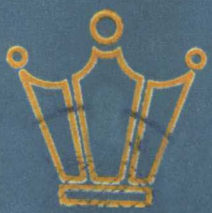
数论基础

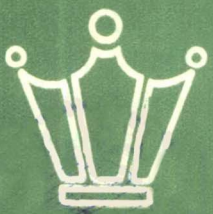
王杰官 编著



福建科学技术出版社

数论基础

王杰官 编著



福建科学技术出版社

数论基础

王杰官 编

福建科学技术出版社出版
（福州得贵巷27号）
福建省新华书店发行
三明市印刷厂印刷
开本787×1092毫米 1/32 18.375印张 2插页 411千字
1987年3月第1版
1987年3月第1次印刷
印数：1—2,400
书号：7211·66 定价3.55元

前　言

数论（The Theory of Numbers）是数学的一个古老分支，它是研究数的性质，特别是整数性质的一门学科。在公元前三世纪，古希腊数学家欧几里德（Euclid，公元前330—公元前275）著的《几何原本》的第八、九、十篇就是专门记载历史上有关数论的成就。例如，用辗转相除法求最大公约数的步骤，至今仍称之为欧几里德算法，他还证明了素数个数的无穷性等等。我国早在公元前后的《孙子算经》里就提出“物不知其数”的问题：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？答曰二十三”。这是世界上最早提出解同余式组

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

的问题。关于解上述同余式组的定理，初等数论书中称为孙子定理，有的外文书中称为中国剩余定理（The Chinese Remainder Theorem）。

数论应该说是古希腊人首创的，十七世纪法国数学家费马（Fermat，1601—1665）对数论作出了巨大的贡献，他的工作决定了这门学科的早期研究方向。德国数学家高斯（Gauss 1777—1856）曾经说过：“数学是科学的皇后，数论是数学的皇后”，这说明，大数学家早就认识到数学在科学中享有的独特地位及数论在数学中享有的独特地位。

世界上的一切事物都不是孤立存在的．数论亦不例外，它并不孤立，而是与数学的其他分支有着密切的关系．例如，欧几里德用初等方法证明了素数的数目是无穷的，十八世纪瑞士数学家欧拉（Euler，1707—1783）用解析方法证明同一命题。高斯二次反转定律既可用初等方法亦可用拓扑方法来证明，近代国外某些数学家还把古老的费马大定理，转为可用拓扑方法来解决的问题。从使用数学方法的不同，数论可分为解析数论、代数数论和数的几何三个主要分支．

数论又称理论算术．整除性（可约性）理论、同余式论（实际上是整除性理论比较复杂的情况）等等都是乘法数论的内容；而把一个数表示成和的形式，如，不定方程的整数解问题、哥德巴赫（Goldbach）猜想、四个平方和问题（拉格朗日～Lagrange～定理）和华林（Waring）问题等等，都是加法数论的内容，加法数论亦称堆垒数论．

十九世纪以前，数论还仅是一系列孤立结果的罗列，1801年高斯的《算术探讨》(Disquisition Arithmetical)一书出版则标志了现代数论的开始．高斯的数论著作有三个主要思想：同余理论、代数数的引进、型的理论．同余理论是总结历史上费马、欧拉、拉格朗日和勒让得（Legendre）等数学家的成就，并引用了“≡”的符号．

整除概念可推广于“除数”为0，即$0\mid 0$，$0\nmid a$（$a\neq 0$），若模m亦允许$m=0$，则以0为模的同余类有无穷多个，即$a\equiv a\pmod 0$，$a\neq b$时，$a\neq b\pmod 0$，所以有理整数相等的关系是同余关系的一个特例．柯西（Cauchy）用i代替整系数多项式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots$$

中的x，得到

$$f(i)\equiv(a_0-a_2+a_4-\cdots)+(a_1-a_3+a_5-\cdots)x \pmod{(i+1)}.$$

柯西的这种思想，用多项式的同余式来定义复数。如实系数多项式

$$f(x)\equiv a+bx \pmod{(x^2+1)}$$

关于模 x^2+1 与 $a+bx$ 同余的任何多项式都表示同一复数 $a+bi$

高斯首先把 i 添加于有理整数环R，得到比R多两个单位（可逆元）$\pm i$ 的一个二次整数环R〔i〕（R只有 ± 1 两个单位，而R〔i〕有 ± 1，$\pm i$ 四个单位），并把合数、素数、同余等概念推广于R〔i〕。例如，$5=(1+2i)(1-2i)$ 在R〔i〕里是合数而不是素数。高斯还证明了，在R〔i〕中可用欧几里德除法求二整数的最大公因数。更广泛地对这些问题的研究产生了代数整数论，它有丰富的内容与方法，当时高斯本人也没有想到，代数数概念的引入与证明费马大定理是分不开的，康米尔（Kummer）把 x^p+y^p（p是素数）分解成

$$(x+y)(x+\alpha y)\cdots(x+\alpha^{p-1}y)$$

这里α是虚的 p 次单位根，也就是，α 是

$$x^{p-1}+x^{p-2}+\cdots+x+1=0 \qquad (1)$$

的一个根，这就把高斯的复整数理论推广到由（1）那样的方程引进代数数。

由于在R〔$\sqrt{-5}$〕中

$$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5}),$$

而2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$都是 R〔$\sqrt{-5}$〕中的素数，因此在二次整数环 R〔$\sqrt{-5}$〕中唯一分解定理不成立。但是若令 $\alpha=\sqrt{2}$，$\beta_1=(1+\sqrt{-5})/\sqrt{2}$，$\beta_2=(1-\sqrt{-5})/\sqrt{2}$，

则 $2=\alpha^2$，$3=\beta_1\beta_2$，且

$$6=\alpha^2\beta_1\beta_2$$

就是唯一分解了．为了解决这个问题，1814年开始康米尔写了一系列论文，创立了理想数的理论，解决了唯一分解定理的存在问题．康米尔还用他的理想数成功地证明了费马大定理对许多素数是成立的．

狄德金采用与康米尔完全不同的方法来重建代数数域中的唯一分解定理，他用代数数类来定义理想，给出了一般的唯一分解定理（理想数的基本定理）．他还创立了现代代数数的理论，奠定了代数数论的基础．代数数论的工作在十九世纪以希尔伯特（Hilbert）的论代数数的著名报告为顶峰，他用新颖、漂亮的方法来重新整理早期的理论，其后，他和其他许多人大大地扩展了代数数论．

型理论的产生，肇源于丢番图（Diophantos）的思想，从研究整数的型表示，引入型等价的概念以及二元二次型的分类等．高斯在《算术探讨》的第五节中系统化并扩展了型的理论，打下研究数的几何的基础．

解析方法导入数论使数论得到很大的发展，欧拉、雅可比（Jacobi)都做了一些工作，解析数论的诞生更应归功于狄利克雷（Dirichlet，1805—1859）．为了证明欧拉和勒让得猜测：每一个算术序列

$$a,\ a+b,\ a+2b,\ \cdots,\ a+nb,\ \cdots (a,\ b)=1$$

中包含无穷多个素数，他引用了分析的方法．又，对不超过 x 的素数个数 $\pi(x)$ 的估值，欧拉、勒让得和高斯等人猜测：

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1$$

在这个问题的研究中，也自然地引入了分析方法．

此外，还有用黎曼（Riemann）ζ函数

$$\zeta(z)=\sum_{n=1}^{\infty}\frac{1}{n^z}\ (z\text{为复数})$$

来证明素数定理等．这些工作奠定了解析数论的基础．

本书共分九章，前六章是数论必不可少的基础知识．我们以欧拉括号和连分数为工具来处理初等数论的若干问题，并较全面地、系统地介绍同余式及同余式组解的存在、数量和解法．第七章代数整数，以二次整数为模型阐明代数整数与有理整数的异同．并在附录中介绍了规尺作图不能问题的判别法．第八章通过数论函数与素数分布，了解解析数论处理问题的方法．第九章介绍二元二次型的简单知识，初步给出求二次曲线上整点的方法．总之，本书主要是使读者初步了解什么是数论，并为进一步学习数论打好基础．作者长期在福建师大担任数论基础课程，深感数论对于数学爱好者的魅力之强，为了爱好者自学方便，使具备高中数学知识及初等微积分的读者都能卒读全书，在讲义的基础上尽量修改，做到通俗易懂、深入浅出以减少自学的困难．书末附有习题解答．

限于作者水平，本书的缺点与错误在所难免．敬希广大读者批评指正．

王杰官

1986年秋于福州

目　录

第一章　整数的整除性理论

整除是数论中的重要概念，本章主要介绍整数的整除的概念和性质，以带余除法和辗转相除法为工具，建立最大公因数和最小公倍数的理论，并证明算术基本定理。此外，还介绍两个很常用的数论函数$[x]$、$\{x\}$，连分数和欧拉括号等内容。

第一节　整除的概念与性质

两个整数的和、差、积仍然是整数，但是一个非零整数去除另一个整数，所得的商却不一定是整数，因此我们有必要引进整除的概念。

我们约定，下面没有特别声明时，小写拉丁字母a，b，c，…，p，q，r，…等等都表示整数；符号“$\forall$”代表“任给”；“$\exists\cdots\ni$”读作“存在……使得”；“$A\Longrightarrow B$”表示“若有A，则有B”；“$A\Longleftrightarrow B$”是指“B是A的充要条件”。

定义1·1　设$a, b\neq 0$，若$\exists q\ni a=bq$，则称b整除a(a divisible by b)，记作

$$b\mid a.$$

或称a被b所整除，记作

$$a\vdots b.$$

此时称b是a的因数（factor）或约数（divisor），a是b的倍数（multiple）。

反之，若不存在这样的q时，则称b不整除a，记作

$b \nmid a$。

这时 b 不是 a 的因数，a不是 b 的倍数。

这个定义可用下列符号简单表示：

$a, b \neq 0, \exists q \ni a = bq \Longleftrightarrow b|a$。

因为在定义1·1中，并不要求存在的 q 是唯一的，所以关于整除的概念，必要时可以排除 $b \neq 0$ 的限制，当 $b = 0$ 且 $a \neq 0$ 时，$b \nmid a$；当 $b = 0$ 且 $a = 0$ 时，$b|a$，这时q不是唯一的。

整除有下列诸性质：

1° $a|b, b|a \Longrightarrow a = \pm b$。

证明 $a|b, b|a \Longrightarrow \exists q_1, q_2 \ni b = aq_1, a = bq_2 \Longrightarrow a = q_1q_2a \Longrightarrow q_1q_2 = 1 \Longrightarrow q_1 = \pm 1$。

即 $a = \pm b$。

2° $a|b, b|c \Longrightarrow a|c$。

证明 $a|b, b|c \Longrightarrow \exists q_1, q_2 \ni b = aq_1, c = bq_2 \Longrightarrow c = aq_1q_2 \Longrightarrow a|c$。

3° $a|b_1, a|b_2, \cdots, a|b_n, \forall k_1, k_2, \cdots, k_n \Longrightarrow a|k_1b_1 + k_2b_2 + \cdots + k_nb_n$*

证明 对 n 用数学归纳法证明之。

A) 当 $n = 1$ 时，显然结论成立。

B) 设 $n = h$ 时，结论成立。即

$a|b_1, \cdots, a|b_h, \forall k_1, \cdots, k_h \Longrightarrow a|k_1b_1 + \cdots + k_hb_h$。

当 $n = h + 1$ 时，若 $a|b_1, \cdots, a|b_h, a|b_{h+1}, \forall k_1, \cdots, k_h, k_{h+1}$，则由归纳法假设及定义1·1，有

* “|”是表示前后二整数的一种关系，它不与“运算关系”连合使用，放在一个式子里。所以此式就是 $a|(k_1b_1 + k_2b_2 + \cdots + k_nb_n)$ 的简写。

$\exists q_1 q_2 \ni k_1 b_1 + k_2 b_2 + \cdots + k_h b_h = a q_1$，$k_{h+1} b_{h+1} = a q_2$

$\Longrightarrow k_1 b_1 + \cdots + k_h b_h + k_{h+1} b_{h+1} = a(q_1 + q_2)$。

$\therefore$ $a \mid k_1 b_1 + \cdots + k_h b_h + k_{h+1} b_{h+1}$

所以 n 为任意自然数时结论成立。

我们把 $k_1 b_1 + \cdots + k_n b_n$ 叫做 $b_1, \cdots, b_n$ 的一个组合，则性质 3°指的是：若 $a \mid b_i (i = 1, \cdots, n)$，则 a 整除 $b_1, \cdots, b_n$ 的任意组合。由性质 3°立即推得

4° $\sum_{i=1}^{n} b_i = 0$，若 $a \mid \sum_{i=1}^{n} b_i - b_j$，

则 $a \mid b_j$，$(j = 1, 2, \cdots, n)$。

在一般的情形下，a 被 b 除时，我们有

定理 1·1 （带余除法）若 $\forall a, b > 0$，则 $\exists q, r \ni$

$$a = bq + r, \quad 0 \leqslant r < b \qquad (1)$$

成立，并且 q 和 r 都是唯一的。

证明 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots,$$

则由亚里士多德公理（Aristoteles，整数集是亚里士多德式的有序集）知，a 必在上面序列的某两项之间，即 $\exists q \ni qb \leqslant a < (q+1)b$ 成立，令 $a - qb = r$，则等式（1）成立。

设 q_1，r_1 亦满足（1），即

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b$$

因而

$$bq_1 + r_1 = bq + r \Longrightarrow b(q_1 - q) = r - r_1 \Longrightarrow$$

$$\Longrightarrow b \mid q_1 - q \mid = \mid r - r_1 \mid, \text{ 而 } \mid r - r_1 \mid < b \Longrightarrow q_1 - q = 0$$

$$\Longrightarrow r = r_1, \ q = q_1。$$

定义 1·2 （1）中的 q，r 分别叫做 a 被 b 除所得的不完

全商(incomplete quotient)和余数(remainder),特别当$r=0$时,q叫做a被b除所得的商(quotient),这时$b|a$。

例1·1 设$b=7$,$a=-115$,则$q=-17$,$r=4$,即$-115=7\times(-17)+4$,$0<4<7$。

当$b=7$,$a=84$时,$q=12$,$r=0$,即$84=7\times12+0$,此时$7|84$。

第二节 最大公因数与最小公倍数

定义1·3 n个整数a_1,a_2,…,a_n,若$d|a_i$($i=1$,2,…,n),则称d为a_1,a_2,…,a_n的一个公因数或公约数(common factor or commondivisor),公因数中最大的一个称为a_1,a_2,…,a_n的最大公因数(greatest common factor),记作

$$(a_1, a_2, \cdots, a_n)。$$

若$(a_1, a_2, \cdots, a_n)=1$,则称$a_1$,$a_2$,…,$a_n$互素(relatively prime or coprime)或互质。若$(a_i, a_j)=1$($i\neq j=1$,2,…,n),则称a_1,a_2,…,a_n两两互素(质)。

显然,若a_1,a_2,…,a_n两两互素,则a_1,a_2,…,a_n互素。反之不一定成立,例如,(12,15,8)=1,但(12,15)=3,(12,8)=4。

若$a_1=a_2=\cdots=a_n=0$,则任一整数都是它们的公因数,但是它们没有一个最大的公因数。若a_1,a_2,…,a_n不全为零,则存在一个最大公因数。

为了在讨论过程中,避免区别正负整数的麻烦,我们先证明

5° 若a_1,a_2,…,a_n是n个不全为零的整数,则

(i) $a_1, a_2, \cdots, a_n$ 与 $|a_1|, |a_2|, \cdots, |a_n|$ 的公因数相同；

(ii) $(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$.

证明 设 d 是 $a_1, a_2, \cdots, a_n$ 的任一公因数，由定义 1·3 知

$$d \mid a_i (i = 1, 2, \cdots, n) \Longrightarrow d \mid |a_i| (i = 1, 2, \cdots, n)$$

即 d 亦是 $|a_1|, |a_2|, \cdots, |a_n|$ 的公因数；反之也是显然的。特别是，若 $d = (a_1, a_2, \cdots, a_n)$，$d' = (|a_1|, |a_2|, \cdots, |a_n|)$，则 $d \mid |a_1|, d \mid |a_2|, \cdots, d \mid |a_n| \Longrightarrow d \leqslant d'$；且 $d' \mid a_1, d' \mid a_2, \cdots, d' \mid a_n \Longrightarrow d' \leqslant d$.

$\therefore \quad d = d'$.

因为 $(0, b) = |b| \ (b \neq 0)$，所以下面不妨只在正整数范围内讨论最大公因数的问题。无特别声明本节下面出现的小写拉丁字母都代表正整数。

容易证明整除的下列诸性质：

6° $(a_i, a_j) = 1 \ (i \neq j = 1, 2, \cdots, n)$

$$\Longrightarrow (a_1, a_2, \cdots, a_n) = 1.$$

7° $b \mid a \Longrightarrow (a, b) = b, \ (b \neq 0)$.

8° 若 $a = bq + c$，则 a，b 的任一公因数都是 b，c 的公因数；反之，b，c 的任一公因数也都是 a，b 的公因数。特别是

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

下面介绍欧几里德算法（Euclidean algorithm）或称辗转相除法，并用以求两个正整数的最大公因数，$\forall a, b,$

由带余除法，得

$$\begin{cases} a = bq_1 + r_2, & 0 < r_2 < b; \\ b = r_2q_2 + r_3, & 0 < r_3 < r_2; \\ \cdots\quad\cdots\quad\cdots\quad\cdots; \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}; \\ r_{n-1} = r_nq_n + r_{n+1}, & r_{n+1} = 0. \end{cases} \tag{2}$$

因为每进行一次除法，余数至少减少1，b是有限整数，故有限次进行带余除法后，必出现余数为0的情况。由性质8°及7°立得

$$(a, b) = (b, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = r_n.$$

定理1·2 任意正整数a和b，则$(a, b) = r_n$，r_n就是(2)中最后一个不等于0的余数。

系1 a，b的一切公因数，都是(a, b)的因数。

例1·2 求(−1859, 1573)。

解

$q_2 = 5$	1573	1859	$1 = q_1$
	1430	1573	$2 = q_3$
	$r_3 = 143$	$r_2 = 286$	
		286	
		0	

$\therefore$ (−1859, 1573) = (1859, 1573) = 143.

系2 设a，b≠0都是整数。

(i) 若m>0，则(am, bm) = (a, b)m；

(ii) 若c>0，c|a，c|b，则$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a, b)}{c}$。

(iii) $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$。

证略。