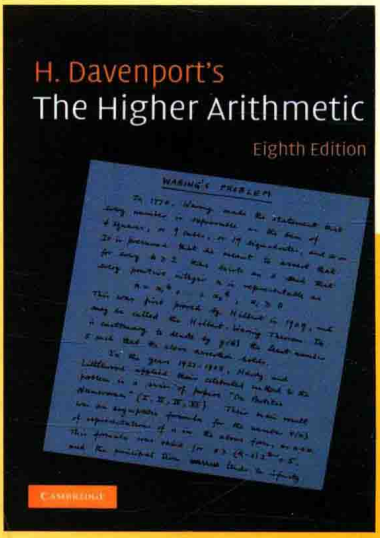
H. Davenport

The Higher Arithmetic

Eighth Edition

高等算术

第8版



CAMBRIDGE

世界图书出版公司
www.wpcbj.com.cn

THE HIGHER ARITHMETIC

AN INTRODUCTION TO THE THEORY OF NUMBERS

Eighth edition

H. Davenport

M.A., SC.D., F.R.S.

late Rouse Ball Professor of Mathematics in the University of Cambridge and Fellow of Trinity College

Editing and additional material by

James H. Davenport

CAMBRIDGE
UNIVERSITY PRESS

图书在版编目（CIP）数据

高等算术：第8版 = The Higher Arithmetic Eighth Edition：英文/（英）达文波特（Davenport，H.）著. —影印本. —北京：世界图书出版公司北京公司，2015.11
ISBN 978-7-5192-0531-7

Ⅰ.①高… Ⅱ.①达… Ⅲ.数论—英文 Ⅳ.①O15

中国版本图书馆CIP数据核字（2015）第287988号

The Higher Arithmetic Eighth Edition
高等算术 第8版

著　　者：H. Davenport
责任编辑：刘　慧　岳利青
装帧设计：任志远

出版发行：世界图书出版公司北京公司
地　　址：北京市东城区朝内大街137号
邮　　编：100010
电　　话：010-64038355（发行）　64015580（客服）　64033507（总编室）
网　　址：http://www.wpcbj.com.cn
邮　　箱：wpcbjst@vip.163.com
销　　售：新华书店
印　　刷：三河市国英印务有限公司
开　　本：711mm×1245mm　1/24
印　　张：10.5
字　　数：202千
版　　次：2016年7月第1版　　2016年7月第1次印刷
版权登记：01-2016-1330
ISBN 978-7-5192-0531-7　　**定价**：45.00元

Now into its eighth edition and with additional material on primality testing, written by J. H. Davenport, *The Higher Arithmetic* introduces concepts and theorems in a way that does not require the reader to have an in-depth knowledge of the theory of numbers but also touches upon matters of deep mathematical significance. A companion website (www.cambridge.org/davenport) provides more details of the latest advances and sample code for important algorithms.

Reviews of earlier editions:

'. . . the well-known and charming introduction to number theory . . . can be recommended both for independent study and as a reference text for a general mathematical audience.'
European Maths Society Journal

'Although this book is not written as a textbook but rather as a work for the general reader, it could certainly be used as a textbook for an undergraduate course in number theory and, in the reviewer's opinion, is far superior for this purpose to any other book in English.'
Bulletin of the American Mathematical Society

INTRODUCTION

The higher arithmetic, or the theory of numbers, is concerned with the properties of the natural numbers 1, 2, 3, ... These numbers must have exercised human curiosity from a very early period; and in all the records of ancient civilizations there is evidence of some preoccupation with arithmetic over and above the needs of everyday life. But as a systematic and independent science, the higher arithmetic is entirely a creation of modern times, and can be said to date from the discoveries of Fermat (1601–1665).

A peculiarity of the higher arithmetic is the great difficulty which has often been experienced in proving simple general theorems which had been suggested quite naturally by numerical evidence. 'It is just this,' said Gauss, 'which gives the higher arithmetic that magical charm which has made it the favourite science of the greatest mathematicians, not to mention its inexhaustible wealth, wherein it so greatly surpasses other parts of mathematics.'

The theory of numbers is generally considered to be the 'purest' branch of pure mathematics. It certainly has very few direct applications to other sciences, but it has one feature in common with them, namely the inspiration which it derives from *experiment*, which takes the form of testing possible general theorems by numerical examples. Such experiment, though necessary in some form to progress in every part of mathematics, has played a greater part in the development of the theory of numbers than elsewhere; for in other branches of mathematics the evidence found in this way is too often fragmentary and misleading.

As regards the present book, the author is well aware that it will not be read without effort by those who are not, in some sense at least, mathematicians. But the difficulty is partly that of the subject itself. It cannot be evaded by using imperfect analogies, or by presenting the proofs in a way

which may convey the main idea of the argument, but is inaccurate in detail. The theory of numbers is by its nature the most exact of all the sciences, and demands exactness of thought and exposition from its devotees.

The theorems and their proofs are often illustrated by numerical examples. These are generally of a very simple kind, and may be despised by those who enjoy numerical calculation. But the function of these examples is solely to illustrate the general theory, and the question of how arithmetical calculations can most effectively be carried out is beyond the scope of this book.

The author is indebted to many friends, and most of all to Professor Erdős, Professor Mordell and Professor Rogers, for suggestions and corrections. He is also indebted to Captain Draim for permission to include an account of his algorithm.

The material for the fifth edition was prepared by Professor D. J. Lewis and Dr J. H. Davenport. The problems and answers are based on the suggestions of Professor R. K. Guy.

Chapter VIII and the associated exercises were written for the sixth edition by Professor J. H. Davenport. For the seventh edition, he updated Chapter VII to mention Wiles' proof of Fermat's Last Theorem, and is grateful to Professor J. H. Silverman for his comments.

For the eighth edition, many people contributed suggestions, notably Dr J. F. McKee and Dr G. K. Sankaran. Cambridge University Press kindly re-typeset the book for the eighth edition, which has allowed a few corrections and the preparation of an electronic complement: `www.cambridge.org/davenport`. References to further material in the electronic complement, when known at the time this book went to print, are marked thus: ♠:0.

CONTENTS

Introduction *page* viii

I Factorization and the Primes 1
1. The laws of arithmetic 1
2. Proof by induction 6
3. Prime numbers 8
4. The fundamental theorem of arithmetic 9
5. Consequences of the fundamental theorem 12
6. Euclid's algorithm 16
7. Another proof of the fundamental theorem 18
8. A property of the H.C.F 19
9. Factorizing a number 22
10. The series of primes 25

II Congruences 31
1. The congruence notation 31
2. Linear congruences 33
3. Fermat's theorem 35
4. Euler's function $\phi(m)$ 37
5. Wilson's theorem 40
6. Algebraic congruences 41
7. Congruences to a prime modulus 42
8. Congruences in several unknowns 45
9. Congruences covering all numbers 46

III Quadratic Residues 49
1. Primitive roots 49
2. Indices 53
3. Quadratic residues 55
4. Gauss's lemma 58
5. The law of reciprocity 59
6. The distribution of the quadratic residues 63

IV Continued Fractions 68
1. Introduction 68
2. The general continued fraction 70
3. Euler's rule 72
4. The convergents to a continued fraction 74
5. The equation $ax - by = 1$ 77
6. Infinite continued fractions 78
7. Diophantine approximation 82
8. Quadratic irrationals 83
9. Purely periodic continued fractions 86
10. Lagrange's theorem 92
11. Pell's equation 94
12. A geometrical interpretation of continued fractions 99

V Sums of Squares 103
1. Numbers representable by two squares 103
2. Primes of the form $4k + 1$ 104
3. Constructions for x and y 108
4. Representation by four squares 111
5. Representation by three squares 114

VI Quadratic Forms 116
1. Introduction 116
2. Equivalent forms 117
3. The discriminant 120
4. The representation of a number by a form 122
5. Three examples 124
6. The reduction of positive definite forms 126
7. The reduced forms 128
8. The number of representations 131
9. The class-number 133

VII Some Diophantine Equations 137
1. Introduction 137
2. The equation $x^2 + y^2 = z^2$ 138
3. The equation $ax^2 + by^2 = z^2$ 140
4. Elliptic equations and curves 145
5. Elliptic equations modulo primes 151
6. Fermat's Last Theorem 154
7. The equation $x^3 + y^3 = z^3 + w^3$ 157
8. Further developments 159

VIII Computers and Number Theory 165
1. Introduction 165
2. Testing for primality 168
3. 'Random' number generators 173
4. Pollard's factoring methods 179
5. Factoring and primality via elliptic curves 185
6. Factoring large numbers 188
7. The Diffie–Hellman cryptographic method 194
8. The RSA cryptographic method 199
9. Primality testing revisited 200

Exercises 209
Hints 222
Answers 225

Bibliography 235

Index 237

I

FACTORIZATION AND THE PRIMES

1. *The laws of arithmetic*

The object of the higher arithmetic is to discover and to establish general propositions concerning the natural numbers $1, 2, 3, \ldots$ of ordinary arithmetic. Examples of such propositions are the fundamental theorem (I.4)* that *every natural number can be factorized into prime numbers in one and only one way*, and Lagrange's theorem (V.4) that *every natural number can be expressed as a sum of four or fewer perfect squares*. We are not concerned with numerical calculations, except as illustrative examples, nor are we much concerned with numerical curiosities except where they are relevant to general propositions.

We learn arithmetic experimentally in early childhood by playing with objects such as beads or marbles. We first learn addition by combining two sets of objects into a single set, and later we learn multiplication, in the form of repeated addition. Gradually we learn how to calculate with numbers, and we become familiar with the laws of arithmetic: laws which probably carry more conviction to our minds than any other propositions in the whole range of human knowledge.

The higher arithmetic is a deductive science, based on the laws of arithmetic which we all know, though we may never have seen them formulated in general terms. They can be expressed as follows.

* References in this form are to chapters and sections of chapters of this book.

Addition. Any two natural numbers a and b have a *sum*, denoted by $a + b$, which is itself a natural number. The operation of addition satisfies the two laws:

$$a + b = b + a \quad \textit{(commutative law of addition)},$$
$$a + (b + c) = (a + b) + c \quad \textit{(associative law of addition)},$$

the brackets in the last formula serving to indicate the way in which the operations are carried out.

Multiplication. Any two natural numbers a and b have a *product*, denoted by $a \times b$ or ab, which is itself a natural number. The operation of multiplication satisfies the two laws

$$ab = ba \quad \textit{(commutative law of multiplication)},$$
$$a(bc) = (ab)c \quad \textit{(associative law of multiplication)}.$$

There is also a law which involves operations both of addition and of multiplication:

$$a(b + c) = ab + ac \quad \textit{(the distributive law)}.$$

Order. If a and b are any two natural numbers, then either a is equal to b or a is *less than* b or b is *less than* a, and of these three possibilities exactly one must occur. The statement that a is less than b is expressed symbolically by $a < b$, and when this is the case we also say that b is greater than a, expressed by $b > a$. The fundamental law governing this notion of order is that

$$\textit{if} \quad a < b \quad \textit{and} \quad b < c \quad \textit{then} \quad a < c.$$

There are also two other laws which connect the notion of order with the operations of addition and multiplication. They are that

$$\textit{if} \quad a < b \quad \textit{then} \quad a + c < b + c \quad \textit{and} \quad ac < bc$$

for any natural number c.

Cancellation. There are two laws of cancellation which, though they follow logically from the laws of order which have just been stated, are important enough to be formulated explicitly. The first is that

$$\textit{if} \quad a + x = a + y \quad \textit{then} \quad x = y.$$

This follows from the fact that if $x < y$ then $a + x < a + y$, which is contrary to the hypothesis, and similarly it is impossible that $y < x$, and therefore $x = y$. In the same way we get the second law of cancellation, which states that

$$\textit{if} \quad ax = ay \quad \textit{then} \quad x = y.$$

Subtraction. To subtract a number b from a number a means to find, if possible, a number x such that $b + x = a$. The possibility of subtraction is related to the notion of order by the law that *b can be subtracted from a if and only if b is less than a.* It follows from the first cancellation law that if subtraction is possible, the resulting number is unique; for if $b + x = a$ and $b + y = a$ we get $x = y$. The result of subtracting b from a is denoted by $a - b$. Rules for operating with the minus sign, such as $a - (b - c) = a - b + c$, follow from the definition of subtraction and the commutative and associative laws of addition.

Division. To divide a number a by a number b means to find, if possible, a number x such that $bx = a$. If such a number exists it is denoted by $\frac{a}{b}$ or a/b. It follows from the second cancellation law that if division is possible the resulting number is unique.

All the laws set out above become more or less obvious when one gives addition and multiplication their primitive meanings as operations on sets of objects. For example, the commutative law of multiplication becomes obvious when one thinks of objects arranged in a rectangular pattern with a rows and b columns (fig. 1); the total number of objects is ab and is also ba. The distributive law becomes obvious when one considers the arrangement of objects indicated in fig. 2; there are $a(b + c)$ objects altogether and these are made up of ab objects together with ac more objects. Rather less obvious, perhaps, is the associative law of multiplication, which asserts that $a(bc) = (ab)c$. To make this apparent, consider the same rectangle as in fig. 1, but replace each object by the number c. Then the sum of all the numbers in any one row is bc, and as there are a rows the total sum is $a(bc)$. On the other hand, there are altogether ab numbers each of which is c, and therefore the total sum is $(ab)c$. It follows that $a(bc) = (ab)c$, as stated.

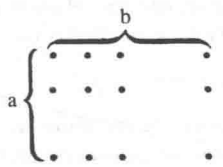


Fig. 1

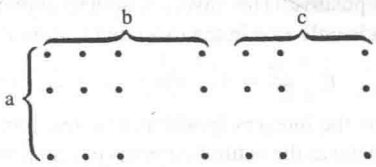


Fig. 2

The laws of arithmetic, supplemented by the principle of induction (which we shall discuss in the next section), form the basis for the logical development of the theory of numbers. They allow us to prove general theorems about the natural numbers without it being necessary to go back to the primitive meanings of the numbers and of the operations carried out

on them. Some quite advanced results in the theory of numbers, it is true, are most easily proved by counting the same collection of things in two different ways, but there are not very many such.

Although the laws of arithmetic form the logical basis for the theory of numbers (as indeed they do for most of mathematics), it would be extremely tedious to refer back to them for each step of every argument, and we shall in fact assume that the reader already has some knowledge of elementary mathematics. We have set out the laws in detail in order to show where the subject really begins.

We conclude this section by discussing briefly the relationship between the system of natural numbers and two other number-systems that are important in the higher arithmetic and in mathematics generally, namely the *system of all integers* and the *system of all rational numbers*.

The operations of addition and multiplication can always be carried out, but those of subtraction and division cannot always be carried out within the natural number system. It is to overcome the limited possibility of subtraction that there have been introduced into mathematics the number 0 and the negative integers $-1, -2, \ldots$. These, together with the natural numbers, form the system of all integers:

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

within which subtraction is always possible, with a unique result. One learns in elementary algebra how to define multiplication in this extended number-system, by the 'rule of signs', in such a way that the laws of arithmetic governing addition and multiplication remain valid. The notion of order also extends in such a way that the laws governing it remain valid, with one exception: the law that if $a < b$ then $ac < bc$ remains true only if c is positive. This involves an alteration in the second cancellation law, which is only true in the extended system if the factor cancelled is not 0:

$$\textit{if} \quad ax = ay \quad \textit{then} \quad x = y, \quad \textit{provided that} \quad a \neq 0.$$

Thus the integers (positive, negative and zero) satisfy the same laws of arithmetic as the natural numbers except that subtraction is now always possible, and that the law of order and the second cancellation law are modified as just stated. The natural numbers can now be described as the *positive integers*.

Let us return to the natural numbers. As we all know, it is not always possible to divide one natural number by another, with a result which is itself a natural number. If it is possible to divide a natural number b by a natural number a within the system, we say that a is a *factor* or *divisor* of b, or that b is a *multiple* of a. All these express the same thing. As illustrations

of the definition, we note that 1 is a factor of every number, and that a is itself a factor of a (the quotient being 1). As another illustration, we observe that the numbers divisible by 2 are the even numbers $2, 4, 6, \ldots$, and those not divisible by 2 are the odd numbers $1, 3, 5, \ldots$.

The notion of divisibility is one that is peculiar to the theory of numbers, and to a few other branches of mathematics that are closely related to the theory of numbers. In this first chapter we shall consider various questions concerning divisibility which arise directly out of the definition. For the moment, we merely note a few obvious facts.

(i) *If a divides b then $a \leqq b$* (that is, a is either less than or equal to b). For $b = ax$, so that $b - a = a(x - 1)$, and here $x - 1$ is either 0 or a natural number.

(ii) *If a divides b and b divides c then a divides c.* For $b = ax$ and $c = by$, whence $c = a(xy)$, where x and y denote natural numbers.

(iii) *If two numbers b and c are both divisible by a, then $b + c$ and $b - c$ (if $c < b$) are also divisible by a.* For $b = ax$ and $c = ay$, whence

$$b + c = a(x + y) \text{ and } b - c = a(x - y).$$

There is no need to impose the restriction that $b > c$ when considering $b - c$ in the last proposition, if we extend the notion of divisibility to the integers as a whole in the obvious way: an integer b is said to be divisible by a natural number a if the quotient $\frac{b}{a}$ is an integer. Thus a negative integer $-b$ is divisible by a if and only if b is divisible by a. Note that 0 is divisible by every natural number, since the quotient is the integer 0.

(iv) *If two integers b and c are both divisible by the natural number a, then every integer that is expressible in the form $ub + vc$, where u and v are integers, is also divisible by a.* For $b = ax$ and $c = ay$, whence $ub + vc = (ux + vy)a$. This result includes those stated in (iii) as special cases; if we take u and v to be 1 we get $b + c$, and if we take u to be 1 and v to be -1 we get $b - c$.

Just as the limitation on the possibility of subtraction can be removed by enlarging the natural number system through the introduction of 0 and the negative integers, so also the limitation on the possibility of division can be removed by enlarging the natural number system through the introduction of all positive fractions, that is, all fractions $\frac{a}{b}$, where a and b are natural numbers. If both methods of extension are combined, we get the *system of rational numbers*, comprising all integers and all fractions, both positive and negative. In this system of numbers, all four operations

of arithmetic—addition, multiplication, subtraction and division—can be carried out without limitation, except that division by zero is necessarily excluded.

The main concern of the theory of numbers is with the natural numbers. But it is often convenient to work in the system of all integers or in the system of rational numbers. It is, of course, important that the reader, when following any particular train of reasoning, should note carefully what kinds of numbers are represented by the various symbols.

2. *Proof by induction*

Most of the propositions of the theory of numbers make some assertion about every natural number; for example Lagrange's theorem asserts that every natural number is representable as the sum of at most four squares. How can we prove that an assertion is true for *every natural number*? There are, of course, some assertions that follow directly from the laws of arithmetic, as for instance algebraic identities like

$$(n+1)^2 = n^2 + 2n + 1.$$

But the more interesting and more genuinely arithmetical propositions are not of this simple kind.

It is plain that we can never prove a general proposition by verifying that it is true when the number in question is 1 or 2 or 3, and so on, because we cannot carry out infinitely many verifications. Even if we verify that a proposition is true for every number up to a million, or a million million, we are no nearer to establishing that it is true always. In fact it has sometimes happened that propositions in the theory of numbers, suggested by extensive numerical evidence, have proved to be wide of the truth.

It may be, however, that we can find a *general argument* by which we can prove that *if* the proposition in question is true for all the numbers

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

then it is true for the next number, n. If we have such an argument, then the fact that the proposition is true for the number 1 will imply that it is true for the next number, 2; and then the fact that it is true for the numbers 1 and 2 will imply that it is true for the number 3, and so on indefinitely. The proposition will therefore be true for every natural number if it is true for the number 1.

This is the principle of proof by induction. The principle relates to propositions which assert that something is true for every natural number, and in order to apply the principle we need to prove two things: first, that the

assertion in question is true for the number 1, and secondly that *if* the assertion is true for each of the numbers $1, 2, 3, \ldots, n-1$ preceding any number n, *then* it is true for the number n. Under these circumstances we conclude that the proposition is true for every natural number.

A simple example will illustrate the principle. Suppose we examine the sum $1 + 3 + 5 + \cdots$ of the successive odd numbers, up to any particular one. We may notice that

$$1 = 1^2, 1 + 3 = 2^2, 1 + 3 + 5 = 3^2, 1 + 3 + 5 + 7 = 4^2,$$

and so on. This suggests the general proposition that *for every natural number n, the sum of the first n odd numbers is* n^2. Let us prove this general proposition by induction. It is certainly true when n is 1. Now we have to prove that the result is true for any number n, and by the principle of induction we are entitled to suppose that it is already known to be true for any number less than n. In particular, therefore, we are entitled to suppose that we already know that the sum of the first $n - 1$ odd numbers is $(n - 1)^2$. The sum of the first n odd numbers is obtained from this by adding the nth odd number, which is $2n - 1$. So the sum of the first n odd numbers is

$$(n - 1)^2 + (2n - 1),$$

which is in fact n^2. This proves the proposition generally.

Proofs by induction are sometimes puzzling to the inexperienced, who are liable to complain that 'you are assuming the proposition that is to be proved'. The fact is, of course, that a proposition of the kind now under consideration is a proposition with an infinity of cases, one for each of the natural numbers $1, 2, 3, \ldots$; and all that the principle of induction allows us to do is to suppose, when proving any one case, that the preceding cases have already been settled.

Some care is called for in expressing a proof by induction in a form which will not cause confusion. In the example above, the proposition in question was that *the sum of the first n odd numbers is* n^2. Here n is any one of the natural numbers, and, of course, the statement means just the same if we change n into any other symbol, provided we use the same symbol in the two places where it occurs. But once we have embarked on the proof, n becomes a particular number, and we are then in danger of using the same symbol in two senses, and even of writing such nonsense as 'the proposition is true when n is $n - 1$'. The proper course is to use different symbols where necessary.

From a commonsense point of view, nothing can be more obvious than the validity of proof by induction. Nevertheless it is possible to debate whether the principle is in the nature of a *definition* or a *postulate* or an *act*