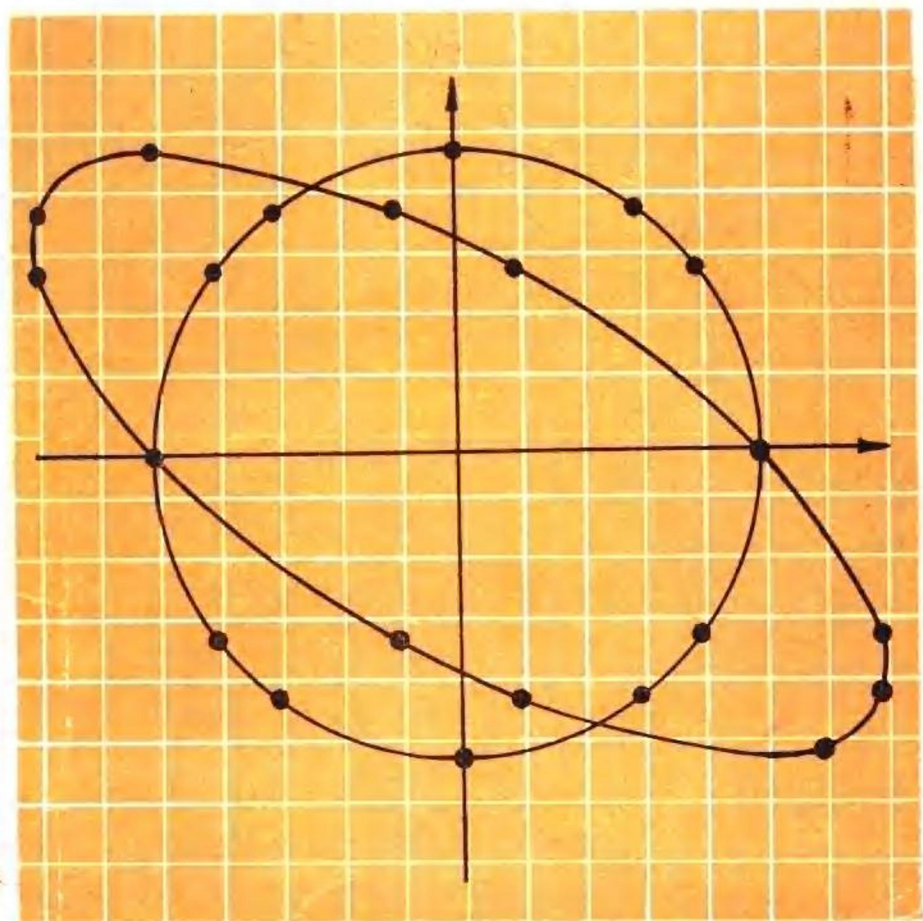


〔英〕 R. P. 布恩 著 于秀源 译

潘承彪 裴卓明 校

数论入门



高等教育出版社

数论入门

[英] R.P. 布恩 著

于秀源 译

潘承彪 校

裘卓明

741/104/111

高等教育出版社

内 容 简 介

本书系根据英国剑桥大学出版社 (Cambridge University Press) 1982 年出版的 R. P. 布恩 (R. P. Burn) 所著《数论入门》 (A pathway into number theory) 译出。

本书以一系列练习的形式编写, 书中在处理数学的直观性与严格性的关系方面有独到之处, 是一本便于自学的读物。阅读本书只需具备现代高中数学基础知识。

本书每章附有注记与答案, 章末还有历史注记, 记述了数论中一些著名定理的发现与发展。

本书可作为高等院校的教学参考书和习题集, 也可供中学教师、自学者学习。

数 论 入 门

[英] R. P. 布恩 著 于秀源 译

潘承彪 裘卓明 校

*

高等教育出版社出版

高等教育出版社照排中心照排

新华书店北京发行所发行

北 京 印 刷 一 厂 印 装

*

开本 850×1168 1/32 印张 10.375 字数 260 000

1990年 7 月第1版 1990年 7 月第1次印刷

印数 0001—2 490

ISBN7-04-000884-X/O·340

定价 3.00 元

致 谢

我高兴地向对编写本书的方针和方法提出建设性意见的人们表示感谢: Alan Bell 向我指出, 先叙述定义, 尔后是定理, 再后是练习的程序, 与正常的学习过程是相反的; Bill Brookes 则指出了把人们遇到的数学“难点”以及克服它们的过程记录下来的重要意义.

感谢 S. M. Edmonds 博士, 他使我坚定了这个信念: 全部用问题组成一本教材是可行的; 感谢 J. F. Adams 教授, 他提出数论是做这种尝试的一个合适的领域; 感谢 S. J. Patterson 博士, 他建议把平方和做为主要论题, 并且指出由此能引出多少另外的论题, 他还给出了第九章中 Legendre 定理的证明; 感谢 A. F. Beardon 博士, 他给出了第九章中下述定理的证明: 格的等距变换群的子群的指数, 等于子格^①的基本单元的测度; 感谢 Dick Tahta, 他用图形表示出 $\sum_{d|12} \varphi(d)$ 与 Pythagoras 三角形; 感谢 C. W. L. Garner 博士

1980 年春天在进行本书原稿的打字工作时, 他在 Ottawa 的 Carleton 大学为我提供了一个很好的工作环境; 感谢我在 Homerton 的同事们对入门采用的形式所表示的兴趣, 尤其要感谢 Stuart Plunkett, 他分析了直观地表现数的性质的各种方法, 并且提供了一个计算程序, 使我能在图形终端上看到二次型的图象, 他还列出了 $\sum_{d|12} \varphi(d)$ 的数值表; 最后, 我要感谢在 Homerton 的学生们允许我使用他们的数论研究成果, 特别是 Jane Charman 的工作, 它们构成了第三章和第六章的部分内容.

R. P. Burn
Homerton 学院, 剑桥
1981. 1.

① 这是与等距变换子群相对应的那个子格. ——译者注.

引 言

入门的形成

你可曾听过一次数学讲座,听懂了论证的每一步,最后却觉得不理解讲的究竟是什么吗?在读了一本书中某个定理的证明之后,你是否有过同样感觉?如果有过这样的情况,那么你就体验到了大多数数学工作者所共有的感受.

这本关于数论的书汇集了我如何实际地克服一些难点的记录,这些难点是我在学习某些标准教科书时所遇到的.我常常通过研究特例来搞清楚一般性结论,然后,我把这些研究系统地组织起来,使其成为一条通达这些标准定理的“入门途径”;在本书中,这些定理以对学生提问题的形式出现在每节的末尾.

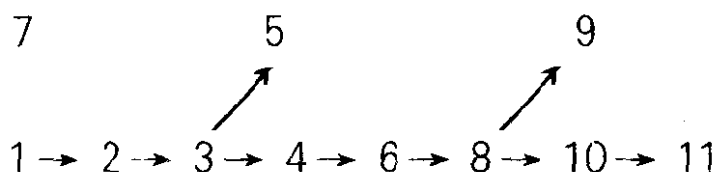
编写入门的起因是有一个学院需要开设一门不讲授的课程.如果入门比别的数论书或大学讲义更为成功,那是因为它比通常的教材更能紧紧地遵循发现的自然过程,并且把逻辑放在一个适当的地位. Hadamard 说过:“严格的目的是,在于说明直观结论的合理性,舍此再无其他.”在完善数学的任何一部分时,形式化、抽象化与一般化都占有重要的地位,但是,它们在发现中的作用则不尽相同.在入门中,我尽可能地用非正式的、特殊的方式来引进新的概念.在注记中有一些关于基础方面的评注,但是Peano公理未收入本书,这是因为它的发表几乎迟于书中的所有数论内容.

在选择材料时,考虑到了未来的教师们的需要.平方和这一论题,将第四,五,六,八,九,十各章连系在一起.作者认为,算术函数及素数分布与中学教学的联系是比较少的.

在十七世纪, Fermat 抱怨几何学统治着他那个时代的数学,以致数本身没有受到应有的重视.数论的许多代表人物与 Fermat

有同样的看法,十分关心他们的学科的独立性,直至十九世纪末期,**Minkowski**才使数学家们再次认识到数与空间的多方面的内在联系.第九章介绍了他的部分工作.此外,我们利用每一个机会去揭示数与几何的相互联系,并且举出数值实例,以便直观地理解数的涵义.(第十章是个例外,因为在**Stark**的教科书(1978)中已经对连分数做了这种几何学的研究).

各章之间的依赖关系如下图箭头所示:



对学生的建议

书中的一系列问题和注记将引导你去完成大学的数论课程.你需要有一个具备开方与倒数运算功能的袖珍计算器,它再有两个存储器就更好了.由于本书采用了特殊的编写方式,每章中的问题大都不需参看前面各章内容即可解决,只有极少数问题需要预先对前一章的知识有详细的了解.每一章的注记包括了解答、评论,有时还包括定义,它们都是应该读的.

如果你打算把这本“入门”从头到尾读完,那么就需要对复数,数学归纳法, 2×2 阶矩阵以及到**Lagrange**定理为止的群论的知识都有一定的了解,这些内容可以在现代六年级教科书——例如中学数学大纲的高级课本(剑桥大学出版社,1979)——中找到.除这些基础知识外,入门不需要其他预备知识.当然,学习过初级分析教程的读者,对连分数的收敛性会有更好的了解;在**Liouville**定理的证明中使用中值定理,也会比本书的讲法更方便.

所列出的参考书侧重于同等水平的内容,而不是为了提供进一步的读物.

在本书中,“问题 31”表示这一章中的问题 31,“问题 31”表示第二章中的问题 31,而“注记 2.31”则表示对问题 2.31 所做的注记.

① 此书已由上海教育出版社出版,中译本名为“英国中学数学教科书”——译者.

目 录

引言	1
第一章 算术基本定理	1
除法算式	1
最大公约数与 Euclid 算法	7
素因数分解的唯一性	9
素数的无限性	13
Mersenne 素数	14
注记与答案	14
历史注记	22
第二章 模加法与 Euler 的 φ 函数	23
同余类与中国剩余定理	23
群 $(\mathbb{Z}_n, +)$ 及其生成元	27
Euler 的 φ 函数	33
Euler 函数对约数求和	37
注记与答案	39
历史注记	50
第三章 模乘法	51
Fermat 定理	51
Wilson 定理	58
一次同余方程	58
Fermat - Euler 定理	59
联立一次同余方程	60
关于多项式的 Lagrange 定理	61
原根	68
Chevalley 定理	72

注记与答案	73
历史注记	84
第四章 二次剩余	85
二次剩余与 Legendre 符号	85
Gauss 引理	88
二次互反律	91
注记与答案	96
历史注记	107
第五章 方程 $x^n + y^n = z^n$ ($n = 2, 3, 4$)	108
方程 $x^2 + y^2 = z^2$	108
方程 $x^4 + y^4 = z^4$	112
方程 $x^2 + y^2 + z^2 = t^2$	114
方程 $x^3 + y^3 = z^3$	114
注记与答案	122
历史注记	133
第六章 平方和	135
二平方之和	135
四平方之和	138
三平方之和	141
注记与答案	141
历史注记	153
第七章 分析	155
Ferrers 图	155
生成函数	156
Euler 定理	160
注记与答案	162
历史注记	171
第八章 二次型	172
幺模变换	172
等价二次型	176

判别式	180
正规表示	182
约化型	184
定二次型的自守变换	186
注记与答案	187
历史注记	207
第九章 数的几何	209
正方形格的子群	209
二维的 Minkowski 定理	214
立方体格的子群	220
三维的 Minkowski 定理	224
关于 $ax^2 + by^2 + cz^2 = 0$ 的 Legendre 定理	226
注记与答案	229
历史注记	241
第十章 连分数	242
无理平方根	242
收敛性	243
纯循环连分数	250
Pell 方程	254
关于二次无理数的 Lagrange 定理	257
不定型 $ax^2 - by^2$ 的自守变换	259
注记与答案	261
历史注记	277
第十一章 无理数的有理逼近	278
自然逼近	278
Farey 数列	280
Hurwitz 定理	282
Liouville 定理	286
注记与答案	290
历史注记	302
参考书目	303

定义与定理	306
索引	315
英汉人名对照表	321

第一章 算术基本定理

除 法 算 式

1. 观察表 1.1, 如果用同样的方法向下延续, 它能否包含我们指定的任何一个正整数?

2. 表 1.1 中的每个数与它下面的数有什么关系?

3. 简洁地描述由 0 以下的一列数所组成的整个集合.

4. 如果在 0 以下的一列中取两个数并把它们相加, 那么它们的和必在表的哪一位置?

5. 表 1.1 的整个排列可以看做是以 0 下面的一列数与表头上的三个数 1, 2, 3 下面的各列数的加法表. 利用你对 0 以下的一列数的简单描述, 对于由 1 以下的一列数所组成的整个集合, 给出一个比较简洁的描述, 并对由另外的两列数组成的集合也都给出类似的简洁描述.

6. 如果两个数都在第二列, 那么大数与小数的差在什么位置?

7. 如果两个数都在第三列, 那么大数与小数的差在什么位置? 试用具有一般性的表示方法对于所有这种数对来证明你的结论.

8. 如果两个数都在第四列, 那么大数与小数的差在什么位置? 证明你的结论.

9. 如果从第二列中取两个数, 那么它们的和在什么位置? 一般地证明你的结论.

10. 如果从第四列中取两个数, 那么它们的和在什么位置? 一般地证明你的结论.

11. 有没有一般规则, 可填出一列中的数与另一列 (包括本列) 中的数的加法表? 如果在这个表中只用到各个列的表头上的数

表 1.1

0	1	2	3	0	1	2	3
4	5	6	7	100	101	102	103
8	9	10	11	104	105	106	107
12	13	14	15	108	109	110	111
16	17	18	19	112	113	114	115
20	21	22	23	116	117	118	119
24	25	26	27	120	121	122	123
28	29	30	31	124	125	126	127
32	33	34	35	128	129	130	131
36	37	38	39	132	133	134	135
40	41	42	43	136	137	138	139
44	45	46	47	140	141	142	143
48	49	50	51	144	145	146	147
52	53	54	55	148	149	150	151
56	57	58	59	152	153	154	155
60	61	62	63	156	157	158	159
64	65	66	67	160	161	162	163
68	69	70	71	164	165	166	167
72	73	74	75	168	169	170	171
76	77	78	79	172	173	174	175
80	81	82	83	176	177	178	179
84	85	86	87	180	181	182	183
88	89	90	91	184	185	186	187
92	93	94	95	188	189	190	191
96	97	98	99	192	193	194	195
				196	197	198	199

(0, 1, 2, 3), 那么所得到的表就是模 4 的加法表的一个例子, 这样的表用 $(\mathbb{Z}_4, +)$ 表示.

+	在 0 列 中的 数	在 1 列 中的 数	在 2 列 中的 数	在 3 列 中的 数
在 0 列 中的 数				
在 1 列 中的 数				
在 2 列 中的 数				
在 3 列 中的 数				

12. 表 1.1 中同一列中的两个数被称为对模 4 同余^①。我们记 $5 \equiv 13 \pmod{4}$ 。请你给出 $a \equiv b \pmod{4}$ 的代数定义。

13. 每个正整数是否恰好能表示成四个形式 $4q, 4q+1, 4q+2, 4q+3$ 中的一个 ($q \geq 0$ 是某个整数)? 如何判断一个特定的数 (例如 1553) 是这些形式中的哪一种?

14. 研究关于表 1.1 的列的乘法结果, 能否构造一个类似于上述加法表的乘法表?

15. 在表 1.2 中, 用五个列来列出正整数. 对于由每一列中的数所组成的集合, 给出一个一般性的描述。

① 见第二章问题 4 及其注。——译者注。

16. 每个正整数是否恰好能表示成五个形式 $5q, 5q + 1, 5q + 2, 5q + 3, 5q + 4$ 中的一个 ($q \geq 0$ 是某个整数)? 如何判断一个特定的数 (例如 6666) 是这些形式中的哪一种?

表 1.2

0	1	2	3	4	100	101	102	103	104
5	6	7	8	9	105	106	107	108	109
10	11	12	13	14	110	111	112	113	114
15	16	17	18	19	115	116	117	118	119
20	21	22	23	24	120	121	122	123	124
25	26	27	28	29	125	126	127	128	129
30	31	32	33	34	130	131	132	133	134
35	36	37	38	39	135	136	137	139	139
40	41	42	43	44	140	141	142	143	144
45	46	47	48	49	145	146	147	148	149
50	51	52	53	54	150	151	152	153	154
55	56	57	58	59	155	156	157	158	159
60	61	62	63	64	160	161	162	163	164
65	66	67	68	69	165	166	167	168	169
70	71	72	73	74	170	171	172	173	174
75	76	77	78	79	175	176	177	178	179
80	81	82	83	84	180	181	182	183	184
85	86	87	88	89	185	186	187	188	189
90	91	92	93	94	190	191	192	193	194
95	96	97	98	99	195	196	197	198	199

17. 做出模 5 的加法表与乘法表, 至少对每个表中的两个表值给出正规的证明.

18. 表 1.1 是用四个列来列出正整数, 而表 1.2 是用五个列来列出正整数. 一般地, 如果用 b 个列来列出正整数 (包括数 0), 那么, 第一行是哪些数? 第一列是哪些数? 每个正整数是否可以表示成第一行中的一个数与第一列中的一个数的和? 如果整数 a 和 bq 在同一行, 那么 $bq, b(q+1)$ 及 a 这三个数之间有什么关系? 推出 $a = bq + r$, 其中 $r = 0$ 或 r 是小于 b 的正整数.

19. 设 a 和 b 是正整数, q_1, q_2, r_1, r_2 都是正整数或零, 而且 r_1 和 r_2 都小于 b . 再设 $a = bq_1 + r_1 = bq_2 + r_2$. 证明 r_1 与 r_2 的差是 b 的倍数, 从而推出 $r_1 = r_2$ 以及 $q_1 = q_2$.

(问题 18 与 19 合在一起就给出了除法算式).

20. 在表 1.3 中, 所有的列都从 0, 1, 2, 3 这一行出发向上和向下双方延伸. 对由每一列中的数组成的集合给出一般性描述. 问题 11 中得到的列的加法表对向上延伸的列是否仍成立? 问题 14 中得到的列的乘法表对向上延伸的列是否仍成立?

21. 数 -161 属于表 1.3 的哪一列 (假定已将它延伸)?

22. 在由数组成的加法群 $(\mathbb{Z}, +)$ 中, 用 $4\mathbb{Z}$ 表示表 1.3 中第一列的数所成的子集, 其它列中的数所成的子集则分别用 $4\mathbb{Z} + 1, 4\mathbb{Z} + 2$ 及 $4\mathbb{Z} + 3$ 表示. 用群论的语言描述 $(\mathbb{Z}, +)$ 的这四个子集.

23. 试提出一个对于任何整数 a 和任何正整数 b 都适用的除法算式.

24. 验证你所提出的除法算式.

除法算式可说是同余算术的基础. 在本章的其余部分, 我们将用它来证明关于自然数因数分解的一些基本性质. 在和 $\mathbb{N}$ 不同的某些数系中, 有时也可以证明类似的除法算式, 从而也可以推出因数分解唯一性定理, 例如, 见问题 5.53.

表 1.3

-100	-99	-98	-97
-96	-95	-94	-93
-92	-91	-90	-89
-88	-87	-86	-85
-84	-83	-82	-81
-80	-79	-78	-77
-76	-75	-74	-73
-72	-71	-70	-69
-68	-67	-66	-65
-64	-63	-62	-61
-60	-59	-58	-57
-56	-55	-54	-53
-52	-51	-50	-49
-48	-47	-46	-45
-44	-43	-41	-41
-40	-39	-38	-37
-36	-35	-34	-33
-32	-31	-30	-29
-28	-27	-26	-25
-24	-23	-22	-21
-20	-19	-18	-17
-16	-15	-14	-13
-12	-11	-10	-9
-8	-7	-6	-5
4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63
64	65	66	67
68	69	70	71
72	73	74	75
76	77	78	79
80	81	82	83
84	85	86	87
88	89	90	91
92	93	94	95
96	97	98	99

最大公约数与 Euclid 算法

25. 对下面给出的两个数集链, 指出沿箭头移动的规律, 以及何时停止的规律:

$\{57, 36\} \rightarrow \{21, 36\} \rightarrow \{21, 15\} \rightarrow \{6, 15\} \rightarrow \{6, 9\} \rightarrow \{6, 3\} \rightarrow \{3, 3\} = \{3\}$ 停止.

$\{98, 175\} \rightarrow \{98, 77\} \rightarrow \{21, 77\} \rightarrow \{21, 56\} \rightarrow \{21, 35\} \rightarrow \{21, 14\} \rightarrow \{7, 14\} \rightarrow \{7, 7\} = \{7\}$ 停止.

从 $\{170, 130\}$ 开始, 照上面的模式, 做出一个数集链.

26. 如果 $a > b$, 那么, 按照问题 25 中的模式, $\{a, b\}$ 的后继者是什么? 如果链是从两个正整数开始的, 为什么在链中不会出现负整数和零?

27. 用问题 25 中给出的第一个数集链, 对下面的每个方程, 找出一对整数 x, y :

$$57 = 57x + 36y,$$

$$36 = 57x + 36y,$$

$$21 = 57x + 36y,$$

$$15 = 57x + 36y,$$

$$6 = 57x + 36y,$$

$$9 = 57x + 36y,$$

$$3 = 57x + 36y.$$

28. 用问题 25 中给出的第二个数集链, 将数 175, 98, 77, 21, 56, 35, 14, 7 都写成 $98x + 175y$ 的形式, 其中 x, y 是整数.

29. 数集 $\{57x + 36y \mid x, y \in \mathbb{Z}\}$ 是否构成 $(\mathbb{Z}, +)$ 的子群? 这个集合中的最小正数是什么? 这个数的每一个倍数是否必在这个集合中? 这个集合中的每个数是否必是这个数的倍数?

30. 对于由数 57 和 36 所生成的 $(\mathbb{Z}, +)$ 的子群给出一个简