古算今谈

王宗儒 编著

民出版社

古算今谈

王宗儒　　编著

華中工学院出版社

内容提要

本书介绍了我国古代著名的《九章算术》、《周髀算经》、《张邱建算经》、《海岛算经》等十部算经，并着重叙述了流传久远的百鸡问题、韩信点兵、勾股定理、圆周率、杨辉三角形、纵横图和幻方、正负术、等差等比级数等我国古代数学的辉煌成就，及其对世界数学的深刻影响．从而培养青少年爱祖国、爱人民、爱科学的热忱，并提高他们学习数学的积极性．也可供数学教师参考之用．

通过本书的学习可以使青少年增加一些数学史方面的知识，也可使他们了解到我国古代数学家的数学观点、治学方法以及严谨的学风．

古算今谈

王宗儒　编　著

责任编辑　李立鹏

*

华中工学院出版社出版

（武昌喻家山）

新华书店湖北发行所发行

华中工学院出版社沔阳印刷厂印刷

*

开本：787×1092　1/32　印张：6.625　字数：142,000

1986年8月第一版　1986年8月第一次印刷

印数：1—3,000

统一书号：13255—052　　定价：1,15元

前　言

我国古代数学是我国古代文化遗产的一个重要部分。每当我们读到中国古代数学史的一些光辉篇章时，就有一种发自肺腑的民族自豪感。特别在课堂上讲授某些数学内容结合提出我国古代数学家当时居于世界领先的学术地位及其精辟见解时，总会使青年学生们情绪高涨，不仅提高了他们学习数学的积极性，而且对于培养学生爱祖国、爱人民、爱科学的思想情操也起了一定的作用。

为了满足青少年数学爱好者的要求，我们把祖国古代在数学上的主要成就与现在中学里所学的数学内容联系起来，写成《古算今谈》这本书。

我国古代数学历史悠久，内容丰富，文字艰深，颇难看懂，为了便于青少年阅读且与中学数学相联系，我们没有按照年代顺序编写，而是按问题的类型来写作，并作了一些必要的注释，尽量做到通俗易懂而有趣味。另一方面，为了使读者对中国古代数学有一个比较系统的了解，专门写了十部算经简单介绍一节。最后，中国古代数学典籍及数学家名言摘录一节，是作者平日的读书札记，着重记录数学观点，治学方法及数学家们的名言。由于个人的知识水平有限，对我国古代数学缺乏系统的学习与研究，其中一定存在不少错误和缺点，请同志们提出批评指正，

王宗儒于衡阳

1985年3月

目　录

一　孙子定理和一次同余式组

孙子定理是我国古代《孙子算经》中的一个题目．这个题目后人称为**物不知数**．《孙子算经》的作者和成书年代均不可考，但在《隋书·经籍志》著录有孙子算经二卷，所以产生于四世纪以前．孙子算经的解法十分简捷有趣，唐朝初年，曾作为算学教科书．更有意义的是：物不知数的解法却与十九世纪德国数学家高斯（Gass1777—1855年）的解法相同，因此，西方数学史称它为**中国剩余定理**．

1　《孙子算经》中的求一术

《孙子算经》下卷有一著名的问题：

今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

答曰：二十三。

术曰：三三数之剩二，置一百四十．五五数之剩三，置六十三，七七数之剩二，置三十．并之，得二百三十三，以二百一十减之，即得．

凡三三数之剩一，则置七十．五五数之剩一，则置二十一，七七数之剩一，则置十五．一百六以上，以一百五减之，即得

上述的方法，可表述如下：

设所求之数为N，则

$$N=140+63+30-210=23.$$

上面这些数据是怎样得出来的呢？可从“术曰”的第二段来说明：

“凡三三数之剩一，则置七十”就是说：每三三数之剩一，就取七十这个数作为基数，这是因为3除余1的数很多，如4，7，10，…而70这个数除满足3除余1外，还是5和7的公倍数。所谓求一术就是要找到这样一个数，用3除余1，同时又能被5和7整除的数中最小的数，这个数就是70，因此，选它为基数。

同样道理，“五五数之剩一，则置二十一。”就是用5除余1，同时又是3和7整除的数中最小的数是21，因此，21作为第二个基数。

“七七数之剩一，则置十五。”就是用7除余1，同时又是3和5整除的数中最小的是15，因此选定15为第三个基数。

于是它们的和：$70+21+15=106$是用3、5、7去除都余1的数，这就是《孙子算经》中的求一术。

“一百六以上，以一百五减之。”是因为3、5、7的最小公倍数是105，106以上的数减去105以后所得余数是不会改变的。例如$106-105=1$，它仍然是用3、5、7去除余1的数，也是符合上述求一术的要求的。

现在来解释“术曰”中第一段的意思：

“三三数之剩二置一百四十。”这是因为70是用3除余1，同时又能被5、7整除的，所以140是用3除余2，同时又能用5、7整除的数。

“五五数之剩三置六十三。”是因为21是用5除余1，同时又能被3、7整除的数，当然63是用5除余3，又可被3、7整除的数。

“七七数之剩二置三十，”同样的道理$15\times2=30$是用7

除余2，同时又能被3、5整除的数。

“并之得二百三十三，”就是$140+63+30=233$。这个数当然是用3除余2，用5除余3，用7除余2的数，但是，它超过了105，所以减去105的2倍即210。$233-210=23$，它仍然是用3、5、7去除余数不变的数，而且是答案中最小的一个数。

这个算法是十分巧妙的，颇有猜迷语的趣味，流传到后世，则有剪管术、鬼谷算、隔墙算、秦王暗点兵、韩信点兵等不同的名称。有的人把它编成诗句，作灯迷，成为民间文娱活动的一个内容；还有一些老人在夏日的树荫下乘凉或冬夜围炉取暖的时候，用它来测试晚辈们的智力。流传的方式多种多样十分有趣。

周密的《志雅堂杂钞》卷下载：鬼谷算，又名隔墙算，其法将钱不拘多少，三三数之，剩一则下七十，剩二则下一百四十；次五数之，剩一则下二十一，剩二则下四十二；次七数之，剩一则下十五，剩二则下三十，总计其数，然后退一百五，或多则退二百一十，之外余推。即得钱数也，有一诗隐括之：

三岁孩儿七十稀，五留廿一事尤奇，

七度上元重相会，寒食清明便可知。

（注：古时每年的正月十五日称为上元节，上元是指15，古称冬至一百零六天后是清明节，寒食节是清明节的前一天，“寒食清明”是指105的意思）.

宋，杨辉《续古摘奇算法》称它为**剪算法**

明，程大位《算法统宗》卷五载：

三人同行七十稀，五树梅花廿一枝，

七子团圆正月半，除百零五便得知。

（注：“除”字古时作“减”字解）.

这首诗通俗易懂，便于记忆，曾流传到日本，很受民间欢迎。

事实上《孙子算经》术曰的后半段，完全同近代数学的数论中的解一次同余式组的方法相同。

据钱宝琮著的《中国数学史》称：欧洲十八世纪中，欧拉（L. Euler 1707-1783年）、拉格朗日（J. Legronge 1736—1813年）等都曾对一次同余式问题进行过研究，德国数学家高斯（K. F. Gauss1777—1855年）于公元1801年出版的《算术研究》中明确地导出了上述定理。当时欧洲的数学家们对中国古数学毫无所知，高斯是通过独立研究得出他的成果的。公元1852年英国基督教士伟烈亚力（Wylie. Alexarder. 1815-1887年）将《孙子算经》中的“物不知数”问题的解法传到欧洲。公元1874年马蒂生（L. Mathiesen）指出孙子的解法符合高斯定理，从而在西文的数学史里将这个定理叫做**中国剩余定理**。

2 孙子定理与一次同余式组

为了进一步理解孙子定理与一次同余式组的关系，现在简要地介绍关于同余式的基础知识，然后再利用一次同余式组来解孙子定理，并在这个基础上把孙子定理加以推广，也就是把高斯定理介绍给读者，并应用它来解答一些更复杂的问题。

定义1 如果a、b都是整数，而m是一个确定的正整数，则当$m|(a-b)$（即m能够整除$(a-b)$）时，称a、b对于模m同余，记作：

$$a\equiv b \pmod{m}.$$

当$m\nmid(a-b)$（即m不能整除$a-b$）时，则称a、b对于模m不同余，记作：

$$a \not\equiv b \pmod{m}.$$

例如，$9|(29-2)$　（9能整除$(29-2)$），记作：

$$29 \equiv 2 \pmod{9}.$$

通俗地说：$29 \div 9 = 3$余2，$2 \div 9 = 0$余2，29和2用9除的余数是相同的，都余2。又例如，$93-(-7)=100=50\times 2$，所以说：

$$93 \equiv -7 \pmod{50}.$$

又如，$161-0=161$不能用8整除，所以说：

$$161 \not\equiv 0 \pmod{8}.$$

定义2　如果a、b都是整数，而m是一个正整数，当$a \not\equiv 0 \pmod{m}$时，我们把

$$ax+b \equiv 0 \pmod{m}$$

叫做模m的一次同余式。

定义3　如果c是使$ax+b\equiv 0 \pmod{m}$成立的一个整数，则$x\equiv c \pmod{m}$叫做$ax+b\equiv 0 \pmod{m}$的一个解。

例　求$256x\equiv 179 \pmod{337}$的整数解。由于

$337=256+81,\qquad 256=81\times 3+13,$

$81=13\times 6+3,\qquad 13=3\times 4+1;$

得到　$1=13-4\times 3=13-4(81-13\times 6)$

$=25\times 13-4\times 81=25(256-81\times 3)-4\times 81$

$=25\times 256-79\times 81=104\times 256-337\times 79.$

就是　$104\times 256-1=337\times 79,$　　所以有

$104\times 256\equiv 1 \pmod{337}.$

由$256x=179 \pmod{337}$得

$$104\times 256x\equiv 104\times 179 \pmod{337}.$$

又由　$104\times 179=55\times 337+81$得

$104\times 179\equiv 81 \pmod{337}.$

所以，$x\equiv 81 \pmod{337}$。

把孙子定理转化成一次同余式组的求解问题，即为

$$x\equiv 2 \pmod 3,\quad x\equiv 3 \pmod 5$$
$$x\equiv 2 \pmod 7.$$

为了有普遍意义，我们把它写成一般的一次同余式的求解问题：

已知m_1,m_2,m_3两两互素，并设

$$M=m_1\cdot m_2\cdot m_3=M_1m_1=M_2m_2=M_3m_3,$$

则同余式组

$$\begin{cases} x\equiv b_1 \pmod{m_1}, \\ x\equiv b_2 \pmod{m_2}, \\ x\equiv b_3 \pmod{m_3} \end{cases} \tag{A}$$

的解是$x\equiv b_1M_1'M_1+b_2M'_2M_2+b_3M_3'M_3$。这里的

$$M_1'M_1\equiv 1 \pmod{m_1},\qquad M_2'M_2\equiv 1 \pmod{m_2}$$
$$M_3'M_3\equiv 1 \pmod{m_3}.$$

证明 因为m_1,m_2,m_3两两互素，即有

$$(m_1,m_2)=(m_2,m_3)=(m_1,m_3)=1,$$

故有 $M_1=\dfrac{M}{m_1}$，于是$(M_1,m_1)=1$.同理有$(M_2,m_2)=1$，$(M_3,m_3)=1$.

由于$(M_1,m)=1$，所以必然存在两个整数M_1'和n_1，使得$M'M_1+m_1n_1=1$，即

$$M_1'M-1=-m_1n_1,\ m_1|(M_1'M-1),$$

故有 $M_1'M\equiv 1 \pmod{m_1}$，于是

$$b_1M_1'M_1\equiv b_1 \pmod{m_1}. \tag{1}$$

另一方面，因为$(m_1,m_2)\equiv 1$，$M_2=\dfrac{M}{m_2}$，则有$m_1|M_2$，于是 $M_2\equiv 0 \pmod{m_1}$因而有

$$b_2 M_2' M_2 \equiv 0 \pmod{m_1}. \qquad (2)$$

同理 $$b_3 M_3' M_3 \equiv 0 \pmod{m_1}. \qquad (3)$$

由于(1),(2),(3)我们有

$$b_1 M_1' M_1 + b_2 M_2' M_2 + b_3 M_3' M_3 \equiv b_1 \pmod{m_1}.$$

它满足于同余式组(A).

如果y也满足于同余式组(A)，即

$$x \equiv y \pmod{m_1}, \quad x \equiv y \pmod{m_2},$$
$$x \equiv y \pmod{m_3}.$$

就是 $m_1 \mid (x-y)$， $m_2 \mid (x-y)$， $m_3 \mid (x-y)$. 因为m_1, m_2，m_3是两两互素的，所以

$$m_1 \cdot m_2 \cdot m_3 \mid (x-y), \quad \text{即} \quad M \mid (x-y),$$

所以 $x \equiv y \pmod{M}$,

于是 $x = b_1 M_1' M_1 + b_2 M_2' M_2 + b_3 M_3' M_3 \pmod{M}$

是满足同余组(A)的唯一正整数解.

前面所引“物不知数”题中：

$$b_1 = 2, \quad b_2 = 3, \quad b_3 = 2;$$
$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7;$$

$$M = m_1 \cdot m_2 \cdot m_3 = 105, M_1 = \frac{105}{3} = 35,$$

$$M_2 = \frac{105}{5} = 21, \quad M_3 = \frac{105}{7} = 15.$$

再由 $M_1' M_1 \equiv 1 \pmod{m_1}$得到

$$M_1' 35 \equiv 1 \pmod{3}, \quad \therefore M'_1 = 2$$

同理 $M_2' 21 \equiv 1 \pmod{5}$， $M_2' = 1$，

$$M_3' 15 \equiv 1 \pmod{7}, \quad M_3' = 1.$$

从而 $x \equiv 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 \pmod{105}$

即 $x \equiv 233 \pmod{105}$， $x = 23 \pmod{105}$.

所以 $x=23+105k\quad(k=0,1,2,\cdots)$。以上是用同余式验证孙子定理。

3 孙子定理的推广

为了进一步理解孙子定理的普遍意义，让我们将其推广到一般形式。

定理 如果$K\geqslant 2$，而$m_1,m_2,m_3,\cdots,m_k$是两两互素的K个正整数，令

$$M=m_1\cdot m_2\cdots m_k=m_1M_1=m_2M_2=\cdots=m_kM_k$$

则同时满足同余式组

$$x=b_1\pmod{m_1},\ x_2=b_2\pmod{m_2},\cdots,x=b_k\pmod{m_k}$$

的正整数解是

$$x=b_1M_1'M_1+b_2M_2'M_2+\cdots+b_kM_k'M_k\pmod{M}\tag{A}$$

这里M_i'是满足同余式

$$M_i'M_i\equiv 1\pmod{m_i}\quad i=1,2,\cdots,K.\tag{1}$$

证明 因为$m_1,m_2,\cdots,m_k$是两两互素的，所以当$i\neq j$时，则有$(m_i,m_j)=1$.由$M_i=\dfrac{M}{m_i}$得到 $(M_i,m_i)=1$，所以

$$(M_1,m_1)=(M_2,m_2)=\cdots=(M_k,m_k)=1.$$

由$(M_1,m_1)=1$知M_1与m_1互素，故总存在两个整数M_1'，n_1使得$M_1\cdot M_1'+m_1n_1=1$，即有

$$M_1M_1'-1=-m_1n_1,\ m_1\mid(M_1M_1'-1).$$

按同余定义，有$M_1'M_1\equiv 1\pmod{m_1}$成立。

同样可知，对于每一个M_i，一定存在一个正整数M'_i使得

$$M'_iM_i\equiv 1\pmod{m_i}. \qquad (2)$$

另一方面，当$i\neq j$时，则由$(m_i,m_j)=1$和$M_j=\dfrac{M}{m_j}$使得$m_i|M_j$，所以有

$$M_j\equiv 0\pmod{m_i},\quad b_jM_j'M_j\equiv 0\pmod{m_i}. \qquad (3)$$

由（2），（3）有

$$b_1M_1'M_1+b_2M_2'M+\cdots+b_kM_k'M$$
$$\equiv b_iM'_iM_i\equiv b_i\pmod{m_i} \qquad (4)$$

由$m_1,m_2,\cdots,m_k$是两两互素的性质，知道(1)式是(A)式的正整数解。

如果y也满足（A）式，则由于（1）式是（A）式的正整数解，则得

$$x\equiv y\pmod{m_1},\ x\equiv y\pmod{m_2},\cdots,x\equiv y\pmod{m_k}.$$

即 $m_1|(x-y)$，$m_2|(x-y)$，$\cdots$，$m_k|(x-y)$。

又因为$m_1,m_2,\cdots m_k$是两两互素的，所以

$$M|(x-y),\ \text{即}\ x\equiv y\pmod{M}.$$

于是$x\equiv b_1M_1'M_1+b_2M_2'M_2+\cdots+b_kM_k'M_k\pmod{M}$是满足（$A$）式的唯一正整数解，因此孙子定理的推广得到证明。

有了这个推广定理，对于那些复杂的数学问题，就能很快地解答出来。下面举一些古算中的题目。用古算的求一术与应用孙子定理的推广来解，两者互相比较，就能弄清我国古代算法与近代算法之间的联系了。

4 古算中的求一术与孙子推广定理

宋，杨辉的《续古摘奇算法》载有下面几个类似的问题：

（1）七数剩一，八数剩二，九数剩三，本题总数几何？

答曰：四百九十八。

术曰：七余一，下二百八十八(题内余一，下二百八十八)。八余一，下四百四十一(题内余二，下八百八十二)。九余一，下二百八十(题内余三，下八百四十)。并之，二千一十，满五百四，去之(去三个五百四)，余四百九十八，合问。

现在用求一术来解释如下：

因为用 7 除余 1，同时又能被 8 和 9 整除的最小正整数是 $288 = 41\times7+1 = 8\times9\times4$.

用 8 除余 1，同时又能被 7 和9整除的最小正整数是$441 = 55\times8+1 = 7\times9\times7$，题内余2，所以 $2\times441 = 882$.

用 9 除 1，同时又能被 7 和 8 整除的最小正整数是 $280 = 9\times31+1 = 7\times8\times5$，题内余 3，所以，$3\times280 = 840$。

相加：$288+882+840 = 2010$.

减去：$3\times(8\times9\times7) = 3\times504 = 1512$.

答曰：$2010-1512 = 498$.

再用解一次同余式组的方法：

$x\equiv1 \pmod{7}$，$x\equiv2 \pmod{8}$，

$x\equiv3 \pmod{9}$；

$m_1 = 7$，$m_2 = 8$，$m_3 = 9$；

$b_1 = 1$，$b_2 = 2$，$b_3 = 3$；

$M = 7\times9\times8 = 504$；

$$M_1 = \frac{504}{7} = 72,\quad M_2 = \frac{504}{8} = 63,\quad M_3 = \frac{504}{9} = 56.$$

设M_1'是一个正整数，它满足

$M_1'M_1\equiv1 \pmod{7}$，则有

$1\equiv M_1'M = 72M_1' \pmod{7}$，$\therefore M_1' = 4$.

同理有

$1\equiv M_2'M_2=63M_2' \pmod{8}$， $\therefore M_2'=7$；

$1\equiv M_3'M_3=56M_3' \pmod{8}$， $\therefore M_3'=5$.

$x\equiv 1\times 72\times 4+2\times 63\times 7+3\times 56\times 5=2010 \pmod{504}$，

$x\equiv 498 \pmod{504}$；

$\therefore x=498+504k \quad (k=0,1,2,\cdots)$.

（2）二数余一，五数余二，七数余三，九数余四，问原数几何？

答曰：一百五十七。

术曰：二数余一，下三百五十(题内余一下三百一十五)；五数余一，下一百二十六(题内余二，下二百五十二)；七数余一，下五百四十(题内余三下一千六百二十)；九数余一，下一百八十(题内余四，下一千一百二十)；并之(三千三百零七)，满六百三十，去之(减去五个六百三十)，余一百五十七，即为总数。

用同余式组求法如下：

$x\equiv 1 \pmod{2}$， $x\equiv 2 \pmod{5}$，

$x\equiv 3 \pmod{7}$， $x\equiv 4 \pmod{9}$.

由高斯同余式定理知：

$m_1=2$， $m_2=5$， $m_3=7$， $m_4=9$；

$b_1=1$， $b_2=2$， $b_3=3$， $b_4=4$；

$$M=2\times 5\times 7\times 9=630;\quad M_1=\frac{M}{2}=315,$$

$$M_2=\frac{M}{5}=126,\quad M_3=\frac{M}{7}=90,\quad M_4=\frac{M}{9}=70.$$

设 $M_1'M\equiv 1 \pmod{2}$，则有

$1\equiv M_1'M_1\equiv 315M_1' \pmod{2}$， $\therefore M_1'=1$；

$1 \equiv M_2' M_2 \equiv 126 M_2' \pmod{5}$, $\therefore M_2' = 1$;

$1 \equiv M_3' M_3 \equiv 90 M_3' \pmod{7}$, $\therefore M_3' = 6$;

$1 \equiv M_4' M_4 \equiv 70 M_4' \pmod{9}$, $\therefore M_4' = 4$;

$$x \equiv 1\times1\times315 + 2\times1\times126 + 2\times6\times9 + 4\times4\times70$$

$$\equiv 157 \pmod{630};$$

于是得到 $x = 157 + 630k$, $k = 0, 1, 2, \cdots$

建议读者用上述方法试解下题：

（3）十一数余三，十二数余二，十三数余一，问原数几何？

从上面的例子可见杨辉的求一术的解法所得答数（指最小正整数解）与应用推广孙子定理所得的结果完全相同。

在民间流传有韩信点兵一类的算题，都可以用古算法中的求一术或推广孙子定理的方法来解。兹举一例。

（4）有兵一队，若排成五行纵队，则末行一人成六行纵队则末行五人成七行纵队，则末行四人，排成十一行纵队，则末行十人，求总兵数。

解：设x为所求兵数，则有

$x \equiv 1 \pmod{5}$, $x \equiv 5 \pmod{6}$,

$x \equiv 4 \pmod{7}$, $x \equiv 10 \pmod{11}$;

取 $m_1 = 5$, $m_2 = 6$, $m_3 = 7$, $m_4 = 11$;

$b_1 = 1$, $b_2 = 5$, $b_3 = 4$, $b_4 = 10$;

$M = 5\times6\times7\times11 = 2310$;

$$M_1 = \frac{2310}{5} = 462, \quad M_2 = \frac{2310}{6} = 385,$$

$$M_3 = \frac{2310}{7} = 330, \quad M_4 = \frac{2310}{11} = 210.$$

设M_1'是一个正整数，它满足$M_1' M_1 \equiv 1 \pmod{5}$则有

$1 \equiv M_1' M_1 = 462 M_1' \equiv 2 M_1' \pmod{5}$, $\therefore M_1' = 3$;