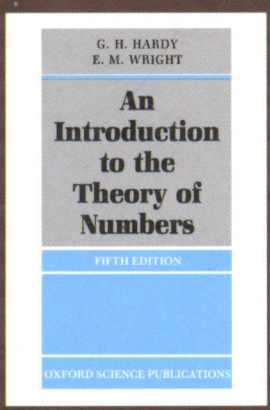
TURING 图灵原版数学·统计学系列

An Introduction to the Theory of Numbers

数论导引

英文版·第5版

[英] G. H. Hardy
E. M. Wright 著



人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵原版数学·统计学系列

An Introduction to the Theory of Numbers

数论导引

（英文版·第5版）

[英] G. H. Hardy
E. M. Wright 著

人民邮电出版社
北　京

图书在版编目（CIP）数据

数论导引：第5版：英文/（英）哈代，（英）爱德华，（英）莱特著.
—北京：人民邮电出版社，2007.3
（图灵原版数学·统计学系列）

ISBN 978-7-115-15611-2

Ⅰ．数… Ⅱ．①哈…②爱…③莱… Ⅲ．数论－研究－英文 Ⅳ．0156

中国版本图书馆CIP数据核字（2006）第150188号

内容提要

本书是一本经典的数论名著，书的内容取材于作者在牛津大学、剑桥大学等大学授课的讲义。书中从各个不同角度对数论进行了阐述，包括素数、无理数、同余、费马定理、同余式、连分数、不定式、二次域、算术函数、分划等等。第二作者为此书每章增加了必要的注解，便于读者理解并进一步学习。

本书读者对象为大学数学专业学生以及对数论感兴趣的专业人士。

图灵原版数学·统计学系列

数论导引（英文版·第5版）

◆ 著 [英]G.H.Hardy E.M.Wright
责任编辑 明永玲 武卫东

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：700×1000 1/16
印张：28.25
字数：542千字 2007年3月第1版
印数：1-3 000册 2007年3月北京第1次印刷

著作权合同登记号 图字：01-2006-7032号

ISBN 978-7-115-15611-2/O1

定价：69.00元

读者服务热线：(010)88593802 印装质量热线：(010)67129223

版权声明

This edition of *An Introduction to the Theory of Numbers, Fifth Edition* is published under licence from Oxford University Press for sale in Mainland part of the People's Republic of China (i. e. excluding the territories of Hong Kong, Macau, Taiwan) only and not for export therefrom.

Copyright © Oxford University Press 1979.

本书由牛津大学出版社授权人民邮电出版社出版，仅限于在中华人民共和国（不包括香港、澳门特别行政区和台湾地区）销售，不得向其他国家或地区销售和出口。

PREFACE TO THE FIFTH EDITION

THE main changes in this edition are in the Notes at the end of each chapter. I have sought to provide up-to-date references for the reader who wishes to pursue a particular topic further and to present, both in the Notes and in the text, a reasonably accurate account of the present state of knowledge. For this I have been dependent on the relevant sections of those invaluable publications, the *Zentralblatt* and the *Mathematical Reviews*. But I was also greatly helped by several correspondents who suggested amendments or answered queries. I am especially grateful to Professors J. W. S. Cassels and H. Halberstam, each of whom supplied me at my request with a long and most valuable list of suggestions and references.

There is a new, more transparent proof of Theorem 445 and an account of my changed opinion about Theodorus' method in irrationals. To facilitate the use of this edition for reference purposes, I have, so far as possible, kept the page numbers unchanged. For this reason, I have added a short appendix on recent progress in some aspects of the theory of prime numbers, rather than insert the material in the appropriate places in the text.

E. M. W.

ABERDEEN
October 1978

此为试读,需要完整PDF请访问: www.ertongbook.com

PREFACE TO THE FIRST EDITION

THIS book has developed gradually from lectures delivered in a number of universities during the last ten years, and, like many books which have grown out of lectures, it has no very definite plan.

It is not in any sense (as an expert can see by reading the table of contents) a systematic treatise on the theory of numbers. It does not even contain a fully reasoned account of any one side of that many-sided theory, but is an introduction, or a series of introductions, to almost all of these sides in turn. We say something about each of a number of subjects which are not usually combined in a single volume, and about some which are not always regarded as forming part of the theory of numbers at all. Thus Chs. XII–XV belong to the 'algebraic' theory of numbers, Chs. XIX–XXI to the 'additive', and Ch. XXII to the 'analytic' theories; while Chs. III, XI, XXIII, and XXIV deal with matters usually classified under the headings of 'geometry of numbers' or 'Diophantine approximation'. There is plenty of variety in our programme, but very little depth; it is impossible, in 400 pages, to treat any of these many topics at all profoundly.

There are large gaps in the book which will be noticed at once by any expert. The most conspicuous is the omission of any account of the theory of quadratic forms. This theory has been developed more systematically than any other part of the theory of numbers, and there are good discussions of it in easily accessible books. We had to omit something, and this seemed to us the part of the theory where we had the least to add to existing accounts.

We have often allowed our personal interests to decide our programme, and have selected subjects less because of their importance (though most of them are important enough) than because we found them congenial and because other writers have left us something to say. Our first aim has been to write an interesting book, and one unlike other books. We may have succeeded at the price of too much eccentricity, or we may have failed; but we can hardly have failed completely, the subject-matter being so attractive that only extravagant incompetence could make it dull.

The book is written for mathematicians, but it does not demand any great mathematical knowledge or technique. In the first eighteen chapters we assume nothing that is not commonly taught in schools, and any intelligent university student should find them comparatively easy reading. The last six are more difficult, and in them we presuppose

a little more, but nothing beyond the content of the simpler university courses.

The title is the same as that of a very well-known book by Professor L. E. Dickson (with which ours has little in common). We proposed at one time to change it to *An introduction to arithmetic*, a more novel and in some ways a more appropriate title; but it was pointed out that this might lead to misunderstandings about the content of the book.

A number of friends have helped us in the preparation of the book. Dr. H. Heilbronn has read all of it both in manuscript and in print, and his criticisms and suggestions have led to many very substantial improvements, the most important of which are acknowledged in the text. Dr. H. S. A. Potter and Dr. S. Wylie have read the proofs and helped us to remove many errors and obscurities. They have also checked most of the references to the literature in the notes at the ends of the chapters. Dr. H. Davenport and Dr. R. Rado have also read parts of the book, and in particular the last chapter, which, after their suggestions and Dr. Heilbronn's, bears very little resemblance to the original draft.

We have borrowed freely from the other books which are catalogued on pp. 417–19, and especially from those of Landau and Perron. To Landau in particular we, in common with all serious students of the theory of numbers, owe a debt which we could hardly overstate.

G. H. H.
E. M. W.

OXFORD
August 1938

REMARKS ON NOTATION

We borrow four symbols from formal logic, viz.

$$\rightarrow, \equiv, \exists, \in.$$

$\rightarrow$ is to be read as 'implies'. Thus

$$l \mid m \rightarrow l \mid n \qquad \text{(p. 2)}$$

means ' "l is a divisor of m" implies "l is a divisor of n" ', or, what is the same thing, 'if l divides m then l divides n'; and

$$b \mid a \;.\; c \mid b \rightarrow c \mid a \qquad \text{(p. 1)}$$

means 'if b divides a and c divides b then c divides a'.

$\equiv$ is to be read 'is equivalent to'. Thus

$$m \mid ka - ka' \equiv m_1 \mid a - a' \qquad \text{(p. 51)}$$

means that the assertions 'm divides $ka-ka'$' and 'm_1 divides $a-a'$' are equivalent; either implies the other.

These two symbols must be distinguished carefully from $\rightarrow$ (tends to) and $\equiv$ (is congruent to). There can hardly be any misunderstanding, since $\rightarrow$ and $\equiv$ are always relations between *propositions*.

$\exists$ is to be read as 'there is an'. Thus

$$\exists\, l \;.\; 1 < l < m \;.\; l \mid m \qquad \text{(p. 2)}$$

means 'there is an l such that (i) $1 < l < m$ and (ii) l divides m'.

$\in$ is the relation of a member of a class to the class. Thus

$$m \in S \;.\; n \in S \rightarrow (m \pm n) \in S \qquad \text{(p. 19)}$$

means 'if m and n are members of S then $m+n$ and $m-n$ are members of S'.

A star affixed to the number of a theorem (e.g. Theorem 15*) means that the proof of the theorem is too difficult to be included in the book. It is not affixed to theorems which are not proved but may be proved by arguments similar to those used in the text.

CONTENTS

I. THE SERIES OF PRIMES (1)

1.1. Divisibility of integers 1
1.2. Prime numbers 1
1.3. Statement of the fundamental theorem of arithmetic 3
1.4. The sequence of primes 3
1.5. Some questions concerning primes 5
1.6. Some notations 7
1.7. The logarithmic function 8
1.8. Statement of the prime number theorem 9

II. THE SERIES OF PRIMES (2)

2.1. First proof of Euclid's second theorem 12
2.2. Further deductions from Euclid's argument 12
2.3. Primes in certain arithmetical progressions 13
2.4. Second proof of Euclid's theorem 14
2.5. Fermat's and Mersenne's numbers 14
2.6. Third proof of Euclid's theorem 16
2.7. Further remarks on formulae for primes 17
2.8. Unsolved problems concerning primes 19
2.9. Moduli of integers 19
2.10. Proof of the fundamental theorem of arithmetic 21
2.11. Another proof of the fundamental theorem 21

III. FAREY SERIES AND A THEOREM OF MINKOWSKI

3.1. The definition and simplest properties of a Farey series 23
3.2. The equivalence of the two characteristic properties 24
3.3. First proof of Theorems 28 and 29 24
3.4. Second proof of the theorems 25
3.5. The integral lattice 26
3.6. Some simple properties of the fundamental lattice 27
3.7. Third proof of Theorems 28 and 29 29
3.8. The Farey dissection of the continuum 29
3.9. A theorem of Minkowski 31
3.10. Proof of Minkowski's theorem 32
3.11. Developments of Theorem 37 34

IV. IRRATIONAL NUMBERS

4.1. Some generalities 38
4.2. Numbers known to be irrational 38
4.3. The theorem of Pythagoras and its generalizations 39

4.4. The use of the fundamental theorem in the proofs of Theorems 43–45 41
4.5. A historical digression 42
4.6. Geometrical proof of the irrationality of $\sqrt{5}$ 44
4.7. Some more irrational numbers 45

V. CONGRUENCES AND RESIDUES
5.1. Highest common divisor and least common multiple 48
5.2. Congruences and classes of residues 49
5.3. Elementary properties of congruences 50
5.4. Linear congruences 51
5.5. Euler's function $\phi(m)$ 52
5.6. Applications of Theorems 59 and 61 to trigonometrical sums 54
5.7. A general principle 57
5.8. Construction of the regular polygon of 17 sides 57

VI. FERMAT'S THEOREM AND ITS CONSEQUENCES
6.1. Fermat's theorem 63
6.2. Some properties of binomial coefficients 63
6.3. A second proof of Theorem 72 65
6.4. Proof of Theorem 22 66
6.5. Quadratic residues 67
6.6. Special cases of Theorem 79: Wilson's theorem 68
6.7. Elementary properties of quadratic residues and non-residues 69
6.8. The order of $a \pmod m$ 71
6.9. The converse of Fermat's theorem 71
6.10. Divisibility of $2^{p-1}-1$ by p^2 72
6.11. Gauss's lemma and the quadratic character of 2 73
6.12. The law of reciprocity 76
6.13. Proof of the law of reciprocity 77
6.14. Tests for primality 78
6.15. Factors of Mersenne numbers; a theorem of Euler 80

VII. GENERAL PROPERTIES OF CONGRUENCES
7.1. Roots of congruences 82
7.2. Integral polynomials and identical congruences 82
7.3. Divisibility of polynomials $(\mathrm{mod}\, m)$ 83
7.4. Roots of congruences to a prime modulus 84
7.5. Some applications of the general theorems 85
7.6. Lagrange's proof of Fermat's and Wilson's theorems 87
7.7. The residue of $\{\frac{1}{2}(p-1)\}!$ 87
7.8. A theorem of Wolstenholme 88
7.9. The theorem of von Staudt 90
7.10. Proof of von Staudt's theorem 91

VIII. CONGRUENCES TO COMPOSITE MODULI

8.1. Linear congruences 94
8.2. Congruences of higher degree 95
8.3. Congruences to a prime-power modulus 96
8.4. Examples 97
8.5. Bauer's identical congruence 98
8.6. Bauer's congruence: the case $p = 2$ 100
8.7. A theorem of Leudesdorf 100
8.8. Further consequences of Bauer's theorem 102
8.9. The residues of 2^{p-1} and $(p-1)!$ to modulus p^2 104

IX. THE REPRESENTATION OF NUMBERS BY DECIMALS

9.1. The decimal associated with a given number 107
9.2. Terminating and recurring decimals 109
9.3. Representation of numbers in other scales 111
9.4. Irrationals defined by decimals 112
9.5. Tests for divisibility 114
9.6. Decimals with the maximum period 114
9.7. Bachet's problem of the weights 115
9.8. The game of Nim 117
9.9. Integers with missing digits 120
9.10. Sets of measure zero 121
9.11. Decimals with missing digits 122
9.12. Normal numbers 124
9.13. Proof that almost all numbers are normal 125

X. CONTINUED FRACTIONS

10.1. Finite continued fractions 129
10.2. Convergents to a continued fraction 130
10.3. Continued fractions with positive quotients 131
10.4. Simple continued fractions 132
10.5. The representation of an irreducible rational fraction by a simple continued fraction 133
10.6. The continued fraction algorithm and Euclid's algorithm 134
10.7. The difference between the fraction and its convergents 136
10.8. Infinite simple continued fractions 138
10.9. The representation of an irrational number by an infinite continued fraction 139
10.10. A lemma 140
10.11. Equivalent numbers 141
10.12. Periodic continued fractions 143
10.13. Some special quadratic surds 146
10.14. The series of Fibonacci and Lucas 148
10.15. Approximation by convergents 151

此为试读,需要完整PDF请访问: www.ertongbook.com

XI. APPROXIMATION OF IRRATIONALS BY RATIONALS

11.1. Statement of the problem 154
11.2. Generalities concerning the problem 155
11.3. An argument of Dirichlet 156
11.4. Orders of approximation 158
11.5. Algebraic and transcendental numbers 159
11.6. The existence of transcendental numbers 160
11.7. Liouville's theorem and the construction of transcendental numbers 161
11.8. The measure of the closest approximations to an arbitrary irrational 163
11.9. Another theorem concerning the convergents to a continued fraction 164
11.10. Continued fractions with bounded quotients 165
11.11. Further theorems concerning approximation 168
11.12. Simultaneous approximation 169
11.13. The transcendence of e 170
11.14. The transcendence of π 173

XII. THE FUNDAMENTAL THEOREM OF ARITHMETIC IN $k(1)$, $k(i)$, AND $k(\rho)$

12.1. Algebraic numbers and integers 178
12.2. The rational integers, the Gaussian integers, and the integers of $k(\rho)$ 178
12.3. Euclid's algorithm 179
12.4. Application of Euclid's algorithm to the fundamental theorem in $k(1)$ 180
12.5. Historical remarks on Euclid's algorithm and the fundamental theorem 181
12.6. Properties of the Gaussian integers 182
12.7. Primes in $k(i)$ 183
12.8. The fundamental theorem of arithmetic in $k(i)$ 185
12.9. The integers of $k(\rho)$ 187

XIII. SOME DIOPHANTINE EQUATIONS

13.1. Fermat's last theorem 190
13.2. The equation $x^2+y^2 = z^2$ 190
13.3. The equation $x^4+y^4 = z^4$ 191
13.4. The equation $x^3+y^3 = z^3$ 192
13.5. The equation $x^3+y^3 = 3z^3$ 196
13.6. The expression of a rational as a sum of rational cubes 197
13.7. The equation $x^3+y^3+z^3 = t^3$ 199

XIV. QUADRATIC FIELDS (1)

14.1. Algebraic fields 204
14.2. Algebraic numbers and integers; primitive polynomials 205
14.3. The general quadratic field $k(\sqrt{m})$ 206

14.4. Unities and primes 208
14.5. The unities of $k(\sqrt{2})$ 209
14.6. Fields in which the fundamental theorem is false 211
14.7. Complex Euclidean fields 212
14.8. Real Euclidean fields 213
14.9. Real Euclidean fields (*continued*) 215

XV. QUADRATIC FIELDS (2)
15.1. The primes of $k(i)$ 218
15.2. Fermat's theorem in $k(i)$ 219
15.3. The primes of $k(\rho)$ 220
15.4. The primes of $k(\sqrt{2})$ and $k(\sqrt{5})$ 221
15.5. Lucas's test for the primality of the Mersenne number M_{4n+3} 223
15.6. General remarks on the arithmetic of quadratic fields 225
15.7. Ideals in a quadratic field 227
15.8. Other fields 230

XVI. THE ARITHMETICAL FUNCTIONS $\phi(n)$, $\mu(n)$, $d(n)$, $\sigma(n)$, $r(n)$
16.1. The function $\phi(n)$ 233
16.2. A further proof of Theorem 63 234
16.3. The Möbius function 234
16.4. The Möbius inversion formula 236
16.5. Further inversion formulae 237
16.6. Evaluation of Ramanujan's sum 237
16.7. The functions $d(n)$ and $\sigma_k(n)$ 239
16.8. Perfect numbers 239
16.9. The function $r(n)$ 241
16.10. Proof of the formula for $r(n)$ 242

XVII. GENERATING FUNCTIONS OF ARITHMETICAL FUNCTIONS
17.1 The generation of arithmetical functions by means of Dirichlet series 244
17.2. The zeta function 245
17.3. The behaviour of $\zeta(s)$ when $s \to 1$ 246
17.4. Multiplication of Dirichlet series 248
17.5. The generating functions of some special arithmetical functions 250
17.6. The analytical interpretation of the Möbius formula 251
17.7. The function $\Lambda(n)$ 253
17.8. Further examples of generating functions 254
17.9. The generating function of $r(n)$ 256
17.10. Generating functions of other types 257

XVIII. THE ORDER OF MAGNITUDE OF ARITHMETICAL FUNCTIONS
18.1. The order of $d(n)$ 260
18.2. The average order of $d(n)$ 263

18.3. The order of $\sigma(n)$ 266
18.4. The order of $\phi(n)$ 267
18.5. The average order of $\phi(n)$ 268
18.6. The number of squarefree numbers 269
18.7. The order of $r(n)$ 270

XIX. PARTITIONS
19.1. The general problem of additive arithmetic 273
19.2. Partitions of numbers 273
19.3. The generating function of $p(n)$ 274
19.4. Other generating functions 276
19.5. Two theorems of Euler 277
19.6. Further algebraical identities 280
19.7. Another formula for $F(x)$ 280
19.8. A theorem of Jacobi 282
19.9. Special cases of Jacobi's identity 283
19.10. Applications of Theorem 353 285
19.11. Elementary proof of Theorem 358 286
19.12. Congruence properties of $p(n)$ 287
19.13. The Rogers–Ramanujan identities 290
19.14. Proof of Theorems 362 and 363 292
19.15. Ramanujan's continued fraction 294

XX. THE REPRESENTATION OF A NUMBER BY TWO OR FOUR SQUARES
20.1. Waring's problem: the numbers $g(k)$ and $G(k)$ 298
20.2. Squares 299
20.3. Second proof of Theorem 366 299
20.4. Third and fourth proofs of Theorem 366 300
20.5. The four-square theorem 302
20.6. Quaternions 303
20.7. Preliminary theorems about integral quaternions 306
20.8. The highest common right-hand divisor of two quaternions 307
20.9. Prime quaternions and the proof of Theorem 370 309
20.10. The values of $g(2)$ and $G(2)$ 310
20.11. Lemmas for the third proof of Theorem 369 311
20.12. Third proof of Theorem 369: the number of representations 312
20.13. Representations by a larger number of squares 314

XXI. REPRESENTATION BY CUBES AND HIGHER POWERS
21.1. Biquadrates 317
21.2. Cubes: the existence of $G(3)$ and $g(3)$ 318
21.3. A bound for $g(3)$ 319
21.4. Higher powers 320

21.5. A lower bound for $g(k)$ 321
21.6. Lower bounds for $G(k)$ 322
21.7. Sums affected with signs: the number $v(k)$ 325
21.8. Upper bounds for $v(k)$ 326
21.9. The problem of Prouhet and Tarry: the number $P(k, j)$ 328
21.10. Evaluation of $P(k, j)$ for particular k and j 329
21.11. Further problems of Diophantine analysis 332

XXII. THE SERIES OF PRIMES (3)

22.1. The functions $\vartheta(x)$ and $\psi(x)$ 340
22.2. Proof that $\vartheta(x)$ and $\psi(x)$ are of order x 341
22.3. Bertrand's postulate and a 'formula' for primes 343
22.4. Proof of Theorems 7 and 9 345
22.5. Two formal transformations 346
22.6. An important sum 347
22.7. The sum $\sum p^{-1}$ and the product $\prod (1-p^{-1})$ 349
22.8. Mertens's theorem 351
22.9. Proof of Theorems 323 and 328 353
22.10. The number of prime factors of n 354
22.11. The normal order of $\omega(n)$ and $\Omega(n)$ 356
22.12. A note on round numbers 358
22.13. The normal order of $d(n)$ 359
22.14. Selberg's theorem 359
22.15. The functions $R(x)$ and $V(\xi)$ 362
22.16. Completion of the proof of Theorems 434, 6 and 8 365
22.17. Proof of Theorem 335 367
22.18. Products of k prime factors 368
22.19. Primes in an interval 371
22.20. A conjecture about the distribution of prime pairs p, $p+2$ 371

XXIII. KRONECKER'S THEOREM

23.1. Kronecker's theorem in one dimension 375
23.2. Proofs of the one-dimensional theorem 376
23.3. The problem of the reflected ray 378
23.4. Statement of the general theorem 381
23.5. The two forms of the theorem 382
23.6. An illustration 384
23.7. Lettenmeyer's proof of the theorem 387
23.8. Estermann's proof of the theorem 386
23.9. Bohr's proof of the theorem
23.10. Uniform distribution

388
390
394
395

XXIV. GEOMETRY OF NUMBERS

24.1. Introduction and restatement of the fundamental theorem
24.2. Simple applications

24.3. Arithmetical proof of Theorem 448 397
24.4. Best possible inequalities 399
24.5. The best possible inequality for $\xi^2+\eta^2$ 400
24.6. The best possible inequality for $|\xi\eta|$ 401
24.7. A theorem concerning non-homogeneous forms 402
24.8. Arithmetical proof of Theorem 455 405
24.9. Tchebotaref's theorem 405
24.10. A converse of Minkowski's Theorem 446 407

APPENDIX
1. Another formula for p_n 414
2. A generalization of Theorem 22 414
3. Unsolved problems concerning primes 415

A LIST OF BOOKS 417

INDEX OF SPECIAL SYMBOLS AND WORDS 420

INDEX OF NAMES 423

I

THE SERIES OF PRIMES (1)

1.1. Divisibility of integers. The numbers

$$\ldots, -3, -2, -1, 0, 1, 2, \ldots$$

are called the *rational integers*, or simply the *integers*; the numbers

$$0, 1, 2, 3, \ldots$$

the *non-negative integers*; and the numbers

$$1, 2, 3, \ldots$$

the *positive integers*. The positive integers form the primary subject-matter of arithmetic, but it is often essential to regard them as a sub-class of the integers or of some larger class of numbers.

In what follows the letters

$$a, b, \ldots, n, p, \ldots, x, y, \ldots$$

will usually denote integers, which will sometimes, but not always, be subject to further restrictions, such as to be positive or non-negative. We shall often use the word 'number' as meaning 'integer' (or 'positive integer', etc.), when it is clear from the context that we are considering only numbers of this particular class.

An integer a is said to be *divisible* by another integer b, not 0, if there is a third integer c such that

$$a = bc.$$

If a and b are positive, c is necessarily positive. We express the fact that a is divisible by b, or b is a *divisor* of a, by

$$b \mid a$$

Thus

$$1 \mid a, \quad a \mid a;$$

and $b \mid 0$ for every b but 0. We shall also sometimes use

$$b \nmid a$$

to express the contrary of $b \mid a$. It is plain that

$$\begin{cases} b \mid a \;.\; c \mid b \rightarrow c \mid a, \\ \qquad b \mid a \rightarrow bc \mid ac \\ c \mid a \;.\; c \mid b \rightarrow c \mid ma+nb \end{cases}$$

if $c \neq 0$, and for all integral m and n.

1.2. Prime numbers. In this section and until § 2.9 the numbers considered are generally positive integers.† Among the positive integers

† There are occasional exceptions, as in §§ 1.7, where e^x is the exponential function of analysis.

此为试读,需要完整PDF请访问: www.ertongbook.com