数学概貌丛书

数论概貌

陈景润著

科学技术文献出版社

数学概貌丛书

数论概貌

陈景润 著

内 容 提 要

数论是一门研究数的性质的科学，有着丰富的内容。本书旨在通俗地向读者介绍数论的基本内容、典型问题和主要方法，全书计分三章，即：初等数论、解析数论、代数数论。书中结合几个主要问题（例如哥德巴赫猜想、费马大定理）而引进若干概念，介绍一些近代的方法和研究成果，以使读者能从中了解数论这一数学分支的大致面貌。

本书是一本科普书，具有中等文化程度的读者即可读懂。

数学概貌丛书

数 论 概 貌

陈景润 著

*

科学技术文献出版社出版

（北京市复兴路15号）

上海市中华印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

开本 850×1156 1/32 印张 2 字数 38,000

1990年2月第1版 1990年2月第1次印刷

印数 1—3,000本

ISBN 7-5023-0660-9/O·50 定价：1.00元

目　录

数论是研究数的性质的一门科学，是数学的一个分支学科.

人类对数论的研究，渊源久远. 早在古希腊时代，就已取得了许多成果.欧几里得(Euclid)的《原本》一书中，就记有素数有无限多个(及其证明)、整数的因数分解、欧几里得除法（即辗转相除法，用以求两个数的最大公因数)、关于完全数的一个著名定理等；作为古希腊的成就，还有寻求素数的埃拉托斯散(Eratosthenes) 筛法，阿基米得(Archimedes)对不定方程所作的研究等. 亚历山大里亚时代的丢番图 (Diophantus) 曾对不定方程进行了深入的研究. 当然，在数论的发展史上，更应该提到的是法国业余数学家费马(P. S. de Fermat)、德国数学家高斯(C. F. Gauss)以及狄利克雷(P.G. Dirichlet).

我国古代，在数论方面也有极其光辉的成就. 例如商高定理(勾股定理)、孙子定理(被西方人称为“中国剩余定理”)都为世人所嘱目.近代，我国数学工作者在解析数论、丢番图方程、一致分布等方面，都作出了重要贡献. 特别是华罗庚教授在三角和估计以及堆垒数论方面，成就卓著. 近三十多年来，我国的数论研究队伍中新人辈出，在哥德巴赫(C. Goldbach)问题、算术级数中的最小素数问题、L 函数的零点问题以及三角和的估计等问题

上，更进一步获得了许多优秀的成果.

数论按照所运用的研究方法的不同，又分为初等数论、解析数论、代数数论、几何数论等，下面择要加以介绍.

一、初 等 数 论

初等数论是仅仅利用初等数学的方法，而不借助于其他数学工具，去研究整数的性质. 它主要包括：整除性、不定方程、同余式、连分数等.

1. 整数的整除性

大家知道，整数对于加法、减法、乘法是封闭的，即：整数加整数、整数减整数、整数乘以整数，其结果仍然是整数. 但是，整数除以整数就不一定得到整数了. 于是，产生了数论的一个基本问题——研究一个整数能否被另一个整数整除的问题：

如果三个不为零的整数 a、b、c，满足

$$a=b\cdot c,$$

我们就说“a 能被 b **整除**”（或“a 能被 c **整除**”），记为 $b|a$（或 $c|a$），并说“b（或 c）是 a 的一个**因数**”；而且，当 b 或 c 不为 a 或 1 时，称 b（或 c）是 a 的一个**真因数**. 否则，就说“a **不能被** b（或 c）**整除**”，记为 $b\nmid a$（或 $c\nmid a$）. 我

们把这个基本问题，称为**整数的整除性**.

我们以 $[\alpha]$ 表示不超过数 α 的最大整数. 例如，$[3]=3$，$[\sqrt{2}]=1$，$[\pi]=3$，$[-\sqrt{2}]=-2$，$[-4.5]=-5$. 那么，显然成立下面的不等式：

$$[\alpha]\leqslant\alpha<[\alpha]+1.$$

对于两个整数 a 和 b (其中 $b>0$)的商，有

$$\left[\frac{a}{b}\right]\leqslant\frac{a}{b}<\left[\frac{a}{b}\right]+1,$$

即

$$0\leqslant a-b\left[\frac{a}{b}\right]<b.$$

于是，我们有

$$a=\left[\frac{a}{b}\right]b+r,\qquad \text{这里 } 0\leqslant r<b.$$

因此，给定任意两个整数 a、b (其中 $b>0$)，必存在整数 q、r，使

$$a=qb+r,\qquad \text{这里 } 0\leqslant r<b.$$

当 $r=0$ 时，就是前面所说的“b 能整除 a”；当 $r\neq0$ 时，即是“b 不能整除 a”.

为了研究整数的整除性，人们把正整数分为如下三类：

(1) 1；它只有 1 为其因数；

(2) p；它只有 1 和 p 为其因数，即 p 大于 1 且无真因数；

(3) n；有真因数.

我们把上述第二类数叫做**素数**（在有些书上也称之为质

数），把上述第三类正整数叫做**复合数**（有些书上也称之为**合数**）. 显然，大于 2 的偶数必有真因数 2，都是复合数.

把素数按照大小进行排列，可以得到下面的数列（通常称为**素数列**）：

$$2,3,5,7,11,13,17,19,23,29,31,37,\cdots\cdots.$$

在古希腊，欧几里得就已证明了素数有无穷多个，他采用了反证法：假设素数只有有限个，不妨设这有限个不同的素数是 p_1、p_2、……、p_n；我们来考察整数 $a=p_1\cdot p_2\cdot\cdots\cdots\cdot p_n+1$，依假定，$a$ 显然异于任一素数，因而是一个复合数；于是，根据复合数的定义，a 应该有一个素因数 p，但 $p\nmid 1$ 而 $p\mid p_1\cdot p_2\cdot\cdots\cdots\cdot p_n$，可知 $p\nmid a$，这就和前面导出的 p 是 a 的素因数产生了矛盾，究其原因，是假设了素数只有有限个是错误的，这就证明了素数有无穷多个.

关于素数分布的研究，是很有趣，又很困难的. 本书在下面的章节里还将讲到.

算术基本定理 每一个大于 1 的整数 n，可唯一地表为

$$n=p_1^{a_1}\cdot p_2^{a_2}\cdot\cdots\cdots\cdot p_k^{a_k}$$

的形状，这里素数 $p_1<p_2<\cdots\cdots<p_k$，而 a_1、a_2、……、a_k 是大于 0 的整数.

这个定理的证明，仅用简单的初等方法就可完成，但定理的结论是非常深刻的. 它反映了素数在整数中的基本作用，揭示了整数的一个基本性质——积性.

2. 最大公因数和最小公倍数

如果 a、b 是非零整数，而整数 q 同时是 a、b 的因数，我们便把 q 叫做 a、b 的**公因数**.

显然，q 的绝对值必不大于 a、b 的绝对值的最小者：

$$|q| \leqslant \min\{|a|, |b|\}.$$

上式表明，两个非零整数的公因数必只有有限多个. 于是，其中一定有一个最大的；我们把 a 和 b 的所有公因数中的最大一个公因数 d，叫做 a 和 b 的**最大公因数**，记作 $d=(a, b)$.

已知两个非零整数 a 和 b，怎样求出它们的最大公因数呢？当然，可以利用上面的算术基本定理；但是，更简单的办法是采用辗转相除法，这一方法最早见于欧几里得的《原本》(公元前三世纪)，我国古算书《九章算术》(约成书于东汉初年，公元一世纪)也记有这一方法.

用辗转相除法求两个非零整数的最大公因数的具体步骤如下：(不妨设 a 与 b 都是正整数，且 $a>b$)

先用 b 除 a，得到正整数 q_1，使

$$a=q_1b+r_1. \qquad (0\leqslant r_1<b)$$

若 $r_1=0$，则由 $a=q_1b$ 知 a 与 b 的最大公因数是 b. 若 $r_1\neq 0$，由 $0<r_1<b$，可再以 r_1 除 b，于是又可得正整数 q_2 和非负整数 r_2，使

$$b=q_2r_1+r_2. \qquad (0\leqslant r_2<r_1)$$

以 (a, b) 表 a 与 b 的最大公因数，则可知

$$(a, b) = (b, r_1).$$

当 $r_2 = 0$ 时，可知 $(a, b) = (b, r_1) = r_1$. 若 $r_2 \neq 0$，则 $0 < r_2 < r_1$，再以 r_2 除 r_1，得正整数 q_3 和非负整数 r_3，使

$$r_1 = q_3 r_2 + r_3. \qquad (0 \leqslant r_3 < r_2)$$

于是，当 $r_3 = 0$ 时，有 $(a, b) = (b, r_1) = (r_1, r_2) = r_2$. 若 $r_3 \neq 0$，则由 $0 < r_3 < r_2$，又可再以 r_3 除 r_2，……. 这样继续辗转相除，由于 $b > r_1 > r_2 > r_3 > \cdots\cdots$ 且各 r_i（这里 $i = 1, 2, 3, \cdots$）皆是非负整数，则一定存在一个正整数 n，使经过 $n+1$ 次辗转相除后，有 $r_{n+1} = 0$ 但 $r_n \neq 0$. 这时，就可得到 $(a, b) = r_n$.

这就通过辗转相除，求出了 a 和 b 的最大公因数.

两个非零整数的最大公因数的性质，主要有：如果 $(a, b) = d$，则存在整数 m、n，使

$$ma + nb = d; \qquad (1)$$

这里的整数 m 和 n，可由辗转相除法求得 $(a, b) = r_n$ 后，逐次向上一算式回代而得.

如果 $(a, b) = 1$，我们称 a 和 b 是**互素**的. 当然，互素的整数中，可以不一定有素数. 例如 $(25, 26) = 1$，但 25 和 26 都是复合数.

对于非零整数 a、b，如果 m 同时是 a、b 的倍数，我们便把 m 叫做 a 和 b 的**公倍数**.

可以看出，a 和 b 的公倍数有无穷多个. 例如，它们的积 ab 即是它们的一个公倍数，而这一乘积的任意倍数都是它们的公倍数. 我们把 a 和 b 的公倍数中的最小的一个数 M，叫做 a 和 b 的**最小公倍数**，记作 $M = \{a, b\}$.

当然，两个非零整数的最小公倍数，也可以利用上面的算术基本定理而求得.

下面，我们来证明关于最大公因数和最小公倍数之间的一个结果：正整数 a 与 b 的乘积，可以表示成

$$ab=(a,b)\cdot\{a,b\}. \tag{2}$$

证明 因 ab 为 a 与 b 的公倍数，而$\{a,b\}$为 a 与 b 的最小公倍数，故存在正整数 q，使

$$ab=q\cdot\{a,b\};$$

从而$\frac{a}{q}=\frac{\{a,b\}}{b}$、$\frac{b}{q}=\frac{\{a,b\}}{a}$；而$\frac{\{a,b\}}{b}$与$\frac{\{a,b\}}{a}$皆为正整数，所以 $q|a$、$q|b$，即 q 为 a、b 的公因数. 又设 g 为 a、b 的任一个公因数，令 $m=\frac{ab}{g}$. 由于$\frac{a}{g}$及$\frac{b}{g}$都是正整数，又 $m=a\left(\frac{b}{g}\right)=b\left(\frac{a}{g}\right)$，故 m 是a 和 b 的公倍数，从而$\{a,b\}|m$，即$\frac{m}{\{a,b\}}$是一个正整数. 又由

$$\frac{m}{\{a,b\}}=\frac{ab}{g\left(\frac{ab}{q}\right)}=\frac{q}{g},$$

故$\frac{q}{g}$也是正整数，即 $g|q$. 由 g 的任意性，可知 $q=(a,b)$，这就证明了(2)式成立.

3. 不 定 方 程

如果未知数的个数多于方程的个数，这样的方程叫

做不定方程．例如，方程

$$ax+by=c,$$

$$ax+by+cz=d,$$

$$ax^2+bxy+cx+dw=0,$$

等等，都是不定方程．

研究整系数不定方程的整数解，是数论中饶有趣味的问题之一．五世纪末，我国古代数学家张丘建曾编写了一部《算经》，书中提出了一个不定方程问题——世界数学史上有名的“百鸡问题”：

> 鸡翁一，值钱五．鸡母一，值钱三．鸡雏三，值钱一．百钱买百鸡，问鸡翁、母、雏各几何？

（用现在的白话文来说，就是：每一个大公鸡的售价是五个钱，每一只母鸡的售价是三个钱，每三个小鸡的售价是一个钱；现有 100 个钱，想买 100 只鸡，问公鸡、母鸡和小鸡各应买几只？）

假设用 x、y、z 分别代表买公鸡、母鸡和小鸡的数目，就得到下面的两个方程

$$\begin{cases}5x+3y+\dfrac{z}{3}=100,\\ x+y+z=100.\end{cases}$$

由这两个方程，我们得到

$$200=300-100$$

$$=3\left(5x+3y+\frac{z}{3}\right)-(x+y+z)$$

$$= 15x + 9y + z - x - y - z$$
$$= 14x + 8y.$$

也就是

$$7x + 4y = 100.$$

我们要解“百鸡问题”，就是要寻求 $7x + 4y = 100$ 的非负整数解.

这里的 $7x + 4y = 100$，是一个二元一次不定方程. 二元一次不定方程的一般形式是

$$ax + by = c, \tag{3}$$

其中 a、b、c 都是整数.

定理 设二元一次不定方程

$$ax + by = c \tag{3}$$

(其中 a、b、c 都是正整数，而$(a, b) = 1$)有一组整数解 $x = x_0$、$y = y_0$，则它的一切整数解可以表示成

$$x = x_0 - bt, \qquad y = y_0 + at \tag{4}$$

的形式，其中 $t = 0$，± 1，± 2，…….

这一定理的证明，可参看一般初等数论书中有关不定方程的讨论，这里从略.

应用这一定理，很容易得出“百鸡问题”的解答. 首先，易见 $s = -1$、$t = 2$ 是不定方程

$$7s + 4t = 1$$

的一组整数解；由此得知 $x = -100$、$y = 200$ 是

$$7x + 4y = 100$$

的一组整数解. 于是，$7x + 4y = 100$ 的一切整数解可以表示成为

$$x=-100-4t,\qquad y=200+7t$$

的形式，其中 $t=0$，±1，±2，……．在“百鸡问题”中，由于 x、y 分别代表公鸡、母鸡的个数，所以必有 $x\geqslant0$、$y\geqslant0$．由 $-100-4t\geqslant0$ 得到 $t\leqslant-25$，由 $200+7t\geqslant0$ 得到 $t\geqslant-\frac{200}{7}$，因此有

$$-\frac{200}{7}\leqslant t\leqslant-25.$$

由于 t 是整数，故有 $t=-28$，-27，-26，-25．又，小鸡的个数是

$$\begin{aligned}z&=100-x-y\\&=100-(-100-4t)-(200+7t)\\&=-3t.\end{aligned}$$

这样，我们就得到了“百鸡问题”的四组解答：

$$\begin{aligned}&x_1=12,\quad y_1=4,\quad z_1=84;\\&x_2=8,\quad y_2=11,\quad z_2=81;\\&x_3=4,\quad y_3=18,\quad z_3=78;\\&x_4=0,\quad y_4=25,\quad z_4=75.\end{aligned}$$

下面再来介绍人们很早就认识了的另一个不定方程：

$$x^2+y^2=z^2,\tag{5}$$

其中 x、y、z 为正整数．上述不定方程，即是通常所谓的求勾股数组的问题．据史料记载，最简单的一组解 $3^2+4^2=5^2$ 至迟在四千多年前就已被发现．古希腊的毕达哥拉斯（Pythagoras）发现了上述不定方程的部分解的公式：设 m 是奇数，

$$x=m,\quad y=\frac{m^2-1}{2},\quad z=\frac{m^2+1}{2}. \tag{6}$$

丢番图也证明了一个部分解的公式：设 m 和 n 是正整数，而 $2mn$ 是一个完全平方数，则

$$\begin{aligned} x&=m+\sqrt{2mn},\\ y&=n+\sqrt{2mn},\\ z&=m+n+\sqrt{2mn}. \end{aligned} \tag{7}$$

现今所用的通解公式则是：设 m 和 n 是正整数，$m>n$，$(m,n)=1$，$2\nmid(m+n)$，则方程(5)的满足条件$(x,y)=1$、$2|x$ 的一切正整数解可表示成：

$$\begin{aligned} x&=2ab,\\ y&=a^2-b^2,\\ z&=a^2+b^2. \end{aligned} \tag{8}$$

通常认为，上式是由罗士琳(公元1789～1853年)得到的，故被称作罗士琳公式.

上面通过“百鸡问题”，介绍了二元一次不定方程的一种一般解法；又介绍了一个二次不定方程——求勾股数组的解，值得注意的是有不少不定方程，解题的特殊性很强，对一个方程适用的方法往往不再适用于另一个方程，要像二元一次方程那样寻求一种“一般解法”实在是很困难的. 迄今为止，关于不定方程尚有许多未知领域，真是向人类智慧的挑战.

谈到不定方程，很值得一提的是方程（5）的推广：$x^3+y^3=z^3$，$x^4+y^4=z^4$，……，一般地，$x^n+y^n=z^n$. 法国业余数学家费马于 1637 年提出了一则猜想(通常称为“费马大定理”)：当 n 是一个大于 2 的整数时，不定方程

$$x^n + y^n = z^n \tag{9}$$

没有正整数解. 费马的这一猜想迄今还未被人们证明. 1976 年时瓦格斯塔夫(S. Wagstaff) 借助于大型电子计算机证得 $2<n<125000$(当然还包括这些数的任何整倍数) 情况下这一猜想是成立的. 1983 年，联邦德国数学家法尔丁斯(G. Faltings) 在《数学创造》杂志上(Invent. Math.)发表了题为《数域上阿贝尔簇的有限性》一文. 在此文章中，他以代数几何为主要工具，证明了莫台尔(L. J. Mordell)1922 年提出的一个猜想：数域上任一个亏格 $\geqslant 2$ 的非奇异射影曲线仅有有限多个点的坐标在此数域中. 注意到 $n\geqslant 3$ 时，方程(9)定义的曲线满足莫台尔猜想的条件. 于是，由莫台尔猜想，立即推出方程(9)对每个 $n\geqslant 3$ 最多只有有限组正整数解. 但是，法尔丁斯的方法并未给出(9)中解的个数或上界估计. 因而费马大定理仍然未能解决. 法尔丁斯这一工作荣获 1986 年度国际数学家大会颁发的菲尔兹奖.

4. 同　　余

如果 a 与 b 都是整数，而 m 是一个正整数；$(a-b)$ 可以被 m 整除，即 $m|(a-b)$时，我们称“a、b 对模 m 同余”，记作 $a\equiv b(\mathrm{mod}\, m)$；当 $m\nmid(a-b)$时，称“a、b 对模 m 不同余”，记作 $a\not\equiv b(\mathrm{mod}\, m)$.

显然，我们有

$a\equiv a\ (\mathrm{mod}\ m)$;

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

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

关于同余，还有下列结果：若

$$a_1\equiv b_1(\mathrm{mod}\,m),$$

$$a_2\equiv b_2(\mathrm{mod}\,m),$$

$$\cdots\cdots\cdots\cdots$$

$$a_n\equiv b_n(\mathrm{mod}\,m),$$

则有

$$a_1\pm a_2\pm\cdots\pm a_n\equiv b_1\pm b_2\pm\cdots\pm b_n(\mathrm{mod}\,m), \tag{10}$$

$$a_1a_2\cdots a_n\equiv b_1b_2\cdots b_n(\mathrm{mod}\,m) \tag{11}$$

例如，由(11)式和 $10\equiv 1(\mathrm{mod}\ 9)$，我们有 $10^n\equiv 1^n(\mathrm{mod}\ 9)$，即

$$10^n\equiv 1(\mathrm{mod}\ 9). \tag{12}$$

又，设正整数

$$a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_0$$

(其中 $0\leqslant a_i\leqslant 9$，$1\leqslant a_n\leqslant 9$；$i=0,1,2,\cdots,n-1$)，则由(10)、(11)和(12)式，有

$$a\equiv a_n+a_{n-1}+\cdots+a_0\ (\mathrm{mod}\ 9). \tag{13}$$

根据(13)式，我们可以很快地判别一个整数能否被9整除：即只需将这个整数的各位数上的数字加起来，看其数字和能否被9整除. 例如221145236415，它的各数位上的数字之和为

$$2+2+1+1+4+5+2+3+6+4+1+5=36,$$

36是能被9整除的，故221145236415亦能被9整除.

我们把

$$ax+b\equiv 0\ (\mathrm{mod}\,m) \tag{14}$$