BOOK REVIEWS

Elementary Number Theory. By J. V. Uspensky and M. A. Heaslet. New York and London, McGraw-Hill, 1939. 10+484 pp.

Numerous historical references and applications of the theory presented, as well as detailed proofs, make this book especially suited to novices in the field. As noted in the introduction "owing to self-imposed limitations in the size of the book, many topics of interest had to be omitted." Analytical and geometrical methods have been avoided, while topics such as continued fractions and integral transformations of forms have been omitted entirely. On the other hand the book covers with thoroughness various fundamental problems which have inspired much of the research in this field. The results are illustrated by numerous examples, some solved in the text, others left to the reader.

The first five chapters are devoted to various problems which can be readily treated without the use of congruences. In fact, the notion of congruence is deferred until the sixth chapter when the reader has become familiar with a number of the fundamental concepts of number theory. The first chapter contains a discussion of elementary properties of integers, a method of computing polygonal numbers, and a discussion of scales of notation. It also contains an analysis, in terms of binary representations of numbers, of the generalized Chinese game of Nim. In the second chapter there is a treatment of common divisors and multiples, and a solution of the Diophantine equation $x^2+y^2=z^2$ in integers. The third chapter contains Lame's theorem, Euclid's least remainder algorithm, and application of this algorithm to the solution of linear Diophantine equations. The fourth chapter is devoted to a discussion of prime numbers. The topics considered are the sieve of Eratosthenes, the unique factorization theorem, the number and sum of divisors of an integer, perfect numbers, Mersennes's numbers, and the distribution of primes. In the fifth chapter there is a discussion of relative primeness, and in particular of Euler's function $\phi(n)$ and Moebius's function $\mu(n)$, with results based on a well known combinatorial theorem. This theorem is applied to the problem of determining the number of primes less than a given integer, and the chapter closes with Meissel's formula for this number.

After the introduction of the concept of "congruence," Chapter 6 is devoted to Fermat's theorem concerning the congruence $a^{p-1}\equiv 1$ (mod p) and the Euler generalization on $a^{\phi(m)}\equiv 1$ (mod m). Several proofs are given for Fermat's theorem, followed by Gauss's proof of Wilson's theorem. Chapter 6 is followed by an appendix on the problem of constructing magic squares with the solution based on the notion of congruence. In Chapter 7 the authors discuss the number of roots of polynomial congruences of arbitrary degree with application to the theory of residues of lth powers of a prime p. First degree Diophantine equations treated in the third chapter are solved here by a little known method due to Voronoi. The chapter closes with the Chinese method for solving sets of linear congruences in one unknown. The theory of linear congruences is applied in an appendix on calendars. Chapter 8 is devoted to residues of powers with special emphasis on primitive roots and indices, and there is an application to the solution of congruences. The concept of "exponent to which a number a belongs modulo m" is applied in an appendix on card shuffling. In Chapter 10 the authors take up various aspects of the theory of quadratic residues. The chapter is concerned primarily with two fundamental problems: Is a number a a quadratic residue or non-residue of a given prime p, and for what prime moduli is a given number a a quadratic residue or non-residue? The first problem is solved by means of a criterion of Euler. For $a=-1$, 2 and -2 the second is solved by elementary direct methods. Legendre and Jacobi's symbols are introduced, and the corresponding quadratic reciprocity laws are proved. The chapter ends with the solution of general quadratic congruences.

In Chapter 11 the authors develop some special aspects of the theory of quadratic forms. The chapter begins with a discussion of Fermat's equation $t^2-au^2=1$, wrongly attributed by Euler to Pell, and the generalization $x^2-ay^2=m$ of this equation. The results are applied to determine conditions that a given number m be prime. The chapter contains Kummer's proof of the reciprocity law based on Fermat's equation, and Dickson's proof that each integer is a sum of four squares. In Chapter 12 results of earlier chapters are applied to special Diophantine equations, such as $x^2+ay^2=z^m$, $x^2+c=y^3$. This is followed by a proof that the equation $x^4+y^4=z^2$ has no solution in integers none of which is zero, a proof accomplished by the standard technique of showing that if $x^4+y^4=z^2$ has a solution (x_1, y_1, z_1), this equation has a solution (x_2, y_2, z_2) with $z_2<z_1$. The final chapter (Chapter 13) is devoted to the general arithmetical identities proved by Liouville by elementary methods. These identities are used to prove that the primes of the form $8k+1$ or $8k+3$ are sums of a square and the double of a square, and are also employed to give an elementary proof of Jacobi's result on the number of repre-

sentations of an integer as a sum of four squares. Finally, a proof, based on these identities, is given for the theorem of Gauss that all integers except those of the form $4^k(8N+7)$, $k \geqq 0$, are representable as a sum of three squares. The idea of this proof goes back to Kronecker.

An exception to the other chapters of the book which form a closely knit and well-integrated unit is Chapter 9 on Bernoulli numbers. This chapter is independent of the rest of the book except for a minor reference to it later. The chapter treats some fundamental properties of Bernoulli numbers. In particular, the authors give Staudt's theorem on the fractional parts of Bernoulli numbers, and use a theorem of Voronoi to yield information on the types of factors which occur in the numerators and denominators of Bernoulli numbers. The chapter ends with Kummer's congruence on Bernoulli's numbers. There are no applications.

Although the style is clear and detailed, more clarity would have been obtained if there had been uniformity in the statement of the theorems and corollaries. Sometimes the theorems and corollaries are incorporated in the text, with a part of the proof, while in other places the theorems and corollaries stand out in paragraphs by themselves. In the treatment of roots of polynomial congruences one misses the important notion of a "field of numbers," since some of the results, such as that a congruence of degree n with prime modulus has no more than n incongruent roots, are merely theorems valid for any field of numbers and in particular for modular fields. The use of the concept of field, so lacking in books on number theory, would emphasize the importance of many of the problems considered. Some number theorists might take exception to the statement, pages 19–20, "The theory of numbers, unlike some other branches of mathematics, is a purely theoretical science without practical applications." Although certainly deficient in this sense compared with other fields of mathematics, such problems as the calendar problems considered in this text seem to fall in the class of practical applications. Historians might take exception to the statement, page 20, "Pierre de Fermat (1601–1665) was the first man to discover really deep properties of numbers."

We mention a few errors that came to our attention. In line 2 from the bottom of page 18 the following phrase "$r_3+s_3=4\leqq k$, so that we adjoin the number 3, and change the units in column l_3 to 0's" should read "$r_3+s_3=4>k$, whence we change one zero in column l_3 to 1." On page 19 the columns (which we write as rows) *, 0, $1\rightarrow 0$, $1\rightarrow 0$, $1\rightarrow 0$, 0, 0 and $0110<1110$, $0110<1101$, $0100<1001$, $10<11$, 100, 10, /440, should read *, 0→1, 1, 1, 1, 0, 0 and 0111<1110, 0111<1101, 0101<1001, 11, 100, 10, /444, respectively. The expression "$n \geqq 4$," line 7, page 89, should read "$10 > n \geqq 4$." In line 15, page 100, the symbol $[n/]$ should be $[n/p]$. On page 194, line 2, the phrase "modulo p^{a-1}" should follow "is congruent." On page 299 the symbol $(p_1\, q)$ in the 9th line from the bottom should read (p_1/q), and $[(p_k - 1)/2]$ in line 3 from the bottom should read $[(p_i - 1)/2]$.

On the whole the authors have succeeded in presenting number theory in a fascinating and highly instructive manner. Their work will fill an important place in the literature.

RUFUS OLDENBURGER

Differential Geometrien in den Kugelräumen. Vol. 1. *Konforme Differentialgeometrie von Liouville und Möbius.* By T. Takasu. Tokyo, Maruzen, 1938. 18+457 pp.

This handsome textbook gives a comprehensive account of the differential geometries in spaces in which spheres are taken as spatial element. It is the outgrowth of a series of fundamental investigations in which the author has been engaged since 1924, and which have, so far, been laid down in 47 papers. He has also used, in the widest and most generous sense of the word, the work of other authors, which he lists in an extensive and probably complete bibliography of 202 titles. This book is, therefore, the most authoritative source on the subject, and the reader will at the same time be pleased with the variety and beauty of the results and amazed at the thoroughness of the work.

The main body of research already has been published in various "Science Reports of the Tôhoku Imperial University," beginning in March, 1928. The present volume often follows the previous publications, but also departs from it, giving more material and more references. The author, in the preface, gives his own classification of the different geometries as derived from Lie's geometry of the spheres, embracing several types of conformal geometry, including that of Laguerre, of affine, and of non-euclidean geometry. We repeat his fundamental principle as follows:

"1. The conformal space of Möbius is a non-euclidean space with movable absolute spheres, hence also with variable curvature.

"2. The space of Laguerre is a euclidean space with movable absolute circles, hence also with variable unit of angular measurement.

"3. The space of Lie is a conformal space with a movable absolute complex of spheres and at the same time a dual-conformal space