
2000j:68205 68W30 11Y16 68-01 68-02

von zur Gathen, Joachim (D-PDRB)**;**
Gerhard, Jürgen (D-PDRB)

★Modern computer algebra. (English. English summary)

Cambridge University Press, *New York*, 1999. *xiv*+753 *pp.* $59.95.
ISBN 0-521-64176-4

This reviewer was first exposed to the beauty and utility of algorithmic algebra and number theory by the second volume of Donald Knuth's The art of computer programming, subtitled Seminumerical algorithms [Second edition, Addison-Wesley Publishing Co., Reading, Mass., 1981; MR 83i:68003]. Knuth used a lively style and a historical approach to explain efficient algorithms on polynomials and integers. Dozens of excellent exercises helped the reader master the material.

The new textbook under review is evidently an intellectual descendant of Knuth's, but with a focus broadened to the algorithmic basis of symbolic computation software such as Maple and Mathematica. Intended for advanced undergraduates or graduate students in computer science and mathematics, it contains a huge amount of material, exuberantly presented, with a panoply of useful and interesting exercises. (Solutions to selected exercises are available at the book's web site, http://www-math.uni-paderborn.de/mca/ .) Following Knuth, the authors explore the historical roots of their subject, and they go Knuth one better by including photographs and color diagrams.

The book is divided into five sections, each named for a famous mathematician. Part I (Euclid) discusses basic operations on integers and polynomials such as multiplication and greatest common divisor. Part II (Newton) deals with Newton iteration and polynomial evaluation and interpolation. Part III (Gauss) covers polynomial arithmetic over finite fields and factorization in $\mathbf{Q}[x]$. Part IV (Fermat) discusses integer factorization and primality testing. Part V (Hilbert) is an introduction to Grobner bases, symbolic integration, and symbolic summation. The emphasis throughout is on design and analysis of efficient algorithms for these problems, with rigorous proofs of running-time estimates. For the most part, these estimates are given using the usual "big-Oh" notation, but sometimes explicit constants are provided. Each section also contains a discussion of applications, such as image compression and cryptography. An appendix entitled "Fundamental concepts" treats the basics of groups, rings, fields, linear algebra, and complexity theory.

The authors evidently have a deep knowledge of and appreciation for their subject. For the most part, the writing is animated and comprehensible, although a few Germanicisms remain (p. 126: "How

many feet is Sesame Street long?"). The illustrations are generally attractive and useful, one exception being that the entire contents of p. 214 is devoted to illustrating the cost of Karatsuba's algorithm through successive approximations to a fractal of dimension $\log_2 3$. Each chapter is introduced by a number of interesting quotations (although on page 8, "Any sufficiently advanced technology is indistinguishable from magic" is mistakenly attributed to Paul Theroux instead of Arthur C. Clarke).

In the final analysis, this lively and exciting volume represents the state of the art in textbooks on computer algebra. Every student and instructor in this area will want a copy.

Jeffrey O. Shallit (3-WTRL-C)