高等学校
数学教材

初等数论

潘承洞 潘承彪 著

第二版

北京大学出版社

高等学校数学基础课教材

初等数论

（第二版）

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

初等数论/潘承洞,潘承彪著. —2版. —北京:北京大学出版社,2003.1

ISBN 7-301-06075-0

Ⅰ.初... Ⅱ.①潘...②潘... Ⅲ.初等数论—高等学校—教材 Ⅳ.0156.1

中国版本图书馆CIP数据核字(2002)第102037号

书　　名:初等数论

著作责任者:潘承洞　潘承彪　著

责任编辑:刘　勇

标准书号:ISBN 7-301-06075-0/O·0560

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

网　　址:http://cbs.pku.edu.cn/cbs.htm

电　　话:邮购部 62752015　发行部 62750672　理科编辑部 62752021

电子信箱:zpup@pup.pku.edu.cn

排　版　者:北京因温特有限公司

印　刷　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

890×1240　A5开本　19.25印张　520千字

1992年9月第一版　2003年1月第二版

2003年1月第8次印刷

印　　数:24001—28000册

定　　价:25.00元

第二版说明

《初等数论》出版已经10年了。根据教学实践，经考虑再版仍保持原书的定位、体系、与风格，对第一版内容除在文字叙述、解释上略作改进润色，改正了若干疏误外，还稍作调整与补充。它们主要是：

（一）在第一章，把原来§4中最大公约数与最小公倍数的定义及和带余数除法无关的性质（即§4的第一部分）移至§2；把原§5“辗转相除法”全部合并到§3；原§6，§7与§8分别改为§5，§6，与§7；增加了§8“容斥原理与$\pi(x)$的计算公式”。当然，习题也作了相应调整。

此外，为了加深对整数、整除、及整除理论的概念、方法的理解与掌握，相应地在附录二中增加了(i)有关一元有理系数多项式集合$\boldsymbol{Q}[x]$与一元整系数多项式集合$\boldsymbol{Z}[x]$的整除理论的习题（第9～19题），及(ii)有关代数数、代数整数的概念与性质，及Gauss整数$\boldsymbol{Z}[\sqrt{-1}]$的整除理论的习题（第20～30题）。这些对需要进一步学习数论知识的读者是有帮助的。

（二）在第二章§2中，稍为仔细地讨论了单位圆周上的有理点。

（三）第三章，在§2中引进了整数与整数集合的‘和’及‘积’的概念和符号，以及用此来证明同余类与剩余系的性质；在§3的最后极简单地描述了所谓‘公开密钥密码系统’。

（四）在第四章，增加了§9“多元同余方程、Chevalley定理”。

（五）第五章习题一增加了第33题，及第九章习题二增加了第29、30题，它们分别给出了命题：‘首项为1的算术数列中有无穷多个素数’的两个不同证明。

（六）第九章§2中Mobius反转公式的讲述和证明作了改变。虽然这较简洁，但原来的有其优点。

（七）在附录四，补充了本书第一版以后各届国际数学奥林匹克竞赛中与数论有关的题。至今共四十三届，82道题。

（八）改进了一些习题的提示与解答，附录中增加的题都没有给出提示。现正文中共有797道题，附录中共有131道题。

（九）增加了名词索引。

保持本书的原样并作以上改动的依据是考虑了：10年来采用本书作为教材的教师们所提出的宝贵意见；学生们在学习中提出的问题、进行的讨论和给出的漂亮的习题解答；本书责任编辑刘勇副编审的宝贵意见；以及10年来，我们对自己为不同的对象（包括中学生、中学教师、大学生以及研究生），按本书内容的不同组合，以不同的方式来进行教学所作的不断总结，仔细寻找教材的不足并加以改进。在这里我谨向以上所有的同志表示衷心感谢！

好像没有一门学科像“初等数论”那样，它最基本的内容可以同时作为中小学师生、大学生以及研究生的一门课程，当然在内容的深浅难易上各有不同。这是一门有其自身特点、不可缺少的基础课。我们深深感到应该也期望有适合不同对象的初等数论教材出现，而这正是我国目前所缺少的。当然，教材必需遵循初等数论的基本理论体系，既不能“把它看作是一些互不相关的有趣的智力竞赛题”的汇集，也不能认为它“只是一些简单的例子，仅把它作为学习代数的预备知识”（见第一版序）。因为，数学是人类文化最重要的组成部分之一，它是日益显示其重要性的一种科学的语言，一种科学的思维方式和强有力的科学工具，而初等数论的思想、概念、方法和理论则是数学思维链中不可或缺的重要一环。尽管近代数论可以包容它，但不能代替它。而且，事实证明：不学好初等数论大概是什么数论也学不好的。

正如第一版序中所说，承洞和我“深知要写好一本初等数论的教材绝非易事”，现在再版修订只能由我一人来承担，错漏不当之处更为难免，切望读者多多指正。

潘承彪

2002年中秋

第一版序

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。为了满足读者不同的需要，除了在这六章中有若干加“*”号

---

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.

* 该书因故未出版。可参看数学百科全书（共五卷，科学出版社，2000）。——再版注.

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 的整数一定可以惟一地(在不计次序的意义下)表为素数的乘积——的正确性好像是理所当然的，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、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

① 关于数论的应用可参看[11]；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.

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，做了大量有益的工作，对此表示最衷心的感谢！

潘承洞　潘承彪
1991 年 11 月于北京

符 号 说 明

书中未加说明的字母均表整数. 以下是全书主要的通用符号，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.

$\boldsymbol{N}$	全体自然数，即正整数组成的集合，见第一章 § 1 式(1)
$\boldsymbol{Z}$	全体整数组成的集合，见第一章 § 1 式(2)
$\boldsymbol{Z}[x]$	全体一元整系数多项式组成的集合，第一章 § 2 例 4
$a \mid b$	a 整除 b，第一章 § 2 定义 1
$a \nmid b$	a 不整除 b，第一章 § 2 定义 1
$p, p', p_1, p_2, \cdots$	表素数(不可约数)，第一章 § 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，第一章 § 2 定义 4
$(a_1, \cdots, a_k)$	$a_1, \cdots, a_k$ 的最大公约数，第一章 § 2 定义 4
$[a_1, a_2]$	a_1 和 a_2 的最小公倍数，第一章 § 2 定义 7
$[a_1, \cdots, a_k]$	$a_1, \cdots, a_k$ 的最小公倍数，第一章 § 2 定义 7
$\delta_m(a)$	a 对模 m 的指数，第一章 § 4 例 5，第五章 § 1 定义 1
$[x]$	实数 x 的整数部分，第一章 § 7 定义 1
$\{x\}$	实数 x 的小数部分，第一章 § 7 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
$\sum_{d \mid a}\left(\prod_{d \mid a}\right)$	对 a 的所有正除数 d 求和(求积)，第一章 § 5 式(15)((17))
$\sum_{p \mid a}\left(\prod_{p \mid a}\right)$	对 a 的所有素除数 p 求和(求积)，第一章 § 5 式(16)((18))
$a \equiv b \pmod m$	a 同余于 b 模 m，第三章 § 1 定义 1
$a \not\equiv b \pmod m$	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

$f(x)\equiv g(x)(\mathrm{mod}\, m)$	多项式 $f(x)$同余于 $g(x)$模 m,第三章 § 1 定义 2,第四章 § 9(i)
$r \bmod m$	包含 r 的模 m 的同余类,第一章 § 3 例 1,第三章 § 2 定义 1
$\bigcup_{y \bmod m}$	对模 m 的任意取定的一组完全剩余系求并,第三章 § 2 式(6)
$\sum_{x \bmod m}\left(\sum_{x \bmod m}'\right)$	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 § 5 推论 6
$\sigma(n)$	除数和函数,第一章 § 5 推论 7
$\varphi(n)$	Euler 函数,第一章 § 8 例 3,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
$\pi(x)$	不超过实数 x 的素数个数
$\mu(n)$	Möbius 函数,第三章 § 2 例 8,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)
$\gamma_{m,g}(a)(\gamma_g(a),\gamma(a))$	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

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. 本章的主要内容是最大公约数理论和数学中最重要、最基本、最著名的定理之一——算术基本定理，即每个大于 1 的正整数必可惟一地表为若干个素数的乘积，前者在 §4 讨论，后者则在 §5 及 §6 讨论. 本章内容是这样安排的：为了使讨论自然和方便，在 §1 中先概述了熟知的有关整数的知识——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即正整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 §2 中，讨论整除的基本概念与最简单的性质（这些性质实质上是不涉及加法、减法运算的），引进了素数、最大公约数、及最小公倍数等概念. 讨论了有关的最简单性质. 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）及辗转相除法. 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，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：存在整数 x, y，使得

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

但在证明中要用到较高的技巧；第二部分是在首先证明上式的基础上，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）. 我们将对上式给出两个不同的证明，一是利用辗转相除法给出的构造性证明，而另一则是直接的非构造性证明. 在 §5，利用 §4 的结论证明了算术基本定理，并给出了它的重要应用. 在 §6 中，我们给出了算术基本定理的不依赖于 §4 的直接证明，并指出由此亦可建立