文章编号:1000-5471(2012)04-0213-04

中国剩余定理及其应用

——基于研究性学习的设计①

李 懋

西南大学 数学与统计学院,重庆 400715

摘要:中国剩余定理在数论及代数理论的研究中起着重要的作用,是一个极其重要的定理.通过中国剩余定理的历史起源来给出该定理及其证明方法,在此基础上对该定理的应用进行了讨论和分析,并给出了一些例子.

关 键 词:中国剩余定理;同余式组;模

中图分类号:G420 **文献标志码**:A

中国剩余定理具有浓厚的历史积淀并已得到广泛的研究[1-6],是数论中的重要定理之一,在代数学和其它数学领域中有非常重要的应用.所以在该定理的教学中,应该采取多种手段、充分利用各种资源(比如课前让学生利用网络、图书馆等资源查阅相关资料,上课时老师讲解、同学讨论交流并总结,课后思考等),将该部分内容的学习组织成一个研究性学习课题.

下面我们主要从中国剩余定理的历史背景出发,讨论该定理及其一些应用.

1 中国剩余定理的背景

我国数学文化历史悠久.古代的数学家提出了许多问题并研究了其解法,如《孙子算经》中的"物不知其数"问题就是其中的一个典型例子."物不知其数"一问为:"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?"用同余符号表示,即为求正整数 x,使 $x\equiv 2(\mathrm{mod}\ 3)$,$x\equiv 3(\mathrm{mod}\ 5)$,$x\equiv 2(\mathrm{mod}\ 7)$.故"物不知其数"问题即为求同余式组解的问题.对于该问题,程大为在《算法统宗》里给出了奇妙的解法,有歌诀:"三人同行七十稀,五树梅花廿一枝,七子团圆正半月,除百零五便得知",得到的解答式为:$2\times 70+3\times 21+2\times 15=233$,减去 105 的 2 倍,得 23,这就是所求的数.到此,"物不知其数"问题就得到了完美的解决.把所用的算法推广就成为著名的中国剩余定理.

2 中国剩余定理及其证明

定理 1(中国剩余定理) 设 $m_1,\cdots,m_k$ 是 k 个两两互素的正整数,那么对整数 $a_1,\cdots,a_k$,一次同余式组

$$x\equiv a_j(\mathrm{mod}\ m_j)\qquad 1\leqslant j\leqslant k \tag{1}$$

对模 $m=m_1\cdots m_k$ 有唯一的解.

证 用构造法来证明.

设 $M_j=\dfrac{m}{m_j}=m_1\cdots m_{j-1}m_{j+1}\cdots m_k$.由 $i\neq j$,$(m_i,m_j)=1$ 有 $(m_j,M_j)=1$,因此对每个 M_j,必存在 M_j',

① 收稿日期:2011-9-20
基金项目:中央高校基本科研业务专项资金(XDJK2010C058);高等学校博士学科点专项科研基金(20100181110073).
作者简介:李 懋(1981-),女,四川眉山人,博士研究生,讲师,主要从事数论的研究.

使得 $M_j'M_j \equiv 1 \pmod{m_j}$. 现在构造 $x = M_1'M_1a_1 + \cdots + M_k'M_ka_k$, 下证这个整数 x 是同余式组(1)解.

由 $m_j \mid M_i$, $j \neq i$, 有 $M_i \equiv 0 \pmod{m_j}$. 因此对于 x 来说, 除了第 j 项外都同余0模 m_j. 故由 $M_j'M_j \equiv 1 \pmod{m_j}$ 有 $x \equiv M_jM_j'a_j \equiv a_j \pmod{m_j}$.

下证任意两个解对模 m 是同余的.

设 x_0 和 x_1 都是同余式组(1)的解. 那么对每个 j ($j=1,\cdots,k$), 有 $x_0 \equiv x_1 \equiv a_j \pmod{m_j}$, 使得 $m_j \mid (x_0 - x_1)$. 由于 $m_1,\cdots,m_k$ 是两两互素的, 所以有 $m \mid (x_0 - x_1)$. 因此 $x_0 \equiv x_1 \pmod{m}$. 这就得到: 同余式组(1)对模 m 的解是唯一的.

注1 (1°) 定理1的证明方法不是唯一的, 还可以用归纳法来证明. 鼓励学生从不同的角度思考问题, 寻求解决问题的各种方法, 启发学生的主动思维;

(2°) 向学生强调: 定理1要求"模两两互素", 如果条件不成立, 那么就不能直接使用定理1求解一次同余式组. 对于模不是两两互素的情形, 请学生思考该如何求解;

(3°) 中国剩余定理是一个非常重要的定理, 在教学过程中, 要加强知识的内在联系, 启发学生面对一个问题时, 把相关知识联系起来, 把问题向纵横两方面作可能的推广.

中国剩余定理实质上刻画了剩余系的结构:

定理2 设 $m_1,\cdots,m_k,m,M_j,M_j'(j=1,\cdots,k)$ 同定理1所设, 再设

$$x = M_1'M_1x^{(1)} + \cdots + M_k'M_kx^{(k)}$$

那么, x 遍历模 m 的完全(简化)剩余系的充要条件是 $x^{(j)}$ 分别遍历 m_j 的完全(简化)剩余系.

定理2的证明过程比较简单, 可请学生课后自行思考.

把中国剩余定理推广到环上, 让学生知道模理想的同余式具有模整数的同余式的基本性质.

环 $A_1,\cdots,A_n$ 的外直和定义为

$$A_1 \oplus \cdots \oplus A_n = \{(x_1, \cdots, x_n)\} \qquad x_i \in A_i,\ i=1,\cdots,n$$

其加法和乘法均按分量定义(各分量自加、自乘).

定理3[5] 设 A 为含幺交换环, 理想 $I_1,\cdots,I_n$ 两两互素. 则有商环的同构

$$A/(I_1\cdots I_n) \longrightarrow (A/I_1) \oplus \cdots \oplus (A/I_n)$$

$$x + (I_1\cdots I_n) \longmapsto (x + I_1, \cdots, x + I_n)$$

也就是说, 任给 $b_1,\cdots,b_n \in A$, 存在 $x \in A$(在模 $I_1,\cdots,I_n$ 意义下唯一), 使

$$x \equiv b_i \pmod{I_i} \qquad i=1,\cdots,n$$

推论 若幺环 A 的理想 $I_1,\cdots,I_n$ 两两互素而且 $I_1 \cap \cdots \cap I_n = (0)$, 则有同构

$$A \cong (A/I_1) \oplus \cdots \oplus (A/I_n)$$

3 中国剩余定理的应用

中国剩余定理的应用很广泛, 下面对其应用举几个简单的例子.

3.1 在同余式组中的应用

有了中国剩余定理及其证明, 我们在求解一次同余式组时就可以直接带入计算了.

我国古代大数学家杨辉在1275年写了一本书叫《续古摘奇算法》, 下面我们从中选出一例求解:

例1 11数余3, 12数余2, 13数余1, 问本数.

解 依题意有 $x \equiv 3 \pmod{11}$, $x \equiv 2 \pmod{12}$, $x \equiv 1 \pmod{13}$. 在定理1中取

$$m_1 = 11 \qquad m_2 = 12 \qquad m_3 = 13$$

$$a_1 = 3 \qquad a_2 = 2 \qquad a_3 = 1$$

此时有

$$m = 11 \cdot 12 \cdot 13 = 1\,716 \qquad M_1 = \frac{1\,716}{11} = 156$$

$$M_2 = \frac{1\,716}{12} = 143 \qquad M_3 = \frac{1\,716}{13} = 132$$

下面求 M_j'. 先求 M_1'，解 $1 \equiv 156M_1' \equiv 2M_1' (\mathrm{mod}\ 11)$ 得 $M_1' \equiv 6(\mathrm{mod}\ 11)$；再求 M_2'，解 $1 \equiv 143M_2' \equiv 11M_2' (\mathrm{mod}\ 12)$ 得 $M_2' \equiv 11(\mathrm{mod}\ 12)$；最后求 M_3'，解 $1 \equiv 132M_3' \equiv 2M_3' (\mathrm{mod}\ 13)$ 得 $M_3' \equiv 7(\mathrm{mod}\ 13)$. 故

$$x \equiv 3 \cdot 6 \cdot 156 + 2 \cdot 11 \cdot 143 + 7 \cdot 132 \cdot 1 \equiv 14(\mathrm{mod}\ 1\ 716)$$

即得 $x = 14 + 1\ 716k$ $(k = 0,1,2,\cdots)$.

3.2　在同余方程中的应用

中国剩余定理不但提供了一次同余式组(1)的解法，对于研究同余方程(方程组)也很有意义.

定理 4　设正整数 m 的标准分解式为 $m = p_1^{r_1} \cdots p_k^{r_k}$，$f(x)$ 是一个整系数的多项式. $f(x) \equiv 0(\mathrm{mod}\ m)$ 有解的充要条件是 $f(x) \equiv 0(\mathrm{mod}\ p_i^{r_i})(i = 1,\cdots,k)$ 有解.

证　如果 $f(x) \equiv 0(\mathrm{mod}\ m)$ 有整数解，那么存在整数 a 使得 $m \mid f(a)$. 由 $p_i^{r_i} \mid m$，有 $p_i^{r_i} \mid f(a)$. 因此同余式 $f(x) \equiv 0(\mathrm{mod}\ p_i^{r_i})(i = 1,\cdots,k)$ 是有解的.

反之，假设同余式 $f(x) \equiv 0(\mathrm{mod}\ p_i^{r_i})(i = 1,\cdots,k)$ 是有解的，则对每个 i，存在整数 a_i 使得 $f(a_i) \equiv 0(\mathrm{mod}\ p_i^{r_i})$. 因为 $p_1^{r_1},\cdots,p_k^{r_k}$ 是两两互素的，由定理 1 知，存在整数 a，使得

$$a \equiv a_i(\mathrm{mod}\ p_i^{r_i}) \qquad i = 1,\cdots,k$$

因此 $f(a) \equiv f(a_i) \equiv 0(\mathrm{mod}\ p_i^{r_i})(i = 1,\cdots,k)$. 因为 $p_i^{r_i} \mid f(a)(i = 1,\cdots,k)$，而 $m = p_1^{r_1} \cdots p_k^{r_k}$，所以 $m \mid f(a)$，故 $f(a) \equiv 0(\mathrm{mod}\ m)$.

3.3　在计算机领域上的应用

中国剩余定理为计算机上的大数计算提供了方法. 该定理告诉我们：对于给定的两两互素的模 $m_1,\cdots,m_k$，小于 $M = m_1 \cdots m_k$ 的正整数 n 是由它的最小正剩余模 $m_j(j = 1,\cdots,k)$ 唯一决定的. 假设计算机的字长只有 100，但是我们希望计算 10^6 的整数，该怎么办？首先要找到比 100 小但是乘积比 10^6 大的两两互素的整数，比如可以选 $m_1 = 99$，$m_2 = 98$，$m_3 = 97$，$m_4 = 95$，把比 10^6 小的整数改写为包含模 m_1,m_2,m_3,m_4 的最小正剩余的四元组；然后，比如求整数和，我们只需要利用已知结论："如果 $x \equiv x_i(\mathrm{mod}\ m_i)$ 和 $y \equiv y_i(\mathrm{mod}\ m_i)$，那么 $x + y \equiv x_i + y_i(\mathrm{mod}\ m_i)$"，分别把它们的最小正剩余模 m_1,m_2,m_3,m_4 相加；最后根据中国剩余定理求解就行了.

例 2　在字长为 100 的计算机上求 $x = 123\ 684$ 与 $y = 413\ 456$ 的和.

解　我们有

$$x \equiv 33(\mathrm{mod}\ 99) \qquad y \equiv 32(\mathrm{mod}\ 99)$$
$$x \equiv 8(\mathrm{mod}\ 98) \qquad y \equiv 92(\mathrm{mod}\ 98)$$
$$x \equiv 9(\mathrm{mod}\ 97) \qquad y \equiv 42(\mathrm{mod}\ 97)$$
$$x \equiv 89(\mathrm{mod}\ 95) \qquad y \equiv 16(\mathrm{mod}\ 95)$$

因此有

$$x + y \equiv 65(\mathrm{mod}\ 99)$$
$$x + y \equiv 2(\mathrm{mod}\ 98)$$
$$x + y \equiv 51(\mathrm{mod}\ 97)$$
$$x + y \equiv 10(\mathrm{mod}\ 95)$$

现在可以利用定理 1 来求 $x + y(\mathrm{mod}\ 99 \cdot 98 \cdot 97 \cdot 95)$，解得

$$x + y \equiv 65 \cdot 903\ 070 \cdot 37 + 2 \cdot 912\ 285 \cdot 33 + 51 \cdot 921\ 690 \cdot 24 + 10 \cdot 941\ 094 \cdot 4 =$$
$$3\ 397\ 886\ 480 \equiv 537\ 140(\mathrm{mod}\ 89\ 403\ 930)$$

因为 $0 < x + y < 89\ 403\ 930$，所以可以得到 $x + y = 537\ 140$.

注 2　例 2 可以让学生自己在计算机上编程实现. 现在计算机已经成为学生学习生活中必不可少的工具，学生利用计算机自己解决问题，从实践、操作等多方面得到丰富的体验，从而更容易激发学生对知识的学习兴趣，使学生以研究性学习者的角色参与到整个定理的证明、应用的过程中来，这对中国剩余定理的教学起到积极的推动作用.

4 通过质疑，感受研究的无止境

中国剩余定理解决的是模两两互素条件下的一次同余式组的求解问题，但是对于模不是两两互素的情况该如何求解？ 提出这一问题后，可以先让学生对一些具体例子进行分析，然后介绍数论中对模不是两两互素情况下的一次同余式组的一般求解方法是将其转化为模两两互素的情形加以解决，从而让学生知道数学研究与其它科学研究一样，是一个前仆后继，永无止境的过程.

参考文献：

[1] 潘承洞，潘承彪. 初等数论 [M]. 2版. 北京：北京大学出版社，2006.
[2] 柯 召，孙 琦. 数论讲义(上册) [M]. 2版. 北京：高等教育出版社，2001.
[3] 闵嗣鹤，严士键. 初等数论 [M]. 3版. 北京：高等教育出版社，2005.
[4] KENNETH H R. Elementary Number Theory and Its Applications [M]. 5th edition. Beijing: China Machine Press, 2005.
[5] 张贤科. 代数数论导引 [M]. 2版. 北京：高等教育出版社，2006.
[6] HONG Shao-fang. Lectures on Elementary Number Theory [M]. Chengdu: Sichuan University Press, 2010.

Chinese Remainder Theorem and its Application
——Design Based on Exploring Study

LI Mao

School of Mathematics and Statistics, Southwest University, Chongqing 400715, China

Abstract: Chinese Remainder Theorem plays an important role in number theory and algebra, it is a very important Theorem. In this paper, the origin of the history of the Chinese Remainder Theorem is introduced, then the Theorem is proved. On that basis, some applications and examples about the Chinese Remainder Theorem are given.

Key words: Chinese Remainder Theorem; the system of congruence; module

责任编辑 廖 坤