數論導引

華羅庚

科學出版社

數論導引

華羅庚

科學出版社

1979

内 容 简 介

全书共二十章，前六章是属于基础知识，内容包括：整数分解，同余式，二次剩余，多项式之性质，素数分布概况，数论函数等；后十四章是就解析数论，代数数论，超越数论，数的几何这几个数论主要分支的基础部分加以介绍，内容包括：三角和，数的分拆，素数定理，连分数，不定方程，二元二次型，模变换，整数矩阵，p-adic 数，代数数论导引，超越数，Waring 问题与 Prouhet-Tarry 问题，数的几何等．书里引述了许多我国古代数学家在数论上的成就，也包含了许多近代数论中的重要成果，例如著者关于完全三角和及最小原根的结果，关于 Prouhet-Tarry 问题的结果，Виноградов 关于最小二次非剩余的结果，Selberg 关于素数定理的初等证明，Roth-Siegel 定理，A. O. Гельфонд 关于 Hilbert 第七问题的证明，Siegel 关于二元二次型类数的定理，Линник 关于 Waring 问题的证明，Шнирельман 关于 Гольдбах 问题的结果，Selberg 的筛法等等；书中也包括了著者许多未经发表的结果．

本书是以深入浅出、循序渐进的笔法写成的，读者可以通过它看出如何从一个简单的概念逐步走向深刻的研究，看出具体与抽象之间的联系．

数 论 导 引

华罗庚 著

*

科学出版社出版

北京朝阳门内大街137号

湖南省新华印刷一厂印刷

新华书店北京发行所发行　　各地新华书店经售

*

1957年7月第一版　　开本：787×1092　1/18

1979年11月第五次印刷　　印张：37 4/9　插页：3

印数：18,997—86,096　　字数：628,000

统一书号：13031·245

本社书号：399·13—1

定价：4.60元

序

本书的序文已经写了不止一次，修改了也不止一次，原因是十多年来作者对数学的认识变化了，客观要求也不同了，而本书的内容也大大地随时代而发展了，因此旧的序文也就不适用于今日了！

一切还是那么清晰地在记忆之中，那是 1940 年左右在昆明联大初次讲授数论的时候，就计划着要写这么一本书．那时根据已有的札记和若干新作就写了八九万字的初稿，估计着再写两三万字，就可以出版了．但是何处可以出版？因此也就上不起劲来完成这一工作了．在美国执教的时候，又补充了些，改写了些，但那时补充和改写都是为了教学而并没有考虑整个书的出版问题．

真正积极认真地工作是解放以后的事．因为我国的参考书少，因此这一本把数论做一个全面介绍的书的写作工作就被提到日程上来．解放后工作更忙了，但是说也奇怪，在同志们的帮助下，工作进行得反而更快了！篇幅大大地增加了，并且添了一半以上的新章节，采取了不少近年来的新成就——可以包括在本书范围之内的新成就．

本书的目的除掉较全面地介绍数论上的若干基础知识以外，作者还试图通过本书体现出几点粗浅的看法：

其一，希望能通过本书具体地说明一下数论和数学中其他部分的关系．在数学史上屡见不鲜地出现过数论中的问题、方法和概念曾经影响过数学的其他部分的发展，同时另一方面也屡见数学中其他部分的方法和结果帮助了数论解决其中的具体问题．但是在今天的数论入门书中往往不能看出这一关联性．并且有一些“自给自足”的数论入门书会给读者以不正确的印象：就是数论是数学中一个孤立的分支．作者试图在本书中就初等数论的范围尽可能地说明，数论和数学中的其他方面有联系．

例如：素数定理与 Fourier 积分的关系(因为受本书性质的限制，我们不能把素数定理和整函数的关系在本书中叙出)；整数之分拆问题，四平方和问题与模函数论的关系；二次型论，模变换与 Лобачевский 几何的关系等.

其二，从具体到抽象是数学发展的一条重要大道，因此具体的例子往往是抽象概念的源泉，而所用的方法也往往是高深数学里所用的方法的依据. 仅仅熟读了抽象的定义和方法而不知道他们具体来源的数学工作者是没有发展前途的，这样的人要搞深刻研究是可能会遇到无法克服的难关的. 数学史上也屡见不鲜地刊载着实际中来的问题和方法促进了数学发展的事实. 象力学、物理学都起过这样的作用. 从数学本身来说，它研究的最基本的对象是"数"与"形"，因此，"几何图形"所引出的几何直觉，和由"数"而引出的具体关系和概念，往往是数学中极丰富的源泉，因此在本书中也尽可能地提出了一些抽象概念的具体例子，作为将来读者进一步学习高深数学的感性知识.

例如本书第四、第十四章中提供了抽象代数中好些概念的具体例子，其中有限域的例子实质上说明了一般有限域的情况.

其三，在开始搞研究工作的时候，最难把握的是质的问题，也就是深度问题. 有时作者孜孜不倦地搞了好久自以为十分深刻的工作，但专家却认为仍极肤浅. 其原因有如下棋，初下者自以为想了不少步，但在棋手看来却极其平易，其主要原因在于棋手对局多，因之十分熟练；看谱多，因之棋谱上已有的若干艰难着子在他看来都在掌握之中. 数学的研究工作亦然，必须勤做，必须多和"高手"下(换言之，把数学大家的结果试与改进)，必须多揣摹成局(指已有的解决有名问题的证明). 经此锻炼自然本领日进. 因此本书中也试图在这一方面做些工作. 虽然由于本书的性质并不能将数论上极深刻的结果包括进去，但是作者仍尽可能地把不同深度的方法与以介绍. 例如在估计 $p(n)$ 之值时，先用最简单之代数方法以得出 $p(n)$ 最粗略的估值，再用略深的方法以得出 $\log p(n)$ 之无穷大之阶. 本书并指出再深入用所谓 Tauberian 方法可以得 $p(n)$ 之无穷大之阶，更指出用高深之模函数论之结果及解析数论的方法可以求出 $p(n)$ 之展开式，在这逐步求精之方法中极易表示出各种不同方法的深度.

本书并不是为了大学教学而写的. 它的内容大大地超过了一个数论课的范围. 因之如果教者要使用本书就必须予以妥善的选择. 一般说来，利用第一至

六章作为基础，另选一些——可以每年不同地选一些——本书的其余部分作为补充材料，是可以成为一个数论入门课的教材的.

基本上说来本书并不假定读者有了很多的数学知识. 大学二年级的同学就能看懂本书的绝大部分，有高等微积分知识的同学就可以除 § 9.2, § 12.14, § 12.15, § 17.9 各节外全部看懂，而那些例外的节仅需要极简单的复变函数论的知识. 自修者也没有什么特殊的困难.

在本书完稿的时候，作者由衷地感谢以下的几位同志：越民义，王元，吴方，严士健，魏道政，许孔时和任建华. 我从 1953 年开始讲授起他们就不断地提意见，有时还替我做了局部的改写工作. 在印讲义和排版时的烦冗工作更不必说了！其中尤以越民义同志的帮助最多. 在此稿用讲义形式油印寄发请提意见的时候，承蒙张远达教授提了宝贵的意见，在此一并致谢.

本书虽然经过了集体的努力，但是错误还可能是很多的. 希望读者们多提意见，从排印的错误一直到内容的欠当. 本书中也包括了很多第一次写上教科书的结果，也有一些是没有发表过的研究札记，因此它们的表达方式还有很大的修改的可能性. 关于这一点，我们殷切地期待着读者们宝贵的建议.

因为迁就原稿，本书还是用简单文言写的，如果读者感到不方便，请提意见，以便再版时修正.

华罗庚

1956 年 9 月，北京

出 版 说 明

本书在第四次印刷时除了对第一版中的若干地方作了小的改动外，还简化了第十七章 §3 代数数的有理逼近定理的证明。并由王元同志写了一篇附录，对本书第一版中所论及的著名数论问题的近几年进展情况作了评述。

符 號 說 明

本書習用符號說明如下：

定理 5.3 表同一章中 §5 之定理 3，餘類推．

定理 2·5·3 表第二章 §5 之定理 3，餘類推．

$[\alpha]$ 表不超過 α 之最大整數，$\{\alpha\}$ 表 α 之分數部分；$\langle\alpha\rangle$ 表 α 和它最靠近之整數間之距離，即 $\min(\alpha-[\alpha], [\alpha]+1-\alpha)$．

$(a, b, \cdots, c)$ 爲諸數 $a, b, \cdots, c$ 之最大公約數；$[a, b, \cdots, c]$ 爲其最小公倍數．

$a|b$ 表 a 除得盡 b；$a\nmid b$ 表 a 除不盡 b．

$p^{\alpha}\|a$ 表 $p^{\alpha}|a$ 但 $p^{\alpha+1}\nmid a$．

$a\equiv b \pmod m$ 表 $a-b$ 爲 m 之倍數；$a\not\equiv b \pmod m$ 表 $a-b$ 不爲 m 之倍數．

$\prod_{\nu=1}^{n} a_\nu = a_1 a_2 \cdots a_n$，$\sum_{\nu=1}^{n} a_\nu = a_1 + a_2 + \cdots + a_n$；$\prod_{d|m} a_d$ 及 $\sum_{d|m} a_d$ 均表 d 過 m 之所有不同因子．

$\left(\frac{n}{p}\right)$ 爲 Legendre 符號，定義見第三章 §1；$\left(\frac{n}{m}\right)$ 爲 Jacobi 符號，定義見第三章 §6；設 $d\equiv 0$ 或 $1 \pmod 4$ 且非平方數，$m>0$，$\left(\frac{d}{m}\right)$ 表示 Kronecker 符號，定義見第十二章 §3．

$\operatorname{ind} n$ 表 n 之指數，定義見第三章 §8．

$\partial^{\circ} f$ 表多項式 $f(x)$ 之次數．

符號 $\ll$，O，o，$\sim$ 之定義見第五章 §1．

$\omega(n)$ 表 n 之不同素因子的個數；$\Omega(n)$ 表 n 之全部素因子的個數．

$\max(a, b, \cdots, c)$ 表 $a, b, \cdots, c$ 諸數中之最大者；$\min(a, b, \cdots, c)$ 則表其中之最小者．

$\Re s$ 表示复虚数 s 的实部．$\bar{s}$ 表 s 的共軛虚数．

γ 表示 Euler 常數．

$\{a, b, c\}$ 表二次型 $ax^2 + bxy + cy^2$，見第十二章 §1.

(z_1, z_2, z_3, z_4) 表四點 z_1, z_2, z_3, z_4 的交比，見第十三章 §3.

$A \overset{L}{=} B$ 表示二方陣 A, B 左結合。

$a \in A$ 表示 a 爲集合 A 之元素；$B \subseteq A$ 或 $A \supseteq B$ 表示集合 B 爲集合 A 之子集。

$N(\mathfrak{M})$ 表模 $\mathfrak{M}$ 之矩，見第十四章 §9。

$\{a_n\}$ 表數貫 $a_1, a_2, \cdots$。

$\sim$ 表示相似，見第十二章 §1，第十三章 §6，第十四章 §5，第十六章 §12.

$[a_0, a_1, \cdots, a_N]$ 或 $a_0 + \dfrac{1}{a_1} + \dfrac{1}{a_2} + \cdots + \dfrac{1}{a_N}$ 表有限連分數；$\dfrac{p_n}{q_n} = [a_0, a_1, \cdots, a_n]$ 表其第 n 個漸近分數。

$S(\alpha) = \alpha^{(1)} + \alpha^{(2)} + \cdots + \alpha^{(n)}$ 表代數數 α 之跡，$N(\alpha) = \alpha^{(1)}\alpha^{(2)}\cdots\alpha^{(n)}$ 表 α 之矩.

$\Delta(\alpha_1, \cdots, \alpha_n)$ 表 $\alpha_1, \cdots, \alpha_n$ 之判別式；$\Delta = \Delta(R(\vartheta))$ 表代數數域 $R(\vartheta)$ 之整底之判別式，亦卽基數，定義見第十六章 §3，§4。

$\varphi(m)$ 之定義見第二章 §3.

$\mathrm{li}\, x$ 之定義見第五章 §2.

$\pi(x)$ 之定義見第五章 §3.

$\mu(m)$ 之定義見第六章 §1.

$d(n)$ 之定義見第六章 §1.

$\sigma(n)$ 之定義見第六章 §1.

$\Lambda(n)$ 之定義見第六章 §1.

$\Lambda_1(n)$ 之定義見第六章 §1.

$\chi(n)$ 之定義見第七章 §2.

$p\ n)$ 之定義見第八章 §2.

$\vartheta(x)$ 之定義見第九章 §1.

$\psi(x)$ 之定義見第九章 §1.

$g(k)$ 之定義見第十八章 §1.

$G(k)$ 之定義見第十八章 §1.

$v(k)$ 之定義見第十八章 §5.

$N(k)$ 之定義見第十八章 §6.

$M(k)$ 之定義見第十八章 §6.

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ 爲 Riemann ζ 函數.

$e(f(x)) = e^{2\pi i f(x)}$, $e_q(f(x)) = e^{2\pi i f(x)/q}$.

$S(a, \chi) = \sum_{n=1}^{m} \chi(n) e^{2\pi i a n/m}$ 爲特徵和, $\tau(\chi) = S(1, \chi)$.

$S(n, m) = \sum_{x=0}^{m-1} e^{2\pi i n x^2/m}$, $(n, m) = 1$, 爲 Gauss 和.

$S(q, f(x)) = \sum_{x=0}^{q-1} e_q(f(x))$.

本表所列符號若在其他意義下使用,在使用之前當有說明.

目　　錄