DICKSON'S HISTORY OF THE THEORY OF NUMBERS.

History of the Theory of Numbers. By LEONARD EUGENE DICKSON. Volume I. Carnegie Institution of Washington, 1919. 486 pp.

IN these days when "pure" science is looked upon with impatience, or at best with good-humored indulgence, the appearance of such a book as this will be greeted with joy by those of us who still believe in mathematics for mathematics' sake, as we do in art for art's sake or for music for the sake of music. For those who can see no use or importance in any studies in mathematics which do not smack of the machine shop or of the artillery field it may be worth while to glance through the index of authors in this volume and note the frequent appearance of names of men whose work in the "practical applications" of mathematics would almost qualify them for a place on the faculty of our most advanced educational institutions. One of the most assiduous students of the theory of numbers was Euler, whose work otherwise was of sufficient importance to attract the notice of a king of Prussia. The devotee of this peculiar branch of science can reassure himself that he is in very good company when he reads the list of authors cited in connection with the famous theorems of Fermat and Wilson in Chapter III; Cauchy, Cayley, d'Alembert, Dedekind, Euler, Gauss, Jacobi, Kronecker, Lagrange, Laplace, Legendre, Leibniz, Steiner, Sylvester, Von Staudt and a host of others, great and small, living and dead, to the number of over two hundred, who have found these absolutely "useless" theorems worthy of their most serious attention. The reviewer is firm in the faith that no great headway will ever be made in any science, least of all in mathematics, by those who are always looking for the penny. He takes comfort also in the fact that great teachers are not found among those who are scornful of mathematics for mathematics' sake. Their race is not likely to be perpetuated, and the chances are that the study of the theory of numbers will become increasingly popular as the years go by.

One is struck in glancing through the book by the remarkable combination of superstition, fancy, scientific curiosity, and patient, plodding experiment that has figured in advancing the science of the theory of numbers. Thus, in the first chapter, which has to do with the theory of perfect numbers, the first name that appears is that of Euclid, who proved that if $p = 1 + 2 + 2^2 + \cdots + 2^n$ is a prime then $2^n p$ is a perfect number, that is, a number which is equal to the sum of its aliquot parts. This solid contribution of Euclid's is followed by fanciful speculations regarding the ethical import of such numbers! "Alcuin of York and Tours explained the occurrence of the number 6 in the creation of the universe on the ground that 6 is a perfect number. The second origin of the human race arose from the deficient number 8. Indeed, in Noah's ark there were eight souls from which sprung the entire human race, showing that the second origin was more imperfect than the first, which was made according to the number 6."

The requirement that p be a prime was soon overlooked by such mystics and we have a long series of writers who state that perfect numbers always end alternately in 6 and 8, and that between any two successive powers of 10 one such number is always to be found. These errors, which would have been discovered by a little patient experiment, persist among writers on the subject till the days of experimental workers like Cataldi, who noted that the fifth and sixth perfect numbers both end in 6. To get this result it was necessary for him to show that 8191 and 131071 were both primes, which he did by the straightforward method of trying as divisors every prime less than their respective square roots. Thus early in the theory arises the fundamental problem; to discover the prime factors of a given number. It was the discovery of a method for factoring such numbers as $a^n \pm 1$ that gave Fermat such power in the investigations concerning perfect numbers, so that, for example, he was able to state that there is no perfect number of 20 or of 21 digits, contrary to the opinion of those who believed that there was a perfect number between any two powers of 10. The efforts of mathematicians since Fermat have resulted in identifying twelve perfect numbers of the type $2^{n-1}(2^n - 1)$ corresponding to the following twelve values of n: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127. The work still goes on. $2^{67} - 1$ was proved composite by Lucas in 1876. The actual factors were not found, however, till 1903, when Professor Cole found them to be 193707721 and 761838257287. The existence of odd perfect numbers has not been as yet proved or disproved.

Chapter II gives the history of the formulas for the number and sum of the divisors of a number, together with the problems proposed by Fermat (*a*) to find a cube which when increased by the sum of its aliquot parts becomes a square, and (*b*) to find a square which when increased by its aliquot parts becomes a cube. A third problem, due to Wallace, is also treated: to find two squares, other that 16 and 25, such that if each is increased by the sum of its aliquot parts the resulting sums are equal. Among the contributors to the history of these matters we note Cardan, Mersenne, Newton, Waring, Descartes, Euler, Kronecker, and others.

Chapter III is devoted to Fermat's and Wilson's theorems, their converses and their generalizations, together with theorems on the symmetric functions of $1, 2, 3, \cdots, p-1$ modulo p. The chapter begins with the astonishing statement that the Chinese seem to have known as early as 500 B.C. that $2^n - 2$ is divisible by n (n a prime). This important theorem, rediscovered some two thousand years later by Fermat, has been the center of an immense amount of activity, beginning with Leibniz who left a proof of it in manuscript. Whether, as Mahnke, who made a careful study of the Leibniz manuscripts seems to believe, Leibniz discovered the theorem independently, before he became acquainted in 1681–2 with Fermat's Varia Opera of 1679, or whether he heard of the theorem when he was in Paris in 1672 or when he was in London in 1673 is a question worth study. There would seem to be no reason to doubt, however, that the manuscript proof of Leibniz is the earliest known, and that to Leibniz also belongs the discovery as early as 1682 of the theorem known as Wilson's theorem, the first published proof of which was given by Lagrange, nearly a century later.

The function $a^{n-1} - 1$ which Fermat found to be always divisible by n is sometimes divisible by n^2, as for example when $n = 11$ and $a = 3$. The question as to when this phenomenon appears was raised by Abel, answered with numerical examples by Jacobi, and studied by Eisenstein, Sylvester and many others. The question has a bearing on Fermat's last theorem, as is shown by Wieferich's theorem that if $x^n + y^n + z^n = 0$

is satisfied by integers x, y, z, prime to n (n an odd prime) then $2^{n-1} - 1$ is divisible by n^2. Chapter IV gives the literature on this subject.

Chapter V is another long one on Euler's φ-function and generalizations of it, together with the related theory of Farey series. Few other functions of analysis have been studied with such enthusiasm by mathematicians of the first rank, and the many remarkable applications of it to other branches of analysis and to geometry are well indicated in this chapter. Euler's function has had an amusing history as to its name and the notation for it. Euler himself gave it no name and at first no notation, later using the notation $\pi(n)$ to denote the number of integers less than n and prime to it. With this definition, of course, $\pi(1) = 0$. If we define the function as the number of integers not greater than n and having with n the greatest common divisor 1 then $\pi(1) = 1$ and this value of the function of unity fits most easily in with formulas connected with it. Gauss introduced the symbol $\varphi(n)$, which seems to have a good chance of becoming permanent. Prouhet proposed the name indicator and the notation $i(n)$, which has had some adherents among French writers in spite of the fact that the name was already preempted for another function by Cauchy. Sylvester named the function the totient function and denoted it by $\tau(n)$. This name with Gauss' notation has been very extensively used among American writers. The literature of this function is so great that students and teachers will find this chapter very valuable, as also the shorter Chapter VI on periodic decimal fractions. An immense amount of work is necessary to discover what others have done in these fields.

Among the by-products in the study of expressions of the form $a^n - 1$, which is itself a by-product of the theory of perfect numbers, are the theories of primitive roots, binomial congruences, more general congruences, Galois imaginaries, and periodic decimal fractions. These matters are treated in Chapters VI, VII, VIII. Chapter VI, on periodic decimal fractions, and Chapter XX on properties of the digits of numbers, as well as much of Chapter XI, come under what might perhaps be called the metrical theory of numbers, having to do with properties which depend on the base employed to represent them.

The theory of the divisibility of factorial expressions seems to have been studied for the first time by Leibniz, who noted in his manuscript that the multinomial coefficients except the first appearing in the expansion of $(a + b + c + \cdots)^n$, where n is a prime, are divisible by n. Legendre followed with a formula for the highest power of a prime to be found in $m!$. The later contributions to this subject are found in Chapter IX.

One of the most interesting of Euler's many discoveries is the formula relating to $\sigma(n)$, the sum of the divisors of n. The values of this function for $n = 1, 2, 3, 4, 5, 6, 7$ are 1, 3, 4, 7, 6, 12, 8 and no one but an Euler would have been able to find any simple law connecting such an irregular series of numbers. It is interesting to find him with his eye always turned toward the fundamental problem of finding the factors of numbers. Even this formula he uses to prove that 101 is a prime. He finds that his formula gives him 102 for the sum, whence he concludes that 101 is a prime. This method should be, but is not, listed among the tests for primality in Chapter XVIII. As it stands it is of no practical use for that problem, but neither is Wilson's theorem, for that matter. In any event it is remarkable that the primality of a number should be made to depend on the sums of the divisors of a certain set of smaller numbers. Chapter X is particularly valuable as giving a list of formulas, scattered through many journals, some of which are given by one author without proof and proved or disproved by others. It is difficult for the ordinary worker to run them down. The theory of partitions, which has such important connection with this subject, is to be given a chapter in Volume II.

Chapter XI is a list of miscellaneous theorems on divisibility and theorems on the greatest common divisor and the least common multiple. Here is indeed a mixture of important work like the results of Cesàro, Gegenbauer, de la Vallée Poussin, Landau, Dedekind and Kronecker, side by side with the amusing note that the consecutive numbers, 242, 243, 244, 245 have each a square factor greater than unity. Here are found also many approximative or asymptotic formulas such as $6x/\pi^2$ for the number of integers not greater than x and divisible by no square greater than unity, the error being less than the square root of x. The history of the familiar rule for casting out 9's and 11's is reserved for Chapter XII, which after giving a faithful account of this matter winds up with a list of over two pages of titles not reported on.

The history of factor tables and lists of primes given in Chapter XIII begins again in the remote days of Eratosthenes. The net result of over twenty centuries of labor seems to be that the list of primes up to ten million is determined with a high degree of accuracy thanks to the work of men drawn from many different races and nations. Some day, perhaps, a machine may be constructed to extend the list further, but the methods used for computing the tables already in existence will hardly serve for higher limits. It should be clearly understood by anyone who contemplates further work in this field that the most troublesome and tedious part of the work lies not so much in the computation as in the actual printing and proof-reading of the results.

There is perhaps no problem in the theory of numbers more fascinating to the scientist, or wider in its appeal to all sorts and conditions of men, than the problem of finding a method for factoring numbers which shall be better than the straightforward one of trying as divisors the primes less than the square root. The invention of a new instrument for studying the heavens must appeal in much the same way to the astronomer. One can easily imagine the delight which Fermat must have taken in his method of factoring a number by expressing it as the difference of two squares. It is one of the few discoveries of the illustrious Frenchman which he condescends to describe in detail. He later improved on this method and found others much more powerful for dealing with numbers of certain forms. Euler was also an indefatigable worker in this direction. He showed by some six pages of calculations that the number 1000081 is expressible in only one way as the sum of two squares and so must be a prime. "Dolendum autem est" he mourns, "hanc methodum non ad omnes numeros explorandos adhiberi posse." He proceeded to extend the method to representation by means of other binary quadratic forms, thus developing the most powerful tool now in our possession for this purpose. Legendre supplemented this method by employing the continued fraction for finding representations of the number. Gauss invented a method of exclusion, and Seelhoff made tables for the same purpose. Many other methods have been proposed, some of which are very successful if the factors are related in particular ways.

An account of all these methods is given in Chapter XIV, while in Chapters XV and XVI appear methods applicable to numbers of special forms like $2^{2n} + 1$ and $a^n \pm b^n$.

In the early years of the thirteenth century Leonardo Pisano noticed the series of numbers 1, 2, 3, 5, 8, 13, $\cdots$, each of which is the sum of the two preceding it. The study of this series and of others like it has yielded many important results. Lucas has hit upon a general theory which includes these series. The whole theory is connected with the theory of linear difference equations with constant coefficients and also with the theory of continued fractions. Chapter XVII gives *the history of this important subject.*

The existence of an infinitude of primes has been known since Euclid. That there are an infinite number of them in any arithmetical progression $mx + n$ where m and n are relatively prime was not proved until 1837, when Dirichlet established it by a very difficult analysis. Dirichlet also found that any primitive binary quadratic form can represent an infinitude of primes. Much important work centers in these great discoveries. Of equal difficulty and importance is the problem of finding either exactly or by an approximative formula the number of primes between given limits. The history of these problems is contained in Chapter XVIII together with the literature connected with Goldbach's conjecture, still neither proved or disproved, that every even number is the sum of two primes. Bertrand's postulate, proved by Tchebycheff, that there is at least one prime between x and $2x - 2$ for x greater than 3 is also treated in this chapter. One can not fail to be impressed with the immense fields of analysis drawn upon in the attacks on these problems.

Chapter XIX gives the history of the function $\mu(n)$ of Moebius which is useful in the inversion of series, and plays an important rôle in the derivation of many approximative formulas.

The last chapter (XX) is devoted to the listing of many curious and amusing properties of numbers, properties chiefly connected with the representation to the base 10. It is hardly likely that any important results will flow from the study of problems like finding numbers like $512 = (5 + 1 + 2)^3$ but such little things serve sometimes to attract students to more serious things.

It may, perhaps, be objected that the book is not so much a history as a list of references from which a history of the theory of numbers might be written. Be that as it may, there is the greatest need for just such a piece of work to promote efficiency among the professional workers in this field and to prevent them from wasting their time on problems that have already been adequately treated, and also to suggest other problems which still defy analysis. It is to be hoped that the second volume will not be long delayed.

D. N. LEHMER.

THE CALCULUS OF PROBABILITY.

Calcolo delle Probabilità. By GUIDO CASTELNUOVO. Albrighi, Segati & C., Milano-Roma-Napoli, 1919. xxiii + 373 pp.

THE increased interest in the calculus of probability which has arisen during the past fifty years has been due in no small part to the brilliant applications of it in the field of physical phenomena. One of the most important of these, first in point of time and a model for the others, is due to Maxwell and has to do with the distribution of velocities of the molecules of a gas. Some of these investigations of physical phenomena on the basis of the laws of probability, operating under an assumed absence of determining physical laws among certain groups of phenomena, have been so successful in accounting for or predicting physical events that the conception has arisen in some quarters of the "laws of nature" as merely certain statements of average among fortui ous occurrences. It is almost uncanny to find relatively constant results of measurements of certain sorts predicted by a mathematical analysis based essentially on an assumption of chance distribution; and yet this is found in not a few important investigations.

A paradoxical situation of this sort will always excite interest. The human mind is peculiarly uncomfortable in the presence of a demonstrated result and an intuitive feeling between which there seems to be disharmony. A disturbance of our equilibrium is produced when we see the theory of probability thus accounting for what seemed to be fixed relations among phenomena. Where there is lack of equilibrium there is