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.

Chapter 4 concerns tests for primality and compositeness. It begins with probable prime tests and Carmichael numbers. Next, the Lucas-Lehmer test and its improvements due to Proth, Pocklington and Lehmer are discussed. The author gives the flavor of the new Adleman-Pomerance-Rumely primality test and its simplification by Cohen and Lenstra.

Chapter 5 on factorization is the longest chapter in the book. It begins with trial division and the GCD method of finding small factors. Then the following factoring algorithms are described: Fermat's difference of squares method and Lehman's improvement of it, Legendre's idea of finding a nontrivial solution to the congruence $x^2 \equiv y^2 \pmod{N}$, Euler's method of expressing $N = a^2 + Db^2$ in two different ways with the same D, Gauss' use of quadratic residues to restrict possible divisors of N, Legendre's use of the continued fraction expansion of $\sqrt{N}$ to produce small quadratic residues of N, Pollard's $p - 1$ and $p + 1$ methods, Pollard's ρ or Monte Carlo method and Brent's improvement of it, Shanks' square forms method, Morrison and Brillhart's continued fraction method and the quadratic sieve method. The author describes the distribution of sizes of prime factors of a typical integer. The factoring algorithms of Schroeppel, Dixon, and Schnorr and Lenstra are mentioned. The chapter closes with a thought-provoking argument that it may be possible to factor integers in polynomial time.

The brief Chapter 6 discusses the Rivest-Shamir-Adleman public-key cryptosystem and its safety.

Nine appendices discuss abstract algebra, elementary number theory, quadratic fields, continued fractions, cyclotomic polynomials, Aurifeuillian factorizations, multiple-precision integer arithmetic on computers, and Stieltjes integration. The book concludes with 34 tables. Most of them list factors of numbers of the form $a^n \pm b^n$ for various a and b up to 10. There is also a short table of primes, a list of primes between 10^n and $10^n + 1000$ for $5 \leqslant n \leqslant 15$, a table of $\pi(x)$ for various $x \leqslant 4 \cdot 10^{16}$, a table of quadratic residues, and tables of coefficients of Gauss' and Lucas' formulas for cyclotomic polynomials.

The author gives PASCAL programs for some of the algorithms he describes. For example, the book contains programs for the sieve of Eratosthenes, for computing $\pi(x)$ with Lehmer's formula, for strong probable primality tests, for Pollard's ρ factoring algorithm and for multiple-precision integer arithmetic.

This volume is the first modern text on factorization and prime testing. It must be welcomed by novices in the field. These subjects have a long history and are advancing swiftly at present, partly in response to the RSA cryptosystem, which requires large primes and whose security depends on the difficulty of factoring integers. This book went to press in February, 1985, and gives a fair description of the state of the art of these subjects at that time. In the same month, H. W. Lenstra, Jr., announced his discovery of the elliptic curve factoring algorithm. Naturally, the book does not mention this beautiful and powerful method, but the reader should be cognizant of it.

S. S. WAGSTAFF, JR.

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907