简明数论

潘承洞 潘承彪 著

北京大学出版社

简 明 数 论

潘承洞 潘承彪 著

北京大学出版社
北 京

图书在版编目(CIP)数据

简明数论/潘承洞,潘承彪著.—北京:北京大学出版社,1998.1

ISBN 7-301-03528-4

Ⅰ.简… Ⅱ.①潘… ②潘… Ⅲ.数论 Ⅳ.0156

书　　名:简明数论

著作责任者:潘承洞　潘承彪　著

责任编辑:王　艳

标准书号:ISBN 7-301-03528-4/O·403

出 版 者:北京大学出版社

地　　址:北京市海淀区中关村北京大学校内　100871

电　　话:出版部 62752015　发行部 62559712　编辑部 62752032

排 印 者:北京大学印刷厂

发 行 者:北京大学出版社

经 销 者:新华书店

850mm×1168mm　32开本　10.75印张　280千字

1998年1月第一版　1998年1月第一次印刷

印　　数:0001—3,000册

定　　价:14.50元

内 容 简 介

本书是初等数论入门教材. 全书共分三十六节，内容包括：整除、不定方程、同余、指数与原根、连分数、数论函数等. 每节配备适量习题，书末附有提示与解答. 本书积累了作者数十年的教学经验，它是在作者编写的《初等数论》(北京大学出版社，1992)基础上，经过几年的教学实践，认真听取各方面意见，将精选的内容加以重新组织并作必要的修改、补充而成. 使其内容更成熟，结构更合理，具有选择面宽，适用范围广等特点.

本书选材精练，推理严谨，重点突出，例题丰富，习题难易适度，对重点内容从不同侧面和不同角度进行论述，使读者能在较短时间内窥见数论的一些真髓.

读者对象为综合性大学、中、高等师范学校数学系、计算机系及其相关专业师生、教师进修学院师生、数学爱好者、中学数学教师、高中学生.

一 点 说 明

1992 年，北京大学出版社出版了我们的《初等数论》，五年来，一些老师采用本书作为教材，他们和其他读者提出了不少宝贵意见. 教学实践中，我们共同感到的问题是：作为基础课，初等数论一般只有 60 学时左右，该书中有些内容、习题、以及从不同角度所作的讨论，显然超出了这要求. 这在使用上带来了一些不便，也加重了学生的经济负担. 在出版社的支持下，根据各方面的意见，我们以原书为基础，选择适当的内容，加以重新组织和必要的修改补充，写成了这一本《简明数论》，可在 60～70 学时内全部讲完.

本书共三十六节，分为三大部分. (一) 整除理论：§1～§14；(二) 同余理论：§15～§31；(三) 连分数：§32～§36. 在安排上的改动主要是把《初等数论》的第八、九章中关于素数分布、数论函数的最基本内容改写后提到了 §10～§14，这样对教学是有利的. 此外，§24 Jacobi 符号和 §29 二项同余方程是作为学生的自学内容. 本书的习题则从《初等数论》的 768 道减少为 390 道. 为了使用方便，书末给出了习题的提示与解答.《初等数论》可作为教师的教学参考书. 我们觉得，对数论有兴趣的读者、有条件的师范数学系学生(因为他们以后要当老师)，还是读《初等数论》为好.

本书是采用《初等数论》作为教材的老师、热心的读者和北大出版社数理编辑室，特别是《初等数论》的责任编辑刘勇同志，共同关心初等数论教学和教材建设的结果. 本书责任编辑王艳同志提出了不少有益的意见和更正. 我们谨致以由衷的感谢!

由于我们水平有限，错误不当之处一定仍有不少，切望大家批评指正.

作 者

一九九七年夏

符 号 说 明

书中未加说明的字母均表整数.以下是全书通用符号,如在个别地方有不同含义则将明确说明.其他符号在所用章节说明.

$a\mid b$	a 整除 b,§2 定义 1
$a\nmid b$	a 不整除 b,§2 定义 1
$p,p',p_1,p_2,\cdots$	表素数,§2 定义 2
$a^k \parallel b$	$a^k\mid b, a^{k+1}\nmid b$
(a_1,a_2)	a_1 和 a_2 的最大公约数,§4 定义 2
$(a_1,\cdots,a_k)$	$a_1,\cdots,a_k$ 的最大公约数,§4 定义 2
$[a_1,a_2]$	a_1 和 a_2 的最小公倍数,§4 定义 5
$[a_1,\cdots,a_k]$	$a_1,\cdots,a_k$ 的最小公倍数,§4 定义 5
$[x]$	实数 x 的整数部分,§6 定义 1
$\{x\}$	实数 x 的小数部分,§6 定义 1
$\sum_{n\leqslant x}\left(\sum_{n<x}\right)$	对不超过(小于)实数 x 的正整数 n 求和
$\sum_{p\leqslant x}\left(\sum_{p<x}\right)$	对不超过(小于)实数 x 的素数 p 求和
$\sum_{d\mid n}\left(\prod_{d\mid n}\right)$	对 n 的所有正除数 d 求和(求积)
$\sum_{p\mid n}\left(\prod_{p\mid n}\right)$	对 n 的所有素除数 p 求和(求积)
$a\equiv b(\mathrm{mod}\ m)$	a 同余于 b 模 m,§15 定义 1
$a\not\equiv b(\mathrm{mod}\ m)$	a 不同余于 b 模 m,§15 定义 1
$a^{-1}(\mathrm{mod}\ m)$ 或 a^{-1}	a 对模 m 的逆,§15 性质Ⅷ
$r \bmod m$	包含 r 的模 m 的同余类,§16 定义 1

$\sum_{x \bmod m}\left(\sum_{x \bmod m}'\right)$	对模 m 的任意取定的一组完全(既约)剩余系(见§16 定义 2(定义 4))求和
$\tau(n)$	除数函数,§5 推论 6
$\sigma(n)$	除数和函数,§11 例 3
$\varphi(n)$	Euler 函数,§13,§16 定义 3
$\left(\frac{d}{p}\right)$	Legendre 符号,§23 定义 1
$\left(\frac{d}{P}\right)$	Jacobi 符号,§24 定义 1
$\pi(x)$	不超过 x 的素数个数
$\mu(n)$	Möbius 函数,§12 式(1)
$\Lambda(n)$	Mangoldt 函数,§14 式(5)
$\omega(n)$	n 的不同的素因数个数,§11 式(3)
$\Omega(n)$	n 的全部素因数个数,§11 式(4)
$\delta_m(a)$	a 对模 m 的指数,§27 定义 1

目　录

§1 整　　数

以 $\boldsymbol{N}$ 表示由全体正整数(即自然数)

$$1,2,3,4,5,\cdots,n,\cdots$$

所组成的集合,以 $\boldsymbol{Z}$ 表示由全体整数

$$\cdots,-n,\cdots,-3,-2,-1,0,1,2,3,\cdots$$

所组成的集合.在整数集合中可以作加法、减法和乘法运算,整数有大小关系(即可以比较大小),有绝对值概念.我们对整数的这些运算、关系、概念,及它们满足的性质是十分熟悉的.两个整数不一定能作除法,即它们的商不一定是整数.

自然数及其运算源于经验,它最本质的属性(用我们熟悉的话来表述)是:

归纳公理　设 S 是 $\boldsymbol{N}$ 的一个子集,满足条件:(i) $1\in S$;(ii)如果 $n\in S$,则 $n+1\in S$.那么,$S=\boldsymbol{N}$.

这公理是我们常用的数学归纳法的基础.

定理 1(数学归纳法)　设 $P(n)$是关于自然数 n 的一个命题.如果

(i) 当 $n=1$ 时,$P(1)$成立;

(ii) 由 $P(n)$成立必可推出 $P(n+1)$成立,

那么,$P(n)$对所有自然数 n 成立.

证　设使 $P(n)$成立的所有自然数 n 组成的集合是 S.S 是 $\boldsymbol{N}$ 的子集.由条件(i)知 $1\in S$;由条件(ii)知,若 $n\in S$,则 $n+1\in S$.所以由归纳公理知 $S=\boldsymbol{N}$.证毕.

由归纳公理还可推出两个在数学中,特别是初等数论中常用的自然数的重要性质.

定理 2(最小自然数原理)　设 T 是 $\boldsymbol{N}$ 的一个非空子集.那

么，必有 $t_0\in T$，使对任意的 $t\in T$ 有 $t_0\leqslant t$，即 t_0 是 T 中的最小自然数.

证 考虑由所有这样的自然数 s 组成的集合 S：对任意的 $t\in T$ 必有 $s\leqslant t$. 由于 1 满足这样的条件，所以 $1\in S$，S 非空. 此外，若 $t_1\in T$（因 T 非空所以必有 t_1），则 $t_1+1>t_1$，所以 $t_1+1\notin S$. 用反证法，由这两点及归纳公理就推出：必有 $s_0\in S$ 使得 $s_0+1\notin S$（为什么）. 我们来证明必有 $s_0\in T$. 因若不然，则对任意的 $t\in T$ 必有 $t>s_0$，因而 $t\geqslant s_0+1$. 这表明 $s_0+1\in S$，矛盾. 取 $t_0=s_0$ 就证明了定理.

定理 3（最大自然数原理） 设 M 是 $\boldsymbol{N}$ 的非空子集. 若 M 有上界，即存在 $a\in\boldsymbol{N}$，使对任意的 $m\in M$ 有 $m\leqslant a$，那么，必有 $m_0\in M$，使对任意的 $m\in M$ 有 $m\leqslant m_0$，即 m_0 是 M 中的最大自然数.

证 考虑由所有这样的自然数 t 组成的集合 T：对任意的 $m\in M$ 有 $m\leqslant t$. 由条件知 $a\in T$，所以 T 非空. 由定理 2 知，集合 T 中有最小自然数 t_0. 我们来证明 $t_0\in M$. 若不然，则对任意的 $m\in M$ 必有 $m<t_0$，因而 $m\leqslant t_0-1$. 这样就推出 $t_0-1\in T$，但这和 t_0 的最小性矛盾. 取 $m_0=t_0$ 就证明了定理.

最小自然数原理是我们常用的第二种数学归纳法的基础.

定理 4（第二种数学归纳法） 设 $P(n)$ 是关于自然数 n 的一个命题. 如果

(i) 当 $n=1$ 时，$P(1)$ 成立；

(ii) 设 $n>1$. 若对所有的自然数 $m<n$，$P(m)$ 成立，则必可推出 $P(n)$ 成立，

那么，$P(n)$ 对所有自然数 n 成立.

证 用反证法. 若定理不成立，设 T 是使 $P(n)$ 不成立的所有自然数组成的集合，T 非空. 由定理 2 知集合 T 必有最小自然数 t_0. 由于 $P(1)$ 成立，所以 $t_0>1$. 由条件(ii)（取 $n=t_0$）知，必有自然数 $m<t_0$ 使 $P(m)$ 不成立. 由 T 的定义知 $m\in T$，但这和 t_0 的最小性矛盾. 证毕.

以上四个定理在应用中有时需作适当变形，这些将安排在习

题中. 初等数论中还要经常用到熟知的盒子原理(即鸽巢原理):

定理 5(盒子原理) 设 n 是一个自然数. 现有 n 个盒子和 $n+1$ 个物体. 无论怎样把这 $n+1$ 个物体放入这 n 个盒子中,一定有一个盒子中被放了两个或两个以上的物体.

证 用反证法. 假设结论不成立,即每个盒子中至多有一个物体,那么,这 n 个盒子中总共有的物体个数$\leqslant n$. 这和有 $n+1$ 个物体放到了这 n 个盒子中相矛盾. 证毕.

习 题 一[①]

1. 设 k_0 是给定的正整数,$P(n)$是关于正整数 n 的一个命题. 如果

(i) 当 $n=k_0$ 时,$P(k_0)$成立;

(ii) 由 $P(n)$成立可推出 $P(n+1)$成立,

那么,$P(n)$对所有正整数 $n\geqslant k_0$ 成立.

2. 在上题的条件下,如果

(i) 当 $n=k_0$ 时 $P(k_0)$成立;

(ii) 设 $n>k_0$. 由对所有的 $m(k_0\leqslant m<n)P(m)$成立可推出 $P(n)$成立,

那么,$P(n)$对所有正整数 $n\geqslant k_0$ 成立.

3. 设 T 是一个由整数组成的集合. 若 T 中有正整数,则 T 中必有最小正整数.

4. 设 T 是一个由整数组成的集合,若 T 有下界,即存在整数 a 使对所有的 $t\in T$,有 $t\geqslant a$,那么,必有 $t_0\in T$,使对所有的 $t\in T$ 有 $t\geqslant t_0$.

5. 设 M 是一个由整数组成的集合. 若 M 有上界,即存在整数 a,使对所有的 $m\in M$ 有 $m\leqslant a$,那么,必有 $m_0\in M$,使对所有的

---

① 做本书的习题必须按照以下要求:只能用这道题之前讲过的内容和做过的题去做,而不许用这道题以后讲的内容. 这是为了更好的理解理论体系的逻辑结构.

$m \in M$有 $m \leqslant m_0$.

6. 设 $a \geqslant 2$ 是给定的正整数. 证明：对任一正整数 n 必有唯一的整数 $k \geqslant 0$，使 $a^k \leqslant n < a^{k+1}$.

§2 整除、素数与合数

定义 1 设 $a,b\in\mathbf{Z},a\neq0$. 如果存在 $q\in\mathbf{Z}$ 使得 $b=aq$,那么就说 b **可被** a **整除**,记作 $a|b$,且称 b 是 a 的**倍数**,a 是 b 的**约数**(也可称为**除数**、**因数**). b 不能被 a 整除就记作 $a\nmid b$.

由定义及乘法运算的性质,立即可推出整除关系有下面性质(注意:符号 $a|b$ 本身包含了条件 $a\neq0$).

定理 1 (i) $a|b\Longleftrightarrow -a|b\Longleftrightarrow a|-b\Longleftrightarrow |a||b|$;

(ii) $a|b$ 且 $b|c\Longrightarrow a|c$;

(iii) $a|b$ 且 $a|c\Longleftrightarrow$ 对任意的 $x,y\in\mathbf{Z}$ 有 $a|bx+cy$;

(iv) 设 $m\neq0$. 那么,$a|b\Longleftrightarrow ma|mb$;

(v) $a|b$ 且 $b|a\Longrightarrow b=\pm a$;

(vi) 设 $b\neq0$. 那么,$a|b\Longrightarrow |a|\leqslant|b|$.

证 (i) 由以下各式两两等价推出:

$$b=aq,\quad b=(-a)(-q),\quad -b=a(-q),\quad |b|=|a||q|.$$

(ii) 因由 $b=aq_1,c=bq_2$ 推出 $c=a(q_1q_2)$.

(iii) 必要性. 因由 $b=aq_1,c=aq_2$ 推出 $bx+cy=a(q_1x+q_2y)$. 取 $x=1,y=0$,及 $x=0,y=1$ 就推出充分性.

(iv) 由乘法相消律知,$m\neq0$ 时,$b=aq$ 等价于 $mb=(ma)q$.

(v) 由 $b=aq_1,a=bq_2$ 知 $a=aq_1q_2$. $a\neq0$ 所以 $q_1q_2=1,q_1=\pm1$.

(vi) 由(i)知 $|b|=|a||q|$. 当 $b\neq0$ 时,$|q|\geqslant1$. 证毕.

这些看来十分简单的性质是非常有用的.

例 1 证明:若 $3|n$ 且 $7|n$,则 $21|n$.

由 $3|n$知 $n=3m$,所以$7|3m$. 由此及$7|7m$得 $7|(7m-2\cdot3m)=m$. 因而有 $21|n$.

例 2 设 $a=2t-1$. 若 $a|2n$，则 $a|n$.

由 $a|2tn$ 及 $2tn=an+n$ 得 $a|(2tn-an)$，即 $a|n$.

例 3 设 a,b 是两个给定的非零整数，且有整数 x,y，使得 $ax+by=1$. 证明：若 $a|n$ 且 $b|n$，则 $ab|n$.

由 $n=n(ax+by)=(na)x+(nb)y$，及 $ab|na, ab|nb$ 即得所要结论. 注意到 $7\cdot 1+3\cdot(-2)=1$，由此也证明了例 1.

例 4 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整系数多项式. 若 $d|b-c$，则 $d|f(b)-f(c)$.

我们有

$$f(b)-f(c)=a_n(b^n-c^n)+a_{n-1}(b^{n-1}-c^{n-1})+\cdots+a_1(b-c),$$

由此及 $d|b^j-c^j$，就推出所要结论.

例 4 常用的形式是：若 $b=qd+c$，那么 $d|f(b)$ 的充要条件是 $d|f(c)$.

由定义知，一个整数 $a\neq 0$，它的所有倍数是

$$qa,\quad q=0,\pm 1,\pm 2,\cdots,$$

这个集合是完全确定的. 零是所有非零整数的倍数. 但对于一个整数 $b\neq 0$，关于它的约数一般就知道得不多了. 显见，$\pm 1,\pm b$（当 $b=\pm 1$ 时只有两个）一定是 b 的约数，它们称为是 b 的**显然约（因、除）数**；b 的其他的约数（如果有的话）称为是 b 的**非显然约（因、除）数**，或**真约（因、除）数**. 由定理 1(vi) 知，$b\neq 0$ 的约数个数只有有限个. 例如，$b=12$ 时，它的全体约数是：

$$\pm 1,\pm 2,\pm 3,\pm 4,\pm 6,\pm 12,$$

其中非显然约数有 8 个. $b=7$ 时，它的全体约数是：

$$\pm 1,\pm 7,$$

它没有非显然约数. 下面关于约数的性质是有用的.

定理 2 设整数 $b\neq 0, d_1,d_2,\cdots,d_k$ 是它的全体约数. 那么，$b/d_1, b/d_2,\cdots,b/d_k$ 也是它的全体约数. 也就是说，当 d 遍历 b 的全体约数时，b/d 也遍历 b 的全体约数. 此外，若 $b>0$，则当 d 遍历 b 的全体正约数时，b/d 也遍历 b 的全体正约数.

证 当 $d_j|b$ 时，b/d_j 是整数，$b=d_j(b/d_j)$，所以 b/d_j 也是 b 的约数，且当 $d_i\neq d_j$ 时，$b/d_i\neq b/d_j$. 这样，$b/d_1,\cdots,b/d_k$ 是 k 个两两不同的 b 的约数. 由于 b 的约数的个数是一定的，这就证明了第一个结论. 由此及 d_j 是正的当且仅当 b/d_j 也是正的，就推出第二个结论. 证毕.

显见 $b\neq 0$ 的全体约数中，一半是正的，一半是负的.

例如，$b=12$ 时，我们有

$$d=\pm 1,\pm 2,\pm 3,\pm 4,\pm 6,\pm 12.$$

$$b/d=\pm 12,\pm 6,\pm 4,\pm 3,\pm 2,\pm 1.$$

上面已经看到，有的数(例如 7)只有显然约数. 这种数在整数中有特别重要的作用. 为此引进

定义 2 设整数 $p\neq 0,\pm 1$. 如果它除了显然约数 $\pm 1,\pm p$ 外没有其他的约数，那么，p 就称为是**素数(或质数)**. 若 $a\neq 0,\pm 1$ 且 a 不是素数，则 a 称为**合数**.

当 $p\neq 0,\pm 1$ 时，由于 p 和 $-p$ 必同为素数或合数，所以，以后若没有特别说明，**素数总是指正的**. 例如

$$2,3,5,7,11,13,17,19,23,29,31$$

都是素数. 由定义立即推出(读者自己证明)：

定理 3 (i) $a>1$ 是合数的充要条件是 $a=de,1<d<a,1<e<a$；

(ii) 若 $d>1,q$ 是素数且 $d|q$，则 $d=q$.

定理 4 若 a 是合数，则必有素数 $p|a$.

证 由定义知 a 必有除数 $d\geqslant 2$. 设集合 T 由 a 的所有除数 $d\geqslant 2$ 组成. 由最小自然数原理知集合 T 中必有最小的自然数，设为 p. p 一定是素数. 若不然，$p\geqslant 2$ 是合数，由定理 3(i)知 p 必有除数 d'：$2\leqslant d'<p$. 显然 d' 属于 T，这和 p 的最小性矛盾. 证毕.

一个整数的除数如果是素数，那么这个除数就称为**素除(因)数**.

定理 5 设整数 $a\geqslant 2$. 那么，a 一定可表为素数的乘积(包括 a