software and interactive programming systems, and the benefits that can accrue from preprocessing (e.g., preliminary transformations) and postprocessing (various convergence acceleration techniques).

Indefinite integration in closed form is the subject of Part II, which includes Risch's Structure Theorem and Liouville's Principle without proofs.

Part III—the core of the book—has six chapters. The first (Chapter 5) deals with univariate integration formulae and their errors, and convergence properties. Included are Newton-Cotes, Clenshaw-Curtis, and Gauss-type formulae. Composite rules, specifically the composite trapezoidal rule and its superiority for periodic functions, are also considered, as well as periodizing transformations making nonperiodic integrands accessible to treatment by the composite trapezoidal rule. The chapter concludes with a brief discussion of Romberg integration. There follows a long chapter on multivariate integration formulae, including principles of construction, number-theoretic formulae, Monte Carlo techniques, and lattice rules, with lengthy discussions of the theoretical underpinnings for these rules. Chapter 7 presents various approaches for dealing with special integration problems: oscillatory integrals, integrals on unbounded domains, Fourier and inverse Laplace transforms, and weakly and strongly singular integrals in one and several variables. Chapter 8 deals with integration algorithms and related matters such as practical error estimation, adaptive and nonadaptive discretization refinement techniques, and methods of enhancing reliability and efficiency. There are many pointers to existing software. The next chapter on parallel numerical integration is a concise introduction to numerical integration software for parallel and distributed computer architectures, while the final chapter deals with issues relating to the assessment of numerical integration software products.

It is not entirely clear what kind of audience will benefit most from this work. The authors anticipate three groups of readers: graduate students, computer scientists and engineers, and researchers in applied numerical analysis and mathematical software development. As a textbook for students (and their instructors) the treatment lacks focus (and exercises!), as the authors tend to pursue all the ramifications of any particular subject, often without full details, and thus would seem to cause bewilderment more than enlightenment among students. The other groups of readers undoubtedly will benefit from the numerous references to the literature and to existing software, and perhaps will appreciate more the practical issues discussed in the book than the (sometimes discursive) theoretical presentations. The reviewer values the book as a useful reference work.

WALTER GAUTSCHI
DEPARTMENT OF COMPUTER SCIENCES
PURDUE UNIVERSITY
WEST LAFAYETTE, IN 47907-1398
E-mail address: wxg@cs.purdue.edu

7[13-01, 13P99, 14-01, 14Q99]—*Computational methods in commutative algebra and algebraic geometry*, by Wolmer V. Vasconcelos, Algorithms and Computation in Mathematics, Vol. 2, Springer-Verlag, New York, NY, 1998, xi+394 pp., 24 cm, hardcover, $79.95

Although fundamental effective approaches to algebra had been explored before (notably by G. Hermann and A. Seidenberg), symbolic algebra really started off in the 1980s, when the first computer algebra systems became widely available. Buchberger's algorithm ruled the waves, and many concrete algorithms were developed and subsequently implemented. In the early 1990s, books appeared that gave good overviews of existing methods. The core algorithms regarding Gröbner bases (such as Buchberger's) were dealt with in [1], [2], and [3]. Although Buchberger's algorithm solves a lot of problems in commutative algebra, quite a few issues require substantially more (and heavier) algorithmic ingredients before they can be handled effectively. Finding the radical of an ideal and its primary decomposition are such problems. They received a fair amount of attention in the literature; the first textbooks to handle them appeared in the mid 1990s, see e.g., [4]. Vasconcelos' book is probably the second in this respect.

The book represents a step forward (on the level of textbooks) in effective commutative algebra. It does not concern itself with complexity of algorithms. (In fact the notion of complexity does not appear in the index, but is used in the last chapter (no. 9) as an abstract measure of the cost of extracting information about a graded module.) By disregarding such aspects and by only rarely writing out algorithms in full, Vasconcelos is able to cover a great deal more than the books mentioned above. The first 269 pages of the book form the proper text. An appendix, which is a 60-page primer on commutative algebra, follows. The book closes with two more appendices: a 25-page text on Hilbert functions by J. Herzog; and a 25-page introduction to the use of the computer algebra package Macaulay2 by the authors of the package, D. Grayson and M. Stillman, and D. Eisenbud. The latter author also contributed a nice short chapter (no. 8) in the main text on how to compute cohomology.

How else can this book start but by discussing Buchberger's algorithm? It does so in just a few pages. Within the first 100 pages (Chapters 1–3), it also deals with primality testing, primary decompositions and Noether normalization. The fact that, in the year following publication of this book, papers like [5] still appear makes it clear that the methods for, say, primary decomposition have not yet crystallized out the way they did for Buchberger's algorithm. Then comes a chapter (no. 5) about finite-dimensional (not necessarily commutative) algebras. It discusses issues like finding the Jacobson radical and idempotents. Compared to Chapter 5 of [6] Vasconcelos deals more with the general theory than with the most recent algorithms. Also, in this chapter (and I fail to see strong connections with the rest of the chapter or its title), the author compares numeric and symbolic methods for finding explicit roots of a set of polynomial equations. Here and elsewhere, he uses a very pleasant expository style and refers to the literature for many details.

The chapters not explicitly mentioned so far (6 and 7) deal with some topics which are of basic importance to algebraic geometry, like integral closure, effective Nullstellensatz, etc. Also finding regular sequences is discussed. Together with Eisenbud's chapter on cohomology, I found these the most illuminating parts of the book. Here too, new methods still keep appearing, see e.g., [7].

Furthermore, Vasconcelos gives a taste of some other new developments, like presentations of the Rees algebra, and Derkesen's new algorithm for determining the invariants of a linearly reductive group. (In the introduction he explains his constrained presentation of invariant theory by referring to [8]).

The key ideas are presented in a succinct and entertaining style. The book is carefully written (I spotted an occasional slip of the pen, e.g., the group G in the discussion on "Reynolds Operators and Lie Algebras" on page 206 should be connected), and is to be recommended as a pleasant introduction to advanced algorithmic methods in commutative algebra.

References

[1] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Math., vol. 3, AMS, ISBN 0-8218-3804-0, Oxford University Press, Oxford, 1994.

[2] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, Berlin, ISBN 3-540-97847-X, 1992.

[3] T. Becker, H. Kredel, V. Weispfenning, *Gröbner bases, A computational approach*, GTM 141, Springer-Verlag, ISBN 0-387-97971-9, 1993.

[4] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Springer Verlag, 1995.

[5] Wolfram Decker, Gert-Martin Gruel, Gerhard Pfister, *Primary decomposition: Algorithms and comparisons*. Algorithmic algebra and number theory (Heidelberg, 1997), 187–220, Springer, Berlin, 1999.

[6] A. M. Cohen et al., *Some tapas of Computer Algebra*, Springer Verlag 1999.

[7] Theo de Jong, *An algorithm for computing the integral closure*, J. Symbolic Comput. **26** (1998), no. 3, 373–277.

[8] Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Vienna, 1993.

Arjeh M. Cohen

8[11-01]—*The Mathematics of Ciphers, Number Theory and RSA Cryptography*, by S. C. Coutinho, A. K. Peters, Ltd., Natick, MA, 1998, xv+196 pp., $23\frac{1}{2}$ cm, hardcover, $30.00

There is no shortage of books these days on the connection between number theory and cryptography, but in and amongst the plethora of such publications this book is unique. Primarily meant for junior undergraduates, this book is an enlightening invitation to number theory by way of the RSA cryptosystem. As the author states, this is a mathematical textbook and not so much a book on cryptography. Moreover, perhaps influenced by the style of his Brazilian compatriot Paulo Ribenboim, the book is written in a friendly, relaxed manner which gently winds its way through some of the fundamental concepts in elementary number theory, stopping along the way for historical asides, detailed examples, some philosophical remarks, and leading eventually to the final destination: the RSA cryptosystem. The book is self-contained, but with many pointers to further reading. There is an abundance of well thought out exercises, more than enough to familiarize the student with the subject matter. It is worth noting that this book would be most useful as an introductory textbook to postsecondary mathematics, as the ideas of theorem proving and generalization are carried out in significant detail and, more importantly, with great care. Even some more skilled high school students would find this book both accessible and inspiring.

The book is organized into eleven chapters, along with a preface on the matter of style, a wonderful introduction concerned with aspects of computation in number theory and some of the history of number theory, an addendum on the recent developments in the area of cryptography and number theory, and an appendix on computing roots and powers.