中国剩余定理
与
Lagrange插值公式

●中国剩余定理的来源

中国剩余定理又称韩信点兵法, 中国剩余定理源出《孙子算经》，原题叫做“物不知数”, 原文如下：

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？

其意即为

“一个整数除以3 余2，除以5 余 3，除以7 余2，求这个整数”

《孙子算经》中不仅给出了答案23，还给出了这个问题的一般解法。

南宋大数学家秦九韶（公元1202-1261 年）在此基础上深入研究了一次同余式理论。并在其著作《数书九章》中明确地系统地叙述了求解一次同余式组的一般计算步骤。高斯在1801年出版的《算术探究》中系统地阐述了一次同余式组的理论。1852年，英国基督教士伟烈亚士将《孙子算经》“物不知数”的解法和秦九韶的“大衍求一术”传到欧洲。1874 年德国人马蒂生指出高斯的算法其实与孙子和泰九韶的方法一致。从此，这一方法在西方数学著作被正式命名为“中国剩余定理”。

秦九韶（公元1202－1261），字道古，安岳人。南宋大数学家秦九韶与李冶、杨辉、朱世杰并称宋元数学四大家。

秦九韶聪敏勤学。宋绍定四年（1231），秦九韶考中进士，先后担任县尉、通判、参议官、州守、同农、寺丞等职。后在湖北、安徽、江苏、浙江等地做官，1261年左右被贬至梅州（今广东梅县），不久死于任所。

秦九韶是一位既重视理论又重视实践，既善于继承又勇于创新的数学家．他所提出的大衍求一术和正负开方术及其名著《数书九章》，是中国数学史上光彩夺目的一页，对后世数学发展产生了广泛的影响．美国著名科学史家G. 萨顿(Sarton，1884－1956)说过，秦九韶是“他那个民族，他那个时代，并且确实也是所有时代最伟大的数学家之一”．

秦九韶的数学成就及对世界数学的贡献主要表现在以下方面：

1、秦九韶的《数书九章》是一部划时代的巨著

2、秦九韶的“大衍求一术”，领先高斯554年，被康托尔称为“最幸运的天才”

3、秦九韶的任意次方程的数值解领先英国人霍纳（W·G·Horner，1786—1837年）572年

● 中国剩余定理

设 $m_0, m_1, \cdots, m_n$ 是n+1个两两互素的正整数，$b_0, b_1, \cdots, b_n$ 是n+1个整数，那么同余方程组：

$$\begin{cases} x \equiv b_0 \pmod{m_0} \\ x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

有唯一解 $x \equiv \left(\sum_{i=0}^{n} b_i M_i M_i'\right) \pmod{m}$

这里 $m = m_0 \cdot m_1 \cdots m_n$，$M_i = \frac{m}{m_i}$，$0 \le i \le n$，其中 M_i' 满足

$$M_i \cdot M_i' \equiv 1 \pmod{m_i}$$

● 利用中国剩余定理，构造拉格朗日插值公式

设 $(x-x_i)$ $i=0,1,\cdots,n$ 是**n+1**个两两互素的多项式, 记

$$m(x)=\prod_{i=0}^{n}(x-x_i),\qquad M_i(x)=\frac{\prod_{i=0}^{n}(x-x_i)}{(x-x_i)},$$

b_i是n+1个不全为0的实数, 存在$f(x)$使得 $f(x_i)=b_i$， $i=0,1,\cdots,n$。

由余式定理 $x-x_i$ 除$f(x)$所得的余式等于 $f(x_i)=b_i$， 即

$$f(x)=f(x_i)(\operatorname{mod}(x-x_i))\ =b_i(\operatorname{mod}(x-x_i))$$

由中国剩余定理，同余方程组：

$$\begin{cases} f(x)\equiv b_0\ (\operatorname{mod} m_0)=b_0\ (\operatorname{mod}(x-x_0)) \\ f(x)\equiv b_1\ (\operatorname{mod} m_1)=b_1\ (\operatorname{mod}(x-x_1)) \\ \qquad\vdots \\ f(x)\equiv b_n\ (\operatorname{mod} m_n)=b_n\ (\operatorname{mod}(x-x_n)) \end{cases}$$

有唯一解。

由同余方程组的性质，可设 $f(x)=\sum_{i=0}^{n} f_i(x)$，其中 $f_0(x), f_1(x), \cdots, f_n(x)$ 满足同余方程组：

$$\begin{cases} f_0(x)\equiv b_0 \pmod{m_0} \\ f_0(x)\equiv 0 \pmod{m_1} \\ \vdots \\ f_0(x)\equiv 0 \pmod{m_n} \end{cases} \quad \begin{cases} f_1(x)\equiv 0 \pmod{m_0} \\ f_1(x)\equiv b_1 \pmod{m_1} \\ \vdots \\ f_1(x)\equiv 0 \pmod{m_n} \end{cases} \quad \cdots \quad \begin{cases} f_n(x)\equiv 0 \pmod{m_0} \\ f_n(x)\equiv 0 \pmod{m_1} \\ \vdots \\ f_n(x)\equiv b_n \pmod{m_n} \end{cases}$$

则 $f(x)=\sum_{i=0}^{n} k_i M_i(x)$，其中 $k_i = f_i(x)(\mathrm{mod}\,(x-x_i))$，再将 $(x-x_i)$ 代入，分别计算 k_i，即 $b_i = f(x_i)=k_i M_i(x_i)$， $i=0,1,\cdots,n$

$$k_i = \frac{b_i}{M_i(x_i)} = \frac{b_i}{(x_i-x_0)(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}$$

最终有

$$f(x)=\sum_{i=0}^{n} k_i M_i = \sum_{i=0}^{n} b_i \cdot M_i(x) M'(x_i)$$

$$= \sum_{i=0}^{n} f(x_i)\frac{(x-x_0)(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_0)(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}$$

拉格朗日插值公式。

不忘初心、谨记责任

民族自信，文化自信

作为中国文化的一个重要组成部分,中国古代数学，由于其自身的历史渊源和独特的发展过程，形成了与西方迥然不同的风格，成为世界数学发展的历史长河中一支不容忽视的源头。与世界其他民族的数学相比，中国数学源远流长，成就卓著。

我认为将来的数学是走中国古代数学的道路，而不是西方的欧几里得的道路。

——**吴文俊**