，能否幫小明搞清楚這筆糊塗帳？

習題 6.6　有一個四位數的正整數且此四位數正整數恰為其各位數字和的立方。試確定此四位數的正整數。

習題 6.7　試證明由 2,3,4,5,6,7,8 七個數字所組合成的 $7!$ 個七位數正整數中沒有一個是完全平方數。

習題 6.8　從 2,3,5,7,9 五個數字中剔除一個數字之後，將剩下的四個數字經適當的排列之後，得到一個完全平方數，試求此完全平方數。[5]

[5] 利用模 9 來剔除數字，用模 10 及模 4 來確認此完全平方數。

習題 6.9　四位數正整數 $aabb$ 為完全平方數，試求此四位數正整數。如果改為六位數正整數 $aaabbb$ ，那結果又如何？

習題 6.10　阿三幫他父親記帳，有一則糊塗帳這樣記著：

"哈密瓜 37 顆計□4Δ7 元"

事後，阿三僅知哈密瓜每顆為整數元且數字Δ比數字□大。你能知道哈密瓜一顆是多少元嗎？

習題 6.11　設 a,b 為整數且滿足 $24\,|\,(ab+1)$ 。證明： $24\,|\,(a+b)$ 。

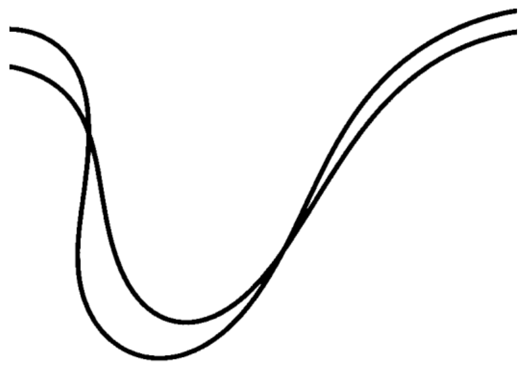
習題 6.12　欲將實數線上的所有格子點塗上顏色，規定相距 3 單位的任兩個整數點必須是不同色；而且相距 4 單位的任兩個整數點也是不同色。試問

(1) 僅用 2 種顏色是否可以完成。

(2) 僅用 3 種顏色是否可以完成。

動手玩數學

神探福爾摩斯追蹤一位騎腳踏車逃跑的盜匪。下圖是盜匪腳踏車前後輪所留下的軌跡。如果你是福爾摩斯的話，你會認為盜匪是騎往哪個方向逃跑的？



挑戰題

有一個正整數 n 使得

$$120^4 + 272^4 + 315^4 + n^4 = 353^4$$

試求此正整數 n 的值。[6]

[6] 將兩邊分別對 2, 3, 5, 11 取同餘。

中國剩餘定理

中國古代的數論知識是遠遠領先其他國家的，中國剩餘定理是其中最具代表性的定理，也是當今數論上常用的一種技術。事實上，中國人習慣稱它為『孫子問題』，用來解決“物不知其數”及“韓信點兵”的問題。宋代數學家秦九韶的“大衍求一術”就是有系統的討論一次同餘方程式解的公式。這與後來高斯的解法本質上是等價的。