“十一五”国家重点图书出版规划项目

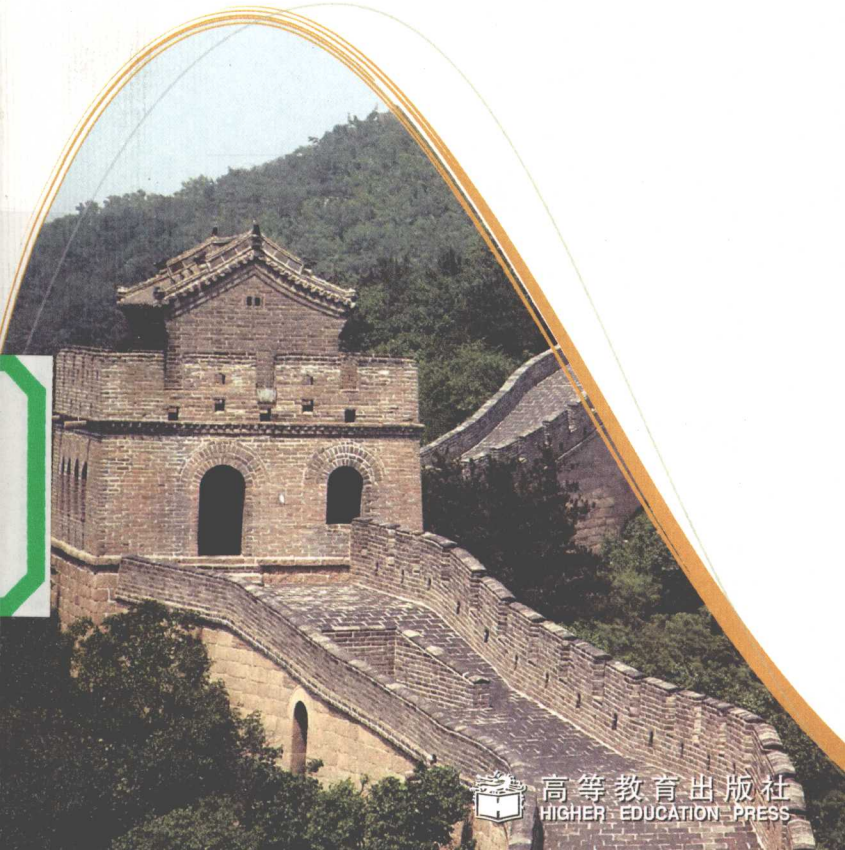
9

□ 数学文化小丛书

李大潜 主编

同余式及其应用

○ 徐诚浩



高等教育出版社
HIGHER EDUCATION PRESS

“十一五”国家重点图书出版规划项目

数学文化小丛书

李大潜　主编

同余式及其应用

高等教育出版社

图书在版编目（CIP）数据

同余式及其应用/徐诚浩. —北京：高等教育出版社，2009.12

（数学文化小丛书/李大潜主编）

ISBN 978-7-04-024544-8

Ⅰ.同… Ⅱ.徐… Ⅲ.同余式-普及读物 Ⅳ.O156.1-49

中国版本图书馆 CIP 数据核字(2009)第 047393 号

策划编辑 李 蕊 **责任编辑** 张耀明

封面设计 张 楠 **版式设计** 张 岚

责任校对 金 辉 **责任印制** 毛斯璐

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
		网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
总 机	010-58581000	**网上订购**	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
		畅想教育	http://www.widedu.com
印 刷	国防工业出版社印刷厂		
开 本	787×960 1/32	**版 次**	2009 年 12 月第 1 版
印 张	2.25	**印 次**	2009 年 12 月第 1 次印刷
字 数	37 000	**定 价**	7.00 元

物料号 24544-00

数学文化小丛书编委会

数学文化小丛书总序

整个数学的发展史是和人类物质文明和精神文明的发展史交融在一起的。数学不仅是一种精确的语言和工具、一门博大精深并应用广泛的科学，而且更是一种先进的文化。它在人类文明的进程中一直起着积极的推动作用，是人类文明的一个重要支柱。

要学好数学，不等于拼命做习题、背公式，而是要着重领会数学的思想方法和精神实质，了解数学在人类文明发展中所起的关键作用，自觉地接受数学文化的熏陶。只有这样，才能从根本上体现素质教育的要求，并为全民族思想文化素质的提高夯实基础。

鉴于目前充分认识到这一点的人还不多，更远未引起各方面足够的重视，很有必要在较大的范围内大力进行宣传、引导工作。本丛书正是在这样的背景下，本着弘扬和普及数学文化的宗旨而编辑出版的。

为了使包括中学生在内的广大读者都能有所收益，本丛书将着力精选那些对人类文明的发展起过重要作用、在深化人类对世界的认识或推动人类对世界的改造方面有某种里程碑意义的主题，由学有

专长的学者执笔，抓住主要的线索和本质的内容，由浅入深并简明生动地向读者介绍数学文化的丰富内涵、数学文化史诗中一些重要的篇章以及古今中外一些著名数学家的优秀品质及历史功绩等内容。每个专题篇幅不长，并相对独立，以易于阅读、便于携带且尽可能降低书价为原则，有的专题单独成册，有些专题则联合成册。

希望广大读者能通过阅读这套丛书，走近数学、品味数学和理解数学，充分感受数学文化的魅力和作用，进一步打开视野、启迪心智，在今后的学习与工作中取得更出色的成绩。

李大潜

2005 年 12 月

目　录

一、同 余 式

人们从孩提时代开始就知道每个星期有七天: 从星期一到星期六, 再加上一个星期日, 接下来又是星期一. 如此周而复始, 直至永远! 如果您要问: 这种全世界通用的叙述和记载日期的方法, 是哪一个国家发明的? 是从什么时候开始应用的? 其根据是什么? 确实无处考证. 关于星期来源唯一可查的出处是《圣经》.《圣经》上说, 上帝在第一天造了光; 第二天造了空气 (天); 第三天造了地和海以及蔬菜与果实; 第四天造了太阳和月亮; 第五天造了鱼和鸟; 第六天造了兽、畜、虫和人; 到了第七天, 万物已造齐, 称为圣日, 他安息了! 可是, 究竟是先有 "星期" 还是先有《圣经》? 实在不得而知!

在本文中, 我们不深入考查 "星期计数法" 的由来, 而是考察它的涵义. 如果某一天是星期一, 那么在它以后的第 8 天、第 15 天、第 22 天、…… 都是星期一. 这些都是星期一的 "天数" 有一个共性: 它们除以 7 所得的余数都是 1. 也就是说, 它们除以 7 是 "同余的".

一般地说, 取定某个自然数 (正整数) m. 如果两个整数 a 和 b, 它们除以 m 以后所得的余数相同, 即

$$a = q_1 m + r, \quad b = q_2 m + r, \quad 0 \leqslant r \leqslant m-1,$$

则称 a 与 b **关于模 m 是同余的**, 简称 a 与 b 关于模 m 同余, 记为

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

此时必有 $a - b = (q_1 - q_2)\, m$, 这也就是说, m 一定整除 $a-b$. 因此, a 与 b 关于模 m 同余当且仅当 m 整除 $a-b$, 或者说, 当且仅当存在整数 k 使得

$$a = b + km.$$

一旦取定一个自然数 m, 那么任意一个整数 a 必与

$$0, 1, 2, \cdots, m-1$$

中的某一个数关于模 m 同余.

显然, $a \equiv 0 \,(\mathrm{mod}\, m)$, 当且仅当 m 整除 a, 即 a 是 m 的倍数.

这里的 "模" 字是一个专门术语, 起源于拉丁字 modulus, 其原义为 "尺度", 通常表示 "约数". 当取模 $m = 7$ 时, 就得到星期计数法.

首先引入同余这个概念并运用这个同余符号的, 是 18 世纪德国数学家、物理学家以及天文学家**高斯** (1777—1855). 他开拓性地创建了严整的整数同余理论, 并得到许多重要的应用, 开创了很多崭新的数学

领域. 可是实际上, 在高斯之前, 人类早就大量地应用自然数之间的同余关系了!

例如, 把一天分为 24 个小时. 今天的 9 时与明天的 9 时的时数关于模 24 是同余的.

在一个钟面上, 把一个圆周等分成 12 个小时, 用时针表示小时数; 再把圆周按一个小时等分成 60 分钟, 用分针表示分钟数; 最后再把圆周按一分钟等分成 60 秒, 用秒针表示秒数. 这里都是在利用时间之间的同余关系.

又如, 把一个圆周角等分成 360 度. 当两个圆周角的始边与终边分别重合时, 它们必相差 360 度的倍数.

再如, 我们把 100 年称为一个 "世纪", 在不同的世纪中, 年数后两位相同的年都是关于模 100 是同余的.

我国采用的 "干支纪年法" 是我国独创、全世界独一无二的纪年方法, 其中, 每 60 年称为一个 "甲子". 这种纪年法是每隔 60 年一个轮回. 再把 12 个 "地支" 与 12 个属相对应, 两个属相相同的人的年龄之差必为 12 的倍数 (或者同龄).

人们最熟悉的十进制计数法, 其表示原理也是利用自然数之间的同余关系.

取定自然数 10, 那么任意一个自然数 a 被 10 除以后, 所得余数必为小于 10 的自然数 (可以是零) a_1:

$$a = q_1 \times 10 + a_1,$$

即 $a \equiv a_1 \pmod{10}$.

当两个自然数 a 和 b 满足

$$a \equiv a_1 \,(\mathrm{mod}\, 10)\,, b \equiv a_1 \,(\mathrm{mod}\, 10)$$

时, 必有 $a - b \equiv 0 \,(\mathrm{mod}\, 10)$. 这就是说, 任意两个自然数, 只要被这个选定的**进位基数** 10 除以后, 所得的余数相同, 那么就可以把这两个自然数视作 "同类". 例如,

$$15, 25, 135, 2345$$

除以 10 后所得余数都是 5. 这一类数的共性就是 "个位数都是 5".

当然对于那些 "个位数都是 a_1" 的自然数, 还可进一步分类. 对于所得的商数 q_1, 被 10 除以后, 所得余数也为小于 10 的自然数 a_2:

$$q_1 = q_2 \times 10 + a_2,$$

即 $q_1 \equiv a_2 \,(\mathrm{mod}\, 10)$, 于是

$$a = (q_2 \times 10 + a_2) \times 10 + a_1 = q_2 \times 10^2 + a_2 \times 10 + a_1.$$

继续对所得的商数 q_2 除以 10, 得到新的商数和余数. 如此经有限步以后, 总可把任意一个自然数 a 唯一地写成

$$a = a_n \times 10^{n-1} + a_{n-1} \times 10^{n-2} + \cdots + a_3 \times 10^2 + a_2 \times 10 + a_1,$$

其中 $a_n, a_{n-1}, \cdots, a_2, a_1$ 都为小于 10 的自然数. 这样就得到以 10 为进位基数的自然数的表示法:

$$a = a_n a_{n-1} \cdots a_3 a_2 a_1,$$

其中每一位上都是小于 10 的自然数. 这些数都是一些商数模 10 以后所得的余数.

凡是个位数相同的自然数都是模 10 同余的; 凡是个位数与十位数对应相同的自然数都是模 100 同余的;…….

一般地说, 自然数的关于取定进位基数 m (自然数) 的表示式, 其实质就是在连续运用对模 m 同余的概念, 每一位上的数字都是关于模 m 的同余数. 这一点, 我们的祖先早已意识到了并加以广泛应用!

例如, 远在四千多年前, 古巴比伦人使用的是六十进制计数法. 他们的重量和货币 (银) 单位都是六十进位的, 而且他们的数字书写方法也是以 60 为基数的. 用现在的符号, 就是

$$12315 = 1 \times 60^2 + 23 \times 60 + 15 = 4995.$$

这里的 $4995 = 4 \times 10^3 + 9 \times 10^2 + 9 \times 10 + 5$ 为十进位数.

取定某个自然数 m, 根据同余的定义, 很容易证明整数之间的同余关系有以下三个**基本性质**:

(1) 反身性: 对于任意整数 a, 必有

$$a \equiv a \big(\bmod m \big).$$

(2) 对称性: 若 $a \equiv b \, (\bmod m)$, 则必有

$$b \equiv a \, (\bmod m) \, .$$

(3) 传递性: 若 $a \equiv b \, (\bmod m) \, , b \equiv c \, (\bmod m)$, 则必有 $a \equiv c \, (\bmod m)$.

我们还经常需要在同余式之间进行运算，此时要用到以下三个**基本公式**：

设 $a \equiv b \pmod{m}, c \equiv d \pmod{m}$，则有

(1) 加、减公式 $a \pm c \equiv b \pm d \pmod{m}$.

(2) 乘法公式 $ac \equiv bd \pmod{m}$.

(3) 乘幂公式 $a^n \equiv b^n \pmod{m}$，其中 n 为正整数.

事实上，根据以下三个等式就可容易地证明这三个公式是正确的：

(1) $(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$.

(2) $ac - bd = a(c - d) + d(a - b)$.

(3) $a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right)$.

有些问题看起来似乎很难，可是只要利用同余式的性质，就不难解决.

例 1 如何证明 $n = 8888^{2222} + 7777^{3333}$ 是 37 的倍数？

【证】 要证明 n 是 37 的倍数，就是要证明

$$n = 8888^{2222} + 7777^{3333} \equiv 0 \pmod{37}.$$

先由

$$8888 = 37 \times 240 + 8, \quad 7777 = 37 \times 210 + 7$$

知道

$$8888 \equiv 8 \pmod{37}, \quad 7777 \equiv 7 \pmod{37}.$$

再由

$$8^2 = 64 = 37 \times 2 - 10, \quad 7^3 = 343 = 37 \times 9 + 10$$

知道

$$8^2 \equiv -10 \pmod{37}, \quad 7^3 \equiv 10 \pmod{37}.$$

于是

$$\begin{aligned} n &= 8888^{2222} + 7777^{3333} \equiv \left(8^2\right)^{1111} + \left(7^3\right)^{1111} \\ &\equiv (-10)^{1111} + (10)^{1111} \equiv 0 \pmod{37}. \end{aligned}$$

这就证明了 n 是 37 的倍数. ■

例 2 任意给定 n 个自然数 (它们未必是连续的自然数), 按任意方法把它们排成

$$a_1, a_2, \cdots, a_n,$$

证明必定存在一对下标 k, l 满足 $1 \leqslant k < l \leqslant n$, 使得

$$a_{k+1} + a_{k+2} + \cdots + a_l \equiv 0 \pmod{n}.$$

这个命题乍一看, 不太相信它是正确的. 那些大大小小的自然数是任取的, 而且排序又是任意的, 竟有如此结论! 其实证明并不难, 因为可求助于同余式.

【证】 任意一个自然数除以 n 以后, 所得的余数必为 $0, 1, 2, \cdots, n-1$ 这 n 个数中的某一个. 构造以下 $n+1$ 个自然数:

$$x_0 = 0, x_1 = a_1, x_2 = a_1 + a_2, x_3 = a_1 + a_2 + a_3,$$
$$\cdots, x_n = a_1 + a_2 + \cdots + a_n.$$

把这 $n+1$ 个自然数都除以 n, 就得到 $n+1$ 个余数, 那么, 其中至少有两个余数相同, 例如

$$x_k \equiv r \pmod{n}, \quad x_l \equiv r \pmod{n}, \quad 1 \leqslant k < l \leqslant n,$$

于是必有 $x_l - x_k = a_{k+1} + \cdots + a_l \equiv 0 \pmod{n}$. ■

这是 "鸽笼原理" 的一个巧妙应用. 鸽笼原理是这样叙述的: 当鸽子数大于鸽笼数时, 必发生 "鸽子同笼" 现象. 这是一个应用广泛的简单原理.

例 3 任意给定两个自然数 k 和 n, 并设 $k \leqslant n$, 证明以下同余式

$$n(n-1)(n-2)\cdots(n-k+1) \equiv 0 \pmod{k!}.$$

【证】 我们知道从 n 件不同的产品中 (不放回地) 任意取出 $k\,(k \leqslant n)$ 件, 不计顺序的不同取法的总数为

$$\mathrm{C}_n^k = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \text{ (称为组合数)}.$$

因为组合数必为自然数, 所以必有

$$n(n-1)(n-2)\cdots(n-k+1) \equiv 0 \pmod{k!}. \quad ■$$

在这本小册子中, 我们将以同余式的应用为主线展开讨论.

二、弃 九 法

我们先介绍同余式的一个初等应用 —— **弃九法**.

如果手头没有计算器, 或者, 当所要计算乘积的两个数字的位数很多, 而计算器无法精确显示时, 总希望有一个简单的办法判断一下两个数相乘所得结果是否有误.

我们可限于考虑两个自然数相乘的情形.

设 x 和 y 是两个自然数, 如果已经得到一个计算式 $xy = z$, 需要检验它有没有算错?

为此, 考虑自然数 $x = a_n a_{n-1} \cdots a_2 a_1$ 的十进制表示式

$$x = a_n \times 10^{n-1} + a_{n-1} \times 10^{n-2} + \cdots + a_2 \times 10 + a_1.$$

它的各位数字之和记为

$$S = a_n + a_{n-1} + \cdots + a_2 + a_1.$$

把同余关系 $10 \equiv 1 \pmod 9$ 代入 x 的十进制表示式,

可知对于任意一个自然数

$$x = a_n a_{n-1} \cdots a_2 a_1$$

必有

$$x \equiv S \pmod 9 .$$

这就是说, 自然数 $x = a_n a_{n-1} \cdots a_2 a_1$ 与它的各位数字之和 $S = a_n + a_{n-1} + \cdots + a_2 + a_1$ 关于模 9 一定是同余的. 我们把这一事实表述为

$$a_n a_{n-1} \cdots a_2 a_1 \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 \pmod 9 .$$

为了检验已得到的计算式 $xy = z$ 是不是有误, 我们先求出三个同余式

$$x \equiv a \pmod 9 , y \equiv b \pmod 9 , z \equiv c \pmod 9 ,$$

这里 a, b, c 都是个位数. 如果 $xy = z$ 是正确的, 根据上节所述的同余式的乘法公式, 必有

$$ab \equiv c \pmod 9 .$$

因此, 当这个同余式不成立时, 就可断定 $xy = z$ 是错误的. 这样就把问题归结为检验三个余数之间的上述同余关系式是不是成立. 至于如何求一个自然数模 9 以后的余数, 可采用如下的**弃九法**:

因为对于任意一个自然数 $x = a_n a_{n-1} \cdots a_2 a_1$, 有

$$a_n a_{n-1} \cdots a_2 a_1 \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 \pmod 9 ,$$