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 crosstalk.

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 prime factors. He proves Pratt's theorem that every prime number has a succinct certificate of primality. He mentions the efficient primality test of Adleman, Pomerance, and Rumely. He describes Fermat's difference of squares factorization method. Draim factorization and Euler's factorization method appear in exercises. He proves Lagrange's theorem that an infinite simple continued fraction is periodic if and only if its value is a quadratic surd. However, he does not mention the continued fraction factoring algorithm or any other one of subexponential order. The book concludes with Pythagorean triples and the algorithmic solution of Pell's equation.

Five tables in an appendix give the least prime factor of each odd number below 10000, values of some arithmetic functions, the least primitive root for each prime below 1000, indices for primes below 100 and continued fractions for nonsquares below 100.

It is unfortunate that the book is marred by a number of typographical errors. Here are some that I noticed: On the copyright page, it should say that the cover refers to Problem 33 of Section 1.2. Problem 16 on page 180 is false. Two pairs of numbers are omitted from the ciphertext in the middle of page 199. On page 245, $p = 487$ is not the least prime for which there is a primitive root which is not also a primitive root modulo p^2. It is the least prime p so that 10 is a primitive root modulo p but not modulo p^2. The rows of the factor table on pages 412–418 are in the wrong order, probably the result of last minute reformatting.

In spite of these and a few other flaws, this volume is an excellent text for a course in elementary number theory with applications.

S. S. Wagstaff, Jr.

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

3[11A41, 11A51, 11N05, 11Y11, 11Y05].—Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985, xvi + 464 pp., 23 cm. Price $44.95.

This clearly written volume brings the reader from elementary facts in number theory to the level of current research in the areas mentioned in the title. Chapter 1 begins with the definition of prime number. Then the author describes the sieve of Eratosthenes and formulas for computing the exact number $\pi(x)$ of primes below x, such as those of Meissel, Lehmer, and Mapes. He mentions the recent improvement of these formulas by Lagarias, Miller, and Odlyzko.

Chapters 2 and 3 deal with the distribution of primes in the large and locally, respectively. The author compares the accuracy of several approximations to $\pi(x)$, such as $x/\ln x$, $\operatorname{li} x$ and Riemann's formula. He discusses the frequency of appearance of twin primes and other constellations. He mentions the inconsistency of the prime k-tuples conjecture with the triangle inequality $\pi(x + y) \leqslant \pi(x) + \pi(y)$, which was once conjectured to hold for all $x, y \geqslant 2$. He compares the distribution of primes in the two series $4n + 1$ and $4n + 3$ and discusses the growth rate of the maximal gaps between consecutive primes.