论同余理论在生活中的应用

张双红,高亚楠

（吉林师范大学 数学学院,吉林 四平 136000）

摘要:同余概念是初等数论的重要组成部分之一,同余的相关定理在初等数学中也占有重要的地位.本文从同余的基本概念、基本性质、相关定理及同余式的解法出发,结合具体实例给出了同余式在生活的一些应用,如RSA算法、检验判断整除等问题。

关键词:同余;孙子定理;整除

doi:10.16083/j.cnki.1671—1580.2017.11.053

中图分类号:O156.1　　**文献标识码:**A　　**文章编号:**1671—1580(2017)11—0181—03

1.引言

数学从古至今一路走来,伴着人类精神文明和物质文明的发展越走越广阔,越来越精深。在这个信息交织、通讯技术高速发展的今天,数学已经不仅仅止步于是一种有效的工具和精确的语言,而是一门会令人十分着迷潜心研究的科学,更是一种先进文化的体现。而同余理论是数论里的核心内容之一,是解决整数问题的有效手段。十九世纪初,现代数论第一人的数学家高斯,出版了《算术研究》一书,并在其中提出了同余的概念及一次同余式组的解法,极大地丰富了数学的内容,为现代同余理论的发展奠定了牢固的基础。[1]同余理论在初等数论中占有重要的地位,是研究整数问题的重要手段,同时,同余理论在日常生活的也有重要的地位。[2][3]

2.同余的基本概念、性质与基本定理

2.1同余的概念

定义1.1.1[4] 给定一个正整数m,把它叫做模。如果用m去除任意两个整数a与b所得的余数相同,我们就说a,b对模m同余,记作 $a\equiv b(\mathrm{mod}\,m)$ 。如果余数不同,我们就说a,b对模m不同余,记作 $a\not\equiv b(\mathrm{mod}\,m)$ 。或整数 a , b 对模 m 同余的充分与必要条件是 $m|(a-b)$,即 $a=b+mt$, t 是整数。

2.2同余的基本性质[4]

甲 $a\equiv a(\mathrm{mod}\,m)$.

乙 若 $a\equiv b(\mathrm{mod}\,m)$,则 $b\equiv a(\mathrm{mod}\,m)$.

丙 若 $a\equiv b(\mathrm{mod}\,m)$, $b\equiv c(\mathrm{mod}\,m)$.

丁(i)若 $a_1\equiv b_1(\mathrm{mod}\,m)$, $a_2\equiv b_2(\mathrm{mod}\,m)$,

则 $a_1+a_2=b_1+b_2(\mathrm{mod}\,m)$.

(ii)若 $a+b\equiv c(\mathrm{mod}\,m)$,则 $a\equiv c-b(\mathrm{mod}\,m)$.

戊 若 $a_1\equiv b_1(\mathrm{mod}\,m)$, $a_2\equiv b_2(\mathrm{mod}\,m)$,

则 $a_1a_2=b_1b_2(\mathrm{mod}\,m)$,

特别地,若 $a\equiv b(\mathrm{mod}\,m)$,则 $ak\equiv bk(\mathrm{mod}\,m)$.

己 若 $a\equiv b(\mathrm{mod}\,m)$,且 $a=a_1d$, $b=b_1d$, $(d,m)=1$,则 $a_1\equiv b_1(\mathrm{mod}\,m)$.

以上的每一条性质都十分简单,但又非常重要,都是我们求解同余组方程和解决相关问题的有力工具。

2.3同余式的相关定理

定理1[4](Euler)

设 m 是大于1的整数, $(a,m)=1$,则 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$.

定理2[4](Fermat)

设 p 是素数,则 $a^p\equiv(\mathrm{mod}\,p)$.

孙子定理[4]

设 m_1 , m_2 ,…, 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 ,…, k ,则同余组 $x\equiv b_1(\mathrm{mod}\,m_1)$, $x\equiv b_2(\mathrm{mod}\,m_2)$,…, $x\equiv b_k(\mathrm{mod}\,m_k)$

收稿日期:2017—05—15
基金项目:吉林师范大学基础教研项目,编号201343。
作者简介:张双红(1977—),女,吉林辽源人,吉林师范大学数学学院,讲师,硕士。研究方向:数学教育。

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

的解是 $x\equiv M_1'M_1b_1+M_2'M_2b_2+\cdots M_k'M_kb_k(\mathrm{mod}\,m)$，其中 $M_i'M_i=1(\mathrm{mod}\,m)$，$i=1,2,\cdots,k$.

孙子定理被称为“中国剩余定理”，在近代数论中有着不可取缔的地位，为整个数学史的发展做出了不可估量的贡献，在近代数论以及现实生活中皆应用广泛，处处可见它数学思想的影子。

3.同余式的应用

3.1物不知数的问题

沿着历史的河流，追溯到公元5世纪中期，在中国古代数学典籍《孙子算经》卷下第26题，提出了物不知数问题：今有物，而不知其数，三三数，之剩二；五五数，之剩三；七七数，之剩二，问该物几何？答：二十又三。[5]

明朝程大位在《孙子歌》中用一首诗解答此题：“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”。[6]

用数学中的符号语言即为：

$x\equiv 2(\mathrm{mod}\,3)$，$x\equiv 3(\mathrm{mod}\,5)$，$x\equiv 2(\mathrm{mod}\,7)$ [7]，

根据孙子定理知：

$m_1=3$，$m_2=5$，$m_3=7$；$b_1=2$，$b_2=3$，$b_3=2$，

$m=m_1m_2m_3=3\times5\times7=105$，$M_1=\dfrac{m}{m_1}=\dfrac{105}{3}=35$，$M_2=\dfrac{m}{m_2}=\dfrac{105}{5}=21$，$M_3=\dfrac{m}{m_3}=\dfrac{105}{7}=15$，由 $M_iM_i'\equiv 1(\mathrm{mod}\,m_i)$，可求 $M_1'=-4$，$M_2'=6$，$M_3'=1$，$x\equiv M_2'M_2b_2+M_3'M_3b_3\equiv 128\equiv 23(\mathrm{mod}\,105)$，求解 $x=23$.

3.2运用同余性质检验判断整除问题

在我们过去的学习中，已经学过如何验证一个整数是否能被2或者5整除，即一个十进位整数的个位上的数码能被2或者5整除。随着我们知识的不断更新，经验的逐步积累，慢慢地遇到了一些相对来讲无法直接判断的整除问题，如：判断一个整数能否被3、7、9、11、13等整除。那么根据同余的性质，下面我们就给出此类整除的判别条件。

1. 判别能被3整除的条件

我们讨论任意一个整数 a，把 a 写成十进制的形式，即 $a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_0$，$0\leqslant a_i<10$.

因为 $10\equiv 1(\mathrm{mod}\,3)$，故可由定理知

$a\equiv a_n+a_{n-1}+\cdots+a_0(\mathrm{mod}\,3)$.

2. 判别能被7整除的条件

我们讨论任意一个整数 a，把 a 写成千进制的形式，即 $a=a_n1000^n+a_{n-1}1000^{n-1}+\cdots+a_0$，$0\leqslant a_i<1000$.

因为 $1000\equiv -1(\mathrm{mod}\,7)$，故可由定理知

$$a\equiv a_0-a_1+a_2-a_3+\cdots\equiv(a_0+a_2+\cdots)-(a_1+a_3+\cdots)$$
$$\equiv\sum_{i=0}^{n}(-1)^ia_i(\mathrm{mod}\,7)$$

运用同余性质检验判断整除是解决星期问题、属相问题、万年历等问题的基础。在生活中除了这些，同余理论还有很多广泛的应用，如太阳黑子的变化周期是11年，我们可用同余的性质准确地推算出下一次太阳黑子运动的年份，为天体科研工作提供有力的帮助；每4年为一个闰年，利用同余的性质我们可以精确地推算出哪一年是闰年；2012年4月份起，在北京“13为一个周期”进行车辆尾号限行轮换，利用同余的性质我们可以简单且有效地推算出何时可以开车出行。而在中国二十四节气中，我们熟知3月21日前后为春分，6月22日前后为夏至，9月23日前后为秋分，12月24日前后为冬至，此四个时令中，每两个相邻时令都是相差三个月，即知其一便可根据同余性质，准确地推导出其余三者。

3.3属相的问题

十二生肖与中国传统文化的十二地支（即子、丑、寅、卯、辰、巳、午、未、申、酉、戌、亥）呈现出一一对应的关系，依次为：子鼠、丑牛、寅虎、卯兔、辰龙、巳蛇、午马、未羊、申猴、酉鸡、戌狗、亥猪。传言先贤文人，为了让全天下的百姓，包括家境贫苦无法读书的人，可以知道自己出生时的年号，就研究出了这种简易的生肖纪年法。下面我们就用同余理论来解释：

设你的周岁年龄为 x，用12来整除 x，$x\equiv a_i(\mathrm{mod}\,12)$，$i=1,2,\cdots12$（$a_i$ 是模12的一个完全剩余系）。再对应下表，便可简单便捷地算出自己的属相。

a_i	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
属相	子鼠	丑牛	寅虎	卯兔	辰龙	巳蛇	午马	未羊	申猴	酉鸡	戌狗	亥猪

例如：小甲今年26岁，即 $x=26$，$26\equiv 2\equiv a_2(\mathrm{mod}\,12)$，则对应上表可知小甲的属相是丑牛。

3.4星期的问题

星期是以连续七天作为一个周期的计时单位，又称为周。在平时生活中，我们通常将星期划分为工作日和休息日，即周一到周五为工作日，周六和周日为休息日，星期在生活中具有十分重要的作用。对于一周之内推算某一天是星期几，是比较简单易算的，但对于推算某一年中某一天是星期几的问题，推算就比较复杂繁琐，但根据同余的性质，就可以非常简便快速地推算此类问题了。

利用同余理论可以在已知某年某日是星期几的条件下，无论是对于过去已经历过的日期，还是

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

对未来的某一天，都能简易且精确地算出某年某日是星期几，让我们试用举例来说明一下。

已知2001年的劳动节是星期二，求2011年的劳动节是星期几？

已知一个星期为7天，要求2011年的劳动节是星期几，即求出2001年的劳动节到2011年的劳动节的总天数除以7的余数即可。显然这个总天数很大，求解略微繁琐，但如今我们根据同余的性质，并加以灵活运用便可无需求出这个总天数。

2001年的劳动节到2011年的劳动节之间有2个闰年和8个平年，即总天数为：$366\times2+365\times8$.因为$366\times2\equiv2\times2\equiv(\mathrm{mod}\,7)$，$365\times8\equiv1\times1\equiv(\mathrm{mod}\,7)$，即可得$366\times2+365\times8\equiv2\times2+1\times1\equiv4+1\equiv5(\mathrm{mod}\,7)$，$5+2=7$，可知2011年的劳动节是星期日。

3.5公钥加密——RSA技术

随着科技的不断进步和Internet的高速发展，通信安全逐渐成为了巨大的潜在隐患，通信安全已渐渐成为人们关注的热点。于是，二十世纪七十年代在美国麻省理工学院（MIT）工作的罗纳德·李维斯特、阿迪·萨莫尔和伦纳德·阿德曼一起提出了RSA公钥加密算法。[8]RSA的实现过程主要是：先将公开的信息翻译成一种“码子”，通常是代表信息内容的数字（例如摩斯码等等），方便起见，称之为“明码”；后将明码翻译成只有通讯的双方能识别的“码子”，称此“码子”为密码；把将明码翻译成密码的方法称为加密程序，当接收方接收到密码后，便可根据双方事先商定的方法将其复原为明码。[9]最后接收方可通过解密出的明码解读出发送方所寄出的通讯信息。

用数学语言来表达就是：设p,q是任意选取两个十进位位数至少超过100位的大质数，N是p和q的乘积，e,d满足：$ed\equiv1(\mathrm{mod}\,\varphi(N))$，$\varphi(N)$表示$N$的欧拉函数值。此处$e,N$和$d$分别为密钥和解钥。设明码为数字$a$，$(0\le a\le N-1)$。然后进行加密程序，即将数字$a$通过转化$a^e\equiv b(\mathrm{mod}\,N)$，$0\le b\le N-1$，得到密码$b$，发送方将此密码$b$发送给接受方，接受方收到密码$b$之后，根据解密程序通过关系式：$b^d\equiv a^{ed}\equiv a^{1+k\varphi(N)}\equiv a(\mathrm{mod}\,N)$，接收方即可将密码$b$还原为明码$a$。特别地，根据Euler定理，当$(a,N)=1$时，上述关系式成立；当$(a,N)\neq1$时，易知，$a^{1+k\varphi(N)}\equiv a(\mathrm{mod}\,P)$，$a^{1+k\varphi(N)}\equiv a(\mathrm{mod}\,q)$成立，故有$\varphi(N)=\varphi(pq)=(p-1)(q-1)$.

运用同余性质检验判断整除是解决星期问题、属相问题、万年历等问题的基础。

4.总结

本文主要从探讨同余定义、性质、相关定理及其应用入手，并通过对同余理论的检验判别整除问题的研究突出同余理论在初等数论中的地位，同时用实例表明同余理论在解决看似复杂的问题上是有明显的优势和便利性的。同时我们也要将理论知识应用于日常生活，从而真正意义上的理解运用同余的性质，真正体会到同余富有智慧的魅力。

［参考文献］

［1］郭小菊.同余法求最大公约数［J］.读与写:教育教学刊，2012(04).

［2］郭海民，白永祥.数论在密码学中的应用［J］.电脑知识与技术，2010(17).

［3］武保强.浅谈同余理论的应用［J］.中小学电教月刊，2010(08).

［4］闵嗣鹤，严士健编.初等数论［M］.北京：高等教育出版社，2003.

［5］马丁玲. 斐波那契《计算之书》研究［D］.上海交通大学，2008.

［6］姜春艳.中国剩余定理探究［J］.武警学院学报，2005(03).

［7］杨天标.孙子定理的推广［J］.德州学院学报，2010(06).

［8］赵文敬，吴彦波. 基于DES和RSA的混合加密算法设计［J］.黑龙江科技信息，2014(30).

［9］胡典顺，李倩. 基于大数分解的RSA加密方法［J］.高等函授学报（自然科学版），2007(05).

The Applications of the Correlation Theorem in Life

ZHANG Shuanghong，GAO Yanan

(School of Mathematics, Jilin Normal University, Jilin Siping 136000 China)

Abstract: The conception of congruence is an important component in the elementary mathematics. The correlation theories of congruence also play an important role in the elementary mathematics. In terms of the basic conception, the basic property, the correlation theories and the method of solving of the congruence, this paper provides some of the applications by illustrating example of the life, such as RSA algorithm, checkout or judgment of exact division problem.

Key words: Congruence; Chinese Sunzi theory; Exact division

［责任编辑：马妍春］

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net