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 the matter; the rigor and detail are out there if you want to look for them.

Given this framework, "Afternotes" is not intended to fulfill all of the needs of a full-fledged textbook. Exercises are few in number and not intended to supplant routine problems or computer projects. Fully two-thirds of the lectures are devoted to matters dealing with linear and nonlinear equations and floating-point arithmetic. Therein lies the strength of the book; Stewart knows just how to illuminate important computational issues, such as effects of conditioning. On the other hand, the remaining third of the lectures deal with standard fare, such as interpolation, numerical integration, and numerical differentiation, and here Stewart manages to hit the high spots with just the right effort for a course at this level.

Notably absent, then, is a section on initial-value problems for ordinary differential equations. One might argue that the course is already packed; nevertheless, inclusion in the notes of a section on ODE's to be used at the discretion of the instructor might be useful.

As befits an expert in the field, Stewart not only covers standard fare skillfully, but it is his introduction to, and treatment of, topics not always encountered at this level, e.g. perturbation theory and backward error analysis, which gives this work much of its value. Other examples of material presented here and not readily found in most texts include a linear-fractional method and a hybrid scheme for solving $f(x) = 0$, and an indication of the role of row vs. column orientation for algorithms for solving linear systems.

As in many texts, a goal here is to point out the nuances and possible pitfalls in numerical computation. This Stewart accomplishes, while at the same time injecting into the presentation an appropriate dose of humor. Notable examples include a spirited conversation between scientist Dr. XYZ and you, the reader, as the numerical analyst, discussing the backward error analysis of summation, and an admonition to "economists and astrologers" on the dangers of unsafe extrapolation (you'll have to read this one for yourselves).

To conclude, we have already seen some reasons (notably, lack of exercises), which prevent this set of notes from being the sole text for a course. We might also ask from the author some guidance concerning his expectation of the reader's knowledge of programming languages, since code segments in differing languages are interspersed throughout the text. But, in the final analysis, what we do have here is an excellent set of notes which might be used to reinforce materials from other sources, or, depending upon the audience, to use as primary lecture material, with a traditional text kept in the bullpen for more detail. Either way, read and enjoy!

Steven M. Serbin
Department of Mathematics
University of Tennessee
Knoxville, TN 37996-1300

15[76-02, 65M60]—*Navier-Stokes equations and nonlinear functional analysis*, by Roger Temam, CBMS-NSF Regional Conference Series in Applied Mathematics, Vol. 66, second edition, SIAM, Philadelphia, PA, 1995, xiv + 141 pp., 25 cm, softcover, $26.50

This short monograph is volume 66 of the CBMS-NSF regional conference series in applied mathematics. It is the revised second edition of a text that was published