數論導引

華羅庚

科學出版社

數論導引

著者 華羅庚

出版者 科學出版社
北京朝陽門大街 117 号
北京市書刊出版業營業許可證出字第 061 号

印刷者 上海中科藝文聯合印刷廠

總經售 新華書店

1957 年 7 月第一版　　書号：0826
1957 年 7 月第一次印刷　　字數：662,000
(滬)道：0001—1,505　　開本：787×1092 1/18
(滬)報：0001—4,581　　印張：37 插頁：3

定價：(10)道林本 9.00 元
報紙本 6.30 元

內　容　提　要

全書共二十章，前六章是屬於基礎性質，內容包括：整數分解，同餘式，二次剩餘，多項式之性質，素數分佈概況，數論函數等；後十四章是就解析數論，代數數論，超越數論，數的幾何這幾個數論主要分支的基礎部分加以介紹，內容包括：三角和，數的分拆，素數定理，連分數，不定方程，二元二次型，模變換，整數矩陣，p-adic 數，代數數論導引，超越數，Waring 問題與 Prouhet-Tarry 問題，數的幾何等。書裏引述了許多我國古代數學家在數論上的成就，也包含了許多近代數論中的重要成果，例如著者關於完全三角和及最小原根的結果，關於 Prouhet-Tarry 問題的結果，Виноградов 關於最小二次非剩餘的結果，Selberg 關於素數定理的初等證明，Roth-Siegel 定理，A. O. Гельфонд 關於 Hilbert 第七問題的證明，Siegel 關於二元二次型類數的定理，Линник 關於 Waring 問題的證明，Шнирельман 關於 Гольдбах 問題的結果，Selberg 的篩法等等；書中也包括了著者許多未經發表的結果。

本書是以深入淺出、循序漸進的筆法寫成的，讀者可以通過它看出如何從一個簡單的概念逐步走向深刻的研究，看出具體與抽象之間的聯系。本書內容廣泛，是數論研究工作者的一本優良參考書。

序

本書的序文已經寫了不止一次，修改了也不止一次，原因是十多年來作者對數學的認識變化了，客觀要求也不同了，而本書的內容也大大地隨時代而發展了，因此舊的序文也就不適用於今日了！

一切還是那麼清晰地在記憶之中，那是1940年左右在昆明聯大初次講授數論的時候，就計劃着要寫這麼一本書．那時根據已有的札記和若干新作就寫了八九萬字的初稿，估計着再寫兩三萬字，就可以出版了．但是何處可以出版？因此也就上不起勁來完成這一工作了．在美國執教的時候，又補充了些，改寫了些，但那時補充和改寫都是爲了教學而並沒有考慮整個書的出版問題．

眞正積極認眞地工作是解放以後的事．因爲我國的參考書少，因此這一本把數論做一個全面介紹的書的寫作工作就被提到日程上來．解放後工作更忙了，但是說也奇怪，在同志們的幫助下，工作進行得反而更快了！篇幅大大地增加了，並且添了一半以上的新章節，採取了不少近年來的新成就——可以包括在本書範圍之內的新成就．

本書的目的除掉較全面地介紹數論上的若干基礎知識以外，作者還試圖通過本書體現出幾點粗淺的看法：

其一，希望能通過本書具體地說明一下數論和數學中其他部分的關係．在數學史上屢見不鮮地出現過數論中的問題、方法和概念曾經影響過數學的其他部分的發展，同時另一方面也屢見數學中其他部分的方法和結果幫助了數論解決其中的具體問題．但是在今天的數論入門書中往往不能看出這一關聯性．並且有一些"自給自足"的數論入門書會給讀者以不正確的印象：就是數論是數學中一個孤立的分支，一點也不能體會出"數學是科學中的皇后，數論是數學中的皇后"[1]的意義．作者試圖在本書中就初等數論的範圍儘可能地說明這一點．

1）這是十八世紀大數學家高斯（Gauss）之言，我們現在並不過分強調這句話的正確性．但這句話却說明了：在歷史上曾經有過大數學家認爲數學在科學中有獨特的地位，及數論在數學中有獨特的地位．

例如：素數定理與 Fourier 積分的關係（因爲受本書性質的限制，我們不能把素數定理和整函數的關係在本書中敍出）；整數之分拆問題，四平方和問題與模函數論的關係；二次型論，模變換與 Лобачевский 幾何的關係等。

其二，從具體到抽象是數學發展的一條重要大道，因此具體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數學裏所用的方法的依據。僅僅熟讀了抽象的定義和方法而不知道他們具體來源的數學工作者是沒有發展前途的，這樣的人要搞深刻研究是可能會遇到無法克服的難關的。數學史上也屢見不鮮地刊載着實際中來的問題和方法促進了數學發展的事實。像力學、物理學都起過這樣的作用。從數學本身來說，它研究的最基本的對象是"數"與"形"，因此，"幾何圖形"所引出的幾何直覺，和由"數"而引出的具體關係和概念，往往是數學中極豐富的源泉，因此在本書中也儘可能地提出了一些抽象概念的具體例子，作爲將來讀者進一步學習高深數學的感性知識。

例如本書第四、第十四章中提供了抽象代數中好些概念的具體例子，其中有限域的例子實質上說明了一般有限域的情況。

其三，在開始搞研究工作的時候，最難把握的是質的問題，也就是深度問題。有時作者孜孜不倦地搞了好久自以爲十分深刻的工作，但專家却認爲仍極膚淺。其原因有如下棋，初下者自以爲想了不少步，但在棋手看來却極其平易，其主要原因在於棋手對局多，因之十分熟練；看譜多，因之棋譜上已有的若干艱難着子在他看來都在掌握之中。數學的研究工作亦然，必須勤做，必須多和"高手"下（換言之，把數學大家的結果試與改進），必須多揣摹成局（指已有的解決有名問題的證明）。經此鍛煉自然本領日進。因此本書中也試圖在這一方面做些工作。雖然由於本書的性質並不能將數論上極深刻的結果包括進去，但是作者仍儘可能地把不同深度的方法與以介紹。例如在估計 $p(n)$ 之值時，先用最簡單之代數方法以得出 $p(n)$ 最粗略的估值，再用略深的方法以得出 $\log p(n)$ 之無窮大之階。本書並指出再深入用所謂 Tauberian 方法可以得 $p(n)$ 之無窮大之階，更指出用高深之模函數論之結果及解析數論的方法可以求出 $p(n)$ 之展開式，在這逐步求精之方法中極易表示出各種不同方法的深度。

本書並不是爲了大學教學而寫的。它的內容大大地超過了一個數論課的範圍。因之如果教者要使用本書就必須予以妥善的選擇。一般說來，利用第一至

六章作爲基礎，另選一些——可以每年不同地選一些——本書的其餘部分作爲補充材料，是可以成爲一個數論入門課的教材的.

基本上說來本書並不假定讀者有了很多的數學知識. 大學二年級的同學就能看懂本書的絕大部分。 有高等微積分知識的同學就可以除 §9.2, §12.14, §12.15, §17.9 各節外全部看懂，而那些例外的節僅需要極簡單的複變函數論的知識. 自修者也沒有什麽特殊的困難.

在本書完稿的時候，作者由衷地感謝以下的幾位同志：越民義，王元，吳方，嚴士健，魏道政，許孔時和任建華。 我從 1953 年開始講授起他們就不斷地提意見，有時還替我做了局部的改寫工作. 在印講義和排版時的煩冗工作更不必說了！ 其中尤以越民義同志的幫助最多. 在此稿用講義形式油印寄發請提意見的時候，承蒙張遠達教授提了寶貴的意見，在此一併致謝.

本書雖然經過了集體的努力，但是錯誤還可能是很多的. 希望讀者們多提意見，從排印的錯誤一直到內容的欠當. 本書中也包括了很多第一次寫上教科書的結果，也有一些是沒有發表過的研究札記，因此它們的表達方式還有很大的修改的可能性. 關於這一點，我們殷切地期待着讀者們寶貴的建議.

因爲遷就原稿，本書還是用簡單文言寫的，如果讀者感到不方便，請提意見，以便再版時修正.

華羅庚

1956 年 9 月，北京

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．

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

$a\equiv b \pmod m$ 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 s 的實部．

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.

$A \fallingdotseq B$ 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

第 一 章

整數之分解

在本章中，如無特別聲明，常以小寫拉丁字母

$$a, b, \cdots, n, \cdots, p, \cdots, x, y, z$$

代表整數. 本章之目的在證明唯一分解定理（定理 5.3），並旁及其應用.

§1. 整除性. 自然數是指 $1, 2, 3, \cdots$ 之一而言；整數乃指

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

之一而言. 故自然數卽正整數. 顯然二整數之和、差、積仍爲整數. 此項性質可述爲："諸整數所成之集，對加、減、乘三種運算自封".

命 α 爲一實數. 今後常以 $[\alpha]$ 表最大之整數不超過 α 者. 例如

$$[3]=3, \quad [\sqrt{2}]=1, \quad [\pi]=3, \quad [-\pi]=-4.$$

若 α 爲正，易見 $[\alpha]$ 卽爲 α 之整數部分；顯然有下之不等式：

$$[\alpha] \leqslant \alpha < [\alpha]+1.$$

今取 α 爲有理數 $\frac{a}{b}$，$b>0$，則有

$$0 \leqslant \frac{a}{b} - \left[\frac{a}{b}\right] < 1,$$

卽

$$0 \leqslant a - b\left[\frac{a}{b}\right] < b.$$

立得

$$a = \left[\frac{a}{b}\right] b + r, \qquad 0 \leqslant r < b.$$

由此可得：

定理 1. 任與二整數 a 及 b $(b>0)$，必有二整數 q 及 r 使

$$a = qb + r, \qquad 0 \leqslant r < b.$$