In addition to the notes and references at the end of each chapter, Rubio provides exercises for each chapter in one appendix, and an 85-page bibliography in another.

Students can test their understanding of this material not only by working through the suggested exercises but also by correcting quite frequent typographical errors; e.g., replacing "$\subseteq$" by "$\supseteq$" near the bottom of page 18, "$\bigcup_{i\in\mathbb{N}}$" by "$\bigcup_{n\in\mathbb{N}}$" in Eq. 1.25, and "$\exists x\psi$" by "$\exists z\psi$" in Definition 1.7d.

Much of this book develops sophisticated mathematical concepts needed for advanced applications of nonstandard analysis, rather than concentrating on just the more familiar concepts needed for certain simpler applications. For example, properties of κ-saturated superstructures are developed for arbitrary infinite cardinals κ, before discussing the embedding of the ordered field $\mathbb{R}$ of reals into the ordered field ${}^*\mathbb{R}$ of hyperreals. Consequently, this book is more for the mathematician seeking powerful new ways to study advanced optimization theory, rather than for the numerical analyst with only a casual interest in nonstandard analysis.

WILLIAM C. DAVIDON
DEPARTMENT OF MATHEMATICS
HAVERFORD COLLEGE
HAVERFORD, PA 19041-14392

12[65-06, 65Y05]—*Parallel processing for scientific computing*, David H. Bailey, Petter E. Bjørstad, John R. Gilbert, Michael V. Mascagni, Robert S. Schreiber, Horst D. Simon, Virginia J. Torczon, and Layne T. Watson (Editors), SIAM Proceedings Series, Society for Industrial and Applied Mathematics, Philadelphia, PA, 1995, xviii + 875 pp., $25\frac{1}{2}$ cm, softcover, $105.00

These are the proceedings of the Seventh SIAM Conference on the topic of the title, held February 15–17, 1995, in San Francisco. Included are minisymposia papers, contributed papers, and short summaries of poster presentations. The nearly 200 papers, organized in three parts, each further subdivided into four chapters, give an impressive account of the current use of parallelism in a vast variety of application areas. Specifically, Part I entitled "Applications", contains chapters on image, signal, and information processing; optimization and control; computational physics; and mathematical applications. Part II, entitled "Algorithms", has chapters on n-body simulation; partial differential equations; sparse linear systems; and eigenvalues. Part III, entitled "Systems", finally concludes with chapters on mesh partitioning and load balancing; languages and compliers; libraries and runtime systems; and visualization and performance. There is a final chapter containing position papers from a Panel Discussion on the question "Is scalable parallel computing a myth?". An author index concludes the volume.

W. G.

13[11-01, 11Yxx]—*A course in computational algebraic number theory*, by Henri Cohen, Graduate Texts in Mathematics, Vol. 138, Springer, Berlin, 1993, xxii + 534 pp., 24 cm, $49.00

The present book is one of the most popular texts on computational number theory. Its attitude is *practical*. For instance, in the first chapter, among some gen-

eral remarks about multiprecision arithmetic, we find: "...Since we will be working mostly with numbers of up to roughly 100 decimal digits..."

The author, Henri Cohen from Bordeaux, is a mathematician of a rare wide culture. He can tell you the details of the special merits of the machine instructions of the Motorola 68040 micro-processor, but also explain the intricacies of modular forms of half-integral weight. He easily manipulates commutative diagrams and discusses the numerical evaluation of several special functions on the same page. Cohen's personal style of writing is quite amusing. The preface to this book reads like a "Who's Who" in computational number theory, and the bibliography comes with a three-line evaluation of the merits of each text. The comments are always friendly and to the point. Often the last line of the evaluation says: "A must on the subject". A judgement that definitely applies to Cohen's own book as well.

The first chapter of the book contains a very readable account of the fundamental number-theoretical algorithms: Euclid's gcd algorithm, computing in $\mathbf{Z}/n\mathbf{Z}$, quadratic residue computations, square roots modulo a prime and a few words about computations in the polynomial ring $\mathbf{F}_p[T]$.

The most important ingredients for many of the more sophisticated algorithms are algorithms for lattice reduction. These are algorithms that compute a basis of rather short and orthogonal vectors of a given integral lattice in Euclidean space. For one-dimensional lattices the usual Euclidean gcd algorithm does the job. In general, the so-called "LLL"-algorithm is used. This algorithm is due to H. W. Lenstra, A. K. Lenstra and L. Lovász. In their paper [2] it was used to construct the first polynomial-time algorithm to factor polynomials with coefficients in $\mathbf{Q}$. This algorithm has very, very many applications and has quickly become the principal building block of many modern, practical number-theoretical algorithms.

Chapter 2 contains a discussion of algorithms involving linear algebra and lattices: how to compute determinants, characteristic polynomials, Gaussian elimination, the Hermite and Smith normal forms, the LLL-algorithm. The author restricts himself mainly to integral lattices and linear algebra over $\mathbf{Z}$ or a finite field. He does not discuss the usual problems of numerical linear algebra. In Chapter 3 the author discusses computational aspects involving polynomials: how to evaluate, how to compute disciminants. He discusses the Berlekamp and Cantor-Zassenhaus factorization algorithms for polynomials over finite fields. Finally he explains the Lenstra-Lenstra-Lovász algorithm to factor polynomials over $\mathbf{Q}$.

The next three chapters contain a description of the basic algorithms to do computations in algebraic number fields. Chapter 4 is of a somewhat auxiliary nature. In it the author discusses certain general problems: the subfield problem, how to represent an ideal, how to test membership. He introduces, without any proofs, the basic concepts of algebraic number theory.

In Chapter 5 the author focuses his attention to quadratic fields. For these fields the computational theory is furthest developed. He explains the close connections between binary quadratic integral forms and ideal classes of the rings of integers of these fields. He explains Shanks's baby-step-giant-step algorithm and Buchmann's subexponentional algorithm to compute the class group. The chapter is concluded with a brief discussion of the so-called Cohen-Lenstra heuristics on the statisical distribution of the class groups.

Chapter 6 contains a description of the fundamental algorithms in algebraic number theory: algorithms to compute the ring of integers of a given number field,

to compute the Galois group of a normal closure of a number field, algorithms to compute the unit group and the ideal class group of the ring of integers. The author is currently developing a program that routinely computes all these things for number fields which are given by a polynomial which is not "too large". At present, the program can handle number fields of degree at most 24 with moderate root discriminant.

Chapter 7 contains a description of several algorithms related to elliptic curves. The author gives an algorithm to transform a cubic curve in $\mathbf{P}^2$ with a point into Weierstrass form; he gives Tate's algorithm to determine the fibers in the Néron model of an elliptic curve over a discrete valuation ring. He gives the doubly exponentially convergent algorithms to compute the period lattice of an elliptic curve over $\mathbf{C}$. The remaining algorithms apply to elliptic curves over number fields: computation of the canonical height of a point, evaluation of the Hasse-Weil L-series and its derivatives, etc.

The 85 pages of the last three chapters contain a description of the currently most popular algorithms for factoring integers and for primality testing. Chapter 8 contains a description of some of the older practical algorithms: the $N-1$ test for proving primality and the Pollard ρ-method, the $p-1$ method and Shanks's class group method for factoring. In Chapter 9 the author discusses the two most efficient practical primality proving methods that are currently known: the "Jacobi sum test" and Atkin's algorithm. The Jacobi sum test was invented by Adleman, Pomerance and Rumely. The author discusses the efficient simplified version due to Hendrik Lenstra and Henri Cohen in detail. It is based on computations with Jacobi sums in cyclotomic fields. Atkin's algorithm, which is based on certain computations with elliptic curves with complex multiplication, is only discussed briefly. The reader is referred to the paper by Atkin and Morain [1] for the practical details. The current implementations of both algorithms routinely handle 1000-digit primes.

In Chapter 10 the modern factoring algorithms are discussed: first the classical continued fraction method, then an algorithm due to Lenstra and Schnorr that exploits class groups of complex quadratic number fields. Lenstra's celebrated elliptic curve method is explained and, finally, Pollard's "Number Field Sieve" is discussed in some detail.

I like this book very much. Its attitude is practical and it is written in plain English: the description of the algorithms is not obscured by the jargon that is often used in theoretical computer science. Therefore, this book is very useful for anyone who actually wishes to use the algorithms to do computations on a computer. It is also very useful for anyone who wishes to use one of the recent powerful computer algebra packages. The book provides a good theoretical background for this purpose.

The author discusses the computational aspects of $\mathbf{Z}/n\mathbf{Z}$, of rings of integers of number fields and of elliptic curves, but some other "natural" rings, such as polynomial rings in several variables over a finite field, or over $\mathbf{Q}$, are not discussed in great detail. For instance, all recent developments involving computational algebraic geometry, Gröbner bases, etc. are never mentioned.

Much of the contents of the book are very fundamental and probably will, like Knuth's 1973 textbooks, be of long-lasting value. But, given the philosophy of the book, some other parts have a somewhat more temporary character. One may

wonder what value the more practical sections of the book and the information on computer algebra packages will have in, say, 20 years from now.

R. S.

References

1. A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68. MR **93m:**11136
2. A. K. Lenstra, H. W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534. MR **84a:**12002