中国剩余定理

维基百科，自由的百科全书

中国剩余定理是数论中的一个关于一元线性同余方程组的定理，说明了一元线性同余方程组有解的准则以及求解方法。也称为**孙子定理**，古有“**韩信点兵**”、“**孙子定理**”、**求一术**（宋 沈括）“**鬼谷算**”（宋 周密）、“**隔墙算**”（宋 周密）、“**剪管术**”（宋 杨辉）、“**秦王暗点兵**”、“**物不知数**”之名。

目录

物不知数

一元线性同余方程组问题最早可见于中国南北朝时期（公元5世纪）的数学著作《孙子算经》卷下第二十六题，叫做“物不知数”问题，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？

即，一个整数除以三余二，除以五余三，除以七余二，求这个整数。《孙子算经》中首次提到了同余方程组问题，以及以上具体问题的解法，因此在中文数学文献中也会将中国剩余定理称为孙子定理。

宋朝数学家秦九韶于1247年《数书九章》卷一、二《大衍类》对“物不知数”问题做出了完整系统的解答。明朝数学家程大位将解法编成易于上口的《孙子歌诀》[1]：

> 三人同行七十希，五树梅花廿一支，七子团圆正半月，除百零五使得知

这个歌诀给出了模数为3、5、7时候的同余方程的秦九韶解法。意思是：将除以3得到的余数乘以70，将除以5得到的余数乘以21，将除以7得到的余数乘以15，全部加起来后除以105，得到的余数就是答案。比如说在以上的物不知数问题里面，使用以上的方法计算就得到

$$70 \times 2 + 21 \times 3 + 15 \times 2 = 233 = 2 \times 105 + 23.$$

因此按歌诀求出的结果就是23.

形式描述

用现代数学的语言来说明的话，中国剩余定理给出了以下的一元线性同余方程组：

$$(S):\quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

有解的判定条件，并用构造法给出了在有解情况下解的具体形式。

中国剩余定理说明：假设整数$m_1, m_2, \ldots, m_n$两两互质，则对任意的整数：$a_1, a_2, \ldots, a_n$，方程组(S)有解，并且通解可以用如下方式构造得到：

1. 设$M = m_1 \times m_2 \times \cdots \times m_n = \prod_{i=1}^{n} m_i$是整数$m_1, m_2, \ldots, m_n$的乘积，并设$M_i = M/m_i, \quad \forall i \in \{1, 2, \cdots, n\}$是除了$m_i$以外的$n$ - 1个整数的乘积。
2. 设$t_i = M_i^{-1}$为M_i模m_i的数论倒数：$t_i M_i \equiv 1 \pmod{m_i}, \quad \forall i \in \{1, 2, \cdots, n\}.$
3. 方程组(S)的通解形式为：$x = a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots + a_n t_n M_n + kM = kM + \sum_{i=1}^{n} a_i t_i M_i, \quad k \in \mathbb{Z}.$在模$M$的意义下，方程组$(S)$只有一个解：$x = \sum_{i=1}^{n} a_i t_i M_i.$

证明

从假设可知，对任何$i \in \{1, 2, \cdots, n\}$，由于$\forall j \in \{1, 2, \cdots, n\},\ j \neq i,\ \gcd(m_i, m_j) = 1$，所以$\gcd(m_i, M_i) = 1.$这说明存在整数$t_i$使得$t_i M_i \equiv 1 \pmod{m_i}.$这样的$t_i$叫做$M_i$模$m_i$的数论倒数。考察乘积$a_i t_i M_i$可知：

$$a_i t_i M_i \equiv a_i \cdot 1 \equiv a_i \pmod{m_i},$$
$$\forall j \in \{1, 2, \cdots, n\},\ j \neq i,\ \ a_i t_i M_i \equiv 0 \pmod{m_j}.$$

所以$x = a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots + a_n t_n M_n$满足：

$$\forall i \in \{1, 2, \cdots, n\},\ \ x = a_i t_i M_i + \sum_{j \neq i} a_j t_j M_j \equiv a_i + \sum_{j \neq i} 0 \equiv a_i \pmod{m_i}.$$

这说明x就是方程组(S)的一个解。

另外，假设x_1和x_2都是方程组(S)的解，那么：

$$\forall i \in \{1, 2, \cdots, n\},\ \ x_1 - x_2 \equiv 0 \pmod{m_i}.$$

而$m_1, m_2, \ldots, m_n$两两互质，这说明$M = \prod_{i=1}^{n} m_i$整除$x_1 - x_2.$所以方程组(S)的任何两个解之间必然相差M的整数倍。而另一方面，$x = a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots + a_n t_n M_n$是一个解，同时所有形式为：

$$a_1 t_1 M_1 + a_2 t_2 M_2 + \cdots + a_n t_n M_n + kM = kM + \sum_{i=1}^{n} a_i t_i M_i, \quad k \in \mathbb{Z}$$

的整数也是方程组(S)的解。所以方程组(S)所有的解的集合就是：

$$\{kM + \sum_{i=1}^{n} a_i t_i M_i\ ; \quad k \in \mathbb{Z}\}.$$

例子

使用中国剩余定理来求解上面的“物不知数”问题，便可以理解《孙子歌诀》中的数字含义。这里的线性同余方程组是：

$$(S): \quad \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

三个模数m_1=3, m_2=5, m_3=7的乘积是M=105，对应的M_1=35, M_2=21, M_3=15. 而可以计算出相应的数论倒数：t_1=2, t_2=1, t_3=1. 所以《孙子歌诀》中的70，21和15其实是这个“物不知数”问题的基础解：

$$70 = 2\times35 \equiv \begin{cases} 1 \pmod 3 \\ 0 \pmod 5 \\ 0 \pmod 7 \end{cases}, \ 21 = 1\times21 \equiv \begin{cases} 0 \pmod 3 \\ 1 \pmod 5 \\ 0 \pmod 7 \end{cases}, \ 15 = 1\times15 \equiv \begin{cases} 0 \pmod 3 \\ 0 \pmod 5 \\ 1 \pmod 7 \end{cases},$$

而将原方程组中的余数相应地乘到这三个基础解上，再加起来，其和就是原方程组的解：

$$2\times70 + 3\times21 + 2\times15 \equiv \begin{cases} 2\times1 + 3\times0 + 2\times0 \equiv 2 \pmod 3 \\ 2\times0 + 3\times1 + 2\times0 \equiv 3 \pmod 5 \\ 2\times0 + 3\times0 + 2\times1 \equiv 2 \pmod 7 \end{cases},$$

这个和是233，实际上原方程组的通解公式为：

$$x = 233 + k\times105,\ k \in \mathbb{Z}.$$

《孙子算经》中实际上给出了最小正整数解，也就是k=-2时的解：x=23.

交换环上的推广

主理想整环

设R是一个主理想整环，$m_1, m_2, \ldots, m_k$是其中的k个元素，并且两两互质。令$M=m_1m_2\ldots m_n$为这些元素的乘积，那么可以定义一个从商环R/MR映射到环乘积R/m_1R × … × R/m_kR的同态：

$$\phi: \ \mathrm{R}/M\mathrm{R} \longrightarrow \mathrm{R}/m_1\mathrm{R} \times \mathrm{R}/m_2\mathrm{R} \times \cdots \times \mathrm{R}/m_k\mathrm{R}$$

$$x + M\mathrm{R} \ \mapsto \ (x + m_1\mathrm{R}, x + m_2\mathrm{R}, \cdots, x + m_k\mathrm{R})$$

并且ϕ是一个环同构。因此ϕ的逆映射也存在。而这个逆映射的构造方式就如同中国剩余定理构造一元线性同余方程组的解一样。由于m_i和M_i=M/m_i互质，所以存在s_i和t_i使得

$$s_i m_i + t_i M_i = 1_\mathrm{R}.$$

而映射

$$\varphi:\ \ \mathrm{R}/m_1\mathrm{R}\times\mathrm{R}/m_2\mathrm{R}\times\cdots\times\mathrm{R}/m_k\mathrm{R}\longrightarrow\mathrm{R}/M\mathrm{R}$$

$$(a_1+m_1\mathrm{R},a_2+m_2\mathrm{R},\cdots,a_k+m_k\mathrm{R})\ \mapsto\ \sum_{i=1}^{k}a_it_iM_i+M\mathrm{R}$$

就是ϕ的逆映射。

$\mathbb{Z}$也是一个主理想整环。将以上的R换成$\mathbb{Z}$，就能得到中国剩余定理。因为

$$a_i+m_i\mathrm{R}=\{x;\ x\ \equiv\ a_i\pmod{m_i}\}$$

一般的交换环

设R是一个有单位元的交换环，$I_1, I_2, \ldots, I_k$是为环$\mathbf{R}$的理想，并且当$i\neq j$时，$I_i+I_j=\mathbf{R}$，则有典范的环同构：

$$\psi:\ \ \mathbf{R}/(I_1\cap\cdots\cap I_k)\longrightarrow\mathbf{R}/I_1\times\cdots\times\mathbf{R}/I_k$$

$$x+I_1\cap\cdots\cap I_n\longmapsto(x+I_1,x+I_2,\cdots,x+I_k).$$

模不两两互质的同余式组

模不两两互质的同余式组可化为模两两互质的同余式组，再用孙子定理直接求解。

84=2^2×3×7,160=2^5×5,63=3^2×7，由推广的孙子定理可得$\begin{cases}x\equiv 23\pmod{84}\\x\equiv 7\pmod{160}\\x\equiv 2\pmod{63}\end{cases}$与$\begin{cases}x\equiv 7\pmod{2^5}\\x\equiv 2\pmod{3^2}\\x\equiv 7\pmod{5}\\x\equiv 23\pmod{7}\end{cases}$同解。[2]

参见

- 埃拉托斯特尼筛法
- 素数判定法则
- 希尔伯特第十问题
- 哥德巴赫猜想
- 孪生素数猜想

参考资料

1. ^ 李俨《大衍求一术的过去和未来》《李俨.钱宝琮科学史全集》卷6 121页《程大位的孙子歌》辽宁教育出版社. 1998
2. ^ 推广的孙子定理 (http://www.cnki.com.cn/Article/CJFDTotal-GLKX201003013.htm).

参考书目

- *数学的100个基本问题*，靳平 主编，ISBN 7-5377-2171-8

取自“http://zh.wikipedia.org/w/index.php?title=中国剩余定理&oldid=30701497”