初等数论

I

陈景润 著

科学出版社

初等数论

I

陈景润 著

科学出版社

1978

内 容 简 介

数论是研究数的性质的一门学科．本书从劳动人民的生产斗争和科学实验的实际经验出发，分析了数论的发生、发展和应用，介绍了数论的初等方法．每章后有习题，并在书末附全部习题解答．本书写得深入浅出，通俗易懂，可供广大青年及科技人员阅读．

初 等 数 论

陈景润 著

科学出版社出版
北京朝阳门内大街137号
国营五二三厂印刷
新华书店北京发行所发行　各地新华书店经售

1978年12月第 一 版　开本：787×1092 1/32
1978年12月第一次印刷　印张：4 3/4
印数：0001—1,256,600　字数：105,000

统一书号：13031·915
本社书号：1299·13—1

定价：0.40 元

序　　言

最近一年来，我收到广大工农兵群众、科技工作人员、中小学校教师和同学的许多来信，希望能够有一些供给具有初中毕业、高中程度的读者阅读的数学方面的参考书，为了满足他们的要求，所以写了这本初等数论．首先我们介绍一下什么叫数论．数论是研究数的性质的一门学科，而初等数论是与算术有极密切联系的，也可以说是算术的继续．算术中很难的问题，用初等数论的方法很容易得到解答．伟大的革命导师马克思曾经研究过数论方面的问题（见本书第三章）．有些人说数论和工农业生产没有直接的关系，我们认为不是这种情况．阅读完本书就可以知道数论和工农业生产有很密切的联系，生产中出现的不少数学问题实际上也可以应用数论方法去解决．有些人说数论很深奥，不是一般大学毕业生能看懂的．阅读完本书以后就可知道数论中的一部分（如初等数论）并不是高不可攀、无法学懂的．即使是解析数论，只要刻苦钻研坚持不懈，也是可以掌握的．

数论是我国劳动人民所擅长的学科．我国古代在数论方面曾有过极其光辉的成就，例如商高定理（勾股数）、孙子定理与圆周率的计算都比西方早．数论也是我国近代数学发展得最早的数学分支之一，有优良的传统，从三十年代开始，在解析数论、丢番图方程、一致分布等方面都有过重要贡献．特别是著名的华罗庚教授在三角和估计与堆垒素数论方面的卓越贡献和优秀成果是国内外公认的．解放后，在毛主席革命路线指引下，我国的数论研究在原有的基础上又有所发展，作出

了一系列重要成果，特别是筛法与哥德巴赫问题的研究，坚持了二十多年，最后获得了优秀的成就.

多年来祸国殃民的“四人帮”出于篡党夺权复辟资本主义的反动政治目的，严重地破坏了我国的科技教育事业. 鼓吹什么“宁要没有文化的劳动者”，对广大劳动人民实行愚民政策，使我国教育质量下降，中学课外参考书的出版大量减少，以至于许多中学生和工农兵群众想用业余时间学习数学，也没有参考书. 以英明领袖华主席为首的党中央，一举粉碎了“四人帮”，挽救了革命，挽救了党，也挽救了我国的科技教育事业. 现在许多中学生和工农兵群众不知疲劳，不分白天和晚上，努力学习马列著作和毛主席著作，刻苦钻研业务，勇于攀登科学技术高峰. 东风浩荡，捷报频传，科技教育战线山花烂漫，形势大好. 因此，我写了这本初等数论，献给广大的数学爱好者，希望能起到抛砖引玉的作用.

本书是把我的老师华罗庚教授的名著《数论导引》中的某些章节写得较详细一些，以便于具有初中毕业、高中程度的同志们阅读. 很多人都知道，数论的习题是很难做的，所以在本书中附有习题的较详细的解答. 本书初稿经过中国科学院数学研究所王元、丁夏畦、于坤瑞和丁平四位同志详细阅读并提出不少宝贵意见. 在写这本书的过程中，得到北京电机厂七·二一大学的领导和教研组的同志们的支持，特别应该提到该大学戚鸣皋同志非常详细地阅读过本书的初稿，并提出了很多宝贵意见，本书的习题解答就是由戚鸣皋同志做的. 另外中国科学技术大学陆洪文老师也很详细地阅读过本书的初稿并提出宝贵意见. 谨在此一并表示感谢.

根据多年来的经验，数论中的不少世界著名难题，例如哥德巴赫猜想，费尔马大定理等，具有初中毕业程度的同志们，经过自学都能明白其意思，但是对于它们的困难程度却了解

得很少，甚至没有了解，以至于许多同志，特别是许多青年同志，盲目地将许多精力浪费在用一些初等数论的办法去证明这些世界著名难题，而不知道要想解决这些世界著名难题，首先需要学习许多非常高深的数论论文，还要经过多年刻苦钻研，然后才有可能从事这方面的研究工作．我认为在最近几十年，关于哥德巴赫猜想、费尔马大定理等世界著名难题是不可能只用初等数论方法而得到证明的．所以希望青年同志们不要走入歧途，不要浪费时间和精力．

由于时间短促，书中可能存在不少问题，希同志们批评指正．

陈景润

1978年1月10日

目　　录

第一章　整数的整除性

§1. 因数和倍数

我们把 1, 2, 3, 4, ···, n, ···这些数叫做正整数，又叫做自然数，其中 1, 3, 5, 7, ···叫做奇数；2, 4, 6, 8, ···叫做偶数.在正整数范围内，很明显，

正整数 + 正整数 = 正整数；

正整数 × 正整数 = 正整数.

但是由正整数减去正整数，得到的可能是正整数，也可能不是正整数。

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

这些数叫做负整数. 而正整数和负整数再加上零，就统一叫做整数。

在整数范围内，我们有

整数 + 整数 = 整数；

整数 − 整数 = 整数；

整数 × 整数 = 整数.

但是整数除整数不一定得整数，究竟什么样的整数除什么样的整数才能得整数呢？ 研究这个问题，就是研究整数的整除性。

以后，如果没有特别声明，我们将用

$$a, b, c, d, \cdots$$

等英文字母表示整数. 当几个字母写在一起时，表示将这几个字母相乘起来. 例如

$$ab = a \times b, \quad abc = a \times b \times c,$$

$$abcd = a \times b \times c \times d$$

等. 但注意数目字写在一起时不表示相乘，例如 55 不是 5×5 而是五十五，234 不是 $2 \times 3 \times 4$ 而是二百三十四. 而当数目字和字母写在一起时，则表示这个数目字和字母相乘. 例如 $2a = 2 \times a$，$15a = 15 \times a$，$99abc = 99 \times a \times b \times c$，$1234abcd = 1234 \times a \times b \times c \times d$.

我们还使用记号 $(-a)$ 来表示 $-a$，即 $(-a) = -a$，又有 $(-a)(-b) = (-a) \times (-b)$，$(-a)b = (-a) \times b$，$a(-b) = a \times (-b)$.

定义 1 设 a，b 是整数，$b \neq 0$. 如果有一个整数 c，它使得 $a = bc$，则 a 叫做 b 的倍数，b 叫做 a 的因数. 我们有时说，b 能整除 a 或 a 能被 b 整除；也有时说，b 能除尽 a，或 a 能被 b 除尽.

如果 b 能整除 a，我们就用 $b|a$ 这个符号来表示它，例如 $2|4$，$3|6$. 由于 $-30 = 6 \times (-5)$，$20 = (-5) \times (-4)$，所以 $6|(-30)$，$(-5)|20$.

如果 b 不能整除 a，我们就写作 $b\nmid a$，例如 $2\nmid 3$，$3\nmid 8$，$(-3)\nmid 5$，$(-5)\nmid 12$.

如果 a 是一个整数，$a \neq 0$，而 m 是一个正整数，则由于 $0 = a \times 0$，$ma = a \times m$，$-ma = a \times (-m)$，所以 0，ma 和 $-ma$ 都是 a 的倍数. 即

$$0,\ a,\ 2a,\ 3a,\ 4a,\ \cdots$$

都是 a 的倍数，而

$$-a,\ -2a,\ -3a,\ -4a,\ \cdots$$

也都是 a 的倍数. 我们使用记号 $|a|$ 来表示

$$|a| = \begin{cases} a, & \text{当 } a \geqslant 0; \\ -a, & \text{当 } a < 0. \end{cases}$$

我们把 $|a|$ 叫做 a 的绝对值，例如 $|2| = |-2| = 2$，$|5| =$

$|-5| = 5$.

引理 1 如果 a, b 是二个整数而 $a|b$, 则

$$(-a)|b, \quad a|(-b), \quad (-a)|(-b), \quad |a|\,||b|.$$

证 因为 $a|b$, 所以由定义 1 有一个整数 c, 它使得 $b = ac$, 故得

$$b = (-a)(-c), \quad -b = a(-c) = (-a)c,$$

$$|b| = |ac| = |a|\,|c|.$$

由于 $a, b, c, -a, -b, -c, |a|, |b|$ 和 $|c|$ 都是整数, 所以有

$$(-a)|b, \quad a|(-b), \quad (-a)|(-b), \quad |a|\,||b|.$$

引理 2 如果 a, b, c 都是整数而 $a|b, b|c$, 则有 $a|c$.

证 因为 $a|b$, 所以由定义 1 有一个整数 d, 它使得 $b = ad$. 又由于 $b|c$, 所以有一个整数 e 它使得 $c = be$. 由 $c = be$ 和 $b = ad$ 有 $c = ade$. 由于 d 和 e 都是整数, 所以 de 也是整数. 由定义 1 和 $c = ade$ 有 $a|c$.

引理 3 如果 a, b 都是整数而 $|a| < |b|$, $|b|\,||a|$, 则有

$$a = 0.$$

证 因为 $|b|\,||a|$, 所以由定义 1 有一个整数 c, 它使得 $|a| = |b|c$. 如果 $|a| = 0$, 则有 $a = 0$. 如果 $|a| > 0$, 则由 $0 < |a| < |b|$ 和 $|a| = |b|c$ 有 $c \geqslant 0$. 如果 $c > 0$, 则由于 c 是整数而有 $c \geqslant 1$. 由 $|a| = |b|c$ 和 $c \geqslant 1$ 有 $|a| \geqslant |b|$, 这和 $|a| < |b|$ 发生矛盾, 所以有 $c = 0$. 由 $c = 0$ 和 $|a| = |b|c$ 有 $a = 0$.

引理 4 如果 a, b 是二个整数, $b \neq 0$, 则一定有并且只有二个整数 q, r, 可使

$$a = bq + r, \quad 0 \leqslant r < |b|$$

成立.

证 如果 $b>0$，则 b 的倍数当从负数到正数，由小到大列出时是

$$\cdots, -4b, -3b, -2b, -b, 0, b, 2b, 3b, 4b, \cdots$$

如果 $b<0$，则 b 的倍数当从负数到正数，由小到大列出时是

$$\cdots, 4b, 3b, 2b, b, 0, -b, -2b, -3b, -4b\cdots$$

现在有两种可能：

(1) 存在有一个整数 q，使得 $a=bq$，故 $r=0$. 本引理成立.

(2) 当 $b>0$ 时，存在有一个整数 q，使得 $qb\leqslant a<(q+1)b$. 而当 $b<0$ 时，存在有一个整数 q，使得 $qb\leqslant a<(q-1)b$. 故有 $a=bq+r$，而 $0\leqslant r<|b|$.

现在要来证明只有唯一的这样一对 q，r，使得 $a=bq+r$，$0\leqslant r<|b|$ 成立.假设还有另外一对 q_1，r_1，可使

$$a=bq_1+r_1,\quad 0\leqslant r_1<|b|$$

成立，那么将上面的二个关系式相减，得

$$0=b(q-q_1)+(r-r_1),$$

也就是 $-b(q-q_1)=r-r_1$. 所以由定义 1 有 $b|(r-r_1)$. 再根据引理 1 得 $|b|\,|r-r_1|$. 因为 $0\leqslant r<|b|$，$0\leqslant r_1<|b|$，所以有

$$|r-r_1|=\begin{cases} r-r_1\leqslant r<|b|, & \text{当 } r\geqslant r_1 \text{ 时},\\ r_1-r\leqslant r_1<|b|, & \text{当 } r<r_1 \text{ 时}. \end{cases}$$

由 $|r-r_1|<|b|$，$|b|\,|r-r_1|$ 和引理 3 得到 $r-r_1=0$，也就是 $r=r_1$. 由 $b\neq 0$ 和 $b(q-q_1)=r_1-r=0$ 得到 $q-q_1=0$，也就是 $q=q_1$.

§2. 素数和复合数

1 这个数只有一个正因数，就是它本身. 任何大于 1 的正整数 a 都最少有二个正因数，就是 1 和 a.

2 只能被 1 和 2 整除，不能被其他正整数整除，同样 3 只能被 1 和 3 整除，不能被其他正整数整除. 我们说 2 是素数，3 也是素数.

4 除了能被 1 和 4 整除，还能被 2 整除. 6 除了能被 1 和 6 整除，还能被 2 和 3 整除. 我们说 4 是复合数，6 也是复合数.

定义 2 一个大于 1 的正整数，只能被 1 和它本身整除，不能被其他正整数整除，这样的正整数叫做素数(有的书上叫做质数).

例如 2, 3, 5, 7, 11, 13, 17, 19 都是素数.

以后我们将常用 p 或 p_1, p_2, p_3, $\cdots$ 表示素数.

定义 3 一个正整数除了能被 1 和本身整除以外，还能被另外的正整数整除，这样的正整数叫做复合数.

例如 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 都是复合数.

由素数与复合数的定义可知，全体正整数可分为三类：

(1) 1 这个数，

(2) 全体素数，

(3) 全体复合数.

当然有无限多的复合数，比如大于 2 的偶数

$$4, 6, 8, 10, 12, \cdots$$

都是复合数.

定义 4 如果一个正整数 a 有一个因数 b，而 b 又是素数，则 b 就叫做 a 的素因数.

例如 $12 = 3 \times 4$，所以 3 和 4 都是 12 的因数，由于 3 是素数而 4 不是素数，所以 3 是 12 的素因数而 4 不是 12 的素因数.

引理 5 如果 a 是一个大于 1 的整数，则 a 的大于 1 的最小因数一定是素数.

证 如果 a 是一个素数，则 a 的大于 1 的因数只有一个，

就是 a，所以 a 的大于 1 的最小因数就是素数 a.

如果 a 是复合数，则 a 除 1 和 a 外一定有其他的正因数. 假设 b 是这些正因数中的最小的，我们将证明 b 不是复合数而是素数. 先假定 b 不是素数而是复合数，则由于 b 是复合数，所以 b 一定有大于 1 而不等于 b 的因数 c. 由 $c|b$，$b|a$ 和引理 2 有 $c|a$，即 c 是 a 的因数，又有 $1<c<b$，这与假设 b 是 a 的大于 1 的最小因数矛盾. 所以 b 不是复合数而是素数. 因此 a 的大于 1 的最小的因数 b 是素数.

这个引理说明了：任何大于 1 的整数都至少有一个素因数.

观察一个正整数 a 是不是素数，是否得用小于 a 大于 1 的整数一一来试除呢？不用.

引理 6 如果 a 是一个大于 1 的整数，而所有 $\leqslant\sqrt{a}$ 的素数都除不尽 a，则 a 是素数.

证 首先证明，如果 a 被 >1 而 $\leqslant\sqrt{a}$ 的整数都除不尽，则 a 是素数. 假设 a 是复合数而 $a=bc$，其中 b 和 c 都是大于 1 的整数. 由于 a 被 >1 而 $\leqslant\sqrt{a}$ 的整数都除不尽，所以由 $b>\sqrt{a}$，$c>\sqrt{a}$，而得 $bc>\sqrt{a}\cdot\sqrt{a}=a$，这与 $bc=a$ 是矛盾的，所以如果 a 被 >1 而 $\leqslant\sqrt{a}$ 的整数都除不尽，则 a 就是素数.

由上可知如果 a 是复合数，则 a 一定有 >1 而 $\leqslant\sqrt{a}$ 的因数. 而由引理 5 知 a 的大于 1 的最小因数一定是素数，故本引理得证.

假设 $n\geqslant 2$ 是一个整数，定义

$$a_1a_2\cdots a_n=\begin{cases}a_1a_2, & \text{当 } n=2 \text{ 时;}\\ a_1a_2a_3, & \text{当 } n=3 \text{ 时;}\\ a_1a_2a_3a_4, & \text{当 } n=4 \text{ 时;}\\ a_1a_2a_3a_4\cdots a_n, & \text{当 } n\geqslant 5 \text{ 时.}\end{cases}$$

引理 7 有无限多个素数.

证 假设素数的个数是有限多个，共有 n 个，就是 $p_1, p_2, p_3, \cdots, p_n$. 其中 $p_1 = 2, p_2 = 3, p_3 = 5, \cdots$. 令 $a = p_1 \cdots p_n + 1$, 如果 a 是素数，则因 a 不等于 $p_1, p_2, \cdots, p_n$ 中的任何一个，故素数的个数最少有 $n + 1$ 个而与假设素数的个数共有 n 个矛盾. 如果 a 不是素数，则由引理 5 知道 a 的大于 1 的最小因数 b 是素数. 由于 $p_1 \cdots p_n$ 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除尽，但 1 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除不尽，所以 a 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除不尽. 因此 b 不等于 $p_1, \cdots, p_n$ 中的任何一个素数，故在 $p_1, \cdots, p_n$ 以外还有素数.

§3. 素数分布的简单概况

素数的分布情况是数论中最有趣味的一个分支，其中的推测和定理，很多都是先由经验得到的. 现有的最完善的素数表是查基尔(Don Zagier)作的，他把不大于 50,000,000 的素数都列出了.(见 The Mathematical Intelligencer, 1977 年 8 月号.)

根据这个素数表可以查出素数的分布有下列情况:

在 1 到 100 中间有 25 个素数，

在 1 到 1000 中间有 168 个素数，

在 1000 到 2000 中间有 135 个素数，

在 2000 到 3000 中间有 127 个素数，

在 3000 到 4000 中间有 120 个素数，

在 4000 到 5000 中间有 119 个素数，

在 5000 到 10000 中间有 560 个素数.

所以这些数字提示我们素数的分布，越往上越稀. 我们将 5000 以内的素数表附在本章之末. 到目前为止所知道的最大素数是 $2^{19937} - 1$. 在证明 $2^{19937} - 1$ 是一个素数时需借助于

电子计算机并用特殊方法．我们有

$$2^{19937}-1>10^{6001}.$$

关于素数的分布有许多问题，有的已经解决了，有的直到现在还没有解决．

首先的问题是关于素数的个数问题．

在数论里经常用 $\pi(x)$ 表示不大于 x 的素数的个数．所以 $\pi(3)=2$，$\pi(100)=25$，$\pi(1000)=168$．

现在就几个不很大的 x 把相应的 $\pi(x)$、$\dfrac{x}{\log x}$ 和它们的比值列表如下

x	$\pi(x)$	$\dfrac{x}{\log x}$	$\dfrac{\pi(x)}{\frac{x}{\log x}}$	$\dfrac{\pi(x)}{x}$
1000	168	144.764…	1.1605…	0.1680
2000	303	263.126…	1.1515…	0.1515
5000	669	587.047…	1.1396…	0.1338
10000	1229	1085.73…	1.1319…	0.1229
50000	5133	4621.166…	1.1107…	0.10266
100000	9592	8685.889…	1.1043…	0.09592

这个表提示我们三点

1）有无限多个素数，

2）当 x 越大时，$\pi(x)$ 与 $\dfrac{x}{\log x}$ 的比值越接近 1，

3）当 x 越大时，$\pi(x)$ 与 x 的比值越接近 0．

阿达马（Hadamard）和德·拉·瓦莱·普森（De la Vall'ee Poussin）各自独立地在 1896 年证明了素数定理，即

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\log x}}=1.$$

由于在素数定理的证明中采用了较多的数学理论，因此

在这个地方把它详细地介绍出来，还是不适时的.

人们发现了许多相邻二个素数的差是 2，例如下列成对的素数

3，5； 5，7； 11，13； 17，19； 29，31；

41，43； 59，61； 71，73； 101，103； …

可以叫作双生素数. 人们要问是否有无限多对双生素数呢？这个问题的解答非常困难. 华罗庚、王元、潘承洞、丁夏畦、尹文霖和陈景润都曾经在这方面进行过不少工作. 这个问题现在最好的结果是：存在有无限多个素数 p，使得 $p+2$ 为不超过二个素数之积. 现在我们所知道的最大素数对是

$$76 \times 3^{169} - 1, \quad 76 \times 3^{169} + 1.$$

这个结果是威廉斯（Willams）和察恩克（Zarnke）得到的.（见 Tom M. Apostol Intro. to Analytic Number Theory, 1976.）

某些数字资料建议：相邻二个素数的差是 2 的素数对可能有无限多对.

我们有

$6 = 3 + 3$， $8 = 3 + 5$， $10 = 5 + 5$，

$12 = 5 + 7$， $14 = 7 + 7$， $16 = 3 + 13$，

$18 = 5 + 13$， $20 = 7 + 13$， $22 = 3 + 19$，

$24 = 5 + 19$， $26 = 3 + 23$， $28 = 5 + 23$，…

由此提示可能有：凡大于 4 的偶数都是二个奇素数之和，这就是著名的哥德巴赫（Goldbach）猜想.

这个哥德巴赫猜想直到现在还没有肯定的或否定的答案，我们认为哥德巴赫猜想是肯定的可能性很大. 这个问题现在最好的结果是：每一充分大的偶数都是一个素数及一个不超过二个素数的乘积之和. 华罗庚、王元、潘承洞、丁夏畦、尹文霖和陈景润都曾经在这方面进行过不少工作.

默森尼（Mersenne）曾经研究过形状为 $2^p - 1$ 的素数，