從《九章算術》到《孫子算經》

著者／張耀祖
義守大學 財務與計算數學系

約成書於南北朝的《孫子算經》中提到“物不知數”問題，南宋數學家秦九韶提出“大衍求一術”，完整地解決了該問題，19 世紀德國數學家高斯也得到相同的結果，現在西方將其稱為“中國剩餘定理”，被認為是中國數學史上最有創造性的成就之一，在近代數位資訊領域中有非常重要的應用。

由於中文方塊字一字一音的特性，極利於數字運算，因而中國人的數位概念極為優異，加上使用先進的十進位值制，以及電腦出現前的最好的計算工具－算籌，發展出了以演算法為特色的中國數學，與發展出演繹為特色的希臘數學東西呼應，為人類數學早期發展的兩大主流。也由於優異的數字計算能力，讓中國人在解代數方程問題方面表現極為突出，比西方更早發展出解一次聯立方程組以及一次同餘方程組的系統解法。

第一類方程問題為“一次聯立方程組”，該類問題出現在漢朝的《九章算術》。《九章算術》全書分為九章，共有 246 個問題，每個問題除了題目、答案之外，還有所謂的“術”，用來說明如何解題。先看第八章“方程”，全章有十八題，其第一題原文如下：

今有上禾三秉，中禾二秉，下禾一秉，實三十九斗；上禾二秉，中禾三秉，下禾一秉，實三十四斗；上禾一秉，中禾二秉，下禾三秉，實二十六斗。

問上、中、下禾實一秉各幾何？

答曰：上禾一秉，九斗四分斗之一，
中禾一秉，四斗四分斗之一，
下禾一秉，二斗四分斗之三。

方程術曰，置上禾三秉，中禾二秉，下禾一秉，實三十九斗，於右方。中、左禾列如右方。以右行上禾遍乘中行而以直除。又乘其次，亦以直除。然以中行中禾不盡者遍乘左行而以直除。左方下禾不盡者，上為法，下為實。實即下禾之實。求中禾，以法乘中行下實，而除下禾之實。餘如中禾秉數而一，即中禾之實。求上禾亦以法乘右行下實，而除下禾、中禾之實。餘如上禾秉數而一，即上禾之實。實皆如法，各得一斗。

換用現在的說法就是：

現在，有上等稻穗三捆、中等稻穗二捆、下等稻穗一捆，共打出三十九斗稻穀；

另外，由上等稻穗二捆、中等稻穗三捆、下等稻穗一捆，共打出三十四斗稻穀；

最後，由上等稻穗一捆、中等稻穗二捆、下等稻穗三捆，共打出二十六斗稻穀。

問上等、中等、下等稻穗一捆各能打出多少稻穀？

若用符號表示則是：

$3x+2y+z=39$　　$2x+3y+z=34$

$x+2y+3z=26$　　$x=?\ y=?\ z=?$

答案是：上等稻穗一捆能打出九又四分之一斗稻穀，中等稻穗一捆能打出四有四分之一斗稻穀，下等稻穗一捆能打出二有四分之三斗稻穀。

也就是：$x = 9\frac{1}{4}$，$y = 4\frac{1}{4}$，$z = 2\frac{3}{4}$

方程的解法是：

置上禾三秉，中禾二秉，下禾一秉，實三十九斗，於右方。中、左禾列如右方。

將第一個條件的上、中、下等稻穗的捆數以及打出稻穀的斗數 3、2、1、39 分別寫在右邊。中間和左邊的作法和右邊一樣，分別寫下第二、第三個條件的上、中、下等稻穗和打出的稻穀的數量。

1	2	3	上禾
2	3	2	中禾
3	1	1	下禾
26	34	39	實

以右行上禾遍乘中行而以直除。又乘其次，亦以直除。

接下來用右邊上等稻穗的數量（3）去乘中間的每一個數字（也就是純量 3 乘上向量），之後用中間新得到的數字串（現在的說法是向量）減掉右邊的數字串（也就是向量減法運算），一直到中間數字串的上等稻穗的數字為零。

因此遍乘就是純量乘上向量，而直除就是向量減法運算。

將最右行的第一個數字 3 乘中行和左行

1	2×3	3
2	3×3	2
3	1×3	1
26	34×3	39

1×3	2×3	3
2×3	3×3	2
3×3	1×3	1
26×3	34×3	39

得到新矩陣

1	6	3
2	9	2
3	3	1
26	102	39

再將中行向量減右行向量

1	6 − 3	3
2	9 − 2	2
3	3 − 1	1
26	102 − 39	39

得到

1	3	3
2	7	2
3	2	1
26	63	39

再減一次，

1	3 − 3	3
2	7 − 2	2
3	2 − 1	1
26	63 − 39	39

得到中行的第一個數為 0

1	0	3
2	5	2
3	1	1
26	24	39

類似的方法，將右行的第一個數字 3 乘上左行，得到

3	0	3
6	5	2
9	1	1
78	24	39

以左行減去右行（一次），可得到如下左、中行第一個位置都為 0 的矩陣

0	0	3
4	5	2
8	1	1
39	24	39

然以中行中禾不盡者遍乘左行而以直除。

再以中行中等稻穗不為零的數字 5 乘左行，之後進行向量減法，一直到左行向量的中等稻穗的數字為零。

0×5	0	3
4×5	5	2
8×5	1	1
39×5	24	39

得到

0	0	3
20	5	2
40	1	1
195	24	39

左行減中行 4 次，

0 − 4×0	0	3
20 − 4×5	5	2
40 − 4×1	1	1
195 − 4×24	24	39

得到左行第二個數字也為 0

0	0	3
0	5	2
36	1	1
99	24	39

左方下禾不盡者，上為法，下為實。實即下禾之實。

法就是除數，而實是被除數。

這裡的意思是，左行下禾數不為零的，以上方的數作為除數，下方的數作為被除數。這裡的實（被除數）就是下禾的斗數（實）99/36。

0	0	3
0	5	2
36	1	1
99	24	39

求中禾，以法乘中行下實，而除下禾之實。餘如中禾秉數而一，即中禾之實。

這裡的除並不是除法，而是減（除去），如同上面的直除。

0	0	3
0	5	2
36	1	1
99	24	39

以左行的法（36）乘上中行，然後中行減左行

0	0×36 − 0	3
0	5×36 − 0	2
36	1×36 − 36	1
99	24×36 − 99	39

得到

0	0	3
0	180	2
36	0	1
99	765	39

求上禾亦以法乘右行下實，而除下禾、中禾之實。餘如上禾秉數而一，即上禾之實。

0	0	3
0	36	2
36	0	1
99	153	39

先以左行下禾之數乘上右行，然後減去左行

0	0	3×36 − 0
0	36	2×36 − 0
36	0	1×36 − 36
99	153	39×36 − 99

得到

0	0	108
0	36	72
36	0	0
99	153	1305

先以中行中禾之數乘上右行，然後減中行兩次

0	0	108 − 2×0
0	36	72 − 2×36
36	0	0 − 2×0
99	153	1305 − 2×153

得到

0	0	36
0	36	0
36	0	0
99	153	999

實皆如法，各得一斗。

各個等級的稻穗都除以捆數後，便得到每捆能打出的斗數。

0	0	1
0	1	0
1	0	0
11/4	17/4	37/4

這個演算法看起來好像很複雜，其實做法非常簡單，只用了兩個步驟，一個是遍乘，就是純量乘上向量，另外就是直除，也就是向量的減法運算，反復地使用這兩個步驟，按照設計好的路線就可以解除每一個未知數的解，這就是演算法的威力。

《九章算術》的第八章為“方程”，一共有 18 個問題，全是一次聯立方程組問題，所解未知數的數量從兩個到六個。其中除了第十三題有六個變數但只有五個方程，其餘十七題的方程數量都與變數數量相等，也就是除了第十三之外的 目都只有唯一的答案。方程章中 18 題都用“方程術”來解題，具體做法是如同上面所 明的，先將題目所給條件列成數字矩陣，再反覆使用兩個技巧：“遍乘”和“直除”，便可求得各個未知數的值。以現在的術語來說，“遍乘”就是“數字乘上向量”，“直除”就是“兩向量相減”，兩個作法中運算的事物都涉及向量，都不再是單純的數字運算，從數學意義上來說，已經進入代數的領域。

“方程術”的做法和現在大學裏線性代數教科書中所用的“高斯消去法”幾乎一樣；《九章算術》的“方程”是世界上已知最早有系統地提到一次聯立方程組及其解法的記載。2010 年美國約翰霍普金斯大學出版社出版了一本《線性代數的中國根源》（The Chinese Roots of Linear Algebra）[1]，作者為美國學者哈特（Roger Hart），書中也強調，西方到了十六、十七世紀才“發現”的一次聯立方程組解法，中國早在千年之前就已經廣為中算學者所熟知。

另外值得一提的是“方程”的第三題就出現了負數，那是因為兩行數直接同時相減，並不保證一定都是大數減小數，當相減的兩行數中有小數減大數時，就會出現負數的情形。用算籌來計算時用不同顏色的算籌代表正負，紅色算籌代表正數，黑色算籌代表負數，此外，也

1 Roger Hart, The Chinese Roots of Linear Algebra, Johns Hopkins University Press, 2010.

有處理負數的運算規則的“正負術”；將負數當成數字來處理，也是世界上最早的記載。坊間有些翻譯書提到印度是世界上最早提到負數的，這是錯誤的。

至於第二類方程“一次同餘方程”，可以說是中國古代算術中最具獨創性的成果。目前已知最早的記載在《孫子算經》中。《孫子算經》的成書年代不詳，學者根據書中提到的事物，推估約成書於南北朝。《孫子算經》上中下三卷，是唐代國子監算學館的教材和明算科的考試用 《算經十書》中的一本。《孫子算經》卷下第二十六題：

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。

這個問題被稱為“物不知數”、“物不知其數”，或是“韓信點兵”，用現在的符號表示如下：

$$X \equiv 2 \pmod 3$$

$$X \equiv 3 \pmod 5$$

$$X \equiv 2 \pmod 7$$

$$X = 2\times70+3\times21+2\times15-210 = 233-210 = 23$$

其中 $X \equiv 2 \pmod 3$ 表示“x 與 2 被 3 除同餘”。例如，$8 \equiv 5 \pmod 3$ 意思是 8 和 5 被 3 除具有相同的餘數。同餘的概念與「≡」符號是德國大數學家高斯（Gauss, Carl Friedrich, 1777-1855）最先引用，目前的數論也都這麼使用。

“物不知數”問題的答案不一定是 23，23 加上任何 105 的倍數都符合問題的要求，像這種答案不是唯一的方程稱之為“不定方程”，還有著名的“百雞問題”也是不定方程，“物不知數”也算是“不定方程”。

《孫子算經》中的“術”給出了答案的形式，可以對 3×5×7=105 個不同餘數組合的問題各給出答案，例如像“三、三數之，賸一；五、五數之，賸二；七、七數之，賸三”這樣，只換餘數，不換除數三、五、七的問題都可以解。然而，如果換了除數，例如分別被五、七、十一除等，《孫子算經》就沒再提供其他的文字，也沒有提到如何去求解除數不為三、五、七的問題。

至於如何去求解？問題的關鍵在於解法中提到的 70、21 和 15 這三個數字，70 可以理解為 2×5×7，而 21=1×3×7、15=1×3×5，這些數與三個除數三、五、七有關。只是，為何要在 70=2×5×7 這個數中多乘一個 2，另外兩個數 21 和 15 則沒有？如果換用其他除數，各要乘上多少？這些問題一直到南宋數學家秦九韶（1202-1261）在西元 1247 年所著的《數書九章》書中提出“大衍求一術”，才給出完整的答案。秦九韶得到的 果完備的程度，還超過五百多年後，德國大數學家高斯在其數論經典著作《算學講話》（Disquisitiones Arithmeticae, 1801）[2] 中所給的答案，只是高斯書中多的是給了證明，這是西方或是希臘數學的傳統，中國則沒有這樣的做法。現在將一次同餘方程組的解法稱為中國剩餘定理。中國剩餘定理在近代工程應用中極為重要，丁存生等人寫了一本書名《中國剩餘定理：在計算、編碼、密碼方面的應用》[3]，全書 7 章、224 頁，專門介紹中國剩餘定理在資訊相關領域方面的應用。

秦九韶在數學方面的傑出工作，讓許多西方科學史學者給予極高的評價，如著名的美國科學史家薩頓（George Sarton, 1884 － 1956）稱讚他“是他那個民族、他那個時代、並且確實也是所有時代最偉大的數學家之一。”也有專書介紹秦九韶的書，比利時學者李倍始（Ulrich Libbrecht）在 1973 年出版了一本《十三世紀的中國數學：秦九韶的數書九章》[4]，全書 608 頁，分為六編、23 章，第五編中從第 14 到第 22 章以 9 章的分量專門介紹中國剩餘定理，並在其中的第 18 章駁斥了許多西方學者認為大衍求一術的作法源自印度阿耶波多（The elder Aryabhata, 476-550 AD）的“粉碎法”（Kuttaka 或 Cuttaca）的說法。第 21 章則是透過比對大量古今中外的可靠史料，舉出 12 位數學家以及 1 本書、2 份手稿對於一次同餘方程組的處理，以 10 個不同的高度來做評比，結果排名第一的是 19 世紀的荷蘭數學家斯蒂爾吉斯（Stieltjes, Thomas Joannes, 1856-1894），18 世紀的瑞士大數學家歐拉（Euler, Leonard, 1707-1783）和 19 世紀的高斯並列第二，秦九韶獨居第三。在表中，歐拉、高斯的得分情形完全相同，證明的部分贏過秦九韶，然而在結果的完整性則不如。李倍始根據這個評比，說：" 考慮到秦九韶所處年代，美國著名科學史家薩頓對於秦九韶的讚揚並沒有過譽。"

有關秦九韶或是大衍求一術的專文極多，甚至還有論文目錄的文章[5]，在吳文俊先生所主編的《中國數學史大系 第五卷－兩宋》[6] 一書中，有關秦九韶的介紹就佔了全書內文 732 頁中的 436 頁，在全書六編中，從第二到第四編分為

2 Gauss C F - Werke, Band 01 - Disquisitiones Arithmeticae (Lipsiae 1801)

3 丁存生、裴定一、A. Salomaa, Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography，World Scientific Press, Singapore, 1998.

4 Ulrich Libbrect, Chinese Mathematics in the Thirteenth Century: The Shu-shu chui-chang of Ch' in Chui-shao (East Asian Science), The MIT Press, 1973; Dover, 2001.

5 王守義：有關秦九韶與《數書九章》的論文目錄 (1960-1990)，安徽科學技術出版社，1992。

6 吳文俊：中國數學史大系（五）兩宋，北京師範大學出版社，1998。

上、中、下三編來作解說，因此本文不再多作介紹。在這篇文章中，我們將重點放在大衍求一術的演算法部分，及其與之前《九章算術》的輾轉相除法，和之後的擴展歐幾里得演算法（extended Euclid's algorithm）以及近代數位影音應用中的一個重要技術——伯利根演算法（Berlekamp algorithm）之間的關聯。

我們首先從“輾轉相除法”介紹起，在中國和希臘都有求最大公因數的演算法，中國的在《九章算術》書中，希臘的在歐幾里得（Euclid，約在西元前 300 年左右）的《幾何原本》書中（約寫於西元前 300 年）；一千多年來，人們都以為中國的輾轉相除法出自《九章算術》，在 1983 年湖北發現了《算數書》[7]（是目前中國最早的數學書，大約在西元前 200 年寫成，比《九章算術》早三百多年），書中也有輾轉相除法的文字記載，讓中國在輾轉相除法的歷史往前提升三百年。三本書的相關文字列舉如下：

約分術曰：以子除母，母亦除子，子母數交等者，即約之矣。（《算數書》）

約分術曰：可半者半之；不可半者，副置分母、子之數，以少減多，更相減損，求其等也。以等數約之。（《九章算術》，方田）

設有不相等的二數，從大數中連續減去小數直到餘數小於小數，再從小數中連續減去餘數，這樣一直作下去，若餘數總是量不盡其前一個數，直到最後的餘數為一個單位，則該二數互質。（《幾何原本》，第七卷命題一）

已知兩個不互質的數，求它們的最大公度數。（《幾何原本》，第七卷命題二）

在《九章算術》書中，“約分術”的目的是要對分數作約分以求得最簡分數（分子分母兩數互質，沒有大於一的公因數），不是真的要求最大公因數。因此，如果完全按照所提的方法作，得到的只是奇數的公因數，因為任何 2 的冪次方的公因數都會在“可半者半之”的過程中被消掉。例如 12 和 18，兩數都是偶數，都“可半”，“半之”之後得到的兩數為 6 和 9，其中只有 6 為偶數，無法同時“可半”，便“副置分母、子之數，以少減多，更相減損，求其等也。”將 6 放在分子，9 放在分母，然後用大數減去小數（原文“以少減多”是說用小數去消減大數的值）

$$\frac{6}{9} \rightarrow \frac{6}{9-6=3} = \frac{6}{3} \rightarrow \frac{6-3=3}{3} = \frac{3}{3}$$

得到了分子分母相等的“等數”3，然後分子分母同時“以等數約之”，就可以得到最簡分數 2/3：

$$\frac{6/3}{9/3} \rightarrow \frac{2}{3}$$

然而，12 和 18 的最大公因數為 6，不是上面得到的數字 3。如果要不論奇偶數都可以得到最大公因數的話，就跳過“可半者半之”這一步驟，直接套用“副置分母、子之數，以少減多，更相減損，求其等也。”此時所得到的等數就是最大公因數（12 和 18 的最大公因數為 6）：

$$\frac{12}{18} \rightarrow \frac{12}{18-12=6} = \frac{12}{6} \rightarrow \frac{12-6=6}{6} = \frac{6}{6}$$

輾轉相除法的不可思議之處在於，最大公因數是透過乘除運算定義的，如果按照字面定義求解，那麼要先分別求出兩個數的所有因數，接著確定出兩個數的公因數，公因數中最大的數就是兩個數的最大公因數。求因數牽涉到因數分解的問題，數字小還好，如果數字大的話，那就是難題，目前最安全的密碼就是建立在大數分解是困難的這個特性上。用上面輾轉相除法來求最大公因數居然只需使用簡單的減法，就可以求出兩數的最大公因數，完全不管兩數的大小，這被認為是演算法的一個典範，也是演算法之祖。

接下來，我們介紹“大衍求一術”：在《孫子算經》的“物不知數”這一問題中，提到的 70、21 和 15 這三個數字中所出現的、1、1，秦九韶在《數書九章》裏稱這些數字為“乘率”，大衍求一術就是求“乘率”的演算法。為什麼 70=2×5×7 這個數中的乘率是 2，而 21=1×3×7 和 15=1×3×5 的乘率都是 1，原因是 5×7=35 乘 2 之後得到的 70 被 3 除的餘數才會是 1，否則，如果乘率取 1，得到的 1×5×7=35 被 3 除的餘數是 2，就無法提供正確的公式。乘率的意義可以由如下的式子看出：

(5×7)× 乘率≡ 1(mod 3)

用現代的說法就是，上式中的乘率就是 5×7 在被 3 除時的倒數。秦九韶稱式子中的 5×7 為“奇數”，而除數 3 為“定數”，亦即：

奇數 × 乘率≡ 1(mod 定數)

求乘率就是求被定數除時，奇數的倒數。書中求乘率的方法如下：

“大衍求一術云：

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（乘），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，以為乘率。

或奇數已見單一者，便為乘率。”

以現在的觀點來看上述文字

初始設定：

1. 在右上方放奇（數），右下方放定（數）。

2. 左上方放數字 1，左下沒提，表示左下為零。

1 奇

0 定

演算法步驟：

1. 先以右上方的奇數去除右下方的定數，得

7 彭浩：張家山漢簡《算數書》注釋，科學出版社，2001。

到的商數與左上方的 1 相乘，得到的乘積，加到左下方的 0。

2. 然後在右行的上下方，用小數去除大數，所得到的餘數會比原來的小數更小，再用餘數去除原來的小數，然後重覆這個過程。（更相減損）

3. 每次除完，所得到的商數，都用來乘上小數所在位置的左方的數字，得到的乘積，便加到大數所在位置的左方的數字上。（左右同步）

終止設定：

一直計算到右上方的奇數變為 1 為止。

此時左上方的數字就是乘率。

如果一開始的奇數已經是 1，乘率就取為 1

乘率　1

＊　＊

用一個例子來說明上述的演算法如何執行。例如“奇”取為 5 而“定”取為 17，求乘率。（如果一開始的奇數比定數大，《數書九章》提到，就用被定數除的餘數當作奇數，所算出來的乘率會是一樣。）

初始設定：

1　5

0　17

演算法步驟：

為了容易了解過程的變化，我們先將演算法步驟中的“除”改為《九章算術》輾轉相除法中的“減”來作示範。請注意右方作減法，左方作加法：

$$\begin{bmatrix}1 & 5\\ 0 & 17\end{bmatrix}\rightarrow\begin{bmatrix}1 & 5\\ 0+1 & 17-5\end{bmatrix}=\begin{bmatrix}1 & 5\\ 1 & 12\end{bmatrix}$$

$$\begin{bmatrix}1 & 5\\ 1 & 12\end{bmatrix}\rightarrow\begin{bmatrix}1 & 5\\ 1+1 & 12-5\end{bmatrix}=\begin{bmatrix}1 & 5\\ 2 & 7\end{bmatrix}$$

$$\begin{bmatrix}1 & 5\\ 2 & 7\end{bmatrix}\rightarrow\begin{bmatrix}1 & 5\\ 2+1 & 7-5\end{bmatrix}=\begin{bmatrix}1 & 5\\ 3 & 2\end{bmatrix}$$

$$\begin{bmatrix}1 & 5\\ 3 & 2\end{bmatrix}\rightarrow\begin{bmatrix}1+3 & 5-2\\ 3 & 2\end{bmatrix}=\begin{bmatrix}4 & 3\\ 3 & 2\end{bmatrix}$$

$$\begin{bmatrix}4 & 3\\ 3 & 2\end{bmatrix}\rightarrow\begin{bmatrix}4+3 & 3-2\\ 3 & 2\end{bmatrix}=\begin{bmatrix}7 & 1\\ 3 & 2\end{bmatrix}$$

若將說明用的運算部分拿掉，就成為：

$$\begin{bmatrix}1 & 5\\ 0 & 17\end{bmatrix}\rightarrow\begin{bmatrix}1 & 5\\ 1 & 12\end{bmatrix}\rightarrow\begin{bmatrix}1 & 5\\ 2 & 7\end{bmatrix}$$

$$\rightarrow\begin{bmatrix}1 & 5\\ 3 & 2\end{bmatrix}\rightarrow\begin{bmatrix}4 & 3\\ 3 & 2\end{bmatrix}\rightarrow\begin{bmatrix}7 & 1\\ 3 & 2\end{bmatrix}$$

當右上方的奇數變為 1 時，左上的 7 就是乘率。

要說明的是，演算的過程中，右行是做“更相減損”（輾轉相處）的，而演算的過程中，左右兩邊是同步運算的，不同的只是右邊是進行減法，而左邊是進行加法，也就是說，右邊減幾次，左邊就要跟著加幾次，次數必須一樣。由於這個“左加右減”的特性，王守義先生將這個“大衍求一術”稱之為“加減求一術”[8]。

現在將上面計算過程中的減法改為除法，就是秦九韶的“大衍求一術”演算法。17 除以 5，得商 3 餘 2：

$$\begin{bmatrix}1 & 5\\ 0 & 17\end{bmatrix}\rightarrow\begin{bmatrix}1 & 5\\ 0+3\times1 & 17-3\times5\end{bmatrix}=\begin{bmatrix}1 & 5\\ 3 & 2\end{bmatrix}$$

$$\begin{bmatrix}1 & 5\\ 3 & 2\end{bmatrix}\rightarrow\begin{bmatrix}1+2\times3 & 5-2\times2\\ 3 & 2\end{bmatrix}=\begin{bmatrix}7 & 1\\ 3 & 2\end{bmatrix}$$

同樣地，將說明用的運算部分拿掉：

$$\begin{bmatrix}1 & 5\\ 0 & 17\end{bmatrix}\rightarrow\begin{bmatrix}1 & 5\\ 3 & 2\end{bmatrix}\rightarrow\begin{bmatrix}7 & 1\\ 3 & 2\end{bmatrix}$$

很容易可以驗證出，7 乘 5 等於 35，被 17 除的餘數是 1。

秦九韶用“大衍求一術”這一個快速、有效的工具，為他的理論提供了保證，讓一次同餘方程組的的問題得到完全的解決，讓強勢的西方數學工作者心服口服，為中國數學在那風雨飄搖、不被承認的年代裏贏得“中國剩餘定理”這一稱號，這也是之前唯一帶有“中國”兩個字的數學結果。

接著，介紹貝祖等式。數字版本首先由法國數學家梅齊里亞克（Claude-Gaspard Bachet de Méziriac, 1581-1638）提出，法國的貝祖（Bézout, Étienne, 1730-1783）則是證明了多項式的版本，現在稱為貝祖等式（Bézout identity 或 Bézout formula），其敘述如下：

對於任意兩個整數 m 和 n，

若 d 是 m 和 n 的最大公因數，

則 d 可以表示為 m 和 n 的倍數之和，

亦即，$d=r\times m+s\times n$，其中 r 和 s 都是整數。

式子中的 r,s 兩數稱為貝祖係數（Bézout coefficients）。要求兩數 m,n 的貝祖係數，可先用輾轉相除法求出 m,n 兩數的最大公因數，再由輾轉相除法的計算過程倒推回去求得所需的貝祖係數，也就是說計算過程要進行兩次，如果只是計算一個問題，倒還無所謂，可是在工程應用中，要進行次數的量極為龐大時，要計算兩次才能求得貝祖係數就不能接受了。對此，將秦九韶的大衍求一術稍加修改，便可做到：對於任意兩個整數 m 和 n，可以同時求得最大公因數 d 以及公式中的 r 和 s 三個整數。作法如下：

首先，將大衍求一術的左右兩行擴充為左中右三行，接著，將原本置於右上、右下的“奇”和“定”改置於左上、左下，中間一行為 1 在上、0 在下，右邊一行則是 0 在上、1 在下，以此做為初始設定，如下圖所示：

奇　1　0

定　0　1

至於 m 和 n 兩數何者為“奇”、何者為“定”？沒有限制，可以任意選取，原因是，原本定數是除數，這裡沒有除數，因此，沒有限制。在此不妨假設“奇”為 m，而“定”為 n，亦即初始設定為：

m　1　0

n　0　1

有了初始設定之後，演算過程則仿照大衍求一術的作法：

1. 對於左行的數字，用小數去除大數，得到商數和餘數，將大數換成餘數，此時的餘數便成了小數，再進行一次新的除法，按照這個做法，反覆進行小數除大數，一直到左行出現零；

2. 在左行每執行一次除法運算，同時也要對中、右兩行執行一次加法運算，作法是：將左行

8 王守義：數書九章新釋，安徽科學技術出版社，1992。

小數所在列的中、右數字各乘以除法得到的商數然後加到大數所在列的中、右數字。

當左行出現零時，就停止演算，不為零的那一列的中、右方的數字提供了所要的係數 r , s。此時，零出現在上方或是下方，會有不同的處理方法。

3. 當左下方為零時，中上的數字就是 m 的係數 r，右上的數字取負號就是的係數 s ：

d r -s

0 * *

4. 當左上方為零時，中下的數字取負號就是 m 的係數 r ，右下的數字就是 n 的係數 s ：

0 * *

d r -s

例如，m=5, n=17，用上述方法求貝祖係數。

$$\begin{matrix}5&1&0\\17&0&1\end{matrix}\rightarrow\begin{matrix}5&1&0\\2&3&1\end{matrix}\rightarrow\begin{matrix}1&7&2\\2&3&1\end{matrix}\rightarrow\begin{matrix}1&7&2\\0&10&3\end{matrix}$$

得到最大公因數 d = 1，而零出現在下方，用 (3) 的公式，得到的貝祖係數 r = 7 , s = - 2 ，而貝祖等式為 1 = 7 × 5 + (-2) × 17。

上面的計算是從秦九韶的大衍求一術發展出來的，現在一般都用擴展歐幾里得演算法 (extended Euclid's algorithm) 來求貝祖係數，其初始設定與上述方法一樣，只是要將大數放在上方，終止設定也是完全一樣，都是在左方出現零的時候停止。然而，演算法的計算過程略有不同：

秦九韶的方法是在中右方進行加法，將小數所在列加上大數所在列的中右方數字乘以商數，

而擴展歐幾里得方法則是進行減法，將小數所在列減去大數所在列的中右方數字乘以商數。

同樣的例子，以秦九韶的方法將大數 17 方在上方再算一次：

$$\begin{matrix}17&1&0\\5&0&1\end{matrix}\rightarrow\begin{matrix}2&1&3\\5&0&1\end{matrix}\rightarrow\begin{matrix}2&1&3\\1&2&7\end{matrix}\rightarrow\begin{matrix}0&5&17\\1&2&7\end{matrix}$$

得到貝祖等式為。再以擴展歐幾里得方法算一次

$$\begin{matrix}17&1&0\\5&0&1\end{matrix}\rightarrow\begin{matrix}2&1&-3\\5&0&1\end{matrix}\rightarrow\begin{matrix}2&1&-3\\1&-2&7\end{matrix}\rightarrow\begin{matrix}0&5&-17\\1&-2&7\end{matrix}$$

兩種方法不同的地方在於，擴展歐幾里得方法的過程中會出現負數，而且都在中下和左上這兩個固定地方，那也是秦九韶方法取負號的地方；由於已經取了負號，當左方出現零的時候，非零的數字就是最大公因數，該列的中右方得到的數字不用再做任何處理，直接當成貝祖係數 r , s。筆者認為，秦九韶不用減法和負數、用加法和正數的原因為，中國數學是用算籌當計算工具，不是用筆算，雖然也可用不同顏色算籌代表負數，然而，綜觀整個計算過程，只有正負號的不同，數字是一樣的，在籌算的過程中，只是算籌的顏色不同， 量是再加上只要演算法簡單、容易算，最後結果數字正確就可以，而負數一直減和正數一直加的效果一樣，這可由比較上兩個演算法的計算過程看出。

前面提到的這些方法不只可以用來求整數的最大公因數，也可以用來求多項式的最大公因式，而多項式也有相應的貝祖等式，也可以用上述方法來求得。現在數位應用如編碼、密碼都以多項式的形式來處理，而處理過程中會用到擴展歐幾里得演算法，尤其是數位影音應用中的編碼，目前非常重要的一個演算法——伯利根演算法（Berlekamp algorithm），已經有多篇論文說明該演算法與擴展歐幾里得演算法等價性[9-11]。可以說都和秦九韶的“大衍求一術”具有相同的演算法精神。

最後，筆者曾參加 2012 年在高雄師範大學舉辦的第二屆中華經學國際學術研討會[12]，並在會議中提出對於幾個中國數學名詞的英文翻譯有一些建議。國父孫中山先生曾說：21 世紀是中國人的世紀。隨著在經濟方面的表現，中國人的地位逐漸被重視，以往被忽視、漠視的科學成就也逐漸為人所知。然而在中文尚未普遍被接受之前，英文還是唯一的世界通用語言，本文提出一些中國數學方面成就的英文譯名建議。

1.《九章算術》譯為“Nine Chapters”：中國的數學書籍中，《算數書》固然比較早，對於後世的影響，《九章算術》算是影響最大的，如同希臘的《幾何原本》，而《幾何原本》的英文譯名就是 Elements，筆者認為“Nine Chapters”會是《九章算術》的合適譯名。

2.《數書九章》譯為“Chin's Nine Chapters”：以秦九韶的《數書九章》數學成就，有必要在許多書名中帶有“九章”二字的書籍中區別出來。

3.“中國剩餘定理”譯為“Chin's Remainder Theorem”：目前中國剩餘定理的英文為“Chinese Remainder Theorem”，簡稱為“CRT”，由於秦九韶是第一個提出完整解法的人，如使用“Chin's Remainder Theorem”，簡稱仍然是“CRT”。

4.“大衍求一術”譯為“Chin's algorithm”：本文嘗試說明大衍求一術的重要性，以前的數學家或許不那麼重視演算法，然而在數位科技時代，演算法的重要性是不容忽視的，基於秦九韶大衍求一術承先啟後的地位，筆者作這樣的建議。

9 Unjeng Cheng, On the Continued Fraction and Berlekamp's Algorithm, IEEE Transactions on Information Theory, vol. IT30, pp. 541-544, May 1984.

10 Jean Louis Dornstetter, On the Equivalence Between Berlekamp's and Euclid's Algorithms, IEEE Transactions on Information Theory, Vol. IY-33, No. 3, pp. 428-431, May 1987.

11 Agnes E. Heydtmann and Jorn M. Jensen, On the Equivalence of the Berlekamp-Massey and the Euclidean Algorithms for Decoding, IEEE Transactions on Information Theory, Vol. IT-46, No. 7, pp. 2614-2624, Nov. 2000.

12 張耀祖：從《孫子算經》談起，通經致用：第二屆中華經學國際學術研討會，81-91，高雄師範大學，2012。