MATHEMATICS OF COMPUTATION
Volume 69, Number 231, Pages 1305–1315
S 0025-5718(00)01249-7
Article electronically published on March 17, 2000

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.

2[65-00, 65-02]—*Handbook of numerical analysis, Vol. VI, Numerical methods for solids* (*Part* 3)*, Numerical methods for fluids* (*Part* 1), P. G. Ciarlet and J. L. Lions (Editors), North-Holland, Amsterdam, 1998, x+689 pp., $24\frac{1}{2}$ cm, hardcover, $164.00

According to its general preface, each volume of the *Handbook of Numerical Analysis* presents in an expository fashion either "basic methods of numerical analysis" or "the numerical solution of actual problems of contemporary interest in applied mathematics." The goal of these volumes is to "thoroughly cover all the major aspects of numerical analysis, by presenting in-depth surveys, which include the most recent trends." Volume VI is dedicated to surveys of numerical methods for solids and numerical methods for fluids. It contains three technical sections plus an obituary of Professor Juan Carlos Simo, the author of the section on numerical analysis and simulation of plasticity.

The first technical section is "Iterative finite element solutions in nonlinear mechanics" by R. M. Ferencz and T. J. R. Hughes. The section begins with a short and clear development of nonlinear solid mechanics and conjugate gradient methods. The overall solution strategy presented is based on finite element discretization, Newton iteration for the nonlinearity with preconditioned conjugate gradient methods for the linearized systems. The primary focus of the article is the presentation of element-by-element preconditioners, developed extensively by Hughes and his coworkers. Element-by-element preconditioning has become a standard engineering tool for solving linearized systems arising in complex applications. Remarkably, it has been studied comparatively little by the numerical analysis community. One way to describe element-by-element preconditioning is as follows. Given a finite element mesh, the elements are "colored" with (as many as necessary) J colors so that all same-color elements do not share nodes. With this coloring, the stiffness matrix A can then be additively decomposed as

$$A = A_1 + A_2 + \cdots + A_J, \quad J \text{ "colors"}.$$

Because of the way the mesh is colored, each color's associated stiffness matrix A_j is similar to a block diagonal matrix with the color-j element stiffness matrices as diagonal blocks. Thus, any calculation with A_j can be performed in a fully parallel fashion using only elemental stiffness matrices. The element-by-element preconditioner is given by the product

$$\prod_{j=1}^{J} (I + A_j)^{-1}.$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Elemental data is the natural logical unit for parallel computation of nonlinear problems as well as for adaptive algorithms because finite element assembly is "embarassingly parallel" at the elemental level. Thus, element-by-element preconditioning is a brilliant idea for massively parallel solution of practical engineering problems. However, this most straightforward version of it has not, however, proven competitive serially on the model Poisson problem with more global preconditioners such as multigrid methods. It seems likely that it has become a preferred method for complex engineering problems not only because of its parallel efficiency but also because of the excellent robustness that such methods seem to have. This article will focus more attention on element-by-element methods and issues of robustness in preconditioners.

The second technical section is "Numerical Analysis and Simulation of Plasticity" by J. C. Simo. This section is a pleasure to read. It begins with a mathematically precise and physically lucid presentation of classical continuum models of plasticity. This is followed by an overview of time integrators satisfying the nonlinear stability conditions necessary for use in plasticity problems. Next there is a mathematically precise development of the nonlinear continuum mechanics of finite strain plasticity followed by one section containing interesting examples of calculations on thermomechanical problems.

The third and last technical section, "Navier-Stokes Equations: Theory and Approximation" by M. Marion and R. Temam, gives a thorough survey of the developments arising from the authors' work on analysis and computation of turbulent flows. This section is the first of several planned articles on numerical methods for fluids. (For work related to this approach, see the recent book of Dubois, Jauberteau and Temam [1]. Complementary treatments of finite elements and fluids are given in the books of Girault and Raviart [2], Gresho and Sani [3] and Gunzburger [4].) Chapter I contains a synopsis of the mathematical theory of the Navier-Stokes equations. Chapters II and III present error analysis for discretizations of the Navier-Stokes equations. With this background, Chapter IV describes nonlinear Galerkin methods, a special method developed by the authors for simulating turbulent flows efficiently. This chapter concludes with several most interesting experiments using a dynamic adaptivity version of the nonlinear Galerkin method.

References

[1] T. Dubois, F. Jauberteau and R. Temam, *Dynamic Multilevel Methods and the Numerical Simulation of Turbulence*, Cambridge University Press, Cambridge, 1999.

[2] V. Girault and P. A. Raviart, *Finite Element Methods for the Navier-Stokes Equations*, Springer-Verlag, Berlin, 1986.

[3] P. M. Gresho and R. L. Sani, *Incompressible Flow and the Finite Element Method*, John Wiley and Sons, Chichester, 1998.

[4] M. D. Gunzburger, *Finite Element Methods for Viscous Incompressible Flow*, Academic Press, Boston, 1989.

William Layton
University of Pittsburg
Pittsburg, PA

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

3[76F05, 76F99, 65-02, 65M70, 76-02, 76D05]—*Dynamic Multilevel Methods and the Numerical Simulation of Turbulence*, by Thierry Dubois, Francois Jauberteau, and Roger Temam, Cambridge University Press, New York, New York, 1999, xix+289 pp., $23\frac{1}{2}$ cm, hardcover, $59.95

This book describes the multilevel methods for time dependent simulations of incompressible turbulence. The authors have performed extensive research in this area and the book is a good source of the state of art in this methodology.

The first three chapters are surveys about the incompressible Navier-Stokes equations, general turbulence theory, and spectral methods. The surveys are brief but references are given for readers desiring more details. Chapter 4 compares DNS (Direct Numerical Simulation) with various turbulence modeling. Long time behavior of the Navier-Stokes equations is discussed in Chapter 5. This is an area in which the third author has done extensive research. This chapter and Chapter 6, which discusses the separation of scales, form the theoretical basis on the applicability of the multilevel methods to incompressible turbulence simulation. In Chapter 7, the basic procedure of multilevel methods is illustrated through a simple system of ODE, which carries many of the essential ingredients of the more complex Navier-Stokes equations but avoids the functional analysis framework. The last three chapters are about the methodology, implementation details, and numerical results of the multilevel methods applied to Navier-Stokes equations in 2D and 3D, both for the periodic cases and for the well-bounded flows. They are based on several recent papers and give the state of the art in the application of this methodology on turbulence simulation.

The authors argue that "new chapters of numerical analysis will have to be written in relation with the multilevel treatment of large evolutionary problems". It is at least safe to say that multilevel or multiresolution methods will play a more important role in large scale scientific computing in the years to come. There is a great challenge to make multilevel methods more efficient. The factor of CPU time saving of the multilevel methods over DNS in this book is about 2 to 2.5. It would certainly appeal to users if this factor can be increased.

Chi-Wang Shu

4[65-01, 65Fxx, 65Y05, 65Y10, 65Y20]—*Numerical linear algebra for high-performance computers*, by Jack J. Dongarra, Iain S. Duff, Danny C. Sorensen, and Henk A. van der Vorst, SIAM, Philadelphia, PA, 1998, xvii+342 pp., $25\frac{1}{2}$ cm, softcover, $37.00

This book is meant to provide helpful information on state-of-the-art numerical linear algebra techniques to be used in advanced high-performance computation to a rather heterogeneous community, ranging from graduate students to professionals in computational sciences. In my opinion, one is also very likely to find extremely good advice for implementing recent and advanced algorithms on sequential machines. Quoting from the authors' preface, " ... this book is a major revision of a previous edition of the book, entitled *Solving Linear Systems on Vector and Shared Memory Computers*", published in 1991; indeed, it contains a lot of new material that covers the recent advances in the development of parallel architecture and software.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

The book is rich with pointers to available software and practical suggestions for its use. The up-to-date bibliography reflects that this is an important and live subject and betrays the fact that the authors are well-known experts in the field who have contributed some of the best-known software packages and algorithms in the area.

Each chapter contains useful introductory sections on the major algorithmic aspects that are followed by more technical and detailed sections. The description of the topics is rather self-contained, therefore the reader is to forced to rely on many other technical books for the algorithmic issues.

Chapter 1 presents the state of the art in parallel architectures, for single and multiple processors. Not surprisingly, much has happened since the previous edition of this book (when vector architectures were still major players). New sections have been devoted to message passing and network-based environments. Chapter 2 has been substantially reduced in scope, limiting the overview of current high-performance computers to MIMD systems with Shared and Distributed Memory.

Chapters 3 and 4 deal with general implementation aspects, such as synchronization, load balancing, indirect addressing and the Message Passing Interface. The section on performance analysis recalls some classical tools while providing helpful suggestions for carrying out practical performance measurements.

The major theme of this book is numerical linear algebra. Its presentation starts in Chapter 5 with dense computations. The major linear algebra kernels (BLAS) are emphasized, which form the basic blocks for LAPACK, the most mature of packages for dense linear algebra. The principal algorithms for solving linear systems and least squares problems are recalled. This chapter also describes ScaLAPACK, whose aim is to provide a linear algebra software standard for distributed memory MIMD computers.

Chapter 6 focuses on direct methods for sparse matrices, for which algorithmic implementations on parallel machines require a mostly ad hoc design. The reader who is not familiar with the area is first introduced to the essential topic of sparse data structures. Then, she/he can follow more closely the technical discussion on sparse orderings, cliques and indirect addressing. Frontal and multifrontal methods make the "sparse" codes amenable to vector and parallel environments: performance results on modern machines give a feeling of the potential of these powerful methods. Useful pointers to public domain and commercial packages are given that will help the user who wants to build applications that employ these packages.

The next three chapters deal with iterative methods of the Krylov subspace variety. This constitutes a major expansion from the previous edition; it is well deserved given that this topic was at the center of one of the most exciting activities in the field of numerical linear algebra and has generated some of the most successful iterative solvers.

The first of these chapters introduces the basic principles and ideas behind Krylov subspaces while Chapter 8 provides a detailed description of several methods that have been proposed in recent years. The basic parallel kernels in iterative methods are mostly BLAS1 operations, together with the step involving the coefficient matrix, usually through a matrix-vector multiplication; most of the analysis of this second phase is postponed to Chapter 10. Chapter 8 also contains useful descriptions of different implementations of the highly successful Conjugate Gradients algorithm. It would have been nice if the authors had also included a discussion on

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

(block) methods for linear systems with multiple right-hand sides, since they are useful in many applications and also make natural use of BLAS2 and BLAS3 computations. The chapter terminates with a discussion on testing iterative methods.

Preconditioning is an important step in iterative approaches; this and parallel implementations are thoroughly presented in Chapter 9. Besides the classical incomplete schemes, a few pages are devoted to the presentation of recent approaches, such as Sparse Approximate Inverse, and Element-by-Element preconditioning, which typically exhibit their best performance in a parallel context. It would have been nice if the authors had opted for a more detailed presentation of domain decomposition methods.

Chapters 10 and 11 describe methods for the standard and generalized eigenvalue problems. After a survey of the most widely used approaches, the very successful package ARPACK is described together with its parallel implementation P_ARPACK (written using MPI). Several important issues are discussed at length, providing the reader with some implementation hints and with a good feeling of the expected performance. Finally, the Appendices gives the necessary information to practically deal with some of the described codes.

In conclusion, in spite of what the authors say in the Preface (" ... Any book that attempts to cover these topics must necessarily be somewhat out of date before it appears"), the book contains a lot of up-to-date material, and I recommend it to computational scientists who deal with linear algebra methods on any of parallel, vector and sequential (!) computer environments. Readers who already own the previous edition will find that this book has been significantly expanded to include recent important advances in numerical linear algebra tools and HPC environments that will make their "HP computational life" much easier.

Valeria Simoncini
Inst. di Analisi Num. del CNR
Castel San Pietro Bologna
Italy

5[65F15, 65F10]—*ARPACK Users' Guide, Solution of Large-Scale Eigenvalue Problems with Implicitly Restarted Arnoldi Methods*, by R. B. Lehoucq, D. C. Sorensen, and C. Yang, SIAM, Philadelphia, PA, 1998, xv+142 pp., $25\frac{1}{2}$ cm, softcover, $39.00

The chief impediment to solving large eigenvalue problems is lack of sufficient memory—a difficulty that has two aspects. In the first place, if the order of the matrix in question is large, the matrix must be represented in some compact form. This limits what we can do with the matrix to simple operations like multiplying it by a vector or, if we are lucky, factoring it so that we have a representation of its inverse. The second aspect is that we cannot hope to store the entire matrix of eigenvectors and must content ourselves with computing a few selected eigenpairs. We are also limited in the number of extra working vectors that we can use to compute these eigenpairs.

Krylov sequence methods are popular in part because they can be made to respect these limitations. The methods proceed by orthogonalizing a Krylov sequence $u, Au, A^2u, \ldots$. When the resulting vectors are arranged in a matrix

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$U_k = (u_1 \cdots u_k)$, they satisfy the relation

$$AU_k = U_k H_k + F_k, \tag{1}$$

where H_k is Hessenberg and F_k is nonzero in only its last column, which is orthogonal to the columns of U_k. Theory (and practice) show that as k increases, the spaces spanned by the U_k contain increasingly good approximations to eigenvectors whose eigenvalues lie on the periphery of the spectrum of A. However, Krylov sequence methods are not necessarily confined to finding such eigenpairs. If we can factor the matrix, we have the option of working with $(A - \sigma I)^{-1}$, which moves the part of the spectrum of A near σ to the periphery—a process known as shift-and-invert enhancement.

When A is Hermitian, the method is known as the Lanczos method. In this case the matrix H_k is tridiagonal, and the vectors u_k satisfy a three-term recurrence. Thus, in principle, it is not necessary to save all the u_i to expand the sequence. In practice, however, the u_i can loose orthogonality, and it is necessary to reorthogonalize them, a costly procedure. It was eventually realized that it is not necessary to reorthogonalize against all preceding vectors, and the algorithm became the method of choice for large Hermitian eigenvalue problems [2, Ch. 13].

When A is non-Hermitian, the method is called the Arnoldi method. Here there is no three-term recurrence, and each new vector must be orthognozied against all the previous vectors. This not only increases the computational work, but raises the possibility that the method will consume the available storage before the required eigenpairs have converged. A cure is to restart the Krylov sequence with a vector containing information on the required eigenvectors. Unfortuantely, good starting vectors are hard to find [1].

Sorensen's implicitly restarted Arnoldi [3] is based on the observation that the matrix H_k contains approximations, called Ritz values, to the eigenvalues of A. If the QR algorithm is used to triangularize H_k in such a way that the eigenvalues that are desired are at the top and the transformations are accumulated in the Arnoldi factorization (1), the factorization can then be truncated to one containing only approximations to the desired eigenpairs. Thus the implicitly restarted Arnoldi algorithm breathes in and out, first expanding the Arnoldi factorization to get better approximations to the desired eigenpairs and then contracting it to get rid of the undesired eigenpairs. Of course there is nothing to keep A from being Hermitian, in which case the algorithm becomes implicitly restarted Lanczos.

The book under review documents the software that Sorensen and his colleagues have built around the idea of implicit restarting. In judging a software package there are three things to take into account: the organization of the software, the accessibility of the user documentation, and the quality of the technical documentation.

ARPACK is soundly designed. An important problem in a package like this is how to get the user to perform the matrix-vector multiplications needed to generate the Arnoldi sequence. The authors have wisely chosen to use reverse communication, a contrived but effective device in which a called routine returns to the calling routine and asks it for further input. The package handles single and double precision, real and complex, and Hermitian and non-Hermitian matrices. It will solve both ordinary and generalized eigenvalue problems with or without shift-and-invert

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

enhancement. The package provides options for tracing and check-pointing the calculations. Calling sequences are necessarily complicated, but there are drivers which cover the majority of cases occuring in practice.

The user documentation is excellent. After leading the reader through a simple example, the authors give a general overview of the capabilities of the package. An appendix contains detailed descriptions of the various drivers. Nothing can make learning to use a package of this magnitude actually easy, but the authors have taken care to see that it is not unnecessarily difficult. I asked students in a class of mine to get ARPACK up and running on problems of their choice. They had little trouble with the project.

Technical documentation can be divided into program details and mathematical underpinnings. Of the former there is none, and the reader must go to the programs to find out what is going on. Fortunately, they are well formatted and commented. I was disappointed in the mathematical description of the algorithm in Chapter 4. There is a lot of information there, but it is not very well organized, and I found parts very tough reading. Important topics (e.g., locking in eigenpairs after they have converged) are slighted while peripheral topics (e.g., block methods) are given undue attention. Since the guide itself is not long, the authors could have easily found extra space for a more leisurely, didactic treatment—a treatment not to be found in the literature.

But this lost opportunity will not be missed by most of the users of ARPACK. The authors, starting from an elegant idea, have produced a sound, well-documented package, which has deservedly become widely popular. We may hope that others with new ideas for solving large eigenvalue problems will hew to the authors' high standards.

References

[1] R. B. Morgan, *On restarting the Arnoldi method for large nonsymmetric eigenvalue problems*, Math. Comp. **65** (1996), 1213–1230. MR **96j:**65028

[2] B. N. Parlett, *The Symmetric Eigenvalue Problem*, Prentice-Hall, Englewoods Cliffs, NJ, 1980. Reissued with revisions by SIAM, Philadelphia, 1998. MR **99c:**65072

[3] D. C. Sorensen, *Implicit application of polynomial filters in a k-step Arnoldi method*, SIAM J. Matrix Anal. Appl. **13** (1992), 357–385. MR **92i:**65076

G. W. STEWART

6[65-02, 65D32, 65Y05, 65Y10, 65Y15, 65Y20]—*Computational Integration*, by Arnold R. Krommer and Christoph W. Ueberhuber, SIAM, Philadelphia, PA, 1998, xx + 445 pp., $25\frac{1}{2}$ cm, softcover, $64.00

The book under review has three major parts entitled, respectively, *Introduction* (86 pages), *Symbolic Integration* (20 pages), *Numerical Integration* (288 pages), and a 23-page bibliography of some 450 items dating mostly from the last 15 years.

Part I contains three chapters. The first deals with various concepts of integrals and their properties: proper and improper Riemann integrals, and Cauchy principal value and Hadamard finite part integrals in one and several variables. Chapter 2 briefly describes selected areas in scientific computing that rely on numerical integration, while Chapter 3 spells out more concretely the types of integration problems occurring in practice. Also discussed are matters of conditioning, available

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

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]).

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

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.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

In Chapter 1 the author presents such fundamental algorithms as the division algorithm, the Euclidean algorithm, and the extended Euclidean algorithm, thereby enabling the student to immediately get "dirty hands". Moreover, a historical discussion on the origins of the word "algorithm" immediately shows that the author is not interested in presenting mathematics as a series of definitions, theorems, and proofs. In Chapter 2 unique factorization is covered, wherein the author very successfully incorporates such concepts as computational complexity, Fermat and Fibonacci numbers, Fermat's factoring method, Mersenne primes, perfect numbers, rep-units, and the irrationality of square roots of nonsquare integers. In Chapter 3 the author discusses prime numbers at length and includes two proofs of the infinitude of prime numbers, the sieve of Erathostenes, the statement of the prime number theorem and history surrounding it. Chapter 4 is concerned with modular arithmetic, an th author succeeds once again by taking a ground-up approach to this, starting with the general notion of an equivalence relation, and including many examples. Some applications to the solvability of Diophantine equations and the notion of invertibility are then presented. Chapter 5 is primarily concerned with finite induction but, more importantly, the essential theorem of this book holding it all together is presented: Fermat's little theorem. Many wonderful exercises are given in this chapter, including such topics as primality testing, the Legendre symbol, and Wieferich numbers. This leads naturally into Chapter 6 which deals with primality testing and Carmichael numbers in considerable detail. This chapter is chock-full of interesting historical tidbits, going back to Leibniz and ending with the famous result of Alford, Granville, and Pomerance. Chapter 7 is the leanest chapter, and covers the required topic of the Chinese Remainder Theorem, along with an application to secret sharing. Chapter 8 is a wonderful digression on the fundamentals of groups. It is a wonderfully laid out chapter, with substantial historical background on the contributions of Cardan, Tartaglia, and Galois. Topics such as modular unit groups, a proof of Fermat's little theorem (and Euler's theorem) all become immediately accessible. A seemingly endless set of exercises is given here. The last three chapters are, in some sense, the destination of the entire book. Chapter 9 has a fairly complete expository on Mersenne and Fermat numbers, including the Lucas–Lehmer primality test for Mersenne numbers, and the current state of the art on factoring and primality of Mersenne numbers. Chapter 10 goes quite a bit further into the topic of primality testing, and also touches on the topic of primitive roots. The Lucas primality test, Pepin's test, and the test of Brillhart, Lehmer, and Selfridge are all described in significant detail. Korselt's characterization of Carmichael numbers is given, along with the complete proof. The final chapter is devoted to the presentation and some implementation considerations of the RSA cryptosystem. Given the nature of the book, one can only expect this to be given in the most rudimentary form, which, nevertheless, the author succeeds in doing very well.

Gary Walsh
Department of Mathematics
University of Ottawa
Ontario, Canada
E-mail address: gwalsh@mathstat.uottawa.ca

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use