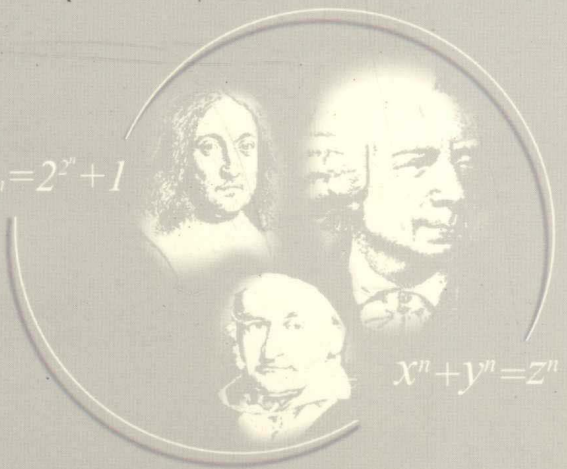
走进数学新课程丛书

初等数论及应用

◉ 冯克勤／编著



北京師範大學 出版社

走进数学新课程丛书

初等数论及其应用

冯克勤　编著

北京师范大学 出版社
北　京

北京师范大学出版社出版发行
（北京新街口外大街19号　邮政编码：100875）
出版人：赖德胜
北京师范大学印刷厂印刷　全国新华书店经销
开本：890mm×1 240mm　1/32　印张：5.75　字数：144千字
2003年7月第1版　2003年7月第1次印刷
定价：6.90元

前　言

初等数论是研究整数性质和不定方程(组)整数解的一门学问,它与几何学是最古老的两个数学分支. 几千年来,数论一直是一个不断发展和十分活跃的研究领域.另一方面,数论也有广泛的实际应用. 特别是20世纪中期以来,数字计算机和数字通信网络蓬勃发展,数论在计算机科学和信息工程上得到许多重大的实际应用,成为工程师不可缺少的数学语言和工具.

初等数论有许多知识和问题是比较通俗易懂的. 在小学就学到整数的分解、素数和整除性的简单知识.不少中学生对数论也有浓厚的兴趣. 最近,北京师范大学严士健先生告诉我,中学打算开设初等数论的选修课(这是《普通高中数学课程标准》(实验稿)中的要求),并邀我为中学教师写一本这方面的读物,这就是本书的来历.

事实上,目前已有不少关于初等数论的优秀读物,这些书的作者们也比我有更丰富的中学教学经验. 我为中学教师和中学生讲课不多,但是在中国科学技术大学教书的时候,与同仁一起从1977年就在数学系为一年级大学生开设初等数论课,一直坚持至今.目前又在清华大学数学科学系为一年级讲数论(共讲16学时,使用余红兵教授和我编写的《整数与多项式》,高等教育出版社),不少学生是喜欢的.

数论中有不少问题,说起来容易,做起来极难. 这本读物的目的不是专门训练做数论难题(这会使一些人望而生畏),而是讲述初等数论中最基本的概念、方法和思想,使读者对数论有一个全面的了解.书中也介绍一些数论应用的例子,再穿插一些数论发展历

史故事. 因为不是教材,可以写得轻松和随意一些. 我希望这本书能使读者开阔眼界,除了学一点数论知识,也能学到一点考虑问题的方法.

本书每节的后面均有一些习题,有一些是数论的计算,著名的数论学家(如高斯、欧拉、华罗庚)都以计算见长(华罗庚在《数论导引》一书中评论高斯,说他"不特老谋,而且深算也"). 另一些标有 * 的习题也是重要的结果,在后面会用到这些结论. 书末附有部分习题的简单提示,对于计算性的习题读者可自行验算结果的正确性.

我最基本的想法是想通过本书使读者感受到数论是有趣的,也是有用的,但不知能否有这样的效果,欢迎批评指正.

冯克勤

2003 年春于清华

简短的历史

1. 自然数的概念产生于人类有文字历史之前. 在生产和生活中,从两只手、两头羊之中抽象出数"2"的概念来,是人类理性的巨大飞跃. 在文字出现之后,不同地区的人们相继采用了各种形式的数字(表达数的文字). 后来又发明了表示大数的方法(各种进位制和位值制)以及数的运算,探讨整数的各种性质和方程(组)的整数解(和有理数解),这就产生了数论.

数论有三千余年的历史,产生于四大文明古国(埃及、巴比伦、印度和中国). 中国最早的数学著作《周髀算经》(约公元 2 世纪)中记载,西周人商高知道直角三角形三边之长 x,y,z 满足方程 $x^2+y^2=z^2$,并且给出此方程一组正整数解 $(x,y,z)=(3,4,5)$(勾三股四弦五). 印度人在公元前也知道此方程的一些整数解,巴比伦人知道一组解(13500,12709,18541). 古代中国对于整数的同余性质有相当深刻的认识,在《孙子算经》中载有"物不知数"问题,给出一次同余方程组的解法. 这种方法在近代已被推广成非常一般的形式,但仍被世人称为"中国剩余定理"(Chinese Remainder Theorem).

2. 古代东方的数学具有鲜明的实践、直觉和算法的特点,古希腊的数学(约公元前 6 世纪至公元 3 世纪)则具有理性和思辨的特征. 毕达哥拉斯(Pythagoras,约公元前 570 年至公元前 500 年)学派的格言是"万物皆数",把数量关系看成是人认识事物的最基本手段. 他们对整数的性质进行着迷地研究. 比如说,发现了前几个偶完全数 6,28 和 496(正整数 n 叫作**完全数**,是指 n 的所有小

于 n 的正因子之和为 n 自身，例如 $6=1+2+3$，$28=1+2+4+7+14$). 欧几里得证明了：若 $p=2^m-1$ 为素数，则 $n=2^{m-1}(2^m-1)$ 必是完全数. 两千年以后欧拉证明了：所有偶完全数均具有上述形式. 而奇完全数是否存在，至今仍是个谜.

古希腊的数论成就集中反映在欧几里得(Euclid，公元前 330 年至公元前 275 年)所写的《几何原本》一书中. 这本书共 13 卷，其中有 5 卷讲数论. 从以下主要内容可看出古希腊数论的深刻性.

(1)欧氏除法算式(即带余除法)：设 a 和 b 是正整数，$a>b$，则存在惟一决定的整数 q 和 r，使得 $a=qb+r$，其中 $q\geqslant 1$，而 $0\leqslant r<b$. 利用这个结果，欧几里得还给出了求最大公因子的辗转相除法.

(2)若素数 p 除尽整数 a 和 b 的乘积 ab，则 p 必除尽 a 或 b.

由此推出下面的算术基本定理.

(3)(算术基本定理)每个整数 $n\geqslant 2$ 都可表示成有限个素数的乘积，并且若不计素因子的次序，其表达式是惟一的.

事实上，欧几里得对于惟一性的陈述和证明只限于 n 是无平方因子的情形. 完整的证明是高斯于 1801 年给出的. 但是从欧几里得时代开始，人们无疑地使用着算术基本定理这块数论的基石.

(4)利用算术基本定理，欧几里得给出了方程 $x^2+y^2=z^2$ 全部(无限多)正整数解的表达式.

(5)素数有无限多个.

欧几里得的证明使用了反证法，这也是数学上第一批使用反证法的命题，而且表明古希腊人在探讨世界中的“无限性”问题.

古希腊的另一本重要数论著作是丢番图(Diophantus，约公元 250 年)的《算术》，书中收集了三百多个数论问题，给出各种二元和三元代数方程(组)(次数$\leqslant$3)寻求整数解和有理数解的方法. 这是世界上第一本离开几何学而专门讲述数论的著作.

3. 世界文明中心逐渐转移到欧洲. 经过中世纪黑暗时期之

后，欧洲于15～16世纪为文艺复兴时代. 基于航海、建筑、绘画和雕刻等发展和需要，画法几何学取得巨大的进步. 17世纪为欧洲产业革命时期，反映连续和变化的微积分和将几何代数化的解析几何的产生和发展是这个世纪数学的重要标志. 而数论在17世纪出现了一位杰出的传奇性人物：费马.

数论在18世纪得到很大的发展，这时的世界数论中心在法国. 除了费马之外，法国数论学家还有拉格朗日(Lagrange，1736—1813年)，勒让得(Legendre，1752—1833年)等，这个时期的大数论学家只有欧拉(Euler，1707—1783年)不是法国人.

费马(Fermat，1601—1665年)一生的主要职业是律师和公务员，数学是他的业余爱好. 他与帕斯卡(Pascal)一起研究过概率论，也是解析几何的创始人之一，但是他对数学的最大贡献是数论. 他的数论思想都写在读书评注和与朋友的通信中，这些工作在他去世后由他儿子整理出版.

1637年，费马在阅读丢番图《算术》一书时，在讲述方程 $x^2+y^2=z^2$ 的那一页写了如下的评注：

“任何立方数都不是两个立方数之和，任何数的四次方都不是两个四次方之和. 一般地，任何一个更高次方均不是两个同次方幂之和. 我有一个确实奇妙的证明，但是地方太小写不下.”

也就是说，费马提出如下的猜想：对于每个正整数 $n\geqslant 3$，方程 $x^n+y^n=z^n$ 没有正整数解.

事实上，人们只看到费马对于 $n=4$ 情形的证明. 他的证明采用了“无穷下降法”. 或许费马认为用这种方法可证明所有 $n\geqslant 3$ 的情形，但事实上远不是这样简单. 过了一百多年，欧拉于1753年才证明了费马猜想在 $n=3$ 时成立.

费马提出了许多猜测，下面是其中的几个.

(1)1640年，费马在给朋友的信中说：若整数 a 不被素数 p 除尽，则 a^{p-1} 被 p 除余1. 这个猜测是在18世纪由拉格朗日证明的，

后人称为费马小定理. 而欧拉把它做了重要的推广.

(2)费马计算了 $F_n=2^{2^n}+1$,发现 $F_0=3,F_1=5,F_2=17,F_3=257$ 和 $F_4=65537$ 都是素数. 于是他猜测:对于所有 $n\geqslant 0$,F_n 都是素数. 但是欧拉发现 F_5 有因子 641,$F_5=641\times 6700417$,从而推翻了费马的这个猜想. 事实上,一直到今天人们还没有发现新的素数 $F_n(n\geqslant 5)$. 目前已算出 F_5 到 F_{11}的素因子分解式. 我们在本书的最后将会看到,近年来人们热衷于分解 F_n,其动机来自于保密通信.

(3)1640 年,费马在给 Mersenne 的信中断言:每个被 4 除余 1 的素数都可表成两个整数的平方和(例如:$5=1^2+2^2,13=2^2+3^2,17=1^2+4^2,29=2^2+5^2,\cdots$). 这个猜测由欧拉于 1756 年证明. 到了 19 世纪初,高斯(Gauss,1777—1855 年)完整地解决了二平方和问题,即完全决定了哪些正整数可以表成两个整数的平方和,而哪些正整数则不能. 勒让得完全解决了正整数表成三整数平方和问题,而拉格朗日证明了:任何正整数都可以表示成四个整数的平方和.

正是费马的诸多猜测引起欧拉对数论的研究兴趣. 他花了近 20 年的时间系统地研究了整数的整除和同余性质. 18 世纪末和 19 世纪初,高斯对于数论也作了深入的探究,完成了初等数论的基本框架,也就是本书所讲的内容. 由于这些理论的建立,费马猜测几乎全都被解决,只有一个留给了后人,那就是关于方程 $x^n+y^n=z^n(n\geqslant 3)$无正整数解的最后一个猜想.

4. 高斯于 1801 年写了《算术探究》一书,世界数论中心从 19 世纪开始转到德国. 除了高斯之外,这个世纪的德国数论学家有库默尔(Kummer,1810—1893 年),狄里克莱(Dirichlet,1805—1859 年),黎曼(Riemann,1826—1866 年),戴德金(Dedekind,1831—1916 年)和希尔伯特(Hilbert,1862—1943 年). 19 世纪是数论的

辉煌世纪.一个突出的标志是产生了两大数论分支:解析数论和代数数论. 解析数论是由黎曼所创,用解析方法(微积分)来研究数论,特别是研究素数的特性. 代数数论是由高斯和库默尔所创,用代数方法研究数论. 高斯在研究二平方和以及更一般问题时引入代数方法,库默尔采用高斯的方法研究费马猜想,证明了当 $3\leqslant n\leqslant 100$ 时,$x^n+y^n=z^n$ 均无正整数解. 他们的方法被戴德金理论化和系统化为代数数论,在 19 世纪末被希尔伯特发展和总结在《数论报告》(1898 年)一书中. 1900 年,希尔伯特在第二次世界数学家大会上作《数学问题》报告,提出了 23 个著名的数学问题,其中有 6 个为数论问题. 这些问题对于 20 世纪的数学发展起了很大的推动作用.

5. 20 世纪是数论蓬勃发展和大丰收的世纪. 这个世纪数论研究的一个突出特点是与几何、代数和分析等其他数学领域的方法、思想和成果相互交叉和渗透,不断产生重大的数论研究成果,证明了许多数论猜想. 一个突出的例子是怀尔斯(Andrew Wiles, 1953—)在 1994 年最终证明了费马猜想. 众所周知,数学没有诺贝尔奖(虽然许多诺贝尔经济奖的得主是数学家). 国际数学界的最高奖有两个:菲尔兹奖和沃尔夫奖. 前者于 1936 年设立,在每次世界数学家大会上,颁发给不超过 40 岁的年轻人. 后者则更着重于对世界数学发展多方面的贡献的综合评价. 迄今为止,获菲尔兹奖的有 44 位数学家(包括丘成桐教授),其中有 9 位是数论学家,最近一次在北京召开的世界数学家大会(2002 年),两位菲尔兹奖得主的工作均属于数论研究领域(与几何学与代数学的深层联系). 除此之外,怀尔斯在柏林国际数学家大会(1998 年)上获得史无前例的菲尔兹特别奖(因为他的年龄超过 40 岁). 在获得沃尔夫奖的 39 位数学家当中(包括陈省身教授),有 6 位是数论学家.

20 世纪数论发展的另一个显著特点是得到广泛而深刻的应

用.这些应用为数论带来许多新鲜的研究问题,反过来也刺激了数论的发展,形成了“计算数论”.

以上就是数论发展的大致轮廓. 本书所讲的内容为由欧拉和高斯等人在18世纪前后建立的初等数论以及20世纪数论应用的一些重要例子.

目　录

第一章　数的整除性

1.1　整除性

我们今后用 $\mathbf{Z}$ 表示整数集合. 熟知整数之间进行加、减、乘法运算,所得结果仍为整数. 但是两个整数相除不必为整数,即集合 $\mathbf{Z}$ 中一般不能作除法. 设 a 和 b 为整数,$b\neq 0$,则 a/b 不一定为整数,即不一定存在整数 c,使 $a=bc$. 由此产生了初等数论中第一个基本概念:数的整除性.

定义 1.1.1　设 $a,b\in\mathbf{Z},b\neq 0$. 如果存在 $c\in\mathbf{Z}$,使得 $a=bc$,则称为 b **整除** a,记成 $b\mid a$,并且称 b 为 a 的一个**因子**(或**约数**),称 a 为 b 的**倍数**. 如果不存在整数 c,使得 $a=bc$,则称 b 不整除 a,记成 $b\nmid a$.

例如,$(-3)\mid 6$,$4\nmid 6$. 对每个整数 n,$(\pm 1)\mid n$. 对每个非零整数 n,$n\mid 0$,$n\mid(\pm n)$.

以下是关于整除性的最基本性质.

引理 1.1.2　以下约定:如果 $x\mid y$,均指 $x,y\in\mathbf{Z}$,且 $x\neq 0$.

(1)若 $a\mid b,b\mid c$,则 $a\mid c$.

(2)若 $a\mid b,b\mid a$,则 $a=\pm b$.

(3)若 $a\mid b,a\mid c$,则对任意 $x,y\in\mathbf{Z},a\mid bx+cy$.

定义 1.1.3　设 a 为任意实数,我们用 $[a]$ 表示不超过 a 的最大整数,叫作 a 的**整数部分**,而 $a-[a]$ 叫作实数 a 的**分数部分**,表

示成$\{a\}$. 于是每个实数a可惟一表示成

$$a=[a]+\{a\},[a]\in\mathbf{Z},0\leqslant\{a\}<1.$$

例如，$[2.1]=2,\{2.1\}=0.1$，

$$[-2.1]=-3,\{-2.1\}=0.9.$$

现在给出整数一个基本性质.

定理 1.1.4(带余除法)　设$a,b\in\mathbf{Z}$，且$b\geqslant 1$，则存在惟一决定的整数q和r，使得$a=qb+r,0\leqslant r<b$.

证明　先证满足条件的整数q和r是存在的. 为此令$q=\left[\frac{a}{b}\right],r=a-qb$，则$q$和$r$均是整数，并且$\frac{r}{b}=\frac{a}{b}-q=\left\{\frac{a}{b}\right\}$. 由$0\leqslant\left\{\frac{a}{b}\right\}<1$，可知$0\leqslant\left\{\frac{a}{b}\right\}b=r<b$.

再证q和r是惟一决定的. 如果又有整数q'和r'，使得　$a=q'b+r',0\leqslant r'<b$，则

$$0=a-a=(qb+r)-(q'b+r')=(q-q')b+(r-r').$$

于是$b\mid r-r'$. 另一方面，由$0\leqslant r,r'<b$可知$|r-r'|<b$. 但是$|r-r'|$是b的倍数，所以只能$r-r'=0$，即$r=r'$. 于是$a-qb=a-q'b$，从而$q=q'$. 证毕. □

作为带余除法的一个应用，我们证明整数集合的一个重要性质.

引理 1.1.5　设S是一个非空整数集合，并且满足以下条件：

(A)若$a,b\in S$，则$a\pm b\in S$；

(B)若$a\in S$，则对任意整数c，均有$ac\in S$.

则存在惟一的整数$d\geqslant 0$，使得S由d的所有倍数构成，即

$$S=d\mathbf{Z}=\{da:a\in\mathbf{Z}\}.$$

证明　若$S=\{0\}$，则取$d=0$(并且只能取$d=0$). 以下设S中存在非零整数a，由性质(A)知$0=a-a\in S$，于是$-a=0-a\in S$.

所以 S 中必包含有正整数. 令 d 是集合 S 中的最小正整数,我们来证 $S=d\mathbf{Z}$. 首先,由 $d\in S$ 和性质(B)可知 $d\mathbf{Z}\subseteq S$. 进而,对 S 中任意整数 a,我们有带余除法

$$a=qd+r,\quad q,r\in\mathbf{Z},0\leqslant r<d.$$

由于 $a,d\in S$ 和性质(A)和(B),可知 $r=a-qd\in S$. 但是 $0\leqslant r<d$,而 d 是 S 中最小的正整数,必然 $r=0$. 这表明 $a=qd\in d\mathbf{Z}$,因此 $S\subseteq d\mathbf{Z}$. 这就证明了 $S=d\mathbf{Z}$. 最后,满足 $S=d\mathbf{Z}$ 的正整数 d 一定是 S 中的最小正整数,从而是惟一的. 证毕. □

注 我们在证明中只用到比(A)弱的命题:"若 $a,b\in S$,则 $a-b\in S$."但是由此不难推出 $a+b$ 也属于 S,因为 $0=b-b\in S$,$-b=0-b\in S$,从而 $a+b=a-(-b)\in S$.

定义 1.1.6 设 p 是大于 1 的整数. 如果 p 的正整数因子只有 1 和 p,称 p 为**素数**(也叫作**质数**).

例如,100 以内的素数为 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89 和 97,共 25 个.

定理 1.1.7 素数有无限多个.

证明 用反证法. 首先,素数是存在的. 假如只有有限个素数 $p_1,p_2,\cdots,p_n(n\geqslant 1)$. 考虑正整数 $N=p_1\cdots p_n+1\geqslant 2$,易知 N 必有素因子 p. 但是 $p_1,\cdots,p_n$ 除不尽 N,所以 p 是 $p_1,p_2,\cdots,p_n$ 以外的素数,这就与假设矛盾. 因此假设不成立,即素数有无限多个. 证毕. □

关于素数有许多有趣的问题,其中不少问题至今未能解决. 这里列举一些重要的问题.

(1)**素数判定** 给了一个正整数 n,如何判定它是否为素数?根据定义,如果 $2,3,\cdots,n-1$ 均除不尽 n,则 n 为素数. 但是当 n