The Theory of Numbers

Robert D. Carmichael

1914

Editors' Preface

The volume called Higher Mathematics, the third edition of which was published in 1900, contained eleven chapters by eleven authors, each chapter being independent of the others, but all supposing the reader to have at least a mathematical training equivalent to that given in classical and engineering colleges. The publication of that volume was discontinued in 1906, and the chapters have since been issued in separate Monographs, they being generally enlarged by additional articles or appendices which wither amplify the former presentation or record recent advances. This plan of publication was arranged in order to meet the demand of teachers and the convenience of classes, and it was also though that it would prove advantageous to readers in special lines of mathematical literature.

It is the intention of the publishers and editors to add other monographs to the series from time to time, if the demand seems to warrant it. Among the topics which are under consideration are those of elliptic functions, the theory of quantics, the group theory, the calculus of variations, and non-Euclidean geometry; possible also monographs on branches of astronomy, mechanics, and mathematical physics may be included. It is the hope of the editors that this Series of Monographs may tend to promote mathematical study and research over a wider field than that which the former volume has occupied.

Preface

The purpose of this little book is to give the reader a convenient introduction to the theory of numbers, one of the most extensive and most elegant disciplines in the whole body of mathematics. The arrangement of the material is as follows: The first five chapters are devolted to the development of those elements which are essential to any study of the subject. The sixth and last chapter is intended to give the reader some indication of the direction of further study with a brief account of the nature of the material in each of the topics suggested. The treatment throughout is made as brief as is possible consistent with clearness and is confined entirely to fundamental matters. This is done because it is believed that in this way the book may best be made to serve its purpose as an introduction to the theory of numbers.

Numerous problems are supplied throughout the text. These have been selected with great care so as to serve as excellent exercises for the student's introductory training in the methods of number theory and to afford at the same time a further colledction of useful results. The exercises marked with a star are more difficult than the others; they will doubtless appeal to the best students.

Finally, I should add that this book is made up from the material used by me in lectures in Indiana University during the past two years; and the selection of matter, especiially of exercises, has been based on the experience gained in this way.

R. D. Carmichael

Contents

Editors' Preface i

Preface ii

1 Elementary Properties of Integers 1

1.1 Fundamental Notions and Laws 1

1.2 Definition of Divisibility. The Unit 2

1.3 Prime Numbers. The Sieve of Eratosthenes 3

1.4 The Number of Primes is Infinite 5

1.5 The Fundamental Theorem of Euclid 6

1.6 Divisibility by a Prime Number 6

1.7 The Unique Factorization Theorem 7

Chapter 1

Elementary Properties of Integers

1.1 Fundamental Notions and Laws

In the present chapter we are concerned primarily with certain elementary properties of the postive integers 1, 2, 3, 4, ... It will sometimes be convenient, when no confusion can arise, to employ the word *integer* or the word *number* in the sense of positive integer.

We shall suppose that the integers are already defined, either by the process of counting or otherwise. We assume further that the meaning of the terms *greater, less, equal, sum, difference, product* is known.

From the ideas and definitions thus assumed to be known follow immediately the theorems:

I. The sum of any two integers is an integer.

II. The difference of any two integers is an integer.

III. The product of any two integers is an integer.

Other fundamental theorems, which we take without proof, are embodied in the following formulas: Here *a, b, c* denote any positive integers.

IV. $a + b = b + a.$

V. $a \times b = b \times a.$

VI. $(a + b) + c = a + (b + c).$

VII. $(a \times b) \times c = a \times (b \times c).$

VIII. $a \times (b + c) = a \times b + a \times c.$

These formulas are equivalent in order to the following five theorems: addition is commutatigve; multiplication is communtative; addition is associative; multiplication is associative; multiplicationis distributive with respect to addition.

EXERCISES

1. Prove the following relations:

$$\begin{aligned} 1+2+3\cdots+n &= \frac{n(n+1)}{2} \\ 1+3+5+\cdots+(2n-1) &= n^2, \\ 1^3+2^3+3^3+\cdots+n^3 &= \left(\frac{n(n+1)}{2}\right)^2 = (1+2+\cdots+n)^2. \end{aligned}$$

2. Find the sum of each of the following series:

$$\begin{aligned} &1^2+2^2+3^2+\cdots+n^2, \\ &1^2+3^2+5^2+\cdots+(2n-1)^2, \\ &1^3+3^3+5^3+\cdots+(2n-1)^3. \end{aligned}$$

3. Discover and establish the law suggested by the equations $1^2 = 0+1, 2^2 = 1+3, 3^2 = 3+6, 4^2 = 6+10, \ldots$; by the equations $1 = 1^3, 3+5 = 2^3, 7+9+11 = 3^3, 13+15+17+19 = 4^3, \ldots$.

1.2 Definition of Divisibility. The Unit

Definitions. An integer a is said to be divisible by an integer b if there exists an integer c such that $a = bc$. It is clear from this definition that a is also divisible by c. The integers b and c are said to be divisors or factors of a; and a is said to be a multiple of b or of c. The process of finding two integers b and c such that bc is equal to a given integer a is called the process of resolving a into factors or of factoring a; and a is said to be resolved into factors or to be factored.

We have the following fundamental theorems:

I. *If b is a dividsor of a and c is a divisor of b, then c is a divisor of a.*

Since b is a divisor of a there exists an integer β such that $a = b\beta$. Since c is a divisor of b there exists an integer γ such that $b = c\gamma$. Substituting this value of b in the equation $a = b\gamma$ we have $a = c\gamma\beta$. But from theorem III of §1.1 it follows that $\gamma\beta$ is an integer; hence, c is a divisor of a, as was to be proved.

II. *If c is a divisor of both a and b, then c is a divisor of the sum of a and b.*

From the hypothesis of the theorem it follows that integers α β exist such that

$$a = c\alpha, \quad b = c\beta.$$

Adding, we have

$$a + b = c\alpha + c\beta = c(\alpha + \beta) = c\delta,$$

where δ is an integer. Hence, c is a divisor of $a + b$.

III. *If c is a divisor of both a and b, then c is a divisor of the difference of a and b.* The proof is analogous to that of the preceding theorem.

Definitions. If a and b are both divisible by c, then c is said to be a common divisor or a common factor of a and b. Every two integers have the common factor 1. The greatest integer which divides both a and b is called the greatest common divisor of a and b. More generally, we define in a similar way a common divisor and the greatest common divisor of n integers $a_1, a_2, \dots, a_n$.

Definitions. If an integer a is a multiple of each of two or more integers it is called a common multiple of these integers. The product of any set of integers is a common multiple of the set. The least integer which is a multiple of each of two or more integers is called their least common multiple.

It is evident that the integer 1 is a divisor of every integer and that it is the only integer which has this property. It is called the unit.

Definition. Two or more integers which have no common factor except 1 are said to be prime to each other or to be relatively prime.

Definition. If a set of integers is such that no two of them have a common divisor besides 1 they are said to be prime each to each.

EXERCISES

1. Prove that $n^3 - n$ is divisble by 6 for every positive integer n.
2. If the product of four consecutive integers is increased by 1 the result is a square number.
3. Show that $2^{4n+1} + 1$ has a factor different from itself and 1 when n is a positive integer.

1.3 Prime Numbers. The Sieve of Eratosthenes

Definition. If an integer p is different from 1 and has no divisor except itself and 1 it is said to be a prime number or to be a prime.

Definition. An integer which has at least one divisor other than itself and 1 is said to be a composie number or to be composite.

All integers are thus divided into three class:

1. The unit;
2. Prime numbers;

3. Composite numbers.

We have seen that the first class contains only a single number. The third class evidently contains an infinitude of numbers; for, it contains all the numbers $2^2, 2^3, 2^4, \ldots$. In the next section we shall show that the second class also contains an infinitude of numbers. We shall now show that every number of the third class contains one of the second class as a factor, by proving the following theorem:

I. *Every integer greater than 1 has a prime factor.*

Let m be an integer which is greater than 1. We have to show that it has a prime factor. If m is prime there is the prime factor m itself. If m is not prime we have

$$m = m_1 m_2$$

where m_1 and m_2 are positive integers both of which are less than m. If either m_1 or m_2 is prime we have thus obtained a prime factor of m. If neither of these numbers is prime, then write

$$m_1 = m_1' m_2', \quad m_1' > 1, mz - 2' > 1.$$

Both m_1' and m_2' are factors of m and each of them is less than m_1. Either we have not found in m_1 or m_2 a prime factor of m or the process can be continued by separating one of these numbers into factors. Since for any given m there is evidently only a finite number of steps possible, it is clear that we must finally arrive at a prime factor of m. From this conclusion, the theorem follows immediately.

Eratosthenes has given a useful means of finding the prime numbers which are less than any given integer m. It may be described as follows:

Every prime except 2 is odd. Hence if we write down every odd number from 3 up to m we shall have it the list every prime less than m except 2. Now 3 is prime. Leave it in the list; but beginning to count from 3 strike out every theird number in the list. Thus every number divisible by 3, except 3 itself, is cancelled. Then begin from 5 and cancel every fifth number. Then begin from the next uncancelled number, namely 7, and strike out every seventh number. Then begin from the next uncancelled number, namely 11, and strike out every eleventh number. Proceed in this way up to m. The uncancelled numbers remaining will be the odd primes not greater than m.

It is obvious that this process of cancellation need not be carred altogether so far as indicated; for if p is a prime greater than $\sqrt{m}$, the cancellation of any p^{th} number from p will merely be a repetition of cancellations effect by means of another factor smaller than p, as one may see by the use of the following theorem.

II. *An integer m is prime if it has no prime factor equal or less than I, where I is the greatest integer whose square is equal to or less than m.*

Since m has no prime factor less than I, it follows from theorem I that it has no factor but unity less than I. Hence, if m is not prime it must be the product of two numbers each greater than I; and hence it must be equal to or greater than$(I + 1)^2$. This contradicts the hypothesis on I; and hence we conclude that m is prime.

EXERCISE

By means of the method Eratosthenes determine the primes less than 200.

1.4 The Number of Primes is Infinite

I. *The number of primes is infinite.*

We shall prove this theorem by supposing that the number of primes is not infinite and showing that this leads to a contradiction. If the number of primes is not infinite there is a greatest prime number, which we shall denote by p. Then form the number

$$N = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot p + 1.$$

Now by theorem 1 of §1.3 N has a prime divisor q. But every non-unit divisor of N is obviously greater than p. Hence q is greater than p, in contradiction to the conclusion that p is the greatest prime. Thus the proof of the theorem is complete.

In a similar way we may prove the following theorem:

II. *Among the integers of the arithmetic progression* 5, 11, 17, 23, …, *there is an infinite number of primes.*

If the number of primes in this sequence is not infinite there is a greatest prime number in the sequence; supposing that this greatest prime number exists we shall denot it by p. Then the number N,

$$N = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot p - 1,$$

is not divisible by any number less than or equal to p. This number N, which is of the form $6n - 1$, has a prime factor. If this factor is of the form $6k - 1$ we have already reached a contradiction, and our theorem is proved. If the prime is of the form $6k_1 + 1$ the complementary factor is of the form $6k_2 - 1$. Every prime factor of $6k_2 - 1$ is greater than p. Hence we may treat $6k_2 - 1$ as we did $6n - 1$, and with a like result. Hence we must ultimately reach a prime factor of the form $6k_3 - 1$; for, otherwise, we should have $6n - 1$ expressed as a product of prime factors all of the form $6t + 1$–a result which is clearly impossible. Hence we must in any case reach a contradiction of the hypothesis. Thus the theorem is proved.

III. *Among the integers of the arithmetic progression* $a, a + d.a + 2d.a + 3d, \ldots$, *there is an infinite number of primes, provided that* a *and* b *are relatively prime.*

For the special case given in theorem III we have an elementary proof; but for the general theorem the proof is difficult. We shall not give it here.

EXERCISES

1. Prove that there is an infinite number of primes of the form $4n - 1$.

2. Show that an odd prime number can be represented as the difference of two squares in one and in only one way.

3. The expression $m^p - n^p$, in which m and n are integers and p is a prime, is either prime to p or is divisible by p^2.

4. Prove that any number except 2 and 3 is of one of the forms $6n+1,\ 6n-1$.

1.5 The Fundamental Theorem of Euclid

If a and b are any two positive integers there exist integers q and r, $q \geqq 0, 0 \leqq r < b$ such that

$$a = qb + r.$$

If a is a multiple of b the theorem is at once verified, r being in this case 0. If a is not a multiple of b it must lie between two consecutive multiples of b; that is, if exists a q such that

$$qb < a < (q+1)b.$$

Hence there is an integer r, $0 < r < b$, such that $a = qb + r$. In case b is greater than a it is evident that $q = 0$ and $r = a$. Thus the proof of the theorem is complete.

1.6 Divisibility by a Prime Number

I. *If p is a prime number and m is any integer, then m either is divisble by p or is prime to p.*

This theorem follows at once from the fact that the only divisors of p are 1 and p.

II. *The product of two integers each less than a given prime number p is not divisible by p.*

Let a be a number which is less than p suppose that b is a number less that p such that ab is divisible by p, and let b be the least number for which ab is so divisible. Evidently there exists an integer m such that

$$mb < p < (m+1)b.$$

Then $p - mb < b$. Since ab is divisible by p it is clear that mab is divisible by p; so is ap also; and hence their difference $ap - mab = a(p - mb)$, is divisible by p. That is, the product of a by an integer less than b is divisible by p, contrary to the assumption that b is the least integer such that ab is divisible by p. The assumption that the theorem is not true has thus led to a contradiction; and thus the theorem is proved.

III. *If neither of two integers is divisible by a given prime number p their product is not divisible by p.*

Let a and b be two integers neither of which is divisible by the prime p. According to the fundamental theorem of Euclid there exist integers m, n, α, β such that

$$\begin{aligned} a &= mp + \alpha, \qquad 0 &< \alpha < p, \\ b &= np + \beta, \qquad 0 &< \beta < p. \end{aligned}$$

Then

$$ab = (mp + \alpha)(np + \beta) = (mnp + \alpha + \beta)p + \alpha\beta.$$

If now we suppose ab to be divisible by p we have $\alpha\beta$ divisible by p. This contradicts II, since α and β are less than p. Hence ab is not divisible by p.

By an application of this theorem to the continued product of several factors, the following result is readily obtained:

IV. *If no one of several integers is divisible by a given prime p their product is not divisible by p.*

1.7 The Unique Factorization Theorem