大衍求一術與二元一次不定方程

文耀光

摘要:「大衍求一術」是中國古代數學家秦九韶用以解一次同餘式組的方法。本文旨在介紹何謂大衍求一術, 以及如何將之轉化爲一遞歸求解形式 (recursive method of solution), 並應用此法求解二元一次不定方程。

I. 引言

給定兩個自然數 a 和 b, 要求取它們的最大公因數 $GCD(a,b)$ 有好幾種方法。現時香港小學數學課程裡討論的「列舉法」、「質因數分解法」和「短除法」都是常用的方法。不過當 a 和 b 的數值很大時, 使用「輾轉相除法」(Euclidean Algorithm) 會比較方便和快捷。此法早在古希臘時代已經被發現, 並且收錄在歐幾里德 (Euclid) 的名著「幾何原本」(約公元前300年) 之中, 其原理如下:

定理1: 設 a、b 是自然數, 且 $a \leq b$。

若 $b = aq + r$, 其中 $0 \leq r < a$, 則 $GCD(a,b) = GCD(r,a)$。

此定理表明, 如果「輾轉」(意指重覆) 使用除法, 可以求取任意兩個自然數的最大公因數。由於每次所產生的被除數 a 及除數 r, 都比原來的被除數 b 及除數 a 爲小, 且 r 爲非負整數, 所以輾轉相除有限步之後, 一定會產生以下的結果:

$$GCD(a,b) = GCD(r,a) = \cdots = GCD(0,c) = c。$$

例1: 求299與247的最大公因數。

解:

1	299	247	4
	247	208	
1	52	39	3
	39	39	
	13		

(用247除299, 得商數1及餘數52)

(用52除247, 得商數4及餘數39)

(用39除52, 得商數1及餘數13)

(用13除39, 得商數3及餘數0)

$\therefore\ GCD(247,299) = GCD(52,247)$

$$
\begin{aligned}
&= GCD(39, 52)\\
&= GCD(13, 39)\\
&= GCD(0, 13)\\
&= 13。
\end{aligned}
$$

輾轉相除法除了可以用來求最大公因數之外, 還可以用來解不定方程。它的原理是基於以下的結果:

定理2: 設 a、b 爲自然數。

若 $d = GCD(a, b)$, 那麼不定方程 $ax + by = d$ 有整數解。

推論1: 設 a、b 爲自然數。

若 $GCD(a, b) = 1$, 那麼不定方程 $ax + by = 1$ 有整數解。

定理3: 設 a、b、c 爲自然數。

不定方程 $ax + by = d$ 有整數解 當且僅當 $GCD(a, b)|d$ 。

有關這些定理的證明, 可以參考潘承彪 (1998), 此處從略。

例2: 求不定方程 $299x + 247y = 13$ 的一般整數解。

解: 根據例1的算式, 將有餘數產生的每一步用橫式表示, 可得:

$$
\begin{aligned}
299 &= 247 + 52\\
247 &= 4 \times 52 + 39\\
52 &= 39 + 13
\end{aligned}
$$

把以上數式逐步倒推而上, 可得:

$$
\begin{aligned}
GCD(299, 247) &= 13\\
&= 52 - 39\\
&= 52 - (247 - 4 \times 52)\\
&= 5 \times 52 - 247\\
&= 5 \times (299 - 247) - 247\\
&= 5 \times 299 - 6 \times 247
\end{aligned}
$$

由此求得 $299x + 247y = 13$ 的一個特殊整數解爲 $x_0 = 5$, $y_0 = -6$。設 k 爲任意整數, 那麼:

$$299(x_0 + \frac{247k}{13}) + 247(y_0 - \frac{299k}{13}) = 13,$$

所以 $299x + 247y = 13$ 的一般整數解爲:

$$x = 5 + 19k, \quad y = -6 - 23k,$$

其中 k 爲任意整數。

這種解不定方程 $ax + by = GCD(a, b)$ 的方法, 稱爲 Extended Euclidean Algorithm (參考 Biggs(1990), Niven(1991) 或 Geddes (1992))。此法雖然簡單易明, 可是在「倒推」的過程中需要不斷整理被除數和除數的係數, 實在是一件相當繁複而且容易出錯的工作。那麼, 是否可以改良一下呢? 讓我們在下一節爲大家介紹。

II. 大衍求一術

中國人在求解一次同餘式組方面的歷史是十分悠久的, 而且成就卓越。大約在公元280至420年間出版的「孫子算經」之中, 記載有一道聞名的一次同餘式問題 (簡稱「孫子問題」) 及其答案如下:

『今有物不知其數, 三三數之剩二, 五五數之剩三, 七七數之剩二, 問物幾何?』答曰:『二十三』。

如果用現代的符號表示,「孫子問題」可以記作以下的一次同餘式組:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \quad (1)$$

如果要解同餘式組 (1), 先要解出一組正整數 α、β、γ, 使其滿足以下的同餘式組 (2):

$$\begin{cases} 35\alpha \equiv 1 \pmod 3 \\ 21\beta \equiv 1 \pmod 5 \\ 15\gamma \equiv 1 \pmod 7 \end{cases} \quad (2)$$

爲什麼呢? 因爲如果 α、β、γ 存在的話, 那麼根據同餘式組 (2) 可得:

$$\begin{cases} 35\alpha \times 2 \equiv 2 \pmod 3 \\ 21\beta \times 3 \equiv 3 \pmod 5 \\ 15\gamma \times 2 \equiv 2 \pmod 7 \end{cases}$$

由此得:

$$\begin{cases} 35\alpha\times2+21\beta\times3+15\gamma\times2\equiv2 \pmod 3 \\ 35\alpha\times2+21\beta\times3+15\gamma\times2\equiv3 \pmod 5 \\ 35\alpha\times2+21\beta\times3+15\gamma\times2\equiv2 \pmod 7 \end{cases}$$

此時易知 $35\alpha\times2+21\beta\times3+15\gamma\times2$ 爲同餘式組 (1) 的一個特殊解。如果 x 是另外一個解, 那麼 $x-(35\alpha\times2+21\beta\times3+15\gamma\times2)$ 必定是3、5、7的公倍數。由於 $lcm(3,5,7)=105$, 所以同餘式組 (1) 的解可表爲:

$$x \equiv 35\alpha\times2+21\beta\times3+15\gamma\times2 \pmod{105}。$$

明白了「孫子問題」的解法後, 可知解決問題的關鍵在於先解出一組正整數 α、β、γ, 使其滿足同餘式組 (2)。由於此題所牽涉的數字比較小, 利用「試誤法」或「大衍求一術」(見以下敍述), 可以得出 $\alpha=2$, $\beta=1$, $\gamma=1$, 因此「孫子問題」的解是:

$$x\equiv70\times2+63\times1+30\times1\equiv23 \pmod{105}。$$

「孫子問題」之解法, 可以推廣成爲以下的中國剩餘定理(Chinese Remainder Theorem):

定理3: (中國剩餘定理) 設 $m_1, m_2, \ldots, m_k$ 是兩兩互質的自然數, 且 $M = m_1\times m_2\times\cdots\times m_k$。如果存在整數 $\alpha_i (i = 1,2,\ldots,k)$ 使得

$$\begin{cases} \frac{M}{m_1}\alpha_1 \equiv 1 \pmod{m_1} \\ \frac{M}{m_2}\alpha_2 \equiv 1 \pmod{m_2} \\ \quad\vdots \\ \frac{M}{m_k}\alpha_k \equiv 1 \pmod{m_k} \end{cases}$$

那麼同餘式組:

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ x \equiv r_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv r_k \pmod{m_k} \end{cases}$$

的解可表爲: $x \equiv \frac{M}{m_1}\alpha_1 r_1 + \frac{M}{m_2}\alpha_2 r_2 + \cdots + \frac{M}{m_k}\alpha_k r_k \pmod M$。

「孫子算經」之後, 由西漢到宋朝的千餘年間, 有很多天文學家和數學家都對一次同餘式問題進行了研究, 到南宋的數學家秦九韶手中, 便發展成爲一個解聯立一次同餘式組的系統方法, 稱爲「大衍求一術」, 記載在他的著作「數書九章」之中。

所謂「大衍求一術」, 是指求整數 α 使其滿足 $\alpha G \equiv 1 \pmod m$ 的方法, 其中 m、G

是給定的互質自然數, m 稱爲「定母」,G 稱爲「衍數」, 而 α 爲「乘率」。如果 $m < G$, 則先以 m 除 G, 得餘數 G_1 (古書稱此爲「奇數」[1]), 然後求整數 α 使其滿足 $\alpha G_1 \equiv 1(\mathrm{mod}\, m)$[2]。根據「數書九章」所述, 求乘率 α 的步驟是 這樣的:

『置奇右上, 定居右下, 立天元一於左上。先以右上除右下, 所得商數與左上一相生, 入左下, 然後乃以右行上下以少除多, 遞互除之, 所得商數隨即遞互累乘, 歸左行上下 , 須使右上末後奇一而止。乃驗左上所得以爲乘率, 或奇數已見單一者便爲乘率。』

這段古文的意思是說: 「運算開始時於右上、右下分別填上 G_1 和 m, 然後於左上、左下分別填上1和0。運算時把右上、右下兩數輾轉相除, 同時把除得的商數與左上、左下兩數輪流增乘, 直至右上數變成1爲止, 此時左上數即爲所求之乘率 α。」

例3: 求同餘式 $3800k \equiv 1 \pmod{27}$ 的一個整數解。

解: 由於$3800 > 27$, 先以27除3800, 取其餘數20, 然後考慮等價的同餘式: $20k \equiv 1 \pmod{27}$。

第一步 $\begin{array}{|cc|}\hline 1 & 20 \\ 0 & 27 \\ \hline\end{array}$ (先在右上、右下分別填上20和27, 然後在左上、左下分別填上1和0。)

第二步 $\begin{array}{|cc|}\hline 1 & 20 \\ 1 & 7 \\ \hline\end{array}$ (以20除27, 得商數1及餘數7。把 7 填入右下, 並將 $1 \times 0 + 1 = 1$ 填入左下。)

第三步 $\begin{array}{|cc|}\hline 3 & 6 \\ 1 & 7 \\ \hline\end{array}$ (以7除20, 得商數2及餘數6。把6填入右上, 並將 $2 \times 1 + 1 = 3$ 填入左上。)

第四步 $\begin{array}{|cc|}\hline 3 & 6 \\ 4 & 1 \\ \hline\end{array}$ (以6除7, 得商數 1 及餘數1。把1填入右下, 並將 $1 \times 3 + 1 = 4$ 填入左下。)

第五步 $\begin{array}{|cc|}\hline 23 & 1 \\ 4 & 1 \\ \hline\end{array}$ (以1除6, 得商數 5 及餘數1。把1填入右上, 並將 $5 \times 4 + 3 = 23$ 填入左上。)

由於右上數已等於1, 此時左上數 $k = 23$ 便是同餘式 $3800k \equiv 1 \pmod{27}$ 的解。

例4: 求同餘式 $1155k \equiv 1 \pmod{13}$ 的一個整數解。

解: 由於$1155 > 13$, 先以13除1155, 取其餘數11, 然後考慮等價的同餘式: $11k \equiv 1(\mathrm{mod}\, 13)$。

第一步 $\begin{array}{|cc|}\hline 1 & 11 \\ 0 & 13 \\ \hline\end{array}$ (先在右上、右下分別填上11和13, 然後在左上、左下分別填上1和0。)

第二步 $\begin{array}{|cc|}\hline 1 & 11 \\ 1 & 2 \\ \hline\end{array}$ (以11除13, 得商數1及餘數2。把 2 填入右下, 並將 $1 \times 0 + 1 = 1$ 填入左下。)

[1]注意: 這裡的所謂「奇數」與我們現今所指的「奇數」是不同義的。
[2]讀者不妨想想爲什麼同餘式 $\alpha G \equiv 1(\mathrm{mod}\, m)$ 與 $\alpha G_1 \equiv 1(\mathrm{mod}\, m)$ 是等價的?

第三步 $\begin{array}{|cc|}\hline 6 & 1 \\ 1 & 2 \\ \hline \end{array}$ (以2除11, 得商數5及餘數1。把 1 填入右上, 並將 $5\times 1+1=6$ 填入左上。)

由於右上數已等於1, 此時左上數 $k=6$ 便是同餘式 $1155k\equiv 1 \pmod{13}$ 的解。

很明顯,「大衍求一術」與「輾轉相除法」的關係是十分密切的。如果我們把「大衍求一術」改寫成常用的「輾轉相除法」去求解一次同餘式問題, 其實亦未嘗不可。

假設要求解之同餘式爲 $\alpha G \equiv 1 \pmod{m}$, 其中 m、G 是給定的互質自然數。那麼我們可以將「大衍求一術」簡化成以下的遞歸關係 (recursive relations) 來計算乘率 α:

$$\begin{cases} c_0 = 1 \\ c_1 = q_1 \\ c_k = q_k c_{k-1} + c_{k-2}\ (1 < k \le n), \end{cases}$$

其中 n 代表輾轉相除時有非零餘數產生的次數, 而 $q_k (1 \le k \le n)$ 代表每次相除時產生的商數, 則所求乘率爲 $\alpha \equiv (-1)^n c_n \pmod{m}$。

此遞歸求解法是源自輾轉相除法的「倒推」過程 (參考錢寶琮 (1964))。要自行推導這個遞歸關係並不困難, 讀者不妨一試, 此文不會細表。不過值得一提的是: 把乘率的解表爲 $\alpha \equiv (-1)^n c_n \pmod{m}$ 會比較將 n 分成「奇」、「偶」兩種情況 (參考袁小明 (1992)) 作個別處理會比較統一和簡潔, 而且更方便把它編寫成電腦程式來進行機械化計算呢!

例5: 求同餘式 $20k \equiv 1 \pmod{27}$ 的一個整數解。(參考例3)

解:

$$\begin{array}{cccc} 2 & 20 & 27 & 1 \\ & 14 & 20 & \\ \hline 6 & 6 & 7 & 1 \\ & 6 & 6 & \\ \hline & & 1 & \end{array}$$

(用20除27, 得商數1及餘數7)
(用7除20, 得商數2及餘數6)
(用6除7, 得商數1及餘數1)
(用1除6, 得商數6及餘數0)

那麼, 我們有 $n=3$, $q_1=1$, $q_2=2$, $q_3=1$。利用上述的遞歸關係, 得:

$$c_1 = 1, \quad c_2 = 3, \quad c_3 = 4。$$

$\therefore$ 所求乘率爲 $k \equiv (-1)^n c_n \equiv -4 \equiv 23 \pmod{27}$。

例6: 求同餘式 $1155k \equiv 1 \pmod{13}$ 的一個整數解。(參考例4)

解: 仿照例4的做法, 考慮等價的同餘式: $11k \equiv 1 \pmod{13}$。

$$\begin{array}{cccc} 5 & 11 & 13 & 1 \\ & 10 & 11 & \\ \hline & 1 & 2 & 2 \\ & & 2 & \\ \hline & & & \end{array}$$

(用11除13, 得商數1及餘數2)
(用2除11, 得商數5及餘數1)
(用1除2, 得商數2及餘數0)

所以得 $n = 2$, $q_1 = 1$, $q_2 = 5$ 及 $c_1 = 1$, $c_2 = 6$。$\therefore$ 所求乘率爲 $k \equiv (-1)^n c_n \equiv 6 \pmod{27}$。

III. 以大衍求一術解不定方程

我們在第一節中討論過求解二元一次不定方程的方法, 稱爲 Extended Euclidean Algorithm。此法雖然簡單, 但缺點是「倒推」的過程相當繁複而且容易出錯。如果使用大衍求一術的話, 可以用較簡潔的步驟進行計算, 現舉例說明如下:

例7: 求 $21x + 15y = 123$ 的一般整數解。

解: 先用輾轉相除法求 GCD(21, 15)。

1	21	15	2
	15	12	
	6	3	2
	6		

(用15除21, 得商數1及餘數6)
(用6除15, 得商數2及餘數3)
(用3除6, 得商數2及餘數0)

由於 $3|123$, 所以$21x + 15y = 123$ 有整數解。若先求得方程 $21x + 15y = 3$ 的一個特殊解 x_0, y_0, 則 $21x + 15y = 123$ 的一般整數解可表爲: $x = 41x_0 + 5k$, $y = 41y_0 - 7k$, 其中 k 爲任意整數。

很明顯, 滿足同餘式 $15y \equiv 3 \pmod{21}$ 的乘率可作爲 y_0。引用輾轉相除法得: $n = 2$, $q_1 = 1$, $q_2 = 2$ 及 $c_1 = 1$, $c_2 = 3$。$\therefore$ $y_0 = (-1)^n c_n = 3$。代入 $21x + 15y = 3$ 得 $x_0 = -2$。$\therefore$ $21x + 15y = 123$ 的一般整數解可表爲: $x = -82 + 5k$, $y = 123 - 7k$, 其中 k 爲任意整數。

例8: 求不定方程 $299x + 247y = 13$ 的一般整數解。(參考例2)

解: 根據例1的輾轉相除法得: $n = 3$, $q_1 = 1$, $q_2 = 4$, $q_3 = 1$ 及 $c_1 = 1$, $c_2 = 5$, $c_3 = 6$。$\therefore$ $y_0 = (-1)^n c_n = -6$。代入 $299x + 247y = 13$ 得 $x_0 = 5$。$\therefore$ $299x + 247y = 13$ 的一般整數解可表爲: $x = 5 + 19k$, $y = -6 - 23k$, 其中 k 爲任意整數。

IV. 結語

大衍求一術是我國數學家秦九韶對數學的一個卓越貢獻, 其重要性不僅僅是爲解決一次同餘式組提供了一個有效的方法, 更重要的是它把輾轉相除法的逆推過程轉化爲一個簡單遞歸的求解形式, 大大減省了逆推時不少繁複的簡化工作 (見例2), 而其中一個重要的應用就是本文所介紹的求解二元一次不定方程的方法。

誠如吳文俊教授所言, 中國古代數學家在解決數學問題時頗著重實用性和具有機械化的特色, 對後世科研和教學都很有啓發性。例如吳文俊在 「吳文俊論數學機械

化」一書中曾經指出: 要求解 $9253k \equiv 1 \pmod{225600}$ 這道題時, D. E. Knuth (美國史丹福大學著名教授及電腦科學家) 在其名著 The Art of Computer Programming 中引述的 Euler 函數法, 即使利用一台現代化電腦也很難快速地完成任務, 因爲要涉及 $9253^{\phi(225600)}$ 的計算。反之, 使用大衍求一術則能很快完成任務。

筆者亦發覺, 現時許多新出版有關數論、離散數學或數學算法的大專參考書籍 (例如 Biggs(1990), Niven(1991) 或 Geddes (1992)), 亦很少討論如何應用大衍求一術求解不定方程的問題, 未免有點可惜。由此引發筆者的一點反思, 就是:「如果僅把數學史作一門獨立的數學科目來研究, 而不注重它與其他數學分支的互相滲透; 又或僅閱讀或教授數學史而不注重如何古爲今用, 也許對數學教育或科研方面是一個重大損失呢!」

參考書目

1. 袁小明 (1992)。「中國古代數學史略」。河北: 河北科學技術出版社。
2. 李信明 (1998)。「中國數學五千年」。臺北: 臺灣書店。
3. 李兆華 (1995)。「中國數學史」。臺北: 文津出版社。
4. 吳文俊 (1995)。「吳文俊論數學機械化」。濟南: 山東教育出版社。
5. 劉鈍、韓琦編 (1997)。「科史薪傳」。遼寧: 遼寧教育出版社。
6. 劉鈍 (1995)。「大哉言數」。遼寧: 遼寧教育出版社。
7. 錢寶琮 (1964)。「中國數學史話」。香港: 香港金文書店。
8. 文耀光、梁志強、吳銳堅 (1998)。「基礎數學引論」(第2版)。香港: 香港教育圖書公司。
9. 王懷權 (1997)。「數學的故鄉」。臺北: 學英文化事業有限公司。
10. 潘承彪 (1998)。「簡明數論」。北京: 北京大學出版社。
11. Norman Biggs (1990). Discrete Mathematics. Oxford: Clarendon Press.
12. I. Niven, H. S. Zuckerman & H. L. Montgomery (1991). An Introduction to the Theory of Numbers (5th edition). New York: John Wiley & Sons.
13. K. O. Geddes, S. R. Czapor & G. Labahn (1992). Algorithms for Computer Algebra. Massachusetts: Kluwer Academic Publishers.
14. Jean-Claude Martzloff (1997). A History of Chinese Mathematics. New York: Springer-Verlag.
15. D. E. Knuth (1968). The Art of Computer Programming: Semi-Numerical Algorithm (Vol. 2). Massachusett: Addison-Wesley.

—本文作者任教於香港教育學院—