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 and proves primality as well (for small integers). The next algorithm, fast modular exponentiation, is used