A Pathway Into Number Theory

HIT

数论经典著作系列

数论入门

[英] R·P·布恩 著　于秀源 译

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

数论入门

A Pathway Into Number Theory

● [英] R·P·布恩 著 ● 于秀源 译

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

数论入门/(英)布恩著;于秀源译. —哈尔滨:
哈尔滨工业大学出版社,2011.3
ISBN 978-7-5603-3206-2

Ⅰ.①数… Ⅱ.①布… ②于… Ⅲ.①数论 Ⅳ.①0156

中国版本图书馆 CIP 数据核字(2011)第 031084 号

A Pathway Into Number Theory, Ed2
by R. P. Burn
通过中华版权代理中心代理取得授权版权登记号
黑版贸审字 08-2010-025 号

策划编辑 刘培杰 甄淼淼
责任编辑 尹 凡
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 哈尔滨工业大学印刷厂
开 本 787mm×1092mm 1/16 印张 17.25 字数 316 千字
版 次 2011 年 3 月第 1 版 2011 年 3 月第 1 次印刷
书 号 ISBN 978-7-5603-3206-2
定 价 38.00 元

第二版前言

自从入门(第一版)出版以来,随着产业的公钥密码术之战和费马(Fermat)最后定理的证明,数论已经悄然进入了公众视野. 这次的第二版包括了一节关于 RSA 密码的内容(第一版已经有了必需的理论),更多的有关高斯(Gauss)整数的材料,一节关于三角数的内容,并且大量地改写了历史注记部分. 大部分修改是由于凯瑟琳哥德斯坦(Catherine Goldstein)的建议;对此,我表示深切的感谢.

经常有人问我,怎样将入门作为大学教科书使用? 问题系列被别出心裁地集合在一起,成为一门不讲课的课程. 如果学生很多,就可能行不通了. 但入门仍然能让教师们组织学生更有创造性地学习. 大学数学教学,通常是讲授,其预期的反馈则是解题和练习. 这样的讲授和反馈的逻辑过程没有充分顾及学习是怎样发生的. 只有数学思想及对这种活动的思考才能导致理解. 教师最好把讲授放在学生已经有了基本概念、并且通过具体练习知识某些定理之后,和在尝试证明比较验证的公式以及解决比较难的问题之前. 入门使这种调整成为可行的. 入门的核心是让学生在正式描述中心数学思想之前,就能参与构思(适当地引进它们,学生们能做到这一点). 这个课程的总课时数不是问题所在,怎样利用时间才是关键.

R. P. BURN
Exeter 大学
1996.1

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.

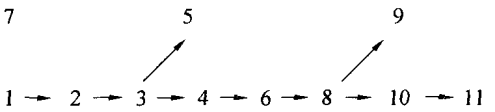
这本关于数论的书汇集了我如何实际地克服一些难点的记录，这些难点是我在学习某些标准教科书时所遇到的. 我常常通过研究特例来搞清楚一般性结论. 然后，我把这些研究系统地组织起来，使其成为一条通达这些标准定理的“入门途径”；在本书中，这些定理以对学生提问题的形式出现在每节的末尾.

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，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联系在一起. 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含义.（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①. 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 2.31”表示第二章中的问题 2.31，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

算术基本定理

第 1 章

除法算式

1. 观察表 1.1. 如果用同样的方法向下延续，它能否包含我们的指定的任何一个正整数$(1,2,\cdots,n,n+1,\cdots)$？

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? 一般的证明你的结论.

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

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(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$(Z_4, +)$表示.

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 $5 \equiv 13 \pmod 4$. 请给出 $a \equiv b \pmod 4$ 的代数定义.

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

① 见第 2 章问题 4 及其注. —— 译者注.

续表 1.1

+	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				

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($q \geqslant 0$ 是某个整数)？如何判断一个特定的数(例如 1 553)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.

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	138	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

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($q \geqslant 0$是某个整数)？如何判断一个特定的数(例如6 666)是这些形式中的哪一种？

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. 一般的,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. 在由整数组成的加法群$(Z,+)$中,用$4Z$表示表1.3中第一列的数所成的子集,其他列中的数所成的子集则分别用$4Z+1,4Z+2$及$4Z+3$表示. 用群论的语言描述$(Z,+)$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	− 42	− 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：

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

$\{98,175\} \to \{98,77\} \to \{21,77\} \to \{21,56\} \to \{21,35\} \to \{21,14\} \to \{7,14\} \to \{7,7\} = \{7\}$ 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 $\{57x + 36y \mid x,y \in \mathbf{Z}\}$ 是否构成 $(Z, +)$ 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 $(Z, +)$ 的子群给出一个简单描述.

31. 数集 $\{98x + 175y \mid x,y \in \mathbf{Z}\}$ 是否构成 $\{Z, +\}$ 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？这个集合中的每一个数是否必是这个数的倍数？

32. 对于由数98与175所生成的 $(Z, +)$ 的子群给出一个简单描述.

33. 对于由非零整数 a 和 b 所生成的 $(Z, +)$ 的子群，给出一个公式化的描述.

设 d 是这个子群中的最小正整数,说明 d 的每一个倍数必属于这个子群的原因.

假设这个子群中有一个数 c 不是 d 的倍数,用除法算式证明这个子群必定包含一个比 d 小的正整数. 这个矛盾就证明了,由 a 和 b 生成的$(Z, +)$ 的子群实际上是由一个数 d 生成的.

34. 设 a 与 b 是非零整数,而且它们所生成的$(Z, +)$ 的子群是由一正整数 d 所生成的,说明为什么有

$$d \mid a \text{ 和 } d \mid b$$

(d 整除 a 和 d 整除 b,或者说,d 是 a 的因数和 d 是 b 的因数). 再回到对于由 a, b 所生成的子群的原始的描述,证明:对于某两个整数 x,y,有 $d = ax + by$. 由此推出:a 和 b 的每一个公因数整除 d. 这说明 d 是 a 和 b 的最大的公因数,即最大公约数,记为 $d = \gcd(a,b)$.

35. 利用上题,说明为什么必有整数 x,y,使得 $2x + 3y = 1$. 根据经验,找一对适合这个方程的整数.

设 $2a + 3b = 1$ 而且 $2c + 3d = 1$,证明对于某个整数 t,有 $2(a - c) = 3(d - b) = 6t$,从而推出:$2x + 3y = 1$ 的每个解都是 $x = -4 + 3t, y = 3 - 2t$ 的形式.

36. 证明整数集合$\{12x + 18y + 27z \mid x,y,z \in \mathbf{Z}\}$ 构成$(Z, +)$ 的子群. 证明这个子群的每个元素都有因数 3. 通过适当选取 x,y,z,证明 3 是这个子群的元素,从而推出这个子群是由 3 生成的循环群,而且 $\gcd(12,18,27) = 3$.

37. 对于由三个非零整数生成的$(Z, +)$ 的子群,叙述并证明与问题 33 类似的结论.

38. 对于三个非零整数的最大公约数,叙述并证明与问题 34 类似的结论.

39. 在问题 25 中,用以寻求两个数的最大公约数的链通常简写为

$$\{57,36\} \to \{36,21\} \to \{21,15\} \to \{15,6\} \to \{6,3\} \text{ 停止}$$

与

$$\{175,98\} \to \{98,77\} \to \{77,21\} \to \{21,14\} \to \{14,7\} \text{ 停止.}$$

这种形式称为 Euclid 算法. 先写较大的数;当较小的数是较大的数的因数时,这过程停止. 看看问题 25 中的哪些步骤在 Euclid 算法中被省略了.

40. 用具有两个储存器的袖珍计算器,或两个计算器,或用笔和纸,计算 $\gcd(107\,360, 30\,866)$.

41. 用除法算式描述 Euclid 算法的每一步,说明链中每对数的最大公约数相同的原因.

42. Fibonacci 数列 1,1,2,3,5,8,13,…(每一项是前面两项之和)的相邻两项能否有大于 1 的最大公约数?