REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

The numbers in brackets are assigned according to the American Mathematical Society classification scheme. The 1980 Mathematics Subject Classification (1985 Revision) can be found in the December index volumes of Mathematical Reviews.

1[11-02].—Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985, xiv + 304 pp., $23\frac{1}{2}$ cm. Price $18.95.

This is the third edition of a book which has become something of a classic. The first edition, reviewed in [1], is a most entertaining introductory text on number theory, organized around a collection of problems, some famous and some not so famous. The second edition, reviewed in [2], contains an additional chapter (Chapter 4), describing the considerable progress which had been made on a number of the problems mentioned in the original edition. The style of this chapter is different from that of the earlier volume in that most of the topics are given a rather brief treatment and several references are provided. Thus, the number of references cited in the second edition increased to 154 from the 34 cited in the first.

The volume under review is the same as the second edition except for the inclusion of a second progress report in Chapter 4. The emphasis of this entire book is on computational number theory, and some indication of the increase in activity in this area of research can be obtained by noting that the second progress report is almost twice as long as the first. Also, there are now 236 entries in the bibliography.

The organization of the material in the second progress report is somewhat different from that of the first. While the latter is, for the most part, a simple compendium of results, the former is really made up of two interesting essays. One of these is about judging conjectures and the other discusses computing and algorithms. The points made in these essays are driven home by the use of many examples taken from recent computational and theoretical work in number theory.

Shanks feels that the word *conjecture* ought to be reserved for an abbreviation of the following statement by a conjecturer.

> "I think this proposition is true but know of no proof for it. I state this seriously, not casually. I have studied the question and examined all the numerical evidence and the heuristic argumentation that is known to me. It is my judgement, based upon this evidence and my current knowledge of the subject that, to a high degree of probability, this proposition is true. If I thought that this evidence were insufficient to warrant this conclusion I would not call this proposition a conjecture. If I were to bet on it I would offer odds."

©1987 American Mathematical Society
0025-5718/87 $1.00 + $.25 per page

After offering this definition he goes on to justify it by using several illustrative examples and anecdotes. Indeed, he goes so far as to "deconjecture" his Conjecture 16, the famous Last "Theorem" of Fermat.

Included in the essay on computing and algorithms is a hilarious account of the recent discovery of the five large Mersenne primes $M_p = 2^p - 1$, where $p = 21701$, 23209, 44497, 86243, 132049. There must now be more to this saga, as Slowinski has since found that M_p is prime for $p = 216091$. Other topics which receive mention are: the Riemann Hypothesis, recent developments in primality testing, and class group structure. It is true that this latter topic is quite advanced, but Shanks points out simple pertinent facts about the class group and then uses cycle graphs to describe it. This treatment is quite understandable to the beginning student.

This is a stimulating, provocative, and informative volume, which should (and can) be read by anyone with an interest in number theory.

H. C. W.

1. Review **73**, *Math. Comp.*, v. 17, 1963, p. 464.
2. Rcview **1**, *Math. Comp.*, v. 38, 1982, pp. 331–332.

2[11–01, 11–04].—Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, Mass., 1984, xii + 452 pp., 24 cm. Price $29.95.

In an incautious moment, Gauss is supposed to have said that if mathematics is the queen of the sciences, then the theory of numbers is, because of its supreme uselessness, the queen of mathematics. Perhaps this reputation for uselessness has contributed to the recent decline in enrollment in elementary number theory classes, now that students demand immediate applications and subject matter which will help them get a good job. At last, here is a text for a number theory course which can satisfy their demands.

This volume covers such standard topics as factorization into primes, congruences, primitive roots and quadratic residues. What sets it apart from other introductory number theory texts is the large number of applications it contains.

After the Chinese Remainder Theorem is proved, its use in computer arithmetic with large integers is described. Later, it is applied to threshold schemes. There is a chapter on applications of congruences to calendar problems, round-robin tournaments and computer hashing functions for data storage. After the existence of primitive roots is established, the author discusses their use in generating pseudorandom numbers and splicing telephone cables to minimize interference and cross-talk.

Another chapter applies number theory to cryptology: The classical affine transformation substitution ciphers and block ciphers are cryptanalyzed. Two modular exponentiation ciphers, the Pohlig-Hellman scheme and the Rivest-Shamir-Adleman public-key cryptosystem, are described. The discussion covers many aspects of these ciphers from how to choose the primes to how to play poker by telephone. The author explains knapsack ciphers and mentions their weakness.

In another chapter, the author describes probable prime tests and Euler and strong pseudoprimes. He shows that a Carmichael number must have at least three