

孫子剩餘定理與高斯剩餘定理

王翼勳

1. 引言

同餘理論是文藝復興時期的產物。1801年高斯「算術研究」系統發展同餘理論，其中一些主要的結果，已經為像費馬和歐拉這樣更早期的數學家所知。

1881年，德國學者馬蒂生首先指出，4世紀「孫子算經」物不知數問題的解法和高斯方法一致。此後西方著作中就將上述解法稱作中國剩餘定理。

我國秦「顓頊曆」等古六曆採用積年。公認西漢末劉歆明確引入上元概念，並實際計算了三統曆和古四分曆的上元積年數據。從劉洪「乾象曆」(223年)起，八十餘家曆法都列出上元以來積年數據作為曆法的第一條數據，直到元郭守敬「授時曆」(1280年)才予廢止。

1208年「開禧曆」演紀積年法，本身就是傳統曆法整數論近千年演繹的結晶，是偉大數學家高斯「算術研究」之前，一個完整的整數論體系。

本文分析傳統曆法整數論的基礎：滿去式、週期齊同原理和以奇入算原理，對比高斯、秦九韶原文原術原意，從而斷定，以伴隨數為特徵的高斯剩餘定理，和可能以乘率為特徵的孫子剩餘定理，都受曆法編制刺激而產生，在各自的文明背景中成長，是同一個數學現象上的奇葩和碩果。

1.1. 物不知數題

公元4世紀「孫子算經」^[1]有一道物不知數題：

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。

術曰：三三數之剩二，置一百四十；五五數之剩三，置六十三；七七數之剩二，置三十。並之，得二百三十三，以二百一十減之，即得。凡三三數之剩一，則置七十；五五數之剩一，則置二十一；七七數之剩一，則置十五。一百六以上，以一百五減之，即得。

由此而提煉歸納出的定理，一般稱孫子剩餘定理，世稱中國剩餘定理。

剩餘定理在近代分析史上佔有極重要地位，相關解法的原則反映在插入理論、代數理論及算子理論（泛函分析）之中，在計算機的設計中也有重要的應用。

古代民間長期流傳著具有類似的數學遊戲，名稱很多，如「隔牆算」、「翦管術」、「秦王暗點兵」、「韓信點兵」、「鬼谷算」等等。

1592年，明代數學家程大位「算法統宗」一書所載「孫子歌」，遠渡重洋，輸入日本，以口訣形式，介紹了70、21和15三個數字的妙用：

三人同行七十稀，五樹梅花廿一枝，七子團圓正月半，除百令五便得知。

1.2. 物不知數題在西方的歷程

中國不定分析史料在西方的歷程，是數學史上一個重要的課題^[2]。

李儼^[3]最早簡略提及馬蒂生、康托、三上義夫和赫師慎的工作。

近年，楊瓊茹^[4]詳盡收集東西方相關史料，增加了朝鮮數學家慶善徵（1616~?）、黃胤錫（1729-1791）內容，有力地推動了這個課題的研究。

在歐洲^[5]，和秦九韶同時代的義大利數學家斐波那契（1170 ~ 1250），在「計算之書」^[6]（1202）中給出了兩個一次同餘問題，從形式到數據，都和物不知數題相仿。

1734年，歐拉在 *Comm. Acad. (Petrop., 7, 1734-5, 46-66; Comm. Arith. Coll., I, 11-20)* 一文研究了不定方程和一次同餘式組的解法^[7]。

1801年，高斯寫下「算術研究」^[8]，完善了同餘理論。

1839年3月畢甌在「亞洲雜誌」(*Journal Asiatique*) 上發表了十二卷本「算法統宗全書總目」。卷五最後，畢甌介紹了「孫子算經」的物不知數題，但沒有給出解法。

1852年英國傳教士偉烈亞力^[7] (A. Wylie, 1815~1887) 在上海英文週報「北華捷報」上發表「中國數學科學札記」，用秦九韶大衍術解釋物不知數題，引起了歐洲學者的重視。

德國學者畢爾那茨基 (K.L. Biernatzki) 在柏林偶然看到了偉烈亞力的論文，將其譯為德文，但作了許多改動，於1856年以「中國之算術」為題發表。

1874年，德國馬蒂生 (Ludwig Matthiessen, 1830~1906) 首先指出物不知數問題的解法和高斯方法一致。

1881年，馬蒂生撰文^[10]論述大衍術，以現代記號表示剩餘問題的解法。馬蒂生給出高斯解法，說明它與中國解法的一致性，並指出其中的 α , β 和 γ ，即為秦九韶的「用數」。事實上，馬蒂生只見過畢爾那茨基的譯文，並無任何其他文獻可依。

德國學者馬蒂生，在他那個年代，利用1801年的高斯「算術研究」，分析1247年的秦九韶大衍總數術，求解4世紀「孫子算經」的物不知數題，時空跨度遙遠。這位東西方不定分析史研究的先驅，開墾草莽，居功至偉，更鞭策今天的人們，研究秦九韶、高斯原文原術原意，挖掘曆法史料，深入到東西方比較數學史的廣闊領域中去。

2. 高斯伴隨數概念及式演化思想

2.1. 剩餘定理的背景

十六世紀以前西方採用的儒略曆，由古羅馬統治者儒略·凱撒採納天文學家索西琴尼的意見，制定於公元前 46 年。凱撒的侄子奧古斯都，在公元前 8 年又作了調整。十六世紀後期，羅馬教皇格雷果里十三世加以修訂，於 1582 年頒行，形成今天全世界通用的公曆。

高斯提到的儒略年，與儒略曆不同，另指儒略日計日法，現代天文學用來計算年代相隔久遠或不同曆法的兩事件之間，所隔的日數。1583年，法國學者 Joseph Justus Scaliger (1540~1609) 創立計日法，取名儒略，是為了紀念其父親義大利學者 Julius Caesar Scaliger (1484~1558)。

儒略日起點，規定在公元前 4713 年 (天文學上記為 -4712 年) 1 月 1 日格林威治時間平午 (世界時 12:00)。每天一個唯一序數，順數而下。如：1996 年 1 月 1 日 12:00:00 的儒略日是 2450084。

小紀 (A)、黃金數 (B) 和太陽循環週期 (C) 三個週期，分別度量起點到觀察者測點的總時間段。參見圖 1: 高斯年序學觀察示意圖。三個週期的乘積 $15 \times 19 \times 28 = 7980$ 年為儒略週期。

小紀 15 年 (A) (indiction cycle): 古羅馬皇帝君士坦丁一世 (Constantine I) 頒佈，每 15 年評定財產價值以供課稅，成為古羅馬用的一個紀元單位。

黃金數 (golden number) 19 年 (B)，太陰週期，或稱默冬章 (Metonic cycle): 經過一太陰週期 19 年，陰曆月年的日序重複，就是 235 朔望月 = 19 回歸年。

太陽循環週期 (solar cycle) 28 年 (C): 經過一太陽循環週期 28 年，星期的日序與年的日序重複，就是 $365.25 \times 28 = 10227$ 日 = 7×1461 ，有 1461 個星期。

年序學觀測中，從儒略日起點到觀察者所測某點的時間段 (z ，相當於傳統曆法積年的概念)，在小紀 15(A)、黃金數 19(B) 和太陽循環週期 28 (C) 三週期固定不變的背景下，不同次觀測得到的餘數 a, b, c 值不同，有 $z \equiv a \pmod{A} \equiv b \pmod{B} \equiv c \pmod{C}$ 。

模 15、19 和 28 固定，因兩兩互質，可直接相乘得固定總模 7980。後續一系列 α, β, γ 值，等等，也都固定。如同高斯所說：「 α 就是 6916。採用同樣方法，我們求得 β 為 4200， γ 為 4845，我們所求的數是 $6916a + 4200b + 4845c$ 的最小餘數。」這樣，每次計算不必從頭開始，只需把餘數 a, b, c 填入 $6916a + 4200b + 4845c$ ，再對總模 7980 取餘數，就解出最小正整數解了。

這就極大地減輕了曆法家的計算，高斯稱讚為「模板」。

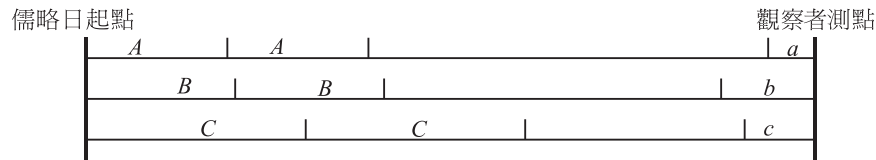


圖 1. 高斯年序學觀察示意圖

一次同餘式組問題中，非兩兩互質模的處理是個極大的難題。這裡，模 15、19 和 28 只有兩兩互質，才能直接相乘得總模。

「算術研究」第 32 節提出模不互質的一次同餘式組，「求出所有的數，它們對於任何數量的已知模具有已知餘數」。

第 32 節先解決模不互質（雙式）子同餘式組的解法，再推廣到多式。指導思想是，任取兩個同餘式，解出值，再吸納第三個同餘式，組成新的模不互質（雙式）子同餘式組。 n 個同餘式的一次同餘式組，共需要經過 $n - 1$ 次處理。最後一次（雙式）子同餘式組的解，就是整個同餘式組的解。最後高斯說，這個過程中，如果模兩兩互質，問題就能方便解決。

第 33 節預言，模兩兩互質，可以產生更令人滿意和一流的方法，就指第 36 節的剩餘定理。

經過大量準備工作，到第 36 節中，高斯得到剩餘定理，十分欣賞，再強調一下：「當所有的模 A, B, C, D ，等等兩兩互質時，使用下列方法通常更為優越。」在計算數 α 需要「用 BCD 等等所乘」之後，高斯又補充一個注「參見第 32 節」，強調各模必須兩兩互質，以使用最小公倍數就求出總模。

2.2. 剩餘定理的原文

「算術研究」第 36 節針對單個原模 A ，論述數 α 的定義。以 B, C, D ，等等字樣，表示論及其它模。涉及年序學的數例，則只提三個模。我們不再處處說明了。原文是：

當所有的模 A, B, C, D ，等等兩兩互質時，使用下列方法通常更為優越。確定一個數 α ，相對於模 A 與 1 同餘，相對於其他模的乘積與 0 同餘。這就是說， α 是由式子 $1/BCD$ 等等 $(\text{mod } A)$ 的一個值（最好是最小值），用 BCD 等等所乘（參見第 32 節）。類似地，令 $\beta \equiv 1 \pmod{B}$ 和 $\equiv 0 \pmod{ACD \text{ etc.}}$ ， $\gamma \equiv 1 \pmod{C}$ 和 $\equiv 0 \pmod{ABD \text{ etc.}}$ ，等等。於是，如果我們要尋找 z ，它與分別相對於模 A, B, C, D 等等的餘數 a, b, c, d 等等同餘，我們能夠記作

$$z \equiv \alpha a + \beta b + \gamma c + \delta d \text{ etc. } (\text{mod } ABCD \text{ etc.}).$$

顯然, $\alpha a \equiv a \pmod{A}$, 並且其餘的 $\beta b, \gamma c$, 等等都 $\equiv 0 \pmod{A}$, 所以 $z \equiv a \pmod{A}$ 。同樣的論證對其他模也成立。當我們要解更多的同類型問題, 對模值不變的 A, B, C, D , 等等, 值 α, β, γ , 等等, 具有恆值時, 這種解作為模板, 是個首選。這個用法起源於年序學問題, 在確定儒略年時的小紀、黃金數和太陽循環週期為已知。這裡 $A = 15, B = 19, C = 28$, 所以, 因式子 $1/(19 \times 28) \pmod{15}$ 或 $1/532 \pmod{15}$ 的值是 13, α 就是 6916。採用同樣方法, 我們求得 β 為 4200, γ 為 4845, 我們所求的數是 $6916a + 4200b + 4845c$ 的最小餘數。這裡 A 是小紀, B 是黃金數, C 是太陽循環週期。

原文中同餘符號, 涉及同餘 $a \equiv c \pmod{b}$ 與 $a = mb + c$ 的等價關係, 請見下文第 3.4 節: 以奇入算的理解。三個式子 $1/(19 \times 28) \pmod{15}$ 、 $1/532 \pmod{15}$ 、 $1/BCD$ 等等 \pmod{A} 相當於現今我們熟悉的同餘式 $(19 \times 28)x \equiv 1 \pmod{15}$ 、 $532x \equiv 1 \pmod{15}$ 、 BCD 等等 $x \equiv 1 \pmod{A}$ 。

第 36 節的要點是, 一個數 z , 與分別相對於模 A, B, C, D 等等的餘數 a, b, c, d 等等同餘。需要對每個原餘數 a, b, c, d , 各伴隨一個特殊的數 $\alpha, \beta, \gamma, \delta$ 等等, 相加成形如 $\alpha a + \beta b + \gamma c + \delta d$ 的總餘數。這樣, 所尋找的 z , 與相對於原模 A, B, C, D 的各別餘數 a, b, c, d , 同餘, 也與相對於總模 $ABCD$ 的總餘數 $\alpha a + \beta b + \gamma c + \delta d$, 同餘。而原模 A, B, C, D 的兩兩互質, 保證直接相乘得到總模 $ABCD$ 。

我們稱 α, β 等等特殊數為伴隨數, 稱以伴隨數為特徵的剩餘定理, 為高斯剩餘定理。

按照現代習慣, 剩餘定理可表達如下:

剩餘定理: 尋找 z , 它與分別相對於兩兩互質模 A, B, C, D 等等的餘數 a, b, c, d 等等同餘, 即有一次同餘式組

$$z \equiv a \pmod{A} \equiv b \pmod{B} \equiv c \pmod{C} \equiv d \pmod{D}。$$

如果有如下數:

$$\begin{aligned} \alpha &\equiv 1 \pmod{A} \equiv 0 \pmod{B} \equiv 0 \pmod{C} \equiv 0 \pmod{D}, \\ \beta &\equiv 0 \pmod{A} \equiv 1 \pmod{B} \equiv 0 \pmod{C} \equiv 0 \pmod{D}, \\ \gamma &\equiv 0 \pmod{A} \equiv 0 \pmod{B} \equiv 1 \pmod{C} \equiv 0 \pmod{D}, \\ \delta &\equiv 0 \pmod{A} \equiv 0 \pmod{B} \equiv 0 \pmod{C} \equiv 1 \pmod{D}, \end{aligned}$$

其中 α 的值, 是由相關同餘式

$$(BCD \text{ 等等})x \equiv 1 \pmod{A}。$$

的一個解(最好是最小值), 再用 BCD 等等所乘得。我們有

$$z \equiv \alpha a + \beta b + \gamma c + \delta d \text{ 等等} \pmod{ABCD \text{ 等等}}。$$

2.3. 伴隨數定義與計算

論證過程中, 高斯以單個原模 A 為代表, 透徹分析, 再推廣到 B, C, D 等等原模。

伴隨數 α 的定義: 假定 A 為本模, 「確定一個數 α , 相對於模 A 與 1 同餘, 相對於其他模的乘積與 0 同餘」, 可表示為:

$$\alpha \equiv 1 \pmod{A} \equiv 0 \pmod{B} \equiv 0 \pmod{C} \equiv 0 \pmod{D}。$$

伴隨數的值「 α 是由式子 $1/BCD$ 等等 \pmod{A} 的一個值 (最好是最小值), 用 BCD 等等所乘」, 由前後兩項因數相乘而成。所說同餘式, 按照現代習慣表示為:

$$(BCD \text{ 等等})x \equiv 1 \pmod{A}。$$

我們觀察計算的值怎樣滿足定義, 先介紹後項因數, 再分析前項因數, 最後講乘積情況。

後項因數「 BCD 等等」, 保證以 A 為本模的伴隨數 α , 內含所有因數, 能整除 B, C, D 等等中任一個, 因而與 0 同餘, 符合定義的「相對於其他模的乘積與 0 同餘」, 即:

$$\alpha \equiv 0 \pmod{B} \equiv 0 \pmod{C} \equiv 0 \pmod{D}。$$

這裡應用「算術研究」第29節整除性質 (見下文第2.5節): 因 δ 整除 a , $ax \equiv 0 \pmod{\delta}$ 。

再觀察前項因數, 凡是滿足特定同餘式: $(BCD \text{ 等等})x \equiv 1 \pmod{A}$ 的「一個值」, 都能使得同餘式左側的 $(BCD \text{ 等等})x$, 對於模 A , 與 1 同餘。不難理解, 當然「最好是最小值」。

最後看兩項乘積的伴隨數 α 。以 $(BCD \text{ 等等})x \equiv 1 \pmod{A}$ 的一個值, 乘上 $(BCD \text{ 等等})$, 構成的乘積 α , 是新同餘式

$$(BCD \text{ 等等})x \equiv BCD \text{ 等等} \pmod{A}$$

的解。不難看到, 係數 $(BCD \text{ 等等})$ 與模 A 互質, 可約去係數和常數的最大公約數 $(BCD \text{ 等等})$:

$$\alpha \equiv 1 \pmod{A},$$

體現第31節性質3(見下文第2.5節): 當 k 和 c 互質時, $bkx \equiv ak \pmod{c}$ 和 $bx \equiv a \pmod{c}$ 等價。新同餘式約簡後, 說的是: 伴隨數 α 符合定義的「相對於模 A 與 1 同餘」。這就論證了, 對原模 A , 伴隨數 α 滿足: $\alpha \equiv 1 \pmod{A} \equiv 0 \pmod{B} \equiv 0 \pmod{C} \equiv 0 \pmod{D}$ 。

最後, 推廣到 B, C, D 等等一般情況, 「同樣的論證對其他模也成立。」

2.4. 同餘式求解

同餘式 $532x \equiv 1 \pmod{15}$ 的求解, 按「算術研究」第30節同餘性質解法, 分三步:

1. 整除性質: 拆分係數: $(35 \times 15 + 7)x \equiv 1 \pmod{15}$ 。根據第29節整除性質, 刪除 $35 \times 15x \equiv 0 \pmod{15}$, 留下 $7x \equiv 1 \pmod{15}$ 。
2. 尋找係數的倍數: 在相對於模15, 而與1同餘的諸多數 $\dots, 1, 16, 31, 46, 61, 76, 91, \dots$ 中, 找到91, 是係數7的13倍: $7x \equiv 91 \pmod{15}$ 。
3. 係數與常數的約簡: 根據第31節同餘性質3(見下一節), 因7與15互質, 同餘號兩邊7和91可同時除以7, 得 $x \equiv 13 \pmod{15}$, 就是同餘式 $532x \equiv 1 \pmod{15}$ 的解。

2.5. 式演化思想

沒有伴隨數, 就無法組織總餘數, 還只是表面現象。深層次的原因是, 伴隨數需要照顧從條件同餘式到結論同餘式的整體演化, 源於與同解方程、同解不等式思想一脈相承的, 式整體演化的大背景。

「算術研究」處理同餘式, 有三條作用極重要的性質, 都顯示式演化的思想。

第29節講到整除性質, 當係數 a 為模 δ 的倍數時, 同餘式左側乘積項與0同餘:

$$\text{因 } \delta \text{ 整除 } a, ax \equiv 0 \pmod{\delta}。$$

第31節第2條性質, 講同餘式約去三項的最大公約數:

$$b\delta x \equiv a\delta \pmod{c\delta} \text{ 和 } bx \equiv a \pmod{c} \text{ 等價。}$$

第31節第3條性質, 講約去係數和常數兩項的最大公約數, 是需要條件的:

$$\text{當 } k \text{ 和 } c \text{ 互質時, } bkx \equiv ak \pmod{c} \text{ 和 } bx \equiv a \pmod{c} \text{ 等價。}$$

3. 傳統曆法整數論史料

我們列出相關史料, 闡明滿去式、齊同原理、以奇入算, 為探索物不知數題, 提供輔佐證據。

3.1. 滿去式史料

中國曆法上應用的推求之術, 公元四世紀的「續漢書·律曆志下」^[11] 就有記載, 古四分曆用「滿」與「不滿」表達: 「推天正術, \dots 滿章法而一, 名為積月, 不滿為閏餘」。曆法推算, 產生不滿, 產生奇, 也刺激產生新的曆法概念。

1247年秦九韶大衍求一術，也說：「諸衍數，各滿定母去之，不滿曰奇。」

我們提出，傳統數學上使用的是滿去式，與現代一次同餘式概念相區別。滿去式各項的稱呼，在不至於混淆的情況下，可用未知數、係數、滿去數（週期、定母、模）與不滿數（奇數、餘數、常數）等術語。

滿去式中奇這個量，在對於滿去數（週期、定母、模）的運算中，能代替原數這個量，簡稱以奇入算，這正是量演化思想的基礎。

3.2. 週期逐級齊同史料

與「孫子算經」同處於公元四世紀的「續漢書·律曆志下」，介紹古四分曆多個週期處理法。從日月週期入手，逐個納入日名干支週期和歲名干支週期。逐級齊同的過程，體現謀求週期完整及端點相會的思想，沒有明確提出最小公倍數概念。

歲首至也，月首朔也。至朔同日謂之章，同在日首謂之部，部終六旬謂之紀，歲朔又復謂之元。是故日以實之，月以閏之，時以分之，歲以周之，章以明之，部以部之，紀以記之，元以原之。然後雖有變化萬殊，贏朒無方，莫不結繫於此而稟正焉。

約定第一歲歲首冬至與第一個朔望月月首，同處於起始點。

古四分曆歲實 $365\frac{1}{4}$ 日和朔望月 $29\frac{499}{940}$ 日，可以齊同成章 19 歲 ($= 365\frac{1}{4} \text{ 日} \times 19 = 29\frac{499}{940} \text{ 日} \times 235 = 6939\frac{3}{4} \text{ 日}$)，歲首冬至與月首合朔會合，在某日 $\frac{3}{4}$ 處（折現今 18 時），稱「至朔同日」。

為達到日的完整，擴大到部 76 歲 ($= 6939\frac{3}{4} \text{ 日} \times 4 = 19 \text{ 歲} \times 4$)，冬至合朔回到日首夜半，稱「同在日首」。

為達到日名干支週期 60 日的完整，擴大到紀 1520 歲 ($= 76 \text{ 歲} \times 20 = 555180 \text{ 日} = 60 \text{ 日} \times 9253 \text{ 日名干支週期}$)，冬至合朔回到甲子日夜半，稱「部終六旬」。

為達到歲名干支週期 60 歲的完整，擴大到元 4560 歲 ($= 1520 \text{ 歲} \times 3 = 60 \text{ 歲} \times 76 \text{ 歲名干支週期}$)，冬至合朔回到甲子歲甲子日夜半，稱「歲朔又復」。

逐級齊同的週期，為需要處理或過剩或不足數據的曆法排布，奠定了堅實的基礎。

3.3. 解單個滿去式史料

四庫館臣「數學九章提要」(1773年)^[12]讚歎秦九韶的歷史功勳：「自秦漢以來，成法相傳，未有言其立法之意者，惟此書大衍術中所載立天元一法，能舉立法之意而言之。」

秦九韶是幸運的，早歲侍親中都，因得訪習於太史，又嘗從隱君子受數學。秦九韶更是勤奮的，多年鑽研，仿照演紀積年法核心求入元歲之術理，改革元數求法，提煉歸納出完善的大衍求

一術。秦九韶感慨「數理精微，不易窺識，窮年致志，感於夢寐，幸而得之，謹不敢隱」，在「數書九章」中編入推氣治曆，治曆推閏，治曆演紀三題，使後人得以窺見 1208年開禧曆演紀積年的計算過程。

1583年的儒略日計日法，固定單個起點、固定三週期，只用來計算年代相隔久遠或不同曆法的兩事件之間相隔日數。中國近千年傳統曆法考慮的數學問題，要遠遠複雜得多。

每編制一部新曆法，曆家就獨立計算一個理想的曆元，作為此曆各種天文週期的共同起點，稱之為上元。上元至少要滿足四個條件：甲子歲甲子日零時冬至合朔。

開禧曆上元，至近期編曆歲歲首（滿足同樣四個條件），演紀積年 7848180 歲。

每日零時到次日零時為一日，開禧曆用調日法調成 16900 份，稱日法 16900，作為所有曆法數據的公分母，從而可以取分子作為整數演算。

各個天象數據週期的組合，需要一個獨立於這些週期之外的、連續完整的紀錄系統。從公元前 722年起就開始使用的 (1) 日名干支週期（紀法 60 日，紀率 $16900 \times 60 = 1014000$ ），和從公元 85 年起就使用的紀法 60 歲的 (2) 歲名干支週期，能輕鬆地解決各週期之首的插入問題。

開禧曆一歲歲實（回歸年長度）為 (3) 歲率 6172608。漫長的演紀積年乘以歲率的總數，除以 (1) 日名干支週期的餘數，為氣骨 193440，甲子日夜半到近期編曆歲歲首冬至的時間段。

一個朔望月的朔策，為 (4) 朔率 499067。演紀積年總數除以朔率，餘數為閏骨 163771，甲子日夜半到平朔時刻的時間段。

比照本文圖 1：高斯年序學天象觀察示意圖，上述 (1)(2)(3)(4) 四個週期的數理背景，可以引入整數論中的一次同餘式組問題。把總歲數記作 N ，演紀積年總分 $6172608 \times N$ 作為 z ，套用圖中字母，日名干支週期為模 A ：1014000，氣骨為餘數 a ：193440。朔率為模 B ：499067，閏骨為餘數 b ：163771，一次同餘式組 $z \equiv a(\text{mod } A) \equiv b(\text{mod } B)$ 有：

$$6172608N \equiv 193440(\text{mod } 1014000) \equiv 163771(\text{mod } 499067)。$$

開禧曆卻分成兩步演算，第一步求入元歲之術理，處理歲率、日名干支週期和歲名干支週期，簡稱氣紀關係。

對氣紀關係的(1)日名干支週期、(2)歲名干支週期和(3)歲率三個週期，開禧曆採用週期齊同處理法，得到新週期氣元 19500 歲。約定第一歲歲首冬至掛靠在甲子歲甲子日夜半，經一氣元 19500 歲後，冬至點、甲子歲歲首和甲子日夜半一會。

用氣元度量演紀積年總歲數，餘數稱入元歲。相關的求入元歲之術理，原文如下：

以四千一百八分為斗定分，與日法以大衍術入之，求得五十二為等數，一百四十四為因率，三百二十五為節率。以甲子六十為紀法，乘等數得三千一百二十為約率。……

為氣定骨，然後以約率三千一百二十除之，得六十二，以因率一百四十四乘之，得八千九百二十八，滿部率三百二十五去之，不滿一百五十三，以紀法六十乘之，得九千一百八十年為入元歲。

1966年，錢寶琮^[13]對演紀積年法作出數論證明，我們摘錄其中求入元歲之術理一段的證明。記歲名干支週期個數為 n ，氣元個數為 m ，附上原術語，供檢索方便。

從上元甲子歲到嘉泰甲子歲的演紀積年，歲數記為 N ，有同餘式

$$6172608(\text{歲率})N \equiv 193440(\text{氣定骨})(\text{mod } 60(\text{紀法}) \times 16900(\text{日法})).$$

由於上元與近期編曆歲同屬於甲子歲， N 能為 60 (紀法) 整除，設 $N = 60(\text{紀法})n$ 。又由於 $6172608 = 365 \times 16900(\text{日法}) + 4108(\text{斗分})$ ，於是 $6172608N \equiv 193440(\text{mod } 60 \times 16900)$ 一式可改寫作：

$$\begin{aligned} 4108(\text{斗分}) \times 60(\text{紀法})n &\equiv 193440(\text{氣定骨})(\text{mod } 60 \times 16900), \\ 79 \times 52(\text{等數}) \times 60(\text{紀法})n &(\text{歲名干支週期個數}) \\ &\equiv 62 \times 60(\text{紀法}) \times 52(\text{等數})(\text{mod } 60(\text{紀法}) \times 52(\text{等數}) \times 325(\text{部率})), \end{aligned}$$

以 60×52 約，化簡為

$$79n \equiv 62(\text{mod } 325).$$

以 79 與 325，用大衍求一術求得乘率 144(乘率) [即 $79 \times 144 \equiv 1(\text{mod } 325)$]，因得

$$n(\text{歲名干支週期個數}) \equiv 62 \times 144(\text{mod } 325) \equiv 153(\text{mod } 325).$$

故

$$N \equiv 9180(\text{入元歲})(\text{mod } 19500(\text{氣元率})),$$

或

$$N = 19500(\text{氣元率})m(\text{氣元個數}) + 9180(\text{入元歲}), m \text{ 為正整數}.$$

漫長的演紀積年，滿去402個氣元 (需要增用朔紀關係數據，另立式再求出402)，不滿數就是求入元歲之術理求出的 9180 歲。數論證明中最後兩式所體現的，就是這樣的含義。

現在體會傳統曆法整數論的量演化思路。

演紀積年滿去日名干支週期，得到氣骨。用實測值構成最基礎的演紀積年滿去式：

$$6172608 \times \text{演紀積年歲數}, \text{滿紀率} 1014000 \text{ 去之}, \text{不滿為氣定骨} 193440.$$

規定上元和近期編曆歲都是甲子歲，保證演紀積年時間段含有整數個歲名干支週期，含有紀法60歲。日名干支週期也含有紀法60日。於是，只演化未知數一個量，把演紀積年歲數，換成60個歲名干支週期個數，稱為歲名干支週期滿去式：

$$(6172608 \times 60) \times \text{歲名干支週期個數}, \text{滿紀率}(16900 \times 60)\text{去之}, \text{不滿爲氣定骨} 193440.$$

上述數論證明的「以79與325，用大衍求一術求得乘率144」，並不是開禧曆求解歲名干支週期滿去式時，核心的數值計算法。秦九韶大衍求一術，要到此後39年才出現。

原文「以四千一百八分爲斗定分，與日法以大衍術入之」，求出乘率144，我們稱斗分日法求乘率術。與常理相比，斗分日法求乘率術數理上並不完善，存在三個偏差：1、入算斗分、日法不互質，2、只計算一個序列和3、以等數標誌乘率。

核心層次之前有預處理層次：

1、紀法利用—歲名干支週期滿去式中，以最大公約數紀法60，約簡係數 (6172608×60) 和滿去項 (16900×60) ，只是兩個量的演化，並不是滿去式整體演化。

2、以奇入算—直接把歲率對日法的奇餘：斗分4108，替代歲率6172608，以奇入算，只是一個量的演化。

這個預處理層次，列式，量演化約簡，建立斗分4108與日法16900之間關係，爲下一步核心層次求乘率作好準備。注意，歲名干支週期滿去式中氣定骨193440，至此并未變動。

3、求出乘率—以斗分和日法求乘率，計算出等數52、乘率144和部率325。

核心層次的數值計算法之後，則是解的後處理層次，包括求最小正整數解和曆法應用。

4、約率應用—等數52與紀法60，組成約率3120，約氣定骨193440得62。

5、乘率應用—乘率144，如其名所述，用來乘。所乘者，是約氣骨所得的常數62。乘積8928，已經是所求未知數：歲名干支週期個數。

取8928滿去部率325，不滿數153，正是歲名干支週期數，最小正整數解。「孫子算經」物不知數題的「一百六以上，以一百五減之」，就是求最小正整數解。

6、乘限校核—設定1億爲演紀積年數，扣除入元歲，所含氣元的個數，稱爲乘限。要求所得元數不超過乘限值，就是要求演紀積年數最大不超過1億。

7、算入元歲—153個歲名干支週期，乘以紀法60歲，共9180歲，取名入元歲。

除了斗分日法求乘率術尚不完善外，求入元歲之術理，系統，合理，嚴謹，是千百年來，多少代曆法家智慧的結晶。

上述七個環節中，以奇入算是最奇特的一步。

3.4. 以奇入算的理解

同餘理論是由高斯在1801年「算術研究」中，系統發展出來的。

現代數論教科書^[14]上, 就同餘式 $a \equiv c \pmod{b}$ 與帶餘除法 $a = mb + c$ 的等價關係, 有這樣兩段評論, 能幫助我們在現代數論背景上, 理解中國古代的以奇入算。現摘錄如下:

同餘按其詞意來說, 就是餘數相同。

我們知道, 若帶餘除法 $a = mb + c$ 成立, 那麼在討論一個 a 的多項式被 b 去除的問題時, c 與 a 是一樣的, 即 a 可用 c 代替, 而其中的部分商 m 不起作用。同餘式符號 $a \equiv c \pmod{b}$ 正是抓住了這一關鍵, 在上面的除法算式中去掉了 m , 保留了 c , 突出了 c 與 a 在討論被整除的問題中兩者起的相同作用。

所以說, 以奇入算在傳統曆法整數論中的地位, 無論怎樣評價, 都不會太高。

4. 秦九韶乘率概念及量演化思想

4.1. 伴隨數與用數計算

沿著不定分析史研究先驅馬蒂生當年走過的路, 我們分別用高斯和秦九韶方法, 試算物不知數題, 觀察所出現的伴隨數與用數, 加深理解。

用高斯剩餘定理, 寫成一次同餘式組:

$$z \equiv 2 \pmod{3} \equiv 3 \pmod{5} \equiv 2 \pmod{7}。$$

關鍵一步, 就是輪流以 $A = 3, B = 5, C = 7$ 為模, 構造常數 1 同餘式, 以「 $(BCD$ 等等) $x \equiv 1 \pmod{A}$ 」的一個解 (最好是最小值)], 再用 BCD 等等其它模所乘, 求出相應伴隨數:

構造 $5 \times 7x_1 \equiv 1 \pmod{3}$, 解出 $x_1 = 2$ 。再乘以 5×7 , α 就是 70。

構造 $3 \times 7x_2 \equiv 1 \pmod{5}$, 解出 $x_2 = 1$ 。再乘以 3×7 , β 就是 21。

構造 $3 \times 5x_3 \equiv 1 \pmod{7}$, 解出 $x_3 = 1$ 。再乘以 3×5 , γ 就是 15。

求總模 $3 \times 5 \times 7 = 105$ 後, 才用餘數 $a = 2, b = 3, c = 2$, 代入 $z \equiv \alpha a + \beta b + \gamma c + \delta d$ 等等 \pmod{ABCD} 等等), 有

$$z = 70(\alpha) \times 2(\text{餘數}) + 21(\beta) \times 3(\text{餘數}) + 15(\gamma) \times 2(\text{餘數}) = 233, z = 233 - 2 \times 105 = 23。$$

大衍總數術一般處理非兩兩互質模題。解物不知數題, 相當於解兩兩互質模的餘米推數題。以表格形式表達, 三項稱為甲、乙、丙。所附數學史界通用字母符號, 僅供檢索。其中, 衍數記 $G_i = \frac{M}{a_i}$, 以 p 記任意整數, 最小正整數解為 $N = \sum_{i=1}^n R_i k_i \frac{M}{a_i} - pM$ 。

秦九韶大衍總數術原文	量的逐級演化	甲	乙	丙
	定數 a_i	3	5	7
	餘數 R_i	2	3	2
以定相乘為衍母	衍母 M	105		
以各定約衍母, 各得衍數	衍數 G_i	35	21	15
諸衍數, 各滿定母去之, 不滿曰奇	奇數 g_i	2	1	1
以奇與定, 用大衍求一入之, 以求乘率	乘率 k_i	2	1	1
置各乘率, 對乘衍數, 得用	用數 $k_i G_i$	$2 \times 35 = 70$	$1 \times 21 = 21$	$1 \times 15 = 15$
其餘各乘正用, 為各總	各總 $k_i G_i R_i$	$2 \times 70 = 140$	$3 \times 21 = 63$	$2 \times 15 = 30$
併總	總數 $\sum_{i=1}^n k_i G_i R_i$	$140 + 63 + 30 = 233$		
滿衍母去之, 不滿為所求率數	解 N	$233 - 2 \times 105 = 23$		

乙、丙項奇數為1, 乘率逕自為1。甲乘率的計算, 以衍數 $5 \times 7 = 35$ 和定數3, 先求出奇數2。再與定數3入大衍求一術。下面第三籌算圖右上得1時, 檢視左上2, 就是乘率。

$$\begin{array}{|c|c|} \hline 1 & 2 \\ \hline & 3 \\ \hline \end{array} \longrightarrow \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 1 & 1 \\ \hline \end{array} \longrightarrow \begin{array}{|c|c|} \hline 2 & 1 \\ \hline 1 & 1 \\ \hline \end{array}。$$

同樣的數值70、21、15, 到高斯解法中, 體現 α , β 和 γ 伴隨數概念, 到秦九韶大衍總數術, 導致「用數」概念, 到明代「孫子歌」中, 成了口訣:「三人同行七十稀, 五樹梅花廿一枝, 七子團圓正月半, 除百令五便得知。」

4.2. 高斯的依賴關係與乘率

借助人們比較熟悉的常數1不定方程, 能夠簡捷明瞭地觀察常數1同餘式的種子作用。

假定形如 $ak - bj = 1$ 的常數1不定方程, 符合可解條件, 約定 a 不小於 b 。未知數特記為 k 和 j , 解為 $k = x_0$ 和 $j = y_0$ 。

常數1不定方程乘以正整數 c , 得 $c \times ak - c \times bj = c \times 1$ 。與之比較, 其他項完全相同的, 常數 c 非1不定方程 $ax - by = c$, 解為: $x = ck = cx_0$ 和 $y = cj = cy_0$ 。

符合可解條件的, 係數與模完全相同, 僅僅常數值不同的所有一次同餘式中, 只有一個的常數, 能取單位1。在理論分析與計算實踐中具有極重要作用, 特命名為單位一同餘式。

單位一同餘式未知數特地用 k , 記作 $ak \equiv 1(\text{mod } b)$, 約定 a 不小於 b 。

其他項完全相同的, 常數 c 非1的同餘式, 記作 $ax \equiv c(\text{mod } b)$ 。

同餘式 $k \equiv 1(\text{mod } b)$ 等價於常數1不定方程 $ak - bj = 1$ 。立即可知, 非單位1同餘式 $x \equiv c(\text{mod } b)$ 的解, 就是 $x = ck$, 源於單位一同餘式 $k \equiv 1(\text{mod } b)$ 解出的 k , 乘以常數 c 。

單位一同餘式這個莖杆一枝, 會引出東西方不定分析史上, 花開兩朵的並蒂蓮。

高斯在「算術研究」第27節中, 關注解 k 的來源式, 描述為對單位一同餘式的依賴:

現在需要增加解同餘式方法的細節。我們首先觀察形如 $ax + t \equiv u$ 的同餘式，這個同餘式是依賴於 $ax \equiv \pm 1$ 的，這裡假定它的模對於 a 互質；因為如果 $x \equiv r$ 滿足後者，則有 $x \equiv \pm(u - t)r$ 會滿足前者。

這裡，高斯以正負號照顧到 t, u 的大小。

中國傳統數學，關注單位一同餘式的解 k ，因後續要用來乘，命名這個特定量為乘率。當然，這裡只是理論上的分析說明，中國古代沒有現代意義的一次同餘式概念。

4.3. 剩餘定理的重新獨立發現

一次同餘式組，由若干個同餘式組合發展而成。原模兩兩互質，是最簡單的一種情況。這些原模，需要綜合處理，方案之一就是輪流作當前模，恰當地組織單位一同餘式。

我們在前面第 4.1 節演算基礎上，挖掘物不知數題中兩兩互質模 3、5、7 的作用。

例如，以 3 作當前模， $5 \times 7 = 35$ 作係數，可組織單位一同餘式，35 與 3 互質，35 不小於 3：

$$35x_1 \equiv 1 \pmod{3}, \quad (1)$$

最小正整數解 $x_1 = 2$ 。係數與模完全相同，常數改取非單位 1 的 $c = 5 \times 7 = 35$ ，形成同餘式：

$$35x_2 \equiv c \pmod{3}, \quad (2)$$

非單位 1 同餘式 (2) 的解就是 $x_2 = x_1c = 2c = 2 \times 5 \times 7 = 70$ 。

伴隨數的計算，利用式 (2) 對式 (1) 的依賴關係，所引出伴隨數 $\alpha = 2c = 70$ ，由兩項所乘：單位一同餘式 $35x_1 \equiv 1 \pmod{3}$ 最小正整數解 2，「用 BCD 等等 (5×7) 所乘」。伴隨數定義，著眼於條件式到結論式的整體演化：

$$\begin{aligned} z &\equiv a \pmod{A} \equiv b \pmod{B} \equiv c \pmod{C} \equiv d \pmod{D}, \\ z &\equiv \alpha a + \beta b + \gamma c + \delta d \text{ 等等} \pmod{ABCD \text{ 等等}}, \end{aligned}$$

前面第 2.3 節分析過，伴隨數在思維上有很高的要求。

如果說，高斯輪流利用兩兩互質原模，構造單位一同餘式，再找到各個伴隨數，費盡周折，曲徑通幽，覓得剩餘定理的話，那麼，就解餘米推數題這類兩兩互質模題而言，秦九韶十分幸運，走上了通幽捷徑。

單位一同餘式一枝莖杆上的兩朵奇葩，結出了兩枚等價的碩果。

前面第 4.1 節清楚顯示，大衍總數術按照量的逐級演化思想，把各個單獨模，齊同得總模，稱衍母。約定「諸衍數，各滿定母去之，不滿曰奇」，先以衍數 35 滿去定數 3，求奇數 2。再

「以奇與定，用大衍求一入之」，求乘率 2。算用數， $2(\text{乘率}) \times 35(\text{衍數}) = 70(\text{用數})$ 。再算各總， $70(\text{用數}) \times 2(\text{餘數}) = 140(\text{各總})$ 。

就在考慮總餘數，這個高斯煞費苦心的環節上，554 年前的秦九韶竟會毫無障礙地把各總相加，「並總」已經得到解。再「滿衍母去之，不滿爲所求率數」，得到最小正整數解。

我們不能不感慨：存在乘率概念的數理環境中，量的逐級演化思想，可能導致秦九韶重新獨立發現剩餘定理。

幾十年來，中國數學史界一直思索，「數書九章」中只提到「九章算術」，從來不提「孫子算經」。我們以爲，有可能就是這個原因。

5. 物不知數題起源探索

當前數學史界一致公認^[15]：「孫子算經裡物不知數問題的解法不是作者的向壁虛造，而很可能是依據當時天文學家的上元積年算法寫出來的。」

同餘理論是西方文藝復興之後的產物。G.H. 哈代說^[16]：「同餘式的理論首先是由高斯系統發展出來的，雖然其中主要的結果已經爲像費馬和歐拉這樣的更早期的數學家已知。」

同餘理論傳入中國之後，爲中國曆法史中國數學史研究提供了銳利的武器。

物不知數題用同餘符號表示，上升表述爲孫子定理，完全正確。但不能就此而認爲四世紀的中國人，就是利用類似現代同餘概念，輕鬆簡捷地導出物不知數題的，因爲數字史料不免產生多種解釋。「同餘理論是把雙刃劍」^[17]，在帶給中國曆法史中國數學史研究極大便利的同時，也可能掩蓋原始思路。

可以肯定，中國古代沒有現代意義的一次同餘式概念。從劉歆直到郭守敬以前，中國曆法家並沒有用同餘理論去推演計算上元積年。與「孫子算經」同一時代的「續漢書·律曆志下」，向我們提供了滿去式的史料，也提供了曆法週期齊同的史料。可以考慮，物不知數題首先把 3、5、7 兩兩齊同成 35、21 和 15，再齊同成 105。

人類文明進展，尤其在古代，是相當重複而不協調的。同一概念或思想，可以有分散的發現，也可以有各自的發展^[18]。文明的不同，研究出發點的不同，認識程度的不同，描述說法的不同，思維重點也會有所不同。要追求歷史的真相，只有仔細考核原文原術原意。

對於最具爭議的「凡三三數之剩一，則置七十」一句，利用類似 $70 \equiv 1(\text{mod } 3) \equiv 0(\text{mod } 5) \equiv 0(\text{mod } 7)$ 的種種表述，都只是起以同餘理論驗證的作用。

我們把 70 看作 35 乘上了 2。所乘這個 2，稱爲乘率，1208 年鮑浣之有求乘率術，1247 年秦九韶有大衍求一術。西漢中期成形的「九章算術」就有個更相減損法：

約分術曰：可半者半之，不可半者，副置分母、子之數，以小減多，更相減損，求其等也。以等數約之。

鮑澆之斗分日法求乘率計算圖,右列上下體現「更相減損,求其等也」,以等數標誌乘率。以秦九韶的大衍求一術,試算物不知數題,必然出現乘率。

公元4世紀時是試算還是另有算法,我們目前確實缺乏直接史料,只能說物不知數題的數理環境可能含有乘率。然而,沒有當時天文學家的上元積年算法,編不出這樣的題目。

如果物不知數題數理內含有乘率,就容易導出用數70、21和15,容易謀求各總直接相加。前面分析過,存在乘率概念的數理環境,可能導致秦九韶重新獨立發現剩餘定理。

天象觀測呼喚數學,推動數學。可能以乘率為特徵的孫子剩餘定理,和以伴隨數為特徵的高斯剩餘定理,都受曆法編制的刺激而產生,在各自的文明背景中成長,卻是同一個數學現象單位一同餘式上的奇葩和碩果,都能反過來深化人們對天象的認識。

參考文獻

1. 「孫子算經」,郭書春校點,見「算經十書」(二)遼寧教育出版社,1998年,pp.1~29;「算經十書」,臺北:九章出版社,2001,pp.257~292。
2. 白尚恕,大衍術與歐洲的不定分析,「秦九韶與數書九章」,吳文俊(主編),1987,北京師範大學出版社。pp.209~313。
3. 李儼,大衍求一術之過去與未來,「中算史論叢」(一),中華學藝社,1933,pp.60~121。
4. 楊瓊茹,中國剩餘定理,「HPM 通訊」,4卷1期,pp.2~10。
5. Libbrecht, Ulrich. 1973. Chinese Mathematics in the Thirteenth Century. Cambridge, Massachusetts, London: The MIT Press. pp. 268~271. pp. 310~328.
6. 斐波那契(義大利),「計算之書」,(美國)西格爾譯,(中國)紀志剛譯,科學出版社,2008.1。
7. Dickson, Leonard E. History of the Theory of Numbers, AMS Chelsea Publishing, 1999.
8. Gauss, Karl Friedrich. 1801. Disquisitiones Arithmeticae. Lipsiae: Gerh Fleischer.
9. 汪曉勤,大衍求一術在西方的歷程,「自然科學史研究」,第18卷第3期,1999年,pp.222~233。
10. L. Matthiessen, Ueber das sogenannte Restproblem in den chinesischen Werken Swan-king von Sun-tsze und Tayen lei schu von Yih-hing. Journal fur die Reine und Angewandte Mathematik, 1881, 91: 254~261.
11. 「續漢書·律曆志下」,「歷代天文律曆等志彙編」,第五冊,中華書局,1976, p.1510。
12. 秦九韶,「數學九章」,「四庫全書」,臺北商務印書館影印文淵閣本,797冊,1986, p. 324。
13. 錢寶琮,秦九韶數書九章研究,「宋元數學史論文集」,科學出版社,1966, pp.60~103。
14. 潘承洞,潘承彪,「初等數論」,北京大學出版社,1992, pp.97~102。
15. 錢寶琮,「中國數學史」,科學出版社,1964。
16. G. H. Hardy, E.M. Wright,「數論導引」,張明堯,張凡譯,人民郵局出版社,2008.10, p.62。
17. 王翼勳,開禧曆上元積年的計算,「天文學報」,第48卷第1期(2007.1) pp. 93~105。
18. 程貞一,「黃鐘大呂」,王翼勳譯,上海科技教育出版社,2007, p.72。

—本文作者退休前任教蘇州大學數學科學學院—