Pure Mathematics 理论数学, 2019, 9(3), 265-269
Published Online May 2019 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2019.93034

Hans汉斯

A Proof of Chinese Remainder Theorem

Jiming Yang

Department of Mathematics, Yuxi Normal University, Yuxi Yunnan
Email: jmy1963@163.com

Received: Apr. 14th, 2019; accepted: Apr. 25th, 2019; published: May 6th, 2019

Abstract

A proof of Chinese Remainder Theorem is given.

Keywords

Chinese Remainder Theorem, Proof, Congruence

孙子定理的一个证明

杨继明

玉溪师范学院数学系，云南 玉溪
Email: jmy1963@163.com

收稿日期：2019年4月14日；录用日期：2019年4月25日；发布日期：2019年5月6日

摘　要

本文给出了孙子定理的一个证明。

关键词

孙子定理，证明，同余式

文章引用: 杨继明. 孙子定理的一个证明[J]. 理论数学, 2019, 9(3): 265-269. DOI: 10.12677/pm.2019.93034

1. 引言

在公元四、五世纪的《孙子算经》中的“物不知数”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?”答案为：“23”。这个问题也就是求解同余式组

$$x\equiv 2\left(\mathrm{mod}\,3\right),x\equiv 3\left(\mathrm{mod}\,5\right),x\equiv 2\left(\mathrm{mod}\,7\right).$$

明朝程大位根据孙子算经里所用的方法用歌谣给出了该题的解法：“三人同行七十稀，五树梅花廿一枝，七子团圆月正半，除百零五便得知。”即解为

$$x\equiv 2\times 70+3\times 21+2\times 15\equiv 233\equiv 23\left(\mathrm{mod}\,105\right).$$

在西方，与《孙子算经》同类的算法，最早见于 1202 年意大利数学家斐波那契的《算经》。1801 年，德国数学家高斯的《算术探究》中，才明确写出了这一问题的求法。

把孙子算经给出的结果加以推广，就得到了著名的孙子定理。孙子定理及其证明参阅[1] [2]。文[3]给出了一个求解孙子问题的简便方法。文[4]研究了一般的线性同余式组的有解判别条件及其求解方法。文[5]把线性同余式组、线性不定方程组、线性代数方程组、常系数线性微分方程组和常系数线性差分方程组统一成为了 R-模上的方程组，并分别给出了各种方程组的解法。

2. 主要结果及应用

下面的定理 1 就是著名的孙子定理。

定理 1 (孙子定理) 设 $m_1,m_2,\cdots,m_k$ 是 k 个两两互质的正整数，

$$m=m_1m_2\cdots m_k,m=m_iM_i,i=1,2,\cdots,k,$$

则同余式组

$$x\equiv b_1\left(\mathrm{mod}\,m_1\right),x\equiv b_2\left(\mathrm{mod}\,m_2\right),\cdots,x\equiv b_k\left(\mathrm{mod}\,m_k\right). \tag{1}$$

的解是

$$x\equiv M_1'M_1b_1+M_2'M_2b_2+\cdots+M_k'M_kb_k\left(\mathrm{mod}\,m\right), \tag{2}$$

其中

$$M_i'M_i\equiv 1\left(\mathrm{mod}\,m_i\right),i=1,2,\cdots,k. \tag{3}$$

文[1]给出了该定理的三种证明方法。下面我们再给出一种证法。

证 因 $m_1,m_2,\cdots,m_k$ 是 k 个两两互质的正整数，故 $\left(M_i,m_i\right)=1,i=1,2,\cdots,k$。于是，满足(3)式的整数 $M_i'\left(i=1,2,\cdots,k\right)$ 是存在的。

要证明同余式组(1)的解是(2)，只需证明(1)式和(2)式等价即可。

设整数 x 满足(1)式，则 $x\equiv b_i\left(\mathrm{mod}\,m_i\right),i=1,2,\cdots,k$，从而

$$M_i'M_ix\equiv M_i'M_ib_i\left(\mathrm{mod}\,m_i\right),i=1,2,\cdots,k.$$

因为当 $i\neq j$ 时，$m_i\mid M_j$，故

$$\left(M_1'M_1+\cdots+M_k'M_k\right)x\equiv M_1'M_1b_1+\cdots+M_k'M_kb_k\left(\mathrm{mod}\,m_i\right),i=1,2,\cdots,k.$$

从而

$$\left(M_1'M_1+\cdots+M_k'M_k\right)x\equiv M_1'M_1b_1+\cdots+M_k'M_kb_k\left(\mathrm{mod}\,m\right). \tag{4}$$

因 $M_i'(i=1,2,\cdots,k)$ 满足(3)式，故

$$M_1'M_1+M_2'M_2+\cdots+M_k'M_k\equiv 1(\bmod m_i),i=1,2,\cdots,k. \tag{5}$$

因 $m_1,m_2,\cdots,m_k$ 两两互质，故由(5)式得

$$M_1'M_1+M_2'M_2+\cdots+M_k'M_k\equiv 1(\bmod m) \tag{6}$$

由(4)和(6)两式即知，(2)式成立。

反之，设整数 x 满足(2)式，则由 $m_i\mid M_j\ (i\neq j)$ 和(3)式得

$$\begin{aligned}x&\equiv M_1'M_1b_1+M_2'M_2b_2+\cdots+M_k'M_kb_k\\&\equiv M_i'M_ib_i\equiv b_i(\bmod m_i),i=1,\cdots,k\end{aligned}.$$

即整数 x 满足(1)式。

应用定理 1 求解孙子问题的例子参见文[1] [2]。下面给出一个更便于求解孙子问题的方法。

定理 2 设 $m_1,m_2,\cdots,m_k$ 是 k 个两两互质的正整数，则同余式组(1)的解为

$$x\equiv c_1+M_1c_2+M_2c_3+\cdots+M_{k-1}c_k(\bmod m), \tag{7}$$

其中，

$$M_i=m_1m_2\cdots m_i,i=1,2,\cdots,k, \tag{8}$$

而 $m=M_k$，

$$\begin{cases}c_1\equiv b_1(\bmod m_1),\\c_2\equiv M_1'(b_2-c_1)(\bmod m_2),\\c_3\equiv M_2'\left[b_3-(c_1+M_1c_2)\right](\bmod m_3),\\\quad\vdots\\c_k\equiv M_{k-1}'\left[b_k-(c_1+M_1c_2+\cdots+M_{k-2}c_{k-1})\right](\bmod m_k),\end{cases} \tag{9}$$

$$M_i'M_i\equiv 1(\bmod m_{i+1}),i=1,2,\cdots,k-1. \tag{10}$$

证 因 $m_1,m_2,\cdots,m_k$ 两两互质，故满足(10)式的整数 M_i' 是存在的。首先证明，

$$c_1+M_1c_2+M_2c_3+\cdots+M_{k-1}c_k\equiv b_i(\bmod m_i),i=1,2,\cdots,k. \tag{11}$$

显然，$c_1+M_1c_2+M_2c_3+\cdots+M_{k-1}c_k\equiv b_i(\bmod m_i),i=1,2$．而当 $3\le i\le k$ 时，由(8)，(9)和(10)式得

$$\begin{aligned}&c_1+M_1c_2+M_2c_3+\cdots+M_{k-1}c_k\equiv c_1+M_1c_2+\cdots+M_{i-2}c_{i-1}+M_{i-1}c_i\\&\equiv c_1+M_1c_2+\cdots+M_{i-2}c_{i-1}+M_{i-1}\cdot M_{i-1}'\left[b_i-(c_1+M_1c_2+\cdots+M_{i-2}c_{i-1})\right]\\&\equiv c_1+M_1c_2+\cdots+M_{i-2}c_{i-1}+1\cdot\left[b_i-(c_1+M_1c_2+\cdots+M_{i-2}c_{i-1})\right]=b_i(\bmod m_i)\end{aligned}.$$

要证明同余式组(1)的解是(7)，只需证明(1)式和(7)式等价即可。设整数 x 满足(1)式，则

$$x\equiv b_i(\bmod m_i),i=1,2,\cdots,k. \tag{12}$$

由(11)和(12)式得

$$x\equiv c_1+M_1c_2+M_2c_3+\cdots+M_{k-1}c_k(\bmod m_i),i=1,2,\cdots,k.$$

但 $m_1,m_2,\cdots,m_k$ 两两互质，故(7)式成立。

反之，设整数 x 满足(7)式，则

$$x\equiv c_1+M_1c_2+M_2c_3+\cdots+M_{k-1}c_k(\bmod m_i),i=1,2,\cdots,k. \tag{13}$$

由(11)和(13)式得，(1)式成立。

推论 设 $m_1,m_2,\cdots,m_k$ 是 k 个两两互质的正整数，$M_i=m_1m_2\cdots m_i\left(i=1,2,\cdots,k\right)$，$m=M_k$，整数 M_i' 满足

$$M_i'M_i\equiv 1\left(\mathrm{mod}\,m_{i+1}\right),i=1,2,\cdots,k-1,$$

c_1 是 b_1 被 m_1 除所得的余数，c_2 是 $M_1'\left(b_2-c_1\right)$ 被 m_2 除所得的余数，c_3 是 $M_2'\left[b_3-\left(c_1+M_1c_2\right)\right]$ 被 m_3 除所得的余数，…，c_k 是 $M_{k-1}'\left[b_k-\left(c_1+M_1c_2+\cdots+M_{k-2}c_{k-1}\right)\right]$ 被 m_k 除所得的余数，则同余式组(1)的解为

$$x\equiv c_1+M_1c_2+\cdots+M_{k-1}c_k\left(\mathrm{mod}\,m\right),\tag{14}$$

其中 $0\le c_1+M_1c_2+\cdots+M_{k-1}c_k\le m-1$。

证 根据定理 2，(14)为同余式组(1)的解．下面证明

$$0\le c_1+M_1c_2+\cdots+M_{k-1}c_k\le m-1.$$

易知，$0\le c_i\le m_i-1,i=1,2,\cdots,k$。故

$$0\le c_1+M_1c_2\le m_1-1+M_1\left(m_2-1\right)=M_1-1+M_1\left(m_2-1\right)=M_2-1,$$

$$0\le c_1+M_1c_2+M_2c_3\le M_2-1+M_2\left(m_3-1\right)=M_3-1,$$

$$\cdots$$

$$0\le c_1+M_1c_2+\cdots+M_{k-1}c_k\le M_{k-1}-1+M_{k-1}\left(m_k-1\right)=M_k-1=m-1.$$

例 1 解同余式组

$$x\equiv 1\left(\mathrm{mod}\,3\right),x\equiv -1\left(\mathrm{mod}\,5\right),x\equiv 2\left(\mathrm{mod}\,7\right),x\equiv -2\left(\mathrm{mod}\,11\right).$$

解 为了更便于应用定理 2 的推论求解，把这个同余式组改写为

$$x\equiv -2\left(\mathrm{mod}\,11\right),x\equiv 2\left(\mathrm{mod}\,7\right),x\equiv -1\left(\mathrm{mod}\,5\right),x\equiv 1\left(\mathrm{mod}\,3\right).$$

这里，$m_1=11,m_2=7,m_3=5,m_4=3,b_1=-2,b_2=2,b_3=-1,b_4=1$。

$$\begin{aligned}&M_1=m_1=11,M_2=m_1m_2=11\times 7=77,\\&M_3=m_1m_2m_3=77\times 5=385,\\&M_4=m_1m_2m_3m_4=385\times 3=1155=m\end{aligned}.$$

取满足 $M_1'M_1\equiv 1\left(\mathrm{mod}\,m_2\right)$ 即 $11M_1'\equiv 1\left(\mathrm{mod}\,7\right)$ 的一个整数 $M_1'=2$。

取满足 $M_2'M_2\equiv 1\left(\mathrm{mod}\,m_3\right)$ 即 $77M_2'\equiv 1\left(\mathrm{mod}\,5\right)$ 的一个整数 $M_2'=-2$。

取满足 $M_3'M_3\equiv 1\left(\mathrm{mod}\,m_4\right)$ 即 $385M_3'\equiv 1\left(\mathrm{mod}\,3\right)$ 的一个整数 $M_3'=1$。

$$b_1=-2\equiv 9\left(\mathrm{mod}\,11\right),c_1=9.$$

$M_1'\left(b_2-c_1\right)=2\left(2-9\right)\equiv 0\left(\mathrm{mod}\,7\right)$，$c_2=0$，则

$$c_1+M_1c_2=9+11\times 0=9.$$

$M_2'\left[b_3-\left(c_1+M_1c_2\right)\right]=2\left(-1-9\right)\equiv 0\left(\mathrm{mod}\,5\right)$，$c_3=0$，则

$$c_1+M_1c_2+M_2c_3=9+77\times 0=9.$$

$M_3'\left[b_4-\left(c_1+M_1c_2+M_2c_3\right)\right]=1\times\left(1-9\right)=-8\equiv 1\left(\mathrm{mod}\,3\right)$，$c_4=1$，则

$$c_1+M_1c_2+M_2c_3+M_3c_4=9+385\times 1=394.$$

故由定理 2 的推论得，该同余式组的解为

$$x \equiv 394 \pmod{1155}.$$

例 2 解同余式组

$$x \equiv b_1 \pmod{11}, x \equiv b_2 \pmod{7}, x \equiv b_3 \pmod{6}, x \equiv b_4 \pmod{5}.$$

解 这里 $m_1 = 11, m_2 = 7, m_3 = 6, m_4 = 5$，

$$M_1 = m_1 = 11, M_2 = m_1 m_2 = 77, M_3 = 462, M_4 = 2310 = m.$$

由 $11M_1' \equiv 1 \pmod{7}$ 取 $M_1' = 2$。

由 $77M_2' \equiv 1 \pmod{6}$ 取 $M_2' = -1$。

由 $462M_3' \equiv 1 \pmod{5}$ 取 $M_3' = -2$。

由 $c_1 \equiv b_1 \pmod{\bmod 11}$ 取 $c_1 = b_1$。

由 $c_2 \equiv M_1'(b_2 - c_1) = 2b_2 - 2b_1 \pmod{7}$ 取 $c_2 = 2b_2 - 2b_1$，则

$$c_1 + M_1 c_2 = b_1 + 11(2b_2 - 2b_1) = 22b_2 - 21b_1.$$

由

$$c_3 \equiv M_2'\left[b_3 - (c_1 + M_1 c_2)\right] = -\left[b_3 - (22b_2 - 21b_1)\right] \equiv -b_3 - 2b_2 + 3b_1 \pmod{6}$$ 取 $c_3 = -b_3 - 2b_2 + 3b_1$，则

$$c_1 + M_1 c_2 + M_2 c_3 = 22b_2 - 21b_1 + 77(-b_3 - 2b_2 + 3b_1) = -77b_3 - 132b_2 + 210b_1.$$

由

$$\begin{aligned} c_4 &\equiv M_3'\left[b_4 - (c_1 + M_1 c_2 + M_2 c_3)\right] \\ &= -2\left[b_4 - (-77b_3 - 132b_2 + 210b_1)\right], \\ &\equiv -2b_4 + b_3 + b_2 \pmod{5} \end{aligned}$$

取 $c_4 = -2b_4 + b_3 + b_2$，则

$$\begin{aligned} &c_1 + M_1 c_2 + M_2 c_3 + M_3 c_4 \\ &= -77b_3 - 132b_2 + 210b_1 + 462(-2b_4 + b_3 + b_2). \\ &= -924b_4 + 385b_3 + 330b_2 + 210b_1 \end{aligned}$$

故由定理 2 得，同余式组的解为

$$x \equiv -924b_4 + 385b_3 + 330b_2 + 210b_1 \pmod{2310},$$

即

$$x \equiv 1386b_4 + 385b_3 + 330b_2 + 210b_1 \pmod{2310}.$$

参考文献

[1] 潘承洞, 潘承彪. 初等数论(第二版) [M]. 北京: 北京大学出版社, 2003.

[2] 闵嗣鹤, 严士健. 初等数论(第三版) [M]. 北京: 高等教育出版社, 2003.

[3] 杨继明. 解一元线性同余式组的一个简便方法[J]. 抚州师专学报(自然科学版), 1996(3): 22-23.

[4] 杨继明, 李桂仙. 关于线性不定方程组与线性同余式组[J]. 甘肃教育学院学报(自然科学版), 2000, 14(2): 16-21.

[5] 杨继明. 关于 R-模上的方程组[J]. 南都学坛, 1994, 14(6): 18-25.

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2160-7583，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：pm@hanspub.org