30 数论
——从同余的观点出发

■ 蔡天新

高等教育出版社
HIGHER EDUCATION PRESS

30

数论
——从同余的观点出发

■ 蔡天新

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

内容简介

本书依据作者多年数论教学心得和研究成果写成。从同余的定义和观点出发，前五章依次讲述整除的算法、同余的性质、同余式理论、平方剩余、原根和 n 次剩余，后两章是有关素数幂模和整数幂模的同余式，不在通常的初等数论范畴却伸手可触。本书的另一特点是，每节内容都有引人入胜的补充读物，借此拓宽读者的知识面和想象力。这些读物或讲述了某一数论问题的初步知识，如佩尔方程和丢番图数组、阿廷猜想和特殊指数和、椭圆曲线和同余数问题、自守形式和模形式；或介绍了整数理论的新问题和新猜想，如完美数问题、格雷厄姆猜想、哥德巴赫猜想、*abc* 猜想、$3x+1$ 问题、华林问题、欧拉数问题、素数链问题、卡塔兰猜想、费尔马大定理等及其延拓。此外，本书重视语言描写，对背景知识和图表予以关注。

本书可供数学及相关专业的大学生、研究生用作教材或参考书，也适合广大的业余数论爱好者和研究者阅读浏览。

图书在版编目（CIP）数据

数论：从同余的观点出发 / 蔡天新著. -- 北京：高等教育出版社，2012.9

ISBN 978-7-04-034834-7

Ⅰ. ①数… Ⅱ. ①蔡… Ⅲ. ①数论 Ⅳ. ① O156

中国版本图书馆 CIP 数据核字（2012）第 210400 号

策划编辑 赵天夫　　责任编辑 赵天夫　　封面设计 赵 阳　　责任印制 赵义民

出版发行	高等教育出版社	咨询电话	400-810-0598
社　址	北京市西城区德外大街4号	网　址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印　刷	北京东君印刷有限公司	网上订购	http://www.landraco.com
开　本	787 mm×1092 mm　1/16		http://www.landraco.com.cn
印　张	13.75	版　次	2012 年 9 月第 1 版
字　数	250 千字	印　次	2012 年 9 月第 1 次印刷
购书热线	010-58581118	定　价	45.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换

物 料 号　34834-00

数论注同余的观点出发

王元

前　言

将近一个世纪以前, 美国出生的英国数学家莫德尔在一篇随笔中写道: “数论是无与伦比的, 因为整数和各式各样的结论, 因为美丽和论证的丰富性. 高等算术 (数论) 看起来包含了数学的大部分罗曼史. 如同高斯给索菲 · 热尔曼的信中所写的, ‘这类纯粹的研究只对那些有勇气探究它的人才会展现最魅人的魔力’.” 或许有一天, 全世界的黄金和钻石会被挖掘殆尽, 可是数论, 却是用之不竭的珍宝.

1801 年, 24 岁的德意志青年高斯出版了《算术研究》, 从而开创了数论研究的新纪元. 这部伟大的著作曾经寄到法国科学院而被拒绝, 但高斯在友人的资助下将它自费出版了. 在那个世纪的末端, 集合论的创始人康托尔这样评价: “《算术研究》是数论的宪章 …… 高斯的出版物就是法典, 比人类其他法典更高明, 因为无论何时何地从未发觉出其中有任何一处错误.” 高斯自己则赞叹, “数学是科学的皇后, 数论是数学的皇后”.

这部杰作的开篇即定义了同余, 任意两个整数 a 和 b 被认为是模 n 同余的, 假如它们的差 $a-b$ 被 n 整除. 高斯首次引进了同余记号,

他用符号 "≡" 表示同余. 于是, 上述定义可表示为

$$a \equiv b \pmod{n}.$$

有了这个方便的同余记号以后, 数论的教科书显得更加简洁美观. 今天, 基础数论教材的开篇大多介绍整除或可除性. 整除和同余式也构成了本书的前两章, 实际上, 整除抑或带余数除法 (在中国、印度和希腊等地有着各自的渊源故事和名称)

$$a = bq + r, \quad 0 \leqslant r < b$$

也等价于同余式 $a \equiv r \pmod{b}$, $0 \leqslant r < b$.

接下来的三章, 无论不定方程, 还是原根和指标, 均与同余有关, 更不要说一次、二次和 n 次剩余了. 不仅如此, 初等数论中最有名的定理, 除了算术基本定理以外, 均与同余有关. 例如, 欧拉–费尔马定理, 威尔逊–高斯定理, 拉格朗日定理和中国剩余定理, 后者的准确名字应为孙子–秦九韶定理, 或秦九韶定理 (参见第三章第 3.1 节).

进入第三章以后, 我们讲述了高斯最得意的、花费许多心血反复论证 (共 8 次) 的二次互反律, 高斯称其为 "算术中的宝石". 设 p 和 q 是不同的奇素数, 则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

这里 $\left(\ \right)$ 为勒让德符号, 当它取 1 或 -1 分别表示二次同余式 $x^2 \equiv a \pmod{n}$ 有解或无解. 这个结果是完美无缺的, 在第六章我们会介绍一个新的同余式, 它有着同样美丽的对称性. 设 $p, q \geqslant 5$ 为不同的奇素数, 则

$$\binom{pq-1}{(pq-1)/2} \equiv \binom{p-1}{(p-1)/2}\binom{q-1}{(q-1)/2} \pmod{pq},$$

此处 $\binom{\ }{\ }$ 为二项式系数.

除了引进同余符号, 高斯还给出了正多边形作图方法和原根存在的充要条件, 前者是有着两千多年历史的数学悬案, 后者的理论虽较完

整仍可以增补 (如原根的乘积、求和同余), 这些在本书的第四章第 5 节和第五章均有展示. 说到原根的存在性, 少不了素幂模同余式, 本书的第七章给出了不少素幂模甚或整数幂模的崭新公式, 包括拉赫曼同余式的推广, 后者在怀尔斯的证明之前一直是研究费尔马大定理的主要工具. 诚如加拿大和爱尔兰两位同行指出, 这一推广 (指从素幂模到整数幂模) 是 1906 年以来的第一次. 又如, 设 n 是任意奇数, 我们证明了

$$(-1)^{\phi(n)/2}\prod_{d|n}\binom{d-1}{(d-1)/2}^{\mu(n/d)}\equiv 4^{\phi(n)}\begin{cases}(\mathrm{mod}\, n^3), & \text{若 } 3\nmid n,\\ (\mathrm{mod}\, n^3/3), & \text{若 } 3|n,\end{cases}$$

其中 $\phi(n),\mu(n)$ 分别为欧拉函数和默比乌斯函数. 当 n 为素数时, 此乃著名的莫利 (Morley) 定理, 即对于任何素数 $p\geqslant 5$,

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{(p-1)/2}\equiv 4^{p-1}(\mathrm{mod}\, p^3).$$

二次型是高斯著作中的重头戏, 尤其是整数表示问题, 拉格朗日证明了, 每一个自然数均可表为 4 个整数的平方和. 本书这方面谈得不多, 但对于著名的华林问题, 我们却有独到深刻的描述. 设 k 和 s 为正整数, 考虑丢番图方程

$$n=x_1+x_2+\cdots+x_s,$$

其中

$$x_1x_2\cdots x_s=x^k.$$

由希尔伯特 1909 年的论证可知, 必定存在 $s=s'(k)$, 使对任意的正整数 n, 均可表成不超过 s 个正整数之和, 且其乘积是 k 次方. 用 $g'(k)(G'(k))$ 分别表示最小的正整数 s, 使对任意 (充分大的) 正整数 n, 上述方程成立. 我们在第七章给出了 $g'(k)$ 的准确值和 $G'(k)$ 的估值, 同时猜测 $G'(3)=3, G'(4)=4$. 一个更为精巧的推测是, 除了 2, 5 和 11, 每个素数均可表成 3 个正整数之和, 它们的乘积为立方数.

之所以能提出这类问题, 是因为我们把整数的加法和乘法结合起来考虑, 这一点受到了 abc 猜想的形式启发, 后者可以轻松地导出费尔马大定理等一系列著名猜想和定理, 其在数论领域的影响力迅速替代了已被证明的费尔马大定理. 事实上, 毕达哥拉斯的完美数和友好数问题也是这两种基本运算的结合, 它们具有恒久的魅力. 正是从这里开始, 我们的想象力获得提升, 渐渐脱离开了同余的观念.

除了新华林问题, 我们把著名的费尔马大定理也做了推广 (第七章第 7.3 节), 即考虑丢番图方程

$$\begin{cases} a+b=c, \\ abc=x^n \end{cases}$$

的正整数解. 设 $d=(a,b,c)$, 当 $d=1, n\geqslant 3$ 时, 该方程等同于费尔马大定理. 也就是说, 无正整数解. 而当 $d>1$ 时, 方程的可解性存在各种可能性. 比如, $d=2, n=4$ 时有解 $(a,b,c,x)=(2,2,4,2)$. 这就提出了一个新问题. 我们的猜测之一是, 当 d 和 n 均为奇素数时, 上述方程均无解. 这是费尔马大定理的完全推广, 且无法由 abc 猜想导出.

高斯在 19 岁那年证明了: 每个自然数均可表示为三个三角形数之和. 这是对费尔马问题的第一个回答, 后者在丢番图的《算术》空白处写下了第 18 条注释: 当 $n\geqslant 3$ 时, 所有自然数均可表示成 n 个 n 角形数之和. 所谓 n 角形数是毕达哥拉斯学派定义的, 即正 n 角形中的角点个数. 特别地, 三角形数为 $0,1,3,6,10,15,21,\cdots$, 即所有形如 $\binom{x}{2}$ 的二项式系数, 其中 10 和 21 分别为保龄球的木瓶和斯诺克的目标球的排列方式和数目.

我们注意到了, 二项式系数有着特殊而奇妙的性质, 它是除了数幂以外最简洁的整数, 因此值得数论学家重视. 二项式系数以及多项式系数在本书中多次出现, 我们甚至定义了形素数 $\binom{p_j^i}{j}$ $(i,j\geqslant 1)$, 将素数与形数结合起来, 其个数与素数个数在无穷意义上是等阶的. 我们猜测 (已验证至 10^7):

每一个大于 1 的自然数均可表示成 2 个形素数之和.

这个猜想的提出无疑受到了哥德巴赫猜想的启发. 后者说的是, 每个大于等于 9 (6) 的奇数 (偶数) 均可表示成 3 (2) 个奇素数之和. 我们认为, 这一点不够一致, 且素数本身是构成整数乘法意义的基本单位, 用在加法上未必是最佳选择. 另外, 随着数的增大, 它的表法数也越来越多, 似乎颇有些浪费了. 与此同时, 我们也提出了下列弱孪生素数猜想: 对于任意正整数 k, 存在无穷多对相邻为 $2k$ 的形素数.

本书的前五章正文和七章各节的补充读物构成了《初等数论》课程的教学内容, 可供大学数学系基础课或选修课每周四节的教学之用. 最后两章不在讲授范围之内, 但它们与同余式紧密相关, 且能够伸手触摸到, 也可算是本书的一大亮点. 至于本书的最大特色, 可能要数每节正常内容后面的补充读物 (可以选讲, 未安排习题). 这种形式是一种尝试, 希望借此拓广读者的知识面和想象力, 递增他们对数论的兴趣和热爱. 事实上, 这些补充读物至少有两个功能:

其一, 介绍了其他数论问题和研究的初步知识, 例如欧拉数和欧拉素数, 阿达马矩阵和埃及分数, 佩尔方程和丢番图数组, 阿廷猜想和特殊指数和, 椭圆曲线和同余数问题, 自守形式和模形式, 等等. 其二, 介绍了与初等数论相关的新问题和新猜想, 除前面提到的以外, 还有格雷厄姆猜想, $3x+1$ 问题, 广义欧拉函数问题, 覆盖同余式组, 素数链和合数链问题, 卡塔兰猜想, 多项式系数非幂, 等等.

可是, 也正因为问题和猜想比较多 (有时较为大胆), 容纳了本人多年的研究经验, 尤其是近年来的思考 (有的尚未发表), 错误在所难免, 期望读者予以发现和纠正. 本书的写作也是对过去 25 年来教授浙江大学《初等数论》课程的小结, 部分内容包括习题的选取得到了近十位研究生和合作者的帮助, 恕不在此一一提及名字, 他们参与研究的某些工作和国内外许多同行的相关成果在书中有所展示.

除此以外, 我要特别感谢前辈数学家王元先生, 他不仅为本书题写了书名, 同时在许多方面予以支持和鼓励. 还有菲尔兹奖得主、剑桥大学教授阿兰·贝克和卡塔兰猜想的证明者、格丁根大学教授普莱达·米

哈伊内斯库的褒奖, 前者称赞新华林问题是 “真正原创性的贡献”, 后者表扬作者 “在当今繁杂的数学世界找到一片属于自己的领地”.

最后, 我想引用高斯的一段话作为结束语, 摘自他为英年早逝的弟子艾森斯坦的论文集所写的导言, “数论提供给我们一座用之不竭的宝库, 储满了有趣的真理, 这些真理不是孤立的, 而是最紧密地相互联系着. 伴随着这门科学的每一次成功发展, 我们不断发现全新的, 有时是完全意想不到的起点. 算术理论的特殊魅力大多来源于我们由数学归纳法轻易获得的重要命题. 这些命题拥有简洁的表达式, 其证明却深埋于斯, 在无数徒劳的努力之后才得以发掘; 即便通过冗长的、人为的手段取得成功以后, 更为清新自然的证明依然藏而不露.”

蔡天新, 2012 年初夏于杭州彩云居

目　录

第一章　整除的算法

1.1　自然数的来历

在人类所有的发明中, 最古老的无疑是数学和诗歌了. 可以说自从有了人类的历史, 就有了这两样东西. 如果说诗歌起源于祈求丰收的祷告, 那么牧人计算家畜的只数便产生了数学. 由此看来, 它们均源于生存的需要. 随着时间的推移, 人类渐渐有了明确的正整数概念: $1, 2, 3, \cdots$, 这些正的整数全体被称为自然数 (natural number, 也有人把 0 算作自然数), 显然有着天然的或来自于自然界的意思.

最初, 因为这些牲畜的财产如此重要, 人们在表达同一数量的不同对象时所用的量词也不尽相同. 例如, 在古英语里使用过 team of horses (共同拉车或拉犁的两匹马), yoke of oxen (共轭的两头牛), span of mules (两只骡), brace of dogs (一对狗), pair of shoes (一双鞋), 等等. 慢慢地, 只剩下 pair 一词较为常用. 至于汉语, 量词的变化更为丰富, 且有许多一直保留至今.

很久以后, 人类才从无数生活经验和社会实践中, 把这样的数 (比如 2) 作为共同性质抽象出来, 这意味着自然数的诞生. 事实上, 它的

意义远不止于此, 英国哲学家罗素 (Russell, 1872—1970) 指出,

> 当人们发现一对雏鸡和两天之间有某种共同的东西 (数字 2) 时, 数学就诞生了.

而在我们看来, 数学的诞生或许要稍晚一些, 即在人们从 "3 只鸡蛋加上 2 只鸡蛋等于 5 只鸡蛋, 3 枚箭矢加上 2 枚箭矢等于 5 枚箭矢, 等等" 中抽象出 "$3+2=5$" 之时. 也就是说, 在我们对自然数实行加法和减法运算以后, 那可能比罗素所定义的要晚上几千年.

当人们需要进行更广泛、深入的数字交流时, 就必须将计数方法系统化. 世界各地的不同民族不约而同地采取了以下方法: 把从 1 开始的若干连续的自然数作为基数, 以它们的组合来表示大于这些数字的数. 换言之, 采用了进位制. 在不同民族和原始部落中, 使用过的有据可查的基数有 2, 3, 4, 5, 8, 9, 10, 12, 16, 20 和 60 等.

如同全才的古希腊哲学家亚里士多德 (Aristotle, 公元前 384—前 322) 所言, 由于 "绝大多数人生来具有 10 个手指这个解剖学事实", 10 进制最终被广泛采纳. 当然, 古代巴比伦人发明的 60 进制仍被保留下来, 作为时间单位之间的一种换算. 至于 2 进制, 有证据表明, 曾被澳大利亚昆士兰原住民和非洲矮人使用过, 而在三千多年前中国一部古老而深邃的典籍《易经》里, 就已在 64 卦里藏匿了这一奥妙.

接下来是 0 的出现和记号. 19 世纪印度 (今巴基斯坦) 出土的 "巴克沙利手稿" 中, 记载了公元前后数个世纪的耆那教数学. 里面出现了完整的 10 进制数, 包括用实心的点书写的零. 至晚 9 世纪, 印度人用圆圈 0 代替了实心. 之后, 0 连同其他 9 个数字记号经阿拉伯传递到了西方, 然后传遍整个世界, 并被诩传为阿拉伯数字.

等到 17 世纪, 德国数学家、哲学家莱布尼茨 (Leibnitz, 1646—1716) 在发明可以计算乘除的轮式计算机以前, 已建立起严格的 2 进制. 他用 0 表示空位, 用 1 表示实位, 所有的自然数均可由这两个数表示. 例如, $1=1$, $2=10$, $3=11$, $4=100$, $5=101$, $\cdots$. 遗憾的是, 莱布尼茨未能将两者联系起来. 直到 20 世纪中叶, 匈牙利出生的美国数

学家冯 · 诺伊曼 (von Neumann, 1903—1957) 在为计算机设计的程序中, 作了一系列重要革新, 才用 2 进制代替 10 进制, 他也因此被誉为“电子计算机之父”.

对任意整数 $b > 1$, b 进制早就建立起来了. 可是, 对素数 p (定义见第 3 节), p 进数 (p-adic 数) 却是晚近才有的概念. 1897 年, 德国数学家亨泽尔 (Hensel, 1861—1941) 通过对绝对值重新进行解释, 将有理数的算术用一种不同于实数系或复数系的方法进行了扩展. 如若 $x = \frac{12}{5} = 2^2 \cdot 3 \cdot 5^{-1}$, 则 $|x|_2 = \frac{1}{4}$, $|x|_3 = \frac{1}{3}$, $|x|_5 = 5$, 而对其余素数 p, $|x|_p = 1$. 故在 5 进数里, 下列级数是收敛的

$$S = 1 + 5 + 5^2 + 5^3 + \cdots,$$

这是因为 $|5^i|_5 = \frac{1}{5^i}$. 不仅如此, 我们还能求出 S 的值. 将上式两端同乘以 5, 可得

$$5S = 5 + 5^2 + 5^3 + \cdots.$$

两式相减, 即得 $-4S = 1$, 因此 $S = -\frac{1}{4}$.

在本书里, 我们感兴趣的主要是 10 进制整数. 在一些东方古国, 都有过从自然界中提取出数的规律的伟大发现, 比如巴比伦人和中国人各自发现了 3 平方数组, 即我们祖先所称的勾股数或古希腊人所称的毕达哥拉斯数. 在中国最早的数学典籍《周髀算经》(至晚公元前 1 世纪) 里, 记载了西周杰出的政治家、军事家、思想家, 文王之子、武王之弟周公 (公元前 11 世纪) 与大夫商高关于测量的一段对话, 其中提到

勾广三, 股修四, 径隅五.

这应该是 $(3, 4, 5)$ 这组最小的勾股数的首次记录. 周公是孔子一生最崇敬的人,《周礼》的作者, 书中提出了六艺, 数是其中之一. 在《周髀算经》里还叙述了周公后人荣方与陈子 (约公元前 6、7 世纪) 的一段对话:

以日下为勾, 日高为股, 勾股各自乘, 并而开方除之, 得斜至日.

此即勾股定理, 用现代数学语言来表达就是,

任意直角三角形两条直角边长的平方和等于斜边长的平方.

不过, 西方人将此结论称为毕达哥拉斯定理, 并早已约定俗成了. 一来古代东西方文化和科技交流几乎隔绝, 二来毕达哥拉斯率先给出了证明. 毕达哥拉斯 (Pythagoras, 公元前 580—前 500) 是古希腊第一个堪称伟大的数学家, 他生活的年代比陈子和荣方略晚. 值得一提的是, 毕达哥拉斯是用诗歌的语言来描述他发现的第一个定理的,

斜边长的平方,
如果我没有弄错,
等于其他两边长的
平方之和.

毕达哥拉斯出生在爱琴海东端的萨摩斯岛 (今希腊), 曾游历埃及和巴比伦, 后来他在克罗内托 (今意大利南方) 创办了一个秘密社团, 广收弟子, 形成了所谓的毕达哥拉斯学派, 其影响绵延后世两千多年. 毕达哥拉斯最早认识到在客观世界中和在音乐中数的重要性, 并提出了 "万物皆数" 这一哲学命题. 在他和他的弟子们关于自然数的种种发现里面, 最有意思的可能要数完美数和亲和数.

完美数与亲和数

所谓完美数或完全数 (perfect number) 是这样一个数, 它等于其真因子的和, 例如 $6, 28$, 这是因为

$$6 = 1 + 2 + 3,$$

$$28 = 1 + 2 + 4 + 7 + 14.$$