and further results, now being prepared by the senior author (D.S.M.) and two collaborators.

B. C. C.

17[65–06, 65D30, 65D32].—H. BRASS & G. H. HÄMMERLIN (Editors), *Numerical Integration III*, International Series of Numerical Mathematics, Vol. 85, Birkhäuser, Basel, 1988, xiv + 325 pp., 24 cm. Price $60.50.

These are the proceedings of the third conference on numerical integration held at the Oberwolfach Mathematics Research Institute November 8–14, 1987. (The proceedings of the 1978 and 1981 conferences were published in Volumes 45 and 57 of the same series.) There are 28 papers, about three quarters of which deal with one-dimensional integration. The great variety of topics addressed during this conference can be gathered from the following list of key words: Computation of convolution integrals, Stieltjes integrals, and principal value integrals; Gauss and Chebyshev type quadrature rules; optimal quadrature; product integration; positivity of interpolatory rules; error estimation and convergence acceleration; theorems of Bernstein-Jackson type; cubature formulae with minimal or almost minimal number of knots; criteria for constructing multidimensional integration rules; quasi-Monte Carlo methods; lattice rules. The volume concludes with a traditional section on open problems.

W. G.

18[11A41, 11Y05, 11Y11].—HIDEO WADA, *Computers and Prime Factorization* (Japanese), Yūsei Publishers, Tōkyō, 1987, 190 pp., 21 cm. Price Yen 1800.

Most methods of obtaining the prime factorization of a given natural number have two steps. In the first step one decides whether the integer is prime or composite. In the second step one finds a nontrivial factor of the integer, if it is composite. The complete prime factorization is produced by performing the two steps recursively while composite factors remain. This book is an introduction to modern algorithms for these two steps.

To decide whether a large integer n is prime or not, one often checks whether it satisfies the conclusion of Fermat's Little Theorem, $b^{n-1} \equiv 1 \pmod{n}$, for some b. If this congruence fails and n is relatively prime to b, then n is definitely composite and we try to factor it. If the congruence holds, then n is almost certain to be prime and we use a *prime-proving algorithm* to show rigorously that n is prime. Rigorous tests for primeness are still much slower than probabilistic ones.

The book begins with some preliminaries from elementary number theory: Euclid's algorithm, congruences and Euler's totient function. The first algorithm after Euclid's is trial division, the only algorithm which factors ǎnd proves primality as well (for small integers). The next algorithm, fast modular exponentiation, is used for a simple prime-proving algorithm based on the converse of Fermat's Little Theorem: If $n - 1 = p_1^{e_1} \cdots p_r^{e_r} \cdot m$, where $m < \sqrt{n}$, and if for each i in $1 \leq i \leq r$ there exists an a_i for which $a_i^{n-1} \equiv 1 \pmod{n}$ but $\gcd(a_i^{(n-1)/p_i} - 1, n) = 1$, then n is prime. Fast exponentiation is also a component of Pollard's two-step $p-1$ factoring algorithm. His Monte Carlo factoring algorithm and the $p+1$ factoring algorithm are presented here, too.

After stating the quadratic reciprocity law, the author tells how to solve quadratic congruences quickly in many cases. This ability is needed for initializing the quadratic sieve factoring algorithm. A later chapter gives details of the multiple-polynomial quadratic sieve algorithm from Silverman [5]. Quadratic reciprocity is used also to derive the tests of Pépin and Lucas for the primality of Fermat and Mersenne numbers, respectively.

The theory of continued fractions of quadratic surds is applied to solving Pell's equation and to factoring integers by the continued fraction method of Morrison and Brillhart. We learn also how to express a prime as a sum of two or four squares.

The beautiful elliptic curve factoring algorithm of H. W. Lenstra, Jr. is described, beginning from the addition formula for the Jacobian elliptic function $\operatorname{sn} x$. The book offers a taste of the fast prime-proving algorithm of Adleman and Rumely. Gauss sums are discussed in this connection, following the treatment in Cohen and Lenstra [1].

A short chapter describes codes, ciphers and the Rivest-Shamir-Adleman public key cryptosystem.

Algorithms are given for extended-precision integer arithmetic, including fast multiplication by the FFT and the Strassen-Schönhage method. At the end of the book, C programs are provided for multiprecise arithmetic and for all algorithms which were described fully earlier in the text. Although the programs have no comments, they are explained carefully.

This book is a fine introduction to the subject for a beginner. It covers a lot of ground in 190 pages. It contains the first treatment of the elliptic curve factoring algorithm in a book and only the second treatment (after that in Riesel [4]) of the Adleman-Rumely primality test. The book takes a practical approach to the subject. It is intended for those who would write fast computer programs to factor and test primality. It does not say much about methods whose interest is only theoretical, such as Dixon's factoring algorithm [2] or Miller's primality test [3] which depends on the Riemann Hypothesis.

S. S. WAGSTAFF, JR.

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

1. H. COHEN & H. W. LENSTRA, JR., "Primality testing and Jacobi sums," *Math. Comp.*, v. 42, 1984, pp. 297–330.

2. JOHN D. DIXON, "Asymptotically fast factorization of integers," *Math. Comp.*, v. 36, 1981, pp. 255–260.

3. GARY MILLER, "Riemann's hypothesis and tests for primality," *J. Comput. System Sci.*, v. 13, 1976, pp. 300–317.

4. HANS RIESEL, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985. (Review **3**, *Math. Comp.*, v. 48, 1987, pp. 439–440.)

5. ROBERT D. SILVERMAN, "The multiple polynomial quadratic sieve," *Math. Comp.*, v. 48, 1987, pp. 329–339.

19[11–06, 11B37, 11B39].—A. N. PHILIPPOU, A. F. HORADAM & G. E. BERGUM (Editors), *Applications of Fibonacci Numbers*, Kluwer, Dordrecht, 1988, xx + 213 pp., $24\frac{1}{2}$ cm. Price $79.00/Dfl.145.00.

This book contains nineteen full length papers from among the twenty-five papers presented at the Second International Conference on Fibonacci Numbers and Their Applications held at San Jose State University, San Jose, California, U.S.A., August 13–16, 1986. While the underlying theme of this conference is the theory and application of linear recurring sequences, the contents of these proceedings are quite varied. Some indication of this diversity is afforded by the following sample of titles: Recurrences Related to the Bessel Functions, Primitive Divisors of Lucas Functions, Fibonacci Numbers and Groups, Asveld's Polynomials $p_j(N)$, Covering the Integers with Linear Recurrences.

H. C. W.