A pathway into number theory

Second edition

R.P. BURN

Number theory is concerned with the properties of the natural numbers: 1, 2, 3, ... During the seventeenth and eighteenth centuries, number theory became established through the work of Fermat, Euler and Gauss. With the hand calculators and computers of today the results of extensive numerical work are instantly available and the road leading to their discoveries may be traversed with comparative ease.

Now in its second edition this book consists of a sequence of exercises that will lead readers from quite simple number work to the point where they can prove algebraically the classical results of elementary number theory for themselves. A modern high-school course in mathematics is sufficient background for the whole book, which, as a whole, is designed to be used as an undergraduate course in number theory to be pursued by independent study without supporting lectures.

A pathway into number theory

R. P. BURN

A pathway into number theory

Second edition

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press

The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521575409
© Cambridge University Press 1982, 1997

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 1982
Reprinted 1989, 1992, 1994
Second edition 1997

A catalogue record for this publication is available from the British Library

ISBN-13 978-0-521-57540-9 paperback
ISBN-10 0-521-57540-0 paperback

Transferred to digital printing 2006

CONTENTS

PREFACE TO THE SECOND EDITION

With industrial warfare over public key cryptography and the proof of Fermat's last theorem, number theory has been uncharacteristically in the public eye since the publication of the first edition of the *Pathway*. This second edition includes a section on RSA codes (for which the necessary theory was already in the first edition), more material than before on Gaussian integers, a section on triangular numbers, and substantially revised historical notes. Most of the improvements are due to the advice of Catherine Goldstein (Paris-Sud) to whom I am deeply grateful.

From time to time I have been asked how to use the *Pathway* for an undergraduate course. The problem sequence was originally put together for a course without lectures. Where student numbers are large this may not be feasible. None the less the existence of the *Pathway* may still enable lecturers to structure their students' learning more creatively. Conventionally in undergraduate mathematics, the initiation of mathematics comes in a lecture to which the expected response is the solution of exercises and problems. This seemingly logical sequence of input and response takes insufficient account of how learning happens. It is only mathematical activity and reflection on that activity which generates understanding, and a lecturer's input may be better placed *after* students have generated the basic notions and conjectured some of the theorems through concrete exercises, and *before* the harder proof-formulation and problem-solving is attempted. It is this restructuring which the *Pathway* makes feasible. The central point of the *Pathway* is to enable students to participate in the formulation of central mathematical ideas *before* a formal treatment (which, suitably introduced, they may well be able to provide themselves). The amount of time for the course is not at issue: just how that time is used is what is at stake.

Exeter University
January 1996 *R. P. Burn*

INTRODUCTION

The construction of the *Pathway*

Have you attended a mathematics lecture, followed each step of the argument, and yet at the end felt that you did not understand what it was about? Have you read a proof of a theorem in a book and felt the same? If so, you have experienced a feeling common to most mathematicians.

This book on number theory has been put together by keeping a record of how I actually resolved the blocks which I encountered as I read a number of standard texts. Time and again, it was the exploration of special cases which illuminated the generalities for me. This collection of explorations was then organised into a sequence in such a way that the 'pathway' would climb towards the standard theorems which occur here as problems for the student at the end of each section.

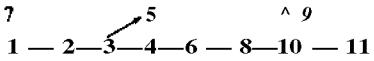
The motivation for assembling the *Pathway* was a college need to mount a course for which lectures would not be given. If the *Pathway* is more successful than some other books or undergraduate lecture courses in number theory, it is because it follows more closely than usual the natural process of discovery, and puts logic in its proper place. The purpose of rigour', said Hadamard, 'is to legitimate the conquests of the intuition, and it has never had any other purpose'. Formality, abstraction and generality have an essential place in the completion of any piece of mathematics, but their role in discovery is varied. In the *Pathway,* the introduction to each new idea is as informal and as specific as I could make it. There are a few remarks about foundations in the notes, but the statement of the Peano axioms postdates almost all of the number theory in the book and is not given here.

In the selection of material, the needs of future teachers have been kept in mind. The theme of sums of squares links chapters 4, 5, 6, 8,

9 and 10. Arithmetic functions and the distribution of primes were thought to offer less connection with school work.

In the seventeenth century, Fermat complained that the mathematics of his time was so dominated by geometry that numbers in their own right had not received their due attention. Many exponents of number theory, in the spirit of Fermat, have been jealous of the autonomy of their subject and it was only late in the nineteenth century that Minkowski made mathematicians once more aware of the rich interplay of number and space. There is a taste of Minkowski's work in chapter 9, and I have taken every opportunity to exploit the inter-relation of geometry and number and to plan the display of numerical information so as to facilitate the visual perception of number patterns. (The exception to this is in chapter 10 because continued fractions have already been explored geometrically at this level, in the textbook of Stark (1978).)

The interdependence of chapters is indicated by arrows here.



Advice to the student

The sequence of questions and notes in this book will lead you through an undergraduate course in number theory. You need a pocket calculator with a square-root function, a reciprocal function, and preferably two memories. Because of the concrete approach adopted here, there are many questions in each chapter which may be tackled without reference to earlier chapters and it is only rarely that a question presupposes detailed knowledge of work in a preceding chapter. The notes on each chapter contain solutions, comments and sometimes definitions, and they are meant to be read.

If you are intending to pursue this 'pathway' from start to finish, you should have some familiarity with complex numbers, mathematical induction, 2x2 matrices and groups up to Lagrange's theorem, as these topics appear in a modern sixth-form course such as the Advanced level books of the *School Mathematics Project* (Cambridge University Press 1979). Apart from this background, the *Pathway* is self-contained, although those who have pursued a first course in analysis will have a richer appreciation of the convergence of continued fractions and the appeal to the mean value theorem in the proof of Liouville's theorem than would be appropriate to develop here.

The bibliography has been annotated to encourage concurrent rather than further reading.

In the text, a reference to 'q 31' refers to question 31 in the same chapter. A reference to 'q2.31' refers to question 31 of chapter 2, and a reference to 'n 2.31' refers to the note on question 2.31. At the foot of each page the reference *%xf* indicates that the notes for the questions on that page appear on page *x*.

Acknowledgements

I am happy to acknowledge my debt to those who have shaped in me the direction and method of construction of this book; to Alan Bell who showed me that the sequence of definition followed by theorem followed by exercise is reversed in the normal process of learning, and to Bill Brookes who pointed out the value of recording one's mathematical 'blocks' and the processes of removing them.

I am grateful to Dr S. M. Edmonds for holding me to my belief that a course consisting of problems could be put together; to Professor J. F. Adams for suggesting number theory as an appropriate field; to Dr S. J. Patterson for suggesting the major theme of sums of squares, for indicating into how many avenues this would lead and for the proof of Legendre's theorem in chapter 9; to Dr A. F. Beardon for the proof that the index of a subgroup of a group of isometries of a lattice is equal to the measure of the fundamental unit of the tessellation in chapter 9; to Dick Tahta for graphical displays of Zd|i2 <*f*>*(d)* and of Pythagorean triangles; to Dr C. W. L. Garner for providing an excellent working environment at Carleton University, Ottawa, while work on the typescript was progressing in the spring of 1980; to my colleagues at Homerton for their interest as the *Pathway* took shape, and most particularly to Stuart Plunkett for his analysis of the various ways in which information about numbers may be visually displayed, for a computer programme which let me watch quadratic forms take shape on a graphics terminal and for the numerical display of £d|i2 <*f*>*(d);* and finally to those students at Homerton whose investigations into number theory I have been allowed to share, and particularly Jane Charman, whose work has shaped parts of chapters 3 and 6.

Homerton College, Cambridge R. P. Burn
January 1981

1

The fundamental theorem of arithmetic

Division algorithm

1 Look at table 1.1. If the same pattern was extended downwards, would it eventually incorporate any positive integer $\{1, 2, 3, \ldots, n, n+1, \ldots\}$ that we might care to name?

2 What is the relation between each number in table 1.1 and the number below it?

3 Give a succinct description of the full set of numbers in the column below 0.

4 If you choose two numbers from the column below 0 and add them together, where in the table must their sum lie?

5 The whole of the array in table 1.1 may be considered as an addition table with the column below 0 down one side and the numbers 1, 2, 3 across the top. Using your brief description of the numbers in the column below 0, devise a comparably succinct description of the full set of numbers in the column below 1, and similarly succinct descriptions of the sets of numbers in the other two columns.

6 If two numbers lie in the second column and the lesser is subtracted from the greater, where does the difference lie?

7 If two numbers lie in the third column and the lesser is subtracted from the greater, where does the difference lie? Try to prove your result in a general way which would apply to all such pairs.

8 If two numbers lie in the fourth column and the lesser is subtracted from the greater, where does the difference lie? Prove it.

Table 1.1

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
100	101	102	103
104	105	106	107
108	109	110	111
112	113	114	115
116	117	118	119
120	121	122	123
124	125	126	127
128	129	130	131
132	133	134	135
136	137	138	139
140	141	142	143
144	145	146	147
148	149	150	151
152	153	154	155
156	157	158	159
160	161	162	163
164	165	166	167
168	169	170	171
172	173	174	175
176	177	178	179
180	181	182	183
184	185	186	187
188	189	190	191
192	193	194	195
196	197	198	199

9 If two numbers are chosen, both from the second column, where does their sum lie? Prove your claim generally.

10 If two numbers are chosen, both from the fourth column in table 1.1, where does their sum lie? Prove your claim generally.

11 Are there general rules which enable you to fill in the table below for addition of numbers by columns? If only the numbers at the heads of the columns are used in this table, the table that results is an example of an *addition* table *modulo* 4. Such a table is denoted by $(Z_4, +)$.

+	Number in column 0	Number in column 1	Number in column 2	Number in column 3
Number in column 0				
Number in column 1				
Number in column 2				
Number in column 3				

12 Two numbers which lie in the same column of table 1.1 are said to be *congruent modulo* 4. We write $5 \equiv 13 \pmod 4$. Give an algebraic definition of $a \equiv b \pmod 4$.

13 Is it true that every positive integer is expressible in exactly one of the forms $4q$, $Aq+1$, $4q+2$, $Aq+3$ for some integer q^Ol How would you determine which of the four types a particular number, say 1553, might be?

14 Investigate the effect of multiplication on the columns of table 1.1. Is it possible to construct a multiplication table analogous to the one above for addition?

Table 1.2

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
100	101	102	103	104
105	106	107	108	109
110	111	112	113	114
115	116	117	118	119
120	121	122	123	124
125	126	127	128	129
130	131	132	133	134
135	136	137	138	139
140	141	142	143	144
145	146	147	148	149
150	151	152	153	154
155	156	157	158	159
160	161	162	163	164
165	166	167	168	169
170	171	172	173	174
175	176	177	178	179
180	181	182	183	184
185	186	187	188	189
190	191	192	193	194
195	196	197	198	199

15 In table 1.2, five columns have been used to display the positive integers. Give a general description for the set of numbers in each of the columns.

16 Is it true that every positive integer is expressible in exactly one of the forms $5q$, $5g+1$, $5q+2$, $5g+3$, $5g+4$ for some integer q^O? How would you determine which of the five types a particular number, say 6666, might be?

17 Make addition and multiplication tables modulo 5. Give a formal justification of at least two entries in each table.

18 Table 1.1 displayed the positive integers in four columns, and table 1.2 displayed the positive integers in five columns. Generally, if the positive integers (with zero) are displayed similarly in b columns, what are the numbers in the first row, and what are the numbers in the first column? Can every positive integer be expressed as the sum of two integers, one in the first row and one in the first column? If the integer a appears in the same row as the integer bq, what is the relationship between the three numbers bq, $b(q+l)$ and a? Deduce that $a=bq+r$, where $r=0$ or r is a positive integer $< b$.

19 If a and b are positive integers, and q_u q_2, r_u r_2 are positive integers or zero, with $r\backslash$ and $r_2 < b$, and if moreover, $a = bq\backslash + r\backslash = bq_2 + r_2$, prove that the difference between $r\backslash$ and r_2 is a multiple of b, and deduce that $r\backslash = r_2$ and $q\backslash = q_2$.

(Questions 18 and 19 together give the *division algorithm.)*

20 In table 1.3, the columns have been extended both upwards and downwards from the row 0, 1, 2, 3. Give general descriptions of the set of numbers in each column. Does the pattern for the addition of columns found in q 11 still hold with the columns extended upwards? Does the pattern for the multiplication of columns found in q 14 still hold with the columns extended upwards?

21 To which column of table 1.3 (if extended) would -161 belong?

22 In the group of integers under addition (Z, +), the subset in the first column of table 1.3 is denoted by 4Z, and in the other columns by $4Z+1$, $4Z+2$ and 4Z4-3 respectively. Describe these four subsets of (Z, 4-) using the language of group theory.

23 Propose a form of the division algorithm which would apply to any integer a and any positive integer b.

Table 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	8	90	91
92	93	94	95
96	97	98	99

24 Justify the form of the division algorithm which you have proposed.

The division algorithm, almost as it stands, is the basis of congruence arithmetic. We shall use it to prove the fundamental facts about the factorisation of natural numbers in the rest of this chapter. In number systems other than N, an analogue of the division algorithm can sometimes be proved, and, in such systems, a unique factorisation theorem follows. See for example, q 5.53.

Greatest common divisor and Euclidean algorithm

25 For the two chains of number sets given here, devise a rule for moving along an arrow, and a rule for when to stop.

{57, 36}-*{21, 36}->{21, 15}->{6,15}-*{6, 9}
->{6, 3}->{3, 3} = {3} stop.

{98,175}->{98,77}-*{21,77}-*{21,56}->{21,35}
→{21, 14}→{7, 14}→{7, 7} = {7} stop.

Construct a sequence of number sets using the same pattern as that given above, starting with {170,130}.

26 If $a > b$, what is the successor to $\{a, b\}$ according to the pattern of chains in q 25? If the chain starts from two positive integers, why can no negative integer, or zero, appear in the chain?

27 Use the first chain of number sets given in q 25 to find a pair of integers JC, y for each of the following equations.

57 = 57*x* + 36y,
36 = 57*x* + 36y,
21 = 57*x* + 36y,
15 = 57x + 36y,
6 = 57* + 36y,
9 = 57x + 36y,
3 = 57x+36y.

28 Use the second chain of number sets given in q 25 to express each of the numbers 175, 98, 77, 21, 56, 35, 14, 7 in the form 98x + 175y, where *x* and y are integers.

29 Does the set of numbers {57* + 36y| JC, y € Z} form a subgroup of (Z, +)? What is the smallest positive number in this set? Must every multiple of this number be in the set? Must every number in the set be a multiple of this number?

30 Suggest a simple description of the subgroup of (Z, +) generated by the numbers 57 and 36.

[17]

31 Does the set of numbers $\{98x + 175y \mid x, y \in Z\}$ form a subgroup of (Z, 4-)? What is the smallest positive number in this set? Must every multiple of this number be in the set? Must every number in the set be a multiple of this number?

32 Suggest a simple description of the subgroup of (Z, +) generated by the numbers 98 and 175.

33 Give a formal description of the subgroup of (Z, +) generated by the non-zero integers a and b.
If d is the smallest positive integer in this subgroup, explain why every multiple of d lies in the subgroup.
If the subgroup were to contain a number c which was not a multiple of d, use the division algorithm to prove that the subgroup would have to contain a positive integer smaller than d. This contradiction establishes that the subgroup of (Z, +) generated by a and b is in fact generated by the single number d.

34 If a and b are non-zero integers and the subgroup of (Z, +) which they generate together is generated by the single positive integer d, explain why

$d \backslash a$ and $d \backslash b$

(d divides a and d divides b, or d is a factor of a and d is a factor of b), and by returning to the original description of the group generated by a and b, prove that $d = ax + by$ for some integers x and y, and deduce that every factor which is common to a and b, divides d. This makes d the highest common factor, or *greatest common divisor* of a and b, and we write $d = \gcd(a, b)$.

35 Use q 34 to explain why there must exist integers x and y such that $2x + 3y = 1$. Find by experiment a pair of integers which satisfy this equation.
If $2a + 3b = 1$ and $2c + 3d = 1$, prove that $2(a - c) = 3(d - b) = 6t$ for some integer t and deduce that every solution of $2x + 3y = 1$ has the form

$$x = -4 + 3t, \quad y = 3 - 2t.$$

36 Prove that the set of integers $\{12JC + 18y + 27z \mid JC, y, z \in Z\}$ forms a subgroup of (Z, +). Prove that every element of this subgroup has a factor 3. By an appropriate choice of JC, y and z, prove that 3 is an element of this subgroup. Deduce that the subgroup is the cyclic group generated by 3 and that gcd (12, 18, 27) = 3.

37 State and prove an analogue of q 33 for subgroups of (Z, +) generated by three non-zero integers.

38 State and prove an analogue of q 34 for the greatest common divisor of three non-zero integers.

39 The chains of q 25 for finding the greatest common divisor of two numbers are usually abbreviated as follows

{57, 36}->{36, 21}-{21, 15}->{15, 6}->{6, 3} stop

and

{175, 98}->{98, 77}->{77, 21}-*{21, 14}->{14, 7} stop,

and in this form are referred to as the *Euclidean algorithm.* The larger number is written first and the process stops when the smaller number is a factor of the larger number. Determine which steps in q 25 have been omitted in the Euclidean algorithm.

40 Use a pocket calculator with two memories, or two calculators, or pencil and paper, to find gcd (107 360, 30 866).

41 Use the division algorithm to describe the steps of the Euclidean algorithm. Explain why each pair in the chain have the same gcd.

42 Is it possible for two adjacent terms in the Fibonacci sequence 1, 1, 2, 3, 5, 8, 13, ..., where each term is the sum of its two predecessors, to have a gcd different from 1?

Unique factorisation into primes

43 A positive integer p, different from 1, is called a *prime number* when its only positive factors are 1 and p. If p is prime and n is a positive integer, what values can gcd (p, n) have?

44 Since $p\backslash a$ implies p ^ a, 2 is a prime number. Since 3 is not a multiple of 2, 3 is a prime number. Since 5 is not a multiple of 2, 3 or 4, 5 is a prime number. List the prime numbers less than 30.

45 In the table below, by using tracing paper if you prefer, delete all the numbers except 2 which are multiples of 2; delete all the numbers except 3 which are multiples of 3; delete all the numbers except 5 which are multiples of 5; delete all the numbers except 7 which are multiples of 7.
Are all those numbers which remain, prime numbers?

1	2	3	4	5	6	7	8	9	1 0
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	100

[18]

Table 1.4

2	4	6	8
10	12	14	16
18	20	22	24
26	28	30	32
34	36	38	40
42	44	46	48
50	52	54	56
58	60	62	64
66	68	70	72
74	76	78	80
82	84	86	88
90	92	94	96
98	100	102	104
106	108	110	112
114	116	118	120
122	124	126	128
130	132	134	136
138	140	142	144
146	148	150	152
154	156	158	160
162	164	166	168
170	172	174	176
178	180	182	184
186	188	190	192
194	196	198	200

Table 1.5

1	5	9	13	17	21	25	29	33	37
41	45	49	53	57	61	65	69	73	77
81	85	89	93	97	101	105	109	113	117
121	125	129	133	137	141	145	149	153	157
161	165	169	173	177	181	185	189	193	197
201	205	209	213	217	221	225	229	233	237
241	245	249	253	257	261	265	269	273	277
281	285	289	293	297	301	305	309	313	317
321	325	329	333	337	341	345	349	353	357
361	365	369	373	377	381	385	389	393	397
401	405	409	412	417	421	425	429	433	437
441	445	449	453	457	461	465	469	473	477
481	485	489	493	497	501	505	509	513	517
521	525	529	533	537	541	545	549	553	557
561	565	569	573	577	581	585	589	593	597
601	605	609	613	617	621	625	629	633	637
641	645	649	653	657	661	665	669	673	677
681	685	689	693	697	701	705	709	713	717
721	725	729	733	737	741	745	749	753	757
761	765	769	773	777	781	785	789	793	797
801	805	809	813	817	821	825	829	833	837
841	845	849	853	857	861	865	869	873	877
881	885	889	893	897	901	905	909	913	917
921	925	929	933	937	941	945	949	953	957
961	965	969	973	977	981	985	989	993	997