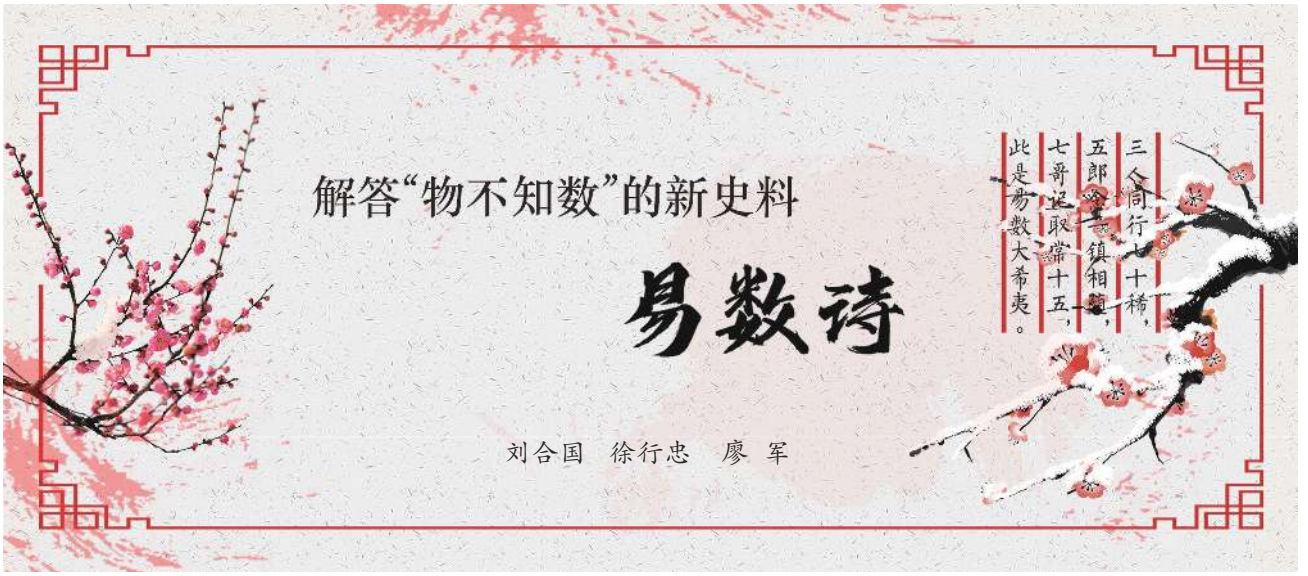

中国剩余定理从数系的运算法则出发，用最典型的线性组合来解决问题，其思想是极其深刻的。它是中国先贤智慧的结晶，也是中华文化的光辉篇章。近两百年来，中外数学史家对这个定理及其历史已经做了大量细致深入的研究，形成了诸多共识。不过，中国剩余定理的形成及其传播与华夏文明密切相连，其影响远远超越了数学范围，形成了一个非常独特的文化现象，这是值得从宏观角度加以专门论述的课题。要做到这点，必须从浩如烟海的古代文献里爬梳出有关定理的原始史料，尽可能复原定理传播的完整链条，这不是一蹴而就的事。作者在读书过程中，发现了一首解答“物不知数”的新歌诀。在南宋淳熙十五年编就的类书《锦绣万花谷》里，其前集之卷三十八留下了一条解答该问题的记录：“易数诗：三人同行七十稀，五郎念一镇相随，七哥记取常十五，此是易数大希夷。（无余者不算。）”在现今流传的数学资料里，都没有提及这首歌诀。“易数诗”问世时，秦九韶还未出生。这首歌诀比秦九韶的后辈周密《志雅堂杂钞》记录的歌诀至少要早 107 年，“易数诗”揭示了当时数学与《易》学之间的密切关系，也可以说揭示了数学对《易》学的依附关系。无疑这是一则关于中国剩余定理传播史的珍稀史料。也许，学问渊深见识高明的有心人可以由此入手，发掘更多的材料，进而从文化史的宏观角度阐述中国剩余定理在华夏文明史上的深层意义。

为行文和阅读方便，我们扼要地引入初等数论里模、同余的概念和符号。若 a 和 b 是任意两个整数，其中 $b>0$，由带余除法，存在两个整数 q 和 r，使得

$$a = bq + r, \qquad 0 \le r < b,$$

而且 q 和 r 都是唯一的，r 叫做 a 被 b 除所得到的余数。如果 $r=0$，我们就说 b 整除 a，记作 $b|a$。给定一个正整数 m，把它叫做模，如果用 m 分别去除整数 a 和 b 所得的余数相同，我们就说 a, b 对模 m 同余，记作 $a \equiv b(\mathrm{mod}\ m)$。这就是说，$a \equiv b(\mathrm{mod}\ m)$ 当且仅当 $m|(a-b)$。例如，$30 = 7\times 4 + 2$, $-5 = 7\times(-1) + 2$,

这样 $30 \equiv -5 \pmod 7$。又由于 $100 - 52 = 24 \times 2$，因而 $100 \equiv 52 \pmod{24}$。

众所周知，同余符号“≡”是大数学家高斯引入的，这是数学史上最成功、最具启发性的符号之一。

“物不知数”及其解答

《孙子算经》是中国古代的一部数学名著，大约成书于公元四百年前后，其卷下之 26 题，即是历史上有名的“物不知数”，中国剩余定理即溯源于此：

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？

用现代数学的语言重现这个问题，即求解同余方程组

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

《孙子算经》不仅给出了“物不知数”的正确答案，而且给出了令人叹为观止的完美解法[1]：

答曰：二十三。

[1] 孙子算经，中国科学技术典籍通汇·数学卷（一），河南教育出版社，郑州，1993.

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。

用数学算式重现“物不知数”的这个解法，即为：

$$140 + 63 + 30 = 233，233 - 210 = 23。$$

更一般些，《孙子算经》的上述文字给出了求解同余方程组

$$\begin{cases} x \equiv a \pmod 3 \\ x \equiv b \pmod 5 \\ x \equiv c \pmod 7 \end{cases}$$

的几个关键数字：70，21，15 和 105，并从这四个数字导出了该同余方程组的答案 r:

$$70a + 21b + 15c = 105q + r，\ 1 \le r \le 105。$$

《孙子算经》的这个解法是迂回的，不是单刀直入的，但它抓住了问题的本质，找到了最关键的节点，通过线性组合得到答案。这是绝顶的智慧！在求解“物不知数”的四个关键数字 70，21，15 和 105 里，105 是容易得到的，它就是三个模 3，5，7 的乘积，即 $3\times5\times7 = 105$，这样如何求出 70，21，15 就成为问题的核心了。借用现代数学的语言，70，21，15 分别满足下面的同余式组：

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 0 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}，\quad \begin{cases} y \equiv 0 \pmod 3 \\ y \equiv 1 \pmod 5 \\ y \equiv 0 \pmod 7 \end{cases}，\quad \begin{cases} z \equiv 0 \pmod 3 \\ z \equiv 0 \pmod 5 \\ z \equiv 1 \pmod 7 \end{cases}$$

于是 70，21，15 能够通过分别解下面的三个同余方程得到：

$$x = 35u \equiv 1 \pmod 3)，\quad y = 21v \equiv 1 \pmod 5)，\quad z = 15w \equiv 1 \pmod 7)$$

《孙子算经》是如何得到 70，21，15 这三个数字的，不见任何典籍记载，现在已经无从知晓。按照当时的数学水平，古人还没有掌握解同余方程的算法程式。不难想见，这些数字不是经过严格的数学理论推导得来，十九是妙手偶得的产物，这更加重了它们的神秘感，也为“物不知数”及其解答披上了一件神秘的外衣。直到秦九韶横空出世，这种局面才被打破。