初等数论

潘承洞　潘承彪　著

北京大学出版社

初 等 数 论

潘承洞　潘承彪　著

北京大学出版社

$a \not\equiv b \pmod m$	a 不同余于 b 模 m，第三章 § 1定义 1
$a^{-1} \pmod m$或 a^{-1}	a 对模 m 的逆，第三章 § 1性质Ⅷ
$r \bmod m$	包含 r 的模 m 的同余类，第三章 § 2 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）剩余系求和，第三章 § 2例 8
$\tau(n)$	除数函数，第一章 § 6推论 6
$\sigma(n)$	除数和函数，第一章 § 6推论 7
$\phi(n)$	Euler 函数，第三章 § 2定义 3
$\left(\frac{d}{p}\right)$	Legendre符号，第四章 § 6定义1
$\left(\frac{d}{P}\right)$	Jacobi 符号，第四章 § 7 定义1
$\pi(x)$	不超过 x 的素数个数
$\mu(n)$	Möbius 函数，第八章 § 1 式(22)
$\Lambda(n)$	Mangoldt 函数，第八章 § 2 式(34)
$\omega(n)$	n 的不同的素因数个数，第九章 § 1 式(5)
$\Omega(n)$	n 的全部素因数个数，第九章 § 1式(6)
$\delta_m(a)$	a 对模 m 的指数，第五章 § 1定义 1
$\gamma_{m,g}(a)(\gamma_g(a),\gamma(a))$	a 对模 m 的以 g 为底的指标，第五章 § 3 定义 1
$\chi(n;k),\chi(n),\chi \bmod k$	模 k 的 Dirichlet(剩余)特征，第九章 § 4 定义 1

内 容 简 介

本书是大学初等数论课教材．全书共分九章．内容包括：整除，不定方程，同余，同余方程，指数与原根，连分数，素数分布的初等结果，数论函数等．书中配有较多的习题，书末附有提示与解答．本书积累了作者数十年教学与科研的经验，遵循少而精的原则，精心选材．为便于学生理解，对重点内容多侧面分析，从不同角度进行阐述．

本书概念叙述清楚，推理严谨，层次分明，重点突出，例题丰富，具有选择面宽，适用范围广，适宜自学等特点．

本书可作为综合大学数学系，计算机系，中、高等师范学校及教师进修院校的教材，也可供数学工作者、中学数学教师和高中学生阅读．

序

初等数论是研究整数最基本的性质，是一门十分重要的数学基础课。它不仅应该是中、高等师范院校数学专业，大学数学各专业的必修课，而且也是计算机科学等许多相关专业所需的课程。中学生（甚至小学生）课外数学兴趣小组的许多内容也是属于初等数论的。

整除理论是初等数论的基础，它是在带余数除法（见第一章§3定理1）的基础上建立起来的。整除理论的中心内容是算术基本定理和最大公约数理论。这一理论可以通过不同的途径来建立，而这些正反映了近代数学中的十分重要的思想、概念与方法。本书的第一章就是讨论整除理论，较全面地介绍了建立这一理论的各种途径及它们之间的相互关系。同余理论是初等数论的核心，它是数论所特有的思想、概念与方法。这一理论是由伟大的数学家C.F.Gauss在其1801年发表的著作《算术研究（Disquisitiones Arithmeticae)》中首先提出并系统研究的。Gauss的这一名著公认为是数论作为数学的一个独立分支的标志①。本书的第三、四、五章就是较深入地讨论同余理论的基本知识，包括同余、同余类、完全剩余系和既约剩余系等基本概念及其性质；一次、二次同余方程和模为素数的同余方程的基本理论；以及既约剩余系的结构。从历史来看，求解不定方程是推进数论发展的最主要的课题，我们在第二、六章讨论了可以用以上建立的整除理

① 关于数论的发展历史可参看：数学百科辞典（科学出版社，1984），中国大百科全书·数学（中国大百科全书出版社，1988），不列颠百科全书（详编）·数学（科学出版社，1992）等三本数学百科全书中的有关条目；以及W.Scharlau和H.Opolka，From Fermat to Minkowski, Springer-Verlag, 1985.

论和同余理论来解的几类最基本的不定方程。一般来说，以上这些就是初等数论的基本内容，是必需掌握的。为了满足不同的需要，除了在这六章中有若干加“*”号的内容外，我们在第七章讨论了连分数与Pell方程，第八章讨论了素数分布的初等结果，及第九章的数论函数，供读者选用（这三章中有些部分要用到一点初等微积分知识，较难的加“*”号表示）。这些也都是初等数论的重要内容。本书的取材严格遵循少而精的原则，及作为基本上适用于前述各类学生的通用教材来安排的。此外，对某些重点内容在正文、例题和习题中从不同角度作适当反复讨论，根据我们的经验，这对全面深入理解和教与学都是有益的。特别要指出的是，这样的安排十分有利于自学。这些内容主要是：最大公约数理论，算术基本定理，剩余类及剩余系的构造，Euler函数，以及某些不定方程。在具体讲授时可根据需要和学时多少，适当选择其中一部分或全部，及选择一部分让学生自学。

数论是研究整数性质的一个数学分支，当然对“整数”本身必须有一个清楚、正确的认识，但要做到这一点并不容易，在附录一中介绍了自然数的Peano公理，对此作一初步讨论。在整数中算术基本定理——每个大于1的整数一定可以唯一地（在不计次序的意义下）表为素数的乘积——的正确性好象是理所当然的，但实则不然。为了较有说服力地向刚接触数论的读者说明，当研究对象稍为扩大一点，即研究所谓代数整数环时，算术基本定理就不一定成立，我们在附录二中讨论了二次整环$\boldsymbol{Z}[\sqrt{-5}]$。初等数论本身有许多有趣应用，在附录三中介绍了四个简单的应用，特别是电话电缆的铺设几乎用到了初等数论的全部基本知识①。大家知道，初等数论在国际数学奥林匹克竞赛中占有愈来愈重要的地位，这些竞赛题的绝大多数都是很好的，对提高大、

① 关于数论的应用可参看[10]；M.R. Schroeder, Number Theory in Science and Communication, Springer-Verlag, 1984；及N.Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1987.

中学生的数学素质是很有帮助的．因此，我们在附录四中列出了至今三十二届竞赛中可用初等数论方法——即第一章的整除理论——来解的51道题（占总数194道题的26.3%）。

初等数论初看起来似乎很简单，但真正教好、学好它并不容易，尤其是习题很不好做．这一方面可能是觉得初等数论的理论没有什么内容，从代数观点来看只是一些简单的例子，仅把它作为学习代数的预备知识，不了解整数本身所包含的丰富而重要的内涵而不加重视；另一方面是忽视初等数论的理论，只把它看作是一些互不相关的有趣的智力竞赛题，因而不认真学习它的理论并用以指导解题．事实上，或许可以说，初等数论是数学中“理论与实践”相结合得最完美的基础课程，近代数学中许多重要思想、概念、方法与技巧都是从对整数性质的深入研究而不断丰富和发展起来的．数论在计算机科学等许多学科，以及离散数学中所起的日益明显的重要作用也绝不是偶然的．这些正是学习初等数论的重要性之所在．

为了比较好地满足教与学的需要，数学基础课教材应当配有适量的、互相联系的、理论与计算并重的例题和习题，通过这些例题和习题能更好地理解、掌握、以及自然地导出所讲述的概念、理论、方法与技巧．我们尽量地按照这一要求去做．为了学好数学基础课必需独立去做较多的习题．本书的习题依每节来安排，正文中共768道题，为了便于教师选用，在书末给出了提示与解答，但希望学生不要轻易就看解答，应该力争由自己独立完成．各附录共有76道题，都没有给出提示与解答。

我们深知要写好一本初等数论的教材绝非易事，虽然，我们从事数论工作数十年，从1978年起就在山东大学与北京大学开设初等数论课，但一直未敢动笔．现在为了适应教学需要，把我们多年所积累的讲稿进行挑选、补充和进一步加工整理，编写成这一本不够成熟，我们也仍不满意的教材，其中疏忽不当以至错误之处在所难免，切望同行和读者多多指正。

本书的出版得到了我们的母校北京大学教材建设委员会和北京大学出版社数理编辑室的大力支持；责任编辑刘勇同志改正了书稿中的许多笔误和疏漏，作了大量有益的工作，对此表示最衷心的感谢！

潘承洞　潘承彪

1991年11月于北京

初 等 数 论

潘承洞 潘承彪 著

责任编辑：刘 勇

*

北京大学出版社出版发行

（北京大学校内）

北京国马印刷厂印刷

新 华 书 店 经 售

*

850×1168毫米 32开本 19.625印张 500千字

1992年9月第一版 1998年4月第五次印刷

印数:13,001—16,000

ISBN 7-301-01848-7/O·285

定价：25,00元

目　录

第一章 整 除

整除理论是初等数论的基础，它是对在小学就学过的整数的算术，主要是涉及除法运算的内容，作抽象的、系统的总结，看起来似乎很简单，但是它的内涵是十分重要而深刻的。本章的主要结果是数学中最重要、最基本、最著名的定理之一——算术基本定理，即每个大于1的正整数必可唯一地表为若干个素数的乘积，这一定理将在§6及§7讨论，分别给出了两个不同的证明。本章内容是围绕这一定理的讨论安排的。为了使讨论自然和方便，在§1中先概述了整数的加法、减法及乘法运算的概念与性质；整数的大小关系及其性质；特别是讨论了自然数的最重要的两个性质：自然数的归纳原理及由此推出的最小自然数原理，这是建立整除理论的基础，在本章及以后各章中经常要用到。在§3中，我们讨论建立整除理论的重要工具：带余数除法，并介绍了它的若干应用。在§2中，讨论整除的最简单的性质，这些性质实质上是不涉及加法、减法运算的；还引进了素数的概念，讨论了与素数有关的最简单性质。在§4中我们建立最大公约数理论，它是整除理论的核心内容，对此我们作了较全面的讨论。在第一部分，给出了不依赖于带余数除法的最大公约数及最小公倍数的性质；第二部分利用带余数除法建立了完整的最大公约数与最小公倍数理论，在这一部分中我们直接从定义出发，不需要利用最大公约数的明确表示式

$$(a,b)=ax+by,$$

但在证明中要用到较高的技巧；第三部分是在证明上式的基础上，利用它重新建立完整的最大公约数理论（不需要最小公倍数的概念与性质）。§5讨论所谓辗转相除法，即Euclid算法，它是

带余数除法的发展，利用它不仅可以证明上式成立，而且给出了寻找最大公约数(a,b)及x,y的有效算法。这一方法是十分有用的，在第七章将用它来建立连分数理论。最后，在§8中，我们引进一个在数学中十分有用的符号——实数x的最大整数部分$[x]$，并讨论它的性质。利用它我们给出了$n!$的素数乘积的表达式，它是除算术基本定理之外，另一个刻画自然数与素数之间关系的十分重要的关系式，我们将在第八章§2给出它的应用。

还应该指出的是，§6给出的算术基本定理的证明是利用§4建立的最大公约数理论，而§7给出的证明是直接的，它仅用到了最小自然数原理及大小关系的性质（实质上就是带余数除法），不需要最大公约数的任何知识。相反的，从算术基本定理出发也可以建立最大公约数与最小公倍数理论。

§1 自然数与整数

自然数，也叫正整数，就是大家所熟悉的

$$1,2,3,\cdots,n,n+1,\cdots. \tag{1}$$

我们以$\boldsymbol{N}$表由全体自然数(1)所组成的集合。整数就是指正整数、负整数及零，即

$$\cdots,-n-1,-n,\cdots,-3,-2,-1,0,1,2,3,\cdots,n,n+1,\cdots. \tag{2}$$

我们以$\boldsymbol{Z}$表由全体整数(2)组成的集合。

在整数集合中可以作**加法运算**“$+$”及其逆运算**减法运算**“$-$”。加法运算满足以下性质：

(i) **结合律** $(a+b)+c=a+(b+c)$， $a,b,c\in\boldsymbol{Z}$。

(ii) **交换律** $a+b=b+a$， $a,b\in\boldsymbol{Z}$。

(iii) **相消律** $a+b=a+c\Longrightarrow b=c$， $a,b,c\in\boldsymbol{Z}$。

(iv) $a+0=a$， $a\in\boldsymbol{Z}$。

(v) 对任意的$a,b\in\boldsymbol{Z}$，必有$x\in\boldsymbol{Z}$使得

$$a=b+x。$$

(v)就是减法运算的定义：$a-b=x$。

在整数集合中可以作乘法运算“·”，但不一定可作乘法的逆运算——除法运算。乘法运算满足以下性质：

(i) **结合律** $(a\cdot b)\cdot c=a\cdot(b\cdot c)$， $a,b,c\in \boldsymbol{Z}$。

(ii) **交换律** $a\cdot b=b\cdot a$， $a,b\in \boldsymbol{Z}$。

(iii) **相消律** 若 $a\neq 0, a\cdot b=a\cdot c$，则 $b=c$， $a,b,c\in \boldsymbol{Z}$。

(iv) $0\cdot a=0$， $a\in \boldsymbol{Z}$。

(v) $1\cdot a=a$， $a\in \boldsymbol{Z}$。

(vi) **分配律** $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$， $a,b,c\in \boldsymbol{Z}$。

为简单起见，乘法 $a\cdot b$ 就记作 ab。

在整数中有**大小（即顺序）关系**，并用符号：$\leqslant,<,\geqslant$，及 $>$等来表示①。整数的顺序有以下性质：

(i) 对任意的 $a,b\in \boldsymbol{Z}$，关系

$$a=b， \quad a<b， \quad b<a$$

有且仅有一个成立。

(ii) **自反性** $a\leqslant a$， $a\in \boldsymbol{Z}$。

(iii) **反对称性** 对任意的 $a,b\in \boldsymbol{Z}$，若 $a\leqslant b$ 且 $b\leqslant a$，则 $a=b$。

(iv) **传递性** 对任意的 $a,b,c\in \boldsymbol{Z}$，若 $a\leqslant b$ 且 $b\leqslant c$，则 $a\leqslant c$，且等号仅当 $a=b, b=c$ 均成立时才成立。

(v) 对任意的 $a,b,c\in \boldsymbol{Z}$， $a+c\leqslant b+c\Longleftrightarrow a\leqslant b$。

(vi) 对任意的 $a,b,c\in \boldsymbol{N}$，若 $c=ab$，则 $a\leqslant c$，等号当且仅当 $b=1$时成立。

(vii) 对任意的 $a,b\in \boldsymbol{Z}$ 及 $c\in \boldsymbol{N}, ac\leqslant bc\Longleftrightarrow a\leqslant b$。

(viii)对任意的 $a,b\in \boldsymbol{Z}$， $a\leqslant b\Longleftrightarrow -a\geqslant -b$。

在整数中还引入了**绝对值的概念**：

---

① $b\geqslant a$即$a\leqslant b$。$a<b$表示$a\leqslant b$且$a\neq b$。$b>a$即$a<b$。

$$|a| = \begin{cases} a, & a \in \boldsymbol{N}, \\ 0, & a = 0, \\ -a, & -a \in \boldsymbol{N}. \end{cases}$$

它显然具有性质：

(i) $|ab| = |a||b|$， $a,b \in \boldsymbol{Z}$.

(ii) $|a+b| \leqslant |a| + |b|$， $a,b \in \boldsymbol{Z}$.

以上列举了一些熟知的有关整数的知识. 对自然数来说它的最重要、最本质的性质是：

归纳原理 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，$S = \boldsymbol{N}$.

这原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 的一种性质或命题. 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 $n+1 \in S$. 所以由归纳原理知 $S = \boldsymbol{N}$. 证毕.

由归纳原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 $t_1 + 1 \notin S$. 由这两点及归纳原理就推出：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 $t \in T$