MATHEMATICS OF COMPUTATION
Volume 66, Number 219, July 1997, Pages 1367–1374
S 0025-5718(97)00877-6

REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

The numbers in brackets are assigned according to the American Mathematical Society classification scheme. The 1991 Mathematics Subject Classification can be found in the annual subject index of *Mathematical Reviews* starting with the December 1990 issue.

13[65-06, 11-06, 11Yxx]—*Mathematics of Computation 1943–1993: A half-century of computational mathematics*, Walter Gautschi (Editor), Proc. Sympos. Appl. Math., Vol. 48, American Mathematical Society, Providence, RI, 1994, xx + 643 pp., 26 cm, $90.00

Already in my student days, *Mathematics of Computation* was one of my favorite journals. Every issue would start with a thick layer of "other people's mathematics", whose sole function, as I imagined, was to keep its real contents hidden from general view. After many pages of finite element methods and quadrature formulas one would, at an always sharply defined point, enter the magical world of primality tests, amicable numbers, and sieving devices—true and tangible mathematics that held an immense fascination for me. No other journal published a higher percentage of papers that I found so immediately appealing. In fact, no other journal published any papers whatsoever in computational number theory, and were it not for *Mathematics of Computation*, I might have thought there was nothing respectable about the entire discipline at all.

Much has happened in computational number theory since I was a student. Theoretical computer scientists discovered it as a playground, invented new methods and reinvented old ones, established the habit of not only *running* algorithms but also *analyzing* them, and have now largely left the field again. Cryptologists found that problems in computational number theory display the right combination of feasibility and intractability that is required for the construction of cryptographic schemes that are both practical and secure—that is, until someone discovers that there is nothing intractable about these problems after all. And, thirdly, researchers in other branches of number theory started using computers as a research tool and developed algorithms in areas where none or few had been before.

Many traditional mathematical journals, both the arithmetically oriented ones and those of a more general signature, responded to the increased fashionability of computational number theory with a notable change in attitude. In addition, computer scientists and cryptologists founded their own journals, and in pure mathematics *Experimental Mathematics* made its appearance. As a result, *Mathematics of Computation* lost its monopoly, but it has done much better than merely surviving. It is universally regarded as the leading journal in computational number theory, representing the full range of current research in the field, and remaining essentially the only one for the purely "numerological" aspects.

In 1993, the 50th birthday of *Mathematics of Computation* was commemorated with an International Conference held in Vancouver. It consisted of a Symposium on Numerical Analysis and a Minisymposium on Computational Number Theory. The latter was dedicated to the memory of D. H. Lehmer, of all of the founders of

the journal the one to be held responsible for its reputation in number theory. The volume under review contains, in Part I, the proceedings of the Symposium, and in Part II those of the Minisymposium.

It is only Part II, which occupies almost a third of the book, that concerns us in this review. It comprises four invited papers and thirteen contributed ones. The latter have no more than six pages each; five of them are in final form, and of seven will a final version appear elsewhere, the status of the thirteenth, which deals with the philosophy of mathematics, being characteristically unclear.

The longest paper in the volume—51 pages, including 6 pages of references—is the "historical essay" *Factoring integers before computers*, by H. C. Williams and J. O. Shallit. Number theorists with an interest in the history of their subject will love perusing this paper; and it must be considered required reading for scholars whose occupation with factoring integers is inspired by its relevance in cryptology. The security of many modern cryptographic schemes depends crucially upon the supposed intrinsic intractibility of certain problems in computational number theory, such as the problem of factoring large integers. It is all too often forgotten that the *only* evidence for the correctness of this supposition is of a historical nature. Whoever wishes to form an independent opinion of the strength of this evidence must study the history of the subject, and the paper of Williams and Shallit is the best place to start.

There is also an invited paper on what, in 1993, promised to be the near *future* of factoring integers. Carl Pomerance speculates that the "number field sieve" will emerge as the method of choice for factoring the hardest numbers, an expectation that has been borne out by the subsequent developments. His beautifully written paper forms an excellent introduction to modern factoring techniques, with special emphasis on the number field sieve. Andrew M. Odlyzko contributed a concise and lucid survey of analytic computations in number theory, with copious references. A fourth invited paper, by Ingrid Biehl and Johannes Buchmann, deals with algorithms in quadratic number fields, addressing a more specialized audience than the other three papers.

No reader whose favorite journal is *Mathematics of Computation* will want to miss this book, which provides them with as much fun as the journal itself does. Even the bivariate splines and Galerkin methods are not absent, to keep up the idea that it would be sinful to devote an entire volume to the pursuit of "big game in the theory of numbers".

H. W. Lenstra, Jr.
Department of Mathematics
University of California at Berkeley
Berkeley, CA 94720-3840

14[65-01]—*Afternotes on numerical analysis*, by G. W. Stewart, SIAM, Philadelphia, PA, 1996, x + 200 pp., $23\frac{1}{2}$ cm, $29.50

Here's numerical analysis with a lean and lively spirit. G. W. "Pete" Stewart has compiled for us a set of notes for an introductory course in numerical analysis. The terminology "Afternotes" is indicative of his practice of writing down his recollections of the lecture just given, while they were fresh in his mind, thus putting his own spin on the material. As befitting of a fledgling audience, this is not a traditional theorem-proof presentation. Rather, the intent is to get to the heart of