AN INTRODUCTION
TO THE
THEORY OF NUMBERS

FIFTH EDITION

BY

G. H. HARDY

AND

E. M. WRIGHT

AN INTRODUCTION TO THE THEORY OF NUMBERS

BY

G. H. HARDY

AND

E. M. WRIGHT

Principal and Vice-Chancellor Emeritus of the University of Aberdeen

FIFTH EDITION

THE ENGLISH LANGUAGE BOOK SOCIETY

AND

OXFORD UNIVERSITY PRESS

1981

Oxford University Press, Walton Street, Oxford OX2 6DP

OXFORD LONDON GLASGOW
NEW YORK TORONTO MELBOURNE WELLINGTON
KUALA LUMPUR SINGAPORE HONG KONG TOKYO
DELHI BOMBAY CALCUTTA MADRAS KARACHI
NAIROBI DAR ES SALAAM CAPE TOWN

First edition 1938
Second edition 1945
Third edition 1954
Fourth edition 1960
Fifth edition 1979
E.L.B.S. edition of fifth edition 1981

Printed in Great Britain
at the University Press, Oxford
by Eric Buckley
Printer to the University

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

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.

$$\rightarrow, \equiv, \exists, \epsilon.$$

$\rightarrow$ 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'.

ϵ is the relation of a member of a class to the class. Thus

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

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. The numbers

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

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

$$0, 1, 2, 3, \dots$$

the *non-negative integers*; and the numbers

$$1, 2, 3, \dots$$

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

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

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

$$b \mid a \,.\, c \mid b \rightarrow c \mid a,$$

$$b \mid a \rightarrow bc \mid ac$$

if $c \neq 0$, and $$c \mid a \,.\, c \mid b \rightarrow c \mid ma+nb$$

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.

there is a sub-class of peculiar importance, the class of primes. A number p is said to be *prime* if

(i) $p > 1$,
(ii) p has no positive divisors except 1 and p.

For example, 37 is a prime. It is important to observe that 1 is not reckoned as a prime. In this and the next chapter we reserve the letter p for primes.†

A number greater than 1 and not prime is called *composite*.

Our first theorem is

THEOREM 1. *Every positive integer, except* 1, *is a product of primes.*

Either n is prime, when there is nothing to prove, or n has divisors between 1 and n. If m is the least of these divisors, m is prime; for otherwise

$$\exists l \,.\, 1 < l < m \,.\, l \mid m;$$

and

$$l \mid m \rightarrow l \mid n,$$

which contradicts the definition of m.

Hence n is prime or divisible by a prime less than n, say p_1, in which case

$$n = p_1 n_1, \qquad 1 < n_1 < n.$$

Here either n_1 is prime, in which case the proof is completed, or it is divisible by a prime p_2 less than n_1, in which case

$$n = p_1 n_1 = p_1 p_2 n_2, \qquad 1 < n_2 < n_1 < n.$$

Repeating the argument, we obtain a sequence of decreasing numbers $n, n_1, \ldots, n_{k-1}, \ldots$, all greater than 1, for each of which the same alternative presents itself. Sooner or later we must accept the first alternative, that n_{k-1} is a prime, say p_k, and then

(1.2.1) $$n = p_1 p_2 \ldots p_k.$$

Thus $$666 = 2.3.3.37.$$

If $ab = n$, then a and b cannot both exceed $\sqrt{n}$. Hence any composite n is divisible by a prime p which does not exceed $\sqrt{n}$.

The primes in (1.2.1) are not necessarily distinct, nor arranged in any particular order. If we arrange them in increasing order, associate sets of equal primes into single factors, and change the notation appropriately, we obtain

(1.2.2) $$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} \quad (a_1 > 0,\ a_2 > 0,\ \ldots,\ p_1 < p_2 < \ldots).$$

We then say that n is expressed in *standard form*.

† It would be inconvenient to have to observe this convention rigidly throughout the book, and we often depart from it. In Ch. IX, for example, we use p/q for a typical rational fraction, and p is not usually prime. But p is the 'natural' letter for a prime, and we give it preference when we can conveniently.