NUMBER THEORY AND ITS HISTORY

By Oystein Ore

STERLING PROFESSOR OF MATHEMATICS
YALE UNIVERSITY

NEW YORK TORONTO LONDON
McGRAW-HILL BOOK COMPANY, INC.
1948

NUMBER THEORY AND ITS HISTORY

Abacist vs. Algorismist

From Gregor Reisch: Margarita Philosophica
Strassbourg 1504

PREFACE

This book is based upon a course dealing with the theory of numbers and its history which has been given at Yale for several years. Although the course has been attended primarily by college students in their junior and senior years it has been open to all interested. The lectures were intended to give the principal ideas and methods of number theory as well as their historical background and development through the centuries. Most texts on number theory contain inserted historical notes but in this course I have attempted to obtain a presentation of the results of the theory integrated more fully in the historical and cultural framework. Number theory seems particularly suited to this form of exposition, and in my experience it has contributed much to making the subject more informative as well as more palatable to the students.

Obviously, only some of the main problems of number theory could be included in this book. In making a selection, topics of systematic and historical importance capable of a simple presentation have been preferred. While many standard aspects of number theory had to be discussed, the treatment is often new, and much material has been added that has not heretofore made its appearance in texts. Also, in several instances I have found it desirable to introduce and define modern algebraic concepts whose usefulness is readily explained by the context.

The questions of number theory are of importance not only to mathematicians. Now, as in earlier days, these problems seem to possess a particular attraction for many laymen, and number theory is notable as one of the few fields of mathematics where the suggestions and conjectures of amateurs or nonprofessional mathematicians have exerted an appreciable influence. It may be mentioned incidentally that there have been few college classes that I can recall in which there were not to be found some students

who had already played with the strange properties of numbers. To make the theory available to readers whose mathematical knowledge may be limited, every effort has been made to reduce to a minimum the technical complications and mathematical requirements of the presentation. Thus, the book is of a more elementary character than many previous texts, and for the understanding of a greater part of the subject matter a knowledge of the simplest algebraic rules should be sufficient. Only in some of the later chapters has a more extended familiarity with mathematical manipulations been presupposed.

I am indebted to Prof. Otto Neugebauer for valuable comments on the historical material and to Paul T. Bateman for numerous suggestions for mathematical improvements that have been embodied in the text. In reading the proofs I was assisted by M. Gerstenhaber and E. V. Schenkman, who have also checked the numerical computations.

ØYSTEIN ORE

NEW HAVEN, CONN.
August, 1948

NUMBER THEORY AND ITS HISTORY

CONTENTS

Chapter 5. The Aliquot Parts

Chapter 6. Indeterminate Problems

Chapter 7. Theory of Linear Indeterminate Problems

Chapter 8. Diophantine Problems

Chapter 9. Congruences

Chapter 10. Analysis of Congruences

Chapter 11. Wilson's Theorem and Its Consequences

Chapter 12. Euler's Theorem and Its Consequences

Chapter 13. Theory of Decimal Expansions

Chapter 14. The Converse of Fermat's Theorem

Chapter 15. The Classical Construction Problems

CHAPTER 1

COUNTING AND RECORDING OF NUMBERS

1–1. Numbers and counting. All the various forms of human culture and human society, even the most rudimentary types, seem to require some concept of *number* and some process for *counting*. According to the anthropologists, every people has some terminology for the first numbers, although in the most primitive tribes this may not extend beyond two or three. In a general way one can say that the process of counting consists in matching the objects to be counted with some familiar set of objects like fingers, toes, pebbles, sticks, notches, or the number words. It may be observed that the counting process often goes considerably beyond the existing terms for numerals in the language.

1–2. Basic number groups. Almost all people seem to have used their fingers as the most convenient and natural counters. In many languages this is easily recognized in the number terminology. In English we still use the term *digits* for the numerals. For numbers exceeding 10 the toes have quite commonly been used as further counters.

Very early in the cultural development it became necessary to perform more extensive counts to determine the number of cattle, of friends and foes, of days and years, and so on. To handle larger figures the counting process must be systematized. The first step in this direction consists in arranging the numbers into convenient *groups*. The choice of such basic groups depends naturally on the matching process used in counting.

The great preponderance of people use a basic *decimal* or *decadic group* of 10 objects, as one should expect from counting on the

fingers. The word for 10 often signifies *one man*. *Quinary systems* based on groups of 5 or *one hand* also occur, but the *vigesimal systems* based on a 20 group are much more common, corresponding of course to a complete count of fingers and toes. Among the American Indian peoples the vigesimal system was in widespread use; best known is the well-developed Mayan system. One finds traces of a 20 system in many other languages. We still count in *scores*. The French *quatre-vingt* for 80 is a remnant of a previously more extensive 20 count. In Danish the 20 system is still used systematically for the names of numbers less than 100.

The largest known basic number, 60, is found in the *Babylonian sexagesimal system*. It is difficult to explain the reasons for such a large unit group. It has been suggested by several authors that it is the result of a merger of two different number systems. We still use this system when measuring time and angles in minutes and seconds. Other basic numbers than those mentioned here are quite rare. We may detect a trace of a 12 or *duodecimal system* in our counts in dozens and gross. Certain African tribes use basic groups of 3 and 4. The *binary* or *dyadic system*, in which 2 or a pair is the basic concept, has been used in a rudimentary form by Australian indigenes. The dyadic system is, however, a system whose simple properties often have a special mathematical usefulness.

1–3. The number systems. When the basic counting group is fixed, the numbers exceeding the first group would be obtained by counting afresh in a new group, then another, and so on. For instance, in a quinary system where the basic five group might be called one *h*(*and*), one would count one *h*. and one, one *h*. and two, 2*h*. (10), 3*h*. and 2 (17), and so on. After one had reached five hands (25), one might say *hand of hands* (*h.h.*) and begin over again. So as an example, one would denote 66 by 2*hh* and 3*h* and 1, that is, $2 \times 25 + 3 \times 5 + 1$. Clearly this process can be extended indefinitely by introducing higher groups

$$hhh = 125 = 5^3, \qquad hhhh = 625 = 5^4$$

In this manner one arrives at a representation of any number as an expression

$$a_n \cdot 5^n + a_{n-1} \cdot 5^{n-1} + \cdots + a_2 \cdot 5^2 + a_1 \cdot 5 + a_0 \quad (1\text{–}1)$$

where each coefficient a_i is one of the numbers 0, 1, 2, 3, 4.

To be quite correct, one should observe that this particular example historically is fictitious, since no people is known to have developed and used a completely general system (1–1) with the base 5. But this systematic procedure for the construction of a number system was certainly the guiding principle in the evolution of our decadic number system and of many other systems. To confirm this assertion further one can turn to the philological analysis of our number terms. Through the laws of comparative linguistics one can trace a word like *eleven* to *one left over*, and similarly *twelve* to *two over*. There is some indication that our fundamental word *ten* may be derived from an Indo-European root meaning *two hands*. The word *hundred* comes from an original term *ten times* (*ten*). It is further interesting to note that the names for *thousand* are unrelated in the various main branches of the Indo-European languages; hence it is probably a rather late construction. The word itself seems to be derived from a Proto-Germanic term signifying *great hundred*.

In our decadic system all numbers are put in a form analogous to (1–1)

$$a_n \cdot 10^n + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \quad (1\text{–}2)$$

where the coefficients take values from 0 to 9. In general, in the subsequent chapters, we shall understand by a *number system with the base b* a system in which we represent the numbers in the form

$$a_n \cdot b^n + \cdots + a_2 \cdot b^2 + a_1 \cdot b + a_0 \quad (1\text{–}3)$$

where the coefficients a_i are numbers from 0 to $b - 1$.

It should be mentioned that relatively few peoples developed their number systems to this perfection. Also, in many languages one finds other methods for the construction of numbers. As an example of irregular construction let us mention that in Welsh the

number words from 15 to 19 indicate 15, $15 + 1$, $15 + 2$, 2×9, $15 + 4$. Subtraction occurs often as a method; for instance, in Latin, *un-de-viginti* $= 20 - 1 = 19$, *duo-de-sexaginta* $= 60 - 2 = 58$. Similar forms exist in Greek, Hindu, Mayan, and other languages.

The Mayan number system was developed to unusually high levels, but the system has one peculiar irregularity. The basic group is 20, but the group of second order is not $20 \times 20 = 400$ as one should expect, but $20 \times 18 = 360$. This appears to be connected with the division of the Mayan year into 18 months each consisting of 20 days, supplemented with 5 extra days. The higher groups in the system are

$$360 \times 20, \quad 360 \times 20^2, \cdots$$

1–4. Large numbers. As one looks at the development of number systems in retrospect it seems fairly simple to construct arbitrarily large numbers. However, in most systems the span of numbers actually used is very limited. Everyday life does not require very large numbers, and in many languages the number names do not go beyond thousands or even hundreds. We mentioned above that the term one thousand seems to have made a relatively late appearance in the Indo-European languages. The Greeks usually stopped at a *myriad* or ten thousand. For a long period the Romans did not have names or symbols for groups above 100,000. There exists in Rome an inscription on the Columna Rostrata commemorating the victory over Carthage at Mylae in the year 260 B.C. in which 31 symbols for 100,000 were repeated to signify 3,100,000. The Hindus had a peculiar attraction to large numbers, and immense figures occur commonly in their mythological tales and also in many of their algebraic problems. As a consequence, there existed particular names for the higher decadic groups to very great powers of 10. For instance, in a myth from the life of Buddha one finds the denominations up to 10^{153}.

Even our own number system has not been developed systematically to this extent. The word for one *million* is a fairly recent

construction, which seems to have originated in Italy around A.D. 1400. The concept one *billion* has not found its final niche in our system. In American and sometimes in French terminology this means one thousand millions (10^9) while in most other countries of the world one billion is one million millions (10^{12}), while one thousand millions is called a *milliard*. It is probably only through the expenditures of the world wars that numbers of this size have reached such common use that confusion is likely to occur. When a *billion* is defined to be a thousand millions, a *trillion* becomes one thousand billions (10^{12}), a *quadrillion* one thousand trillions, and so on. On the other hand when a billion is one million millions, one million billions is a *trillion* (10^{18}), one million trillions is a *quadrillion* (10^{24}), and so on. While this discrepancy is not apt to cause any serious misunderstandings in everyday life, some universal agreement on usage and nomenclature would, nevertheless, be desirable.

The intellectual effort that lies behind a systematic extension of the number system is well illustrated by the fact that Archimedes (278–212 B.C.), the most advanced Greek mathematician, deems it worth while to devote a whole treatise, *The Sand Reckoning*, to this purpose. This work is addressed to his relative, King Gelon of Syracuse, and begins as follows:

> There are some, King Gelon, who think that the number of grains of sand is infinite in multitude; and I mean by the sand not only that which exists about Syracuse and the rest of Sicily, but also that which is found in every region, whether inhabited or uninhabited. Again there are some, who, without regarding it as infinite, nevertheless think that no number has been named which is great enough to exceed its size.

Under this guise of aiming at finding a number exceeding the totality of grains of sand in the universe, as then known, Archimedes proceeds to construct a systematic enumeration method for arbitrarily high numbers.

1–5. Finger numbers. For the communication of numbers from one individual to another it is often desirable to have some other representation than the vocal expressions of the number

names in the language. We now mainly use *written numbers*, a representation which we shall study subsequently. Before the advent of a fairly general writing ability the *finger numbers* were widely used as a universal numerical language. The numbers were indicated by means of different positions of fingers and hands. In a rudimentary way we still occasionally express numbers by our fingers. The finger numbers were in use in Europe both in the classical period and in the Middle Ages; they were used by the Greeks, Romans, Arabs, Hindus, and many other people. The human figures in ancient drawings and statues often show peculiar finger positions which denote numbers. For instance, Pliny states that the statue of Janus on the Forum in Rome represented the number 365, the days in the year, on its fingers.

In the Orient the finger numbers are still in common use. They enable buyers and sellers in the bazaars to bargain about prices independent of language differences. When the bargainers cover their hands with a piece of cloth, the finger numbers have the added advantage that the negotiations are secret to other parties.

Our best information about finger numbers in early times is due to the works of the Venerable Bede (A.D. 673–735), an English Benedictine monk from the cloisters in Wearmouth and Jarrow. His treatise *De temporum ratione* deals with the rules for calculating the date of Easter, and as an introduction it contains a description of the use of finger numbers (Fig. 1–1). The finger numbers were probably only in actual use for fairly moderate figures. Bede's numbers have a natural limit of 10,000, but he enlarges the method rather artificially so that it becomes possible to express numbers up to 1,000,000. To some limited extent it was possible to calculate with finger numbers. In Europe they seem to have disappeared gradually with the ascendency of the Hindu-Arabic number system.

1–6. Recordings of numbers. Neither the spoken numbers nor the finger numbers have any permanency. To preserve numbers for the purpose of records it is necessary to have other representations. Furthermore, without some memory aids the performance of calculations is extremely difficult.

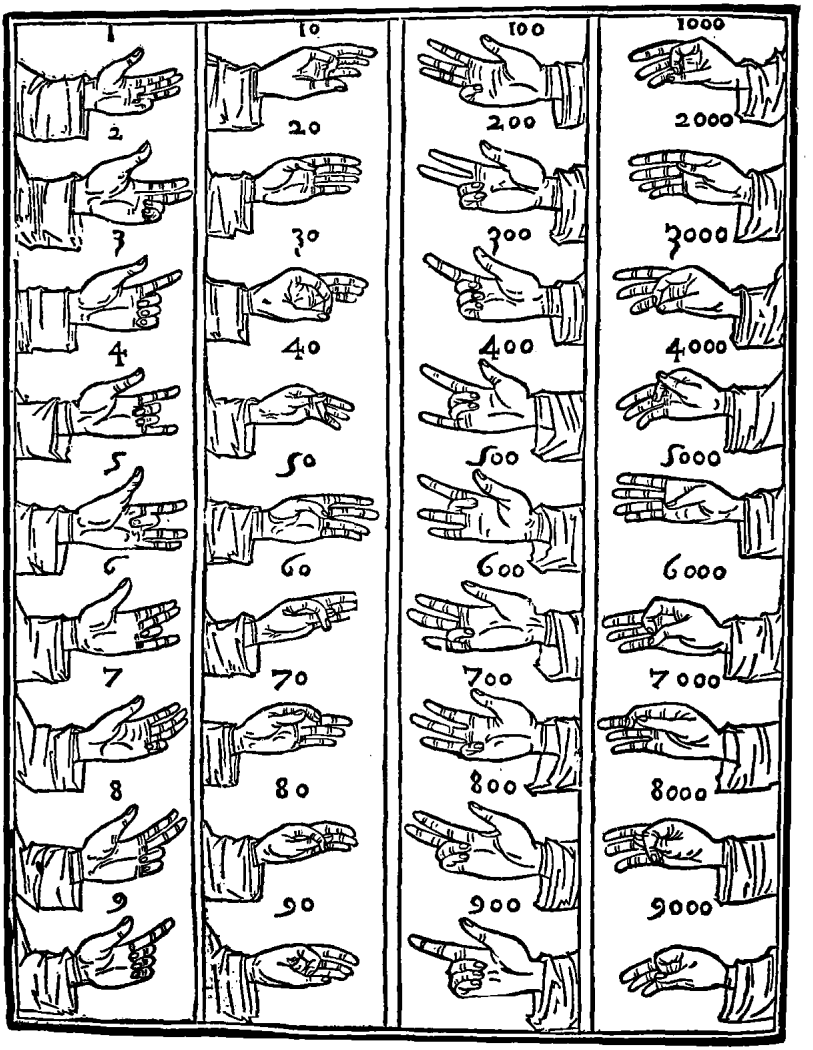

FIG. 1–1. Finger numbers. (*From Luca di Burgo Pacioli, Summa de arithmetica geometria, second edition, Venice,* 1523. *Courtesy of D. E. Smith Collection, Columbia University.*)