

Introduction to Analytic Number Theory



数论经典著作系列

解析数论引论

[美] T·M·阿普斯托 著 赵宏量 唐大明 译



哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS



Introduction to Analytic Number Theory

解析数论引论

● [美] D. M. 阿普斯托 著 ● 赵宏量 唐大明 译



哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容提要

本书共分十四章,将解析数论从古到今几乎所有的重要发现都作了较为简要的论述和介绍.

本书适合大学师生及数论爱好者.

图书在版编目(CIP)数据

解析数论引论/(美)阿普斯托著;赵宏量,唐太明译. —哈尔滨:哈尔滨工业大学出版社,2011.3
ISBN 978-7-5603-3177-5

I. ①解… II. ①阿… ②赵… ③唐… III. ①解析数论—研究 IV. ①O156.4

中国版本图书馆 CIP 数据核字(2011)第 018437 号

Translation from the English language edition

Introduction to Analytic Number Theory by Tom M. Apostol

© 1976 Springer Science + Business Media, Inc.

All Rights Reserved

版权登记号 黑版贸审字 08-2010-026

策划编辑 刘培杰 甄森森 张永芹

责任编辑 王勇钢

封面设计 孙茵艾

出版发行 哈尔滨工业大学出版社

社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006

传 真 0451-86414749

网 址 <http://hitpress.hit.edu.cn>

印 刷 哈尔滨市石桥印务有限公司

开 本 787mm×1092mm 1/16 印张 21 字数 387 千字

版 次 2011 年 3 月第 1 版 2011 年 3 月第 1 次印刷

书 号 ISBN 978-7-5603-3177-5

定 价 48.00 元

(如因印装质量问题影响阅读,我社负责调换)

前 言

本书内容是依据 TOM M. Apostol 所著的《解析数论导引》一书,在 20 余年前就由唐大明初步译出,后经西南师范大学数学系教授赵宏量又对照原文作了进一步的修改、补充、审校和加工;最后又由赵宏量进行了统稿和定稿工作,终于将此书于 1992 年 2 月由西南师范大学出版社出版.出版后受到专业数学工作者多人的好评,认为是国内这方面少有的几本高质量的《解析数论》.当然这本书没有华罗庚教授的《数论导引》的内容丰富,华教授的这本书,内容涉及的范围比 Hardy 与 E. M. Wright 的著作大得多,也深入得多.其中包括了华老自己的不少重要结果,也收入了不少深刻的数论结果,是极为珍贵的.华老的书于 1957 年由科学出版社出版到 1975 年已印刷四次,1982 年还由 Springer 出版社出版了这本书的英文版.

但是我们编译的这本书也有它的特点和不同的写作风格,它把数论从古到今几乎所有的重要发现都作了较为简要的论述和介绍,而且对一些在华罗庚《数论导引》中未加证明的问题,也作了适当的论述和部分证明.

本书是迄今为止国内正式出版的各种数论书方面较为全面和系统的一本高质量的《解析数论》的基础教材,而且内容又比较新颖;最适宜于作为大学本科高年级学生和研究生入门教材,也是自学数论的人可选用的一本优秀读物.特别适宜

于那些对《解析数论》有兴趣和爱好的业余学者,作为研习《解析数论》的极为难得的良好参考资料.书中还列出了吸收消化和吸引历代专业和业余数学爱好者的许多问题及其解决方法的特殊技巧等;本书可能会使许多数学系学生和青年教师产生特殊的兴趣,也可能对社会上那些乐于研究数论问题的人们提供较好的帮助.

本书在时隔 20 年后又重新编辑出版,对原来的内容作了进一步的审校和加工,同时,也更正了原来出版中存在的许多差错,现定名为《解析数论引论》.相信这一次的重新修订出版,一定会受到国内广大数学爱好者、数学专家、业余爱好者的支持和欢迎,特别是今天出版这样较高层次的数学著名作品,对于提高我国的文化科学素养,发展我国的科学技术事业都是具有重要的现实意义的.

书后增加的“哥德巴赫猜想”研究综览对于提高学习兴趣是有帮助的.

赵宏量

2010 年 10 月于西南大学

| | | |
|------------------------------|----|----|
| 历史介绍 | // | 1 |
| 第一章 算术基本定理 | // | 11 |
| 1.1 引言 | // | 11 |
| 1.2 整除性 | // | 12 |
| 1.3 最大公约数 | // | 12 |
| 1.4 素数 | // | 14 |
| 1.5 算术基本定理 | // | 15 |
| 1.6 素数倒数的级数 | // | 16 |
| 1.7 欧几里得算法 | // | 17 |
| 1.8 两个以上的数的最大公约数 | // | 18 |
| 第一章习题 | // | 18 |
| 第二章 数论函数与迪利克雷乘积 | // | 21 |
| 2.1 引言 | // | 21 |
| 2.2 麦比乌斯函数 $\mu(n)$ | // | 21 |
| 2.3 欧拉函数 $\varphi(n)$ | // | 22 |
| 2.4 φ 与 μ 的相互关系 | // | 23 |
| 2.5 $\varphi(n)$ 的一个乘积公式 | // | 24 |
| 2.6 数论函数的迪利克雷乘积 | // | 25 |
| 2.7 迪利克雷逆函数与麦比乌斯反转公式 | // | 27 |
| 2.8 Mangoldt 函数 $\Lambda(n)$ | // | 28 |

- 2.9 积性函数 // 29
- 2.10 积性函数与迪利克雷乘积 // 30
- 2.11 完全积性函数的逆函数 // 32
- 2.12 柳维尔函数 $\lambda(n)$ // 33
- 2.13 除数函数 $\sigma_a(n)$ // 33
- 2.14 广义卷积 // 35
- 2.15 形式幂级数 // 36
- 2.16 数论函数的 Bell 级数 // 37
- 2.17 Bell 级数与迪利克雷乘积 // 38
- 2.18 数论函数的导数 // 39
- 2.19 塞尔伯格等式 // 40
- 第二章习题 // 40

第三章 数论函数的平均值 // 46

- 3.1 引言 // 46
- 3.2 大 O 符号, 函数的渐近等式 // 47
- 3.3 欧拉求和公式 // 48
- 3.4 几个基本渐近公式 // 49
- 3.5 $d(n)$ 的平均阶 // 50
- 3.6 除数函数 $\sigma_a(n)$ 的平均阶 // 53
- 3.7 $\varphi(n)$ 的平均阶 // 54
- 3.8 对于由原点可见的格点分布的应用 // 55
- 3.9 $\mu(n)$ 与 $\Lambda(n)$ 的平均阶 // 57
- 3.10 迪利克雷乘积的部分和 // 57
- 3.11 对 $\mu(n)$ 与 $\Lambda(n)$ 的应用 // 58
- 3.12 迪利克雷乘积的部分和的另一个等式 // 61
- 第三章习题 // 62

第四章 素数分布的几个基本定理 // 66

- 4.1 引言 // 66
- 4.2 切比雪夫函数 $\psi(x)$ 与 $g(x)$ // 67
- 4.3 联系 $g(x)$ 与 $\pi(x)$ 的关系式 // 68
- 4.4 素数定理的几个等价形式 // 71
- 4.5 $\pi(n)$ 与 p_n 的一些不等式 // 73
- 4.6 Shapiro Tauberian 定理 // 76
- 4.7 Shapiro 定理的应用 // 78
- 4.8 部分和 $\sum_{p \leq x} \left(\frac{1}{p}\right)$ 的一个渐近公式 // 80
- 4.9 麦比乌斯函数的部分和 // 81
- 4.10 素数定理初等证明的简短概要 // 87

4.11 塞尔伯格渐近公式 // 88

第四章习题 // 89

第五章 同余 // 95

5.1 同余的定义与基本性质 // 95

5.2 剩余类与完全剩余系 // 98

5.3 一次同余式 // 99

5.4 简化剩余系与欧拉-费马定理 // 101

5.5 模 p 的多项式同余式,拉格朗日定理 // 102

5.6 拉格朗日定理的应用 // 103

5.7 一次同余式组,中国剩余定理 // 104

5.8 中国剩余定理的应用 // 105

5.9 模是素数方幂的多项式同余式 // 107

5.10 交叉分类原理 // 109

5.11 简化剩余系的分解性 // 111

第五章习题 // 113

第六章 有限 Abel 群及其特征 // 115

6.1 定义 // 115

6.2 群和子群的例子 // 116

6.3 群的基本性质 // 116

6.4 子群的结构 // 117

6.5 有限 Abel 群的特征 // 119

6.6 特征群 // 121

6.7 特征的正交关系式 // 121

6.8 迪利克雷特征 // 123

6.9 含有迪利克雷特征的和 // 125

6.10 对于实的非主特征 $\chi, L(1, \chi)$ 不等于零 // 127

第六章习题 // 129

第七章 算术级数里素数的迪利克雷定理 // 131

7.1 引言 // 131

7.2 形如 $4n-1$ 和 $4n+1$ 的素数的迪利克雷定理 // 132

7.3 迪利克雷定理的证明方案 // 133

7.4 引理 7.4 的证明 // 135

7.5 引理 7.5 的证明 // 135

7.6 引理 7.6 的证明 // 137

7.7 引理 7.8 的证明 // 137

7.8 引理 7.7 的证明 // 137

7.9 算术级数里素数的分布 // 139

第七章习题 // 140

第八章 周期数论函数与高斯和 // 141

- 8.1 模 k 的周期函数 // 141
 - 8.2 周期数论函数的有限傅立叶级数的存在性 // 142
 - 8.3 拉马努和及其推广 // 144
 - 8.4 和 $S_k(n)$ 的乘法性质 // 146
 - 8.5 与迪利克雷特征相伴的高斯和 // 148
 - 8.6 具有非零高斯和的迪利克雷特征 // 150
 - 8.7 诱导模与本原特征 // 151
 - 8.8 诱导模的进一步的性质 // 152
 - 8.9 特征的前导子 // 154
 - 8.10 本原特征与可分的高斯和 // 154
 - 8.11 迪利克雷特征的有限傅立叶级数 // 155
 - 8.12 本原特征部分和波利亚不等式 // 156
- 第八章习题 // 158

第九章 二次剩余与二次互反律 // 161

- 9.1 二次剩余 // 161
 - 9.2 勒让德符号及其性质 // 162
 - 9.3 $(-\frac{1}{p})$ 与 $(\frac{2}{p})$ 的值 // 164
 - 9.4 高斯引理 // 165
 - 9.5 二次互反律 // 168
 - 9.6 互反律的应用 // 170
 - 9.7 雅可比符号 // 172
 - 9.8 对丢番图方程的应用 // 175
 - 9.9 高斯和与二次互反律 // 176
 - 9.10 二次高斯和的互反律 // 179
 - 9.11 二次互反律的另一个证明 // 185
- 第九章习题 // 185

第十章 原 根 // 188

- 10.1 数的次数 mod m , 原根 // 188
- 10.2 原根与简化剩余系 // 189
- 10.3 对 $\alpha \geq 3$, 模 2^α 的原根不存在 // 190
- 10.4 对奇素数 p , 模 p 的原根存在 // 190
- 10.5 原根与二次剩余 // 192
- 10.6 模 p^α 的原根存在 // 192
- 10.7 模 $2p^\alpha$ 的原根存在 // 194
- 10.8 其他情况下原根不存在 // 194
- 10.9 模 m 的原根的个数 // 195

- 10.10 指数的计算 // 197
- 10.11 原根与迪利克雷特征 // 200
- 10.12 模 p^α 的实值迪利克雷特征 // 202
- 10.13 模 p^α 的本原迪利克雷特征 // 203
- 第十章习题 // 205

第十一章 迪利克雷级数与欧拉乘积 // 207

- 11.1 引言 // 207
- 11.2 迪利克雷级数绝对收敛的半平面 // 208
- 11.3 由迪利克雷级数定义的函数 // 209
- 11.4 迪利克雷级数的乘积 // 211
- 11.5 欧拉乘积 // 213
- 11.6 迪利克雷级数收敛的半平面 // 215
- 11.7 迪利克雷级数的解析性质 // 217
- 11.8 具有非负系数的迪利克雷级数 // 219
- 11.9 迪利克雷级数表示为迪利克雷级数的指数 // 220
- 11.10 迪利克雷级数的平均值公式 // 222
- 11.11 迪利克雷级数系数的一个积分公式 // 224
- 11.12 迪利克雷级数部分和的一个积分公式 // 225
- 第十一章习题 // 229

第十二章 函数 $\zeta(s)$ 和 $L(s, \chi)$ // 232

- 12.1 引言 // 232
- 12.2 Gamma 函数的性质 // 233
- 12.3 胡尔维茨 zeta 函数的积分表示 // 234
- 12.4 胡尔维茨 zeta 函数的围道积分表示 // 236
- 12.5 胡尔维茨 zeta 函数的解析开拓 // 237
- 12.6 $\zeta(s)$ 与 $L(s, \chi)$ 的解析开拓 // 238
- 12.7 $\zeta(s, a)$ 的胡尔维茨公式 // 239
- 12.8 黎曼 zeta 函数的函数方程 // 242
- 12.9 胡尔维茨 zeta 函数的函数方程 // 243
- 12.10 L -函数的函数方程 // 244
- 12.11 求 $\zeta(-n, a)$ 的值 // 246
- 12.12 伯努利数与伯努利多项式的性质 // 248
- 12.13 $L(0, \chi)$ 的公式 // 250
- 12.14 用有限和逼近 $\zeta(s, a)$ // 251
- 12.15 $|\zeta(s, a)|$ 的不等式 // 253
- 12.16 $|\zeta(s)|$ 与 $|L(s, \chi)|$ 的不等式 // 255
- 第十二章习题 // 256

第十三章 素数定理的解析证明 // 261

- 13.1 证明的方案 // 261
- 13.2 引理 // 263
- 13.3 $\frac{\psi_1(x)}{x^2}$ 的围道积分表示 // 266
- 13.4 直线 $\sigma=1$ 附近 $|\zeta(s)|$ 与 $|\zeta'(s)|$ 的上界 // 268
- 13.5 在直线 $\sigma=1$ 上 $\zeta(s)$ 不为零 // 269
- 13.6 $\left| \frac{1}{\zeta(s)} \right|$ 与 $\left| \frac{\zeta'(s)}{\zeta(s)} \right|$ 的不等式 // 271
- 13.7 素数定理证明的完成 // 272
- 13.8 $\zeta(s)$ 的无零点区域 // 275
- 13.9 黎曼假设 // 277
- 13.10 对除数函数的应用 // 277
- 13.11 对欧拉函数的应用 // 280
- 13.12 特征和的波利亚不等式的推广 // 283
- 第十三章习题 // 284

第十四章 分 拆 // 288

- 14.1 引 言 // 288
- 14.2 分拆的几何表示 // 291
- 14.3 分拆的生成函数 // 291
- 14.4 欧拉五边形数定理 // 294
- 14.5 欧拉五边形数定理的组合证明 // 297
- 14.6 $p(n)$ 的欧拉递推公式 // 298
- 14.7 $p(n)$ 的上界 // 299
- 14.8 雅可比三重积等式 // 301
- 14.9 雅可比等式的推论 // 303
- 14.10 生成函数的对数微分 // 304
- 14.11 拉马努然的分拆等式 // 306
- 第十四章习题 // 307

附 录 “哥德巴赫猜想”研究综览 // 311

特殊符号索引 // 318

编辑手记 // 320

历史介绍

数论是数学的一个分支,它研究整数的性质.如

$1, 2, 3, 4, 5, \dots$

叫做计数数,或者正整数.

正整数无疑是人类的第一个数学创造,假如人们没有计数的能力,那简直是很难想象的,至少在一个有限的范围内.历史的记载证明,早在公元前5700年,古代的沙麦朗(Sumerina)人就有一部历书,所以他们一定掌握了一些算术知识.

公元前2500年沙麦朗人产生了一个以60为基的数系,他们早于巴比伦人成为有熟练计算能力的人.巴比伦人的墓碑中发现有精心制作的数学表格,其日期可追溯至公元前2000年.

当古代文化发展到一定水平时,人们有空闲时间去思考周围的事物,一些人开始去探索周围自然界与数的性质,这种好奇心发展为数字神秘主义或者数字学.甚至在今天,比如3,7,11和13这些数字仍是考虑运气好或坏的预兆.

系统地研究数以前至少有5000年,数字是用于保存记录和商业交往.第一个科学地对整数进行研究,即数论的真正起源,通常认为是希腊人.大约在公元前600年,毕达哥拉斯(Pythagoras)和他的门徒们对整数作过较彻底的研究.他们最早以各种方法对整数进行分类:

偶数: $2, 4, 6, 8, 10, 12, 14, \dots$

奇数: $1, 3, 5, 7, 9, 11, 13, 15, \dots$

素数: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \dots$

复合数: $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, \dots$

素数是仅有约数1和自身的大于1的整数.除去1既不是素数也不是复合数以外,不是素数的整数称为复合数.

毕达哥拉斯还把数与几何图形联系起来,他创建了多边形的思想:三角形数,正方形数,五边形数,等.当然用三角形,正方形,五边形等图形上的点表示数时,这些几何名称的由来是显然的,如图1.1所示.

另一个与几何图形的联系来自著名的毕达哥拉斯定理(我国称为勾股定

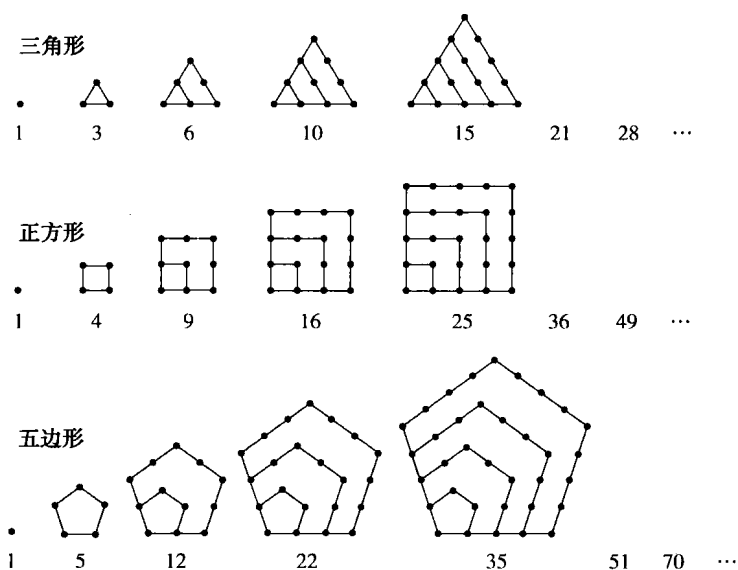


图 1.1

理——译者),它说明,在任何一个直角三角形里,斜边长的平方是两直角边长的平方和(图 1.2). 毕达哥拉斯感兴趣的是边长都是整数的直角三角形,如图 1.3 那样的三角形现在称为毕达哥拉斯三角形,对应的表示边长的三个数 (x, y, z) 称为毕达哥拉斯三数组.



图 1.2

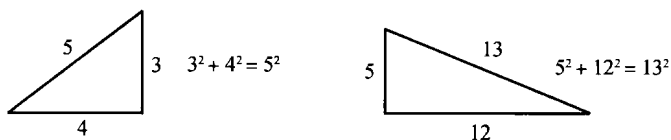


图 1.3

由大约在公元前 1700 年的巴比伦墓碑中发现有毕达哥拉斯数的一个大表格,其中一些数字相当的大. 毕达哥拉斯第一个给出了确定无穷多个三数组的方法,用现代的记号可表述如下:

令 n 是任一大于 1 的奇数,并令

$$x = n, y = \frac{1}{2}(n^2 - 1), z = \frac{1}{2}(n^2 + 1)$$

这样产生的三数组 (x, y, z) 始终是 $z = y + 1$ 的毕达哥拉斯三数组,下面有一些例子

| | | | | | | | | | |
|-----|---|----|----|----|----|----|-----|-----|-----|
| x | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 |
| y | 4 | 12 | 24 | 40 | 60 | 84 | 112 | 144 | 180 |
| z | 5 | 13 | 25 | 41 | 61 | 85 | 113 | 145 | 181 |

此外,还有其他一些毕达哥拉斯三数组,例如

| | | | | |
|-----|----|----|----|-----|
| x | 8 | 12 | 16 | 20 |
| y | 15 | 35 | 63 | 99 |
| z | 17 | 37 | 65 | 101 |

在这些例子里, $z = y + 2$. Plato(前430—前349)发现了一个确定所有这些三数组的方法,用现代的记号可写为公式

$$x = 4n, y = 4n^2 - 1, z = 4n^2 + 1$$

大约在公元前300年,在数学史上发生一件重大事件,《欧几里得基本原理》、一个包含有13卷书的书集发表了,它把数学由数字学转变为演绎推理学. 欧几里得(Euclid)是第一个把数学事实和这些事实的严格证明一起给出的人.

13卷书中有3卷是专门介绍数论的(卷VII、IX和X). 在卷IX里欧几里得证明了有无穷多个素数存在. 他的证明在现代的课堂里仍在讲授. 在卷X里他给出了得到全部毕达哥拉斯三数组的一个方法,虽然他没有给出他的方法的任何证明. 这个方法可概括为公式

$$x = t(a^2 - b^2), y = 2tab, z = t(a^2 + b^2)$$

其中, t, a 和 b 是任意正整数,满足 $a > b, a$ 与 b 互素, a 与 b 一奇一偶.

欧几里得还对毕达哥拉斯提出的另一个问题——找出所有的完全数作出了重要贡献. 数6叫做一个完全数,因为 $6 = 1 + 2 + 3$,即6等于它的所有的真因子的和(即所有小于6的因数的和). 另一个完全数是28,因为 $28 = 1 + 2 + 4 + 7 + 14$,而1,2,4,7和14是28的所有小于28的因数. 希腊人把一个数的真因数统称为它的“部分”,他们把6和28称为完全数,因为每个这样的数等于它的全部的“部分”的和.

在卷IX里,欧几里得发现了所有的偶完全数. 他证明,一个偶数如果有形式

$$2^{p-1}(2^p - 1)$$

则这个偶数一定是完全数,其中 p 和 $2^p - 1$ 都是素数.

两千年以后欧拉(Euler)证明了欧几里得定理的逆定理,即每一个偶完全数一定有欧几里得形式. 例如,对于6和28,我们有

$$6 = 2^{2-1}(2^2 - 1) = 2 \times 3, 28 = 2^{3-1}(2^3 - 1) = 4 \times 7$$

最前面的5个偶完全数是

$$6, 28, 496, 8128 \text{ 和 } 33550326$$

实际上,完全数是很稀少的,迄今(1975年)只知道24个完全数,它们在欧几里得形式中对应着的 p 的值如下:2,3,5,7,13,17,19,31,61,89,107,127,521,607,1 279,2 203,2 281,3 217,4 253,4 423,9 689,9 941,11 213,19 937.

形如 $2^p - 1$ 的数(其中 p 是素数)称为梅森(Mersenne)数,记为 M_p ,这是为了纪念梅森,他在1644年研究了这些数.对于上面表中所列的24个素数 p ,已经知道 M_p 都是素数,而对于其他所有的 $p \leq 257$,除去可能的

$$p = 157, 167, 193, 199, 227, 229$$

之外, M_p 是复合数.而对这几个 p ,还不知道 M_p 是素数或者是复合数.

不知道是否有奇完全数,甚至任何一个的存在性也不知道,但如果存在的话,它一定是很大的,实际上要大于 10^{50} .

现在我们转向从欧几里得时代以来数论历史的简短的描述.

在公元前300年欧几里得以后,到250年另一个希腊数学家,阿历山得鲁的丢番图(Diophantu)以前,在数论方面没有重大进展,丢番图出版过13本书,其中6本保存下来.这是第一个系统地利用代数符号的希腊人的工作,虽然他的代数符号用现代的标准来衡量好像是笨拙的,但丢番图的方法确实能解含有两个或三个未知量的代数方程.他的许多问题来源于数论并且自然地去找这些方程的整数解.未知量具有整数解的方程现在称为丢番图方程,而这些方程的研究就是著名的丢番图解析.毕达哥拉斯三数组的方程 $x^2 + y^2 = z^2$ 就是丢番图方程的一个例子.

丢番图之后,直到17世纪,尽管在远东,——尤其在印度——在500年至1200年这段时间出现数学开始繁荣的证据,但在数论方面没有出现更多的进展.

17世纪,在西欧,数论复兴.由于卓越的法国数学家费马(Fermat, 1601—1665)得到大量的成果,他被公认为近代数论的奠基人.费马的大多数成果是受丢番图工作的影响而得的.他第一个真正深刻地揭示出整数的性质.例如,费马证明了下列令人惊奇的定理.

每一个整数不是一个三角形数就是2或3个三角形数之和;每一个整数不是一个平方数就是2,3或4个平方数之和;每一个整数不是一个五边形数就是2,3,4或5个五边形数之和,等.

费马还发现,每一个形如 $4n + 1$ 的数,例如5,13,17,29,37,41等,是两个平方数之和,例如

$$\begin{aligned} 5 &= 1^2 + 2^2, 13 = 2^2 + 3^2, 17 = 1^2 + 4^2 \\ 29 &= 2^2 + 5^2, 37 = 1^2 + 6^2, 41 = 4^2 + 5^2 \end{aligned}$$

费马时代之后不久,在数论的深入发展方面,欧拉(1703—1783),拉格朗日(Lagrange, 1736—1813),勒让德(Legendre, 1752—1833),高斯(Gauss,

1777—1855) 和迪利克雷(Dirichlet, 1805—1859) 成为突出的名字. 第一本数论教科书在 1798 年由勒让德发表, 三年以后高斯发表了数论专题论文, 把论题变为系统的和美妙的学科的一本书. 虽然他对数学的其他分支和其他学科作出了巨大的贡献, 而高斯本人认为他的数论书是他的最巨大的工作.

高斯时代以后的大约一百年里, 在不同的方向上, 数论有了迅速的进展. 在少数的几页里要给出数论研究这类问题的清楚的断面是不可能的. 这个领域是广阔的并且一些部分需要高等数学高深的学问. 不过数论里有很多问题是很容易阐明的, 这些问题中的一些涉及素数, 我们把本书历史介绍的余下部分专门用于这些问题.

在前面有一个小于 100 的素数表. 小于一千万的素数表由一个美国数学家 D. N. Lehmer 在 1914 年发表. 小于一千万的素数有 664 579 个, 大约有 $6\frac{1}{2}\%$ 的误差, 更近一些, D. H. Lehmer (D. N. Lehmer 的儿子) 计算出小于 100 亿的素数总数有 455 052 512 个, 大约有 $4\frac{1}{2}\%$ 的误差, 虽然所有这些素数的每一个并不一定知道.

素数表的仔细的观察展示出, 素数是以很不规则的方式分布的. 素数表显现出素数之间可以有很长的间隔, 例如, 素数 370 261 后面紧接着 111 个复合数, 在 20 831 323 与 20 831 533 之间没有素数. 容易证明, 素数之间任意大的间隔都是能够出现的.

另一方面, 素数表也指出, 相邻(连续)素数, 例如 3 和 5, 或 101 和 103, 总会重新出现. 差数为 2 的素数对就是著名的孪生素数. 100 000 以内的孪生素数超过 1 000 对, 1 000 000 以内的孪生素数超过 8 000 对. 至今知道的最大的孪生素对是 $76 \cdot 3^{139} - 1$ 与 $76 \cdot 3^{139} + 1$. 很多数学家认为有无穷多个这样的素数对, 但至今没有人能证明它.

素数分布不规则的原因之一是不存在产生所有素数的简单的公式. 一些公式能产生很多素数, 例如, 式子

$$x^2 - x + 41$$

对于 $x = 0, 1, 2, \dots, 40$ 分别给出一个素数, 而

$$x^2 - 79x + 1601$$

对于 $x = 0, 1, 2, \dots, 79$ 也都给出素数, 但是, 没有这样简单的公式能对所有的 x 都给出素数, 甚至利用三次幂和更高次幂也不行. 实际上, 哥德巴赫(Goldbach) 在 1752 年证明了, 没有一个 x 的整系数多项式能对所有的 x 或对所有充分大的 x 都是素数.

某些多项式能表示无穷多个素数, 例如, 当 x 通过整数 $0, 1, 2, 3, \dots$ 时, 一次多项式

$$2x + 1$$

给出所有的奇数,因而给出无穷多个素数.又如多项式

$$4x + 1 \text{ 与 } 4x + 3$$

的每一个都给出无穷多个素数.在1837年发表的一篇著名的研究论文里,迪利克雷证明,如果 a 与 b 都是正整数并且是互素的,那么当 x 通过所有的正整数时,多项式

$$ax + b$$

给出无穷多个素数.这个结果,现在就是众所周知的关于在一个给定的算术级数里素数存在性的迪利克雷定理.

为了证明这个定理,迪利克雷超出整数的范围并引入解析的方法如极限和连续性.根据这个作法,他创建了称为解析数论的一个新的数学分支的基础.在解析数论里,实分析与复分析的概念和方法仅限于与整数有关的问题.

不知道是否有二次多项式 $ax^2 + bx + c (a \neq 0)$ 表示无穷多个素数.然而,迪利克雷利用他的卓有成效的解析的方法证明了,如果 $a, 2b$ 与 c 没有公共素因子,则两个变量的二次多项式

$$ax^2 + abxy + cy^2$$

当 x 和 y 通过所有正整数时,它能表示无穷多个素数.

费马猜想,对于 $n = 0, 1, 2, \dots$,公式 $2^{2^n} + 1$ 总是给出素数.这些数称为费马数并记为 F_n .前5个是 $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ 和 $F_4 = 65\,537$,它们都是素数.但在1732年欧拉发现 F_5 是复合数.实际上

$$F_5 = 2^{32} + 1 = 641 \cdot 6\,700\,417$$

这些数在平面几何里也是有趣的.高斯证明,如果 F_n 是素数, $F_n = p$,那么正 p 边形能用圆规和直尺作出.

超过 F_5 ,还没有出现其他的费马数是素数.实际上,对于 $5 \leq n \leq 16$,每一个费马数 F_n 都是复合数,而且对于下面更多的 n 的孤立的值,已经知道 F_n 是复合数

$n = 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117,$
 $125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 425, 1\,945$

已知的最大的费马复合数是 $F_{1\,945}$,它超过 10^{582} 位数,这个数超过洛杉矶和纽约的电话号码簿的字母的总数.

前面谈到,没有一个简单的公式能给出所有的素数.在这个问题上,我们要谈到在1947年由美国数学家W. H. Mills发现的一个结果.他证明,存在某个大于1但不是整数的数 A ,使得:

对所有的 $x = 1, 2, 3, \dots, [A^{3^x}]$ 是素数,其中 $[A^{3^x}]$ 表示小于等于 A^{3^x} 的最大整数.遗憾的是,没有人知道 A 等于什么.