936.11069
von zur Gathen, Joachim; Gerhard, Juergen
Modern computer algebra. (English)
Cambridge: Cambridge University Press. xiii, 753 p. 29.95; $ 59.95 (1999).
[ISBN 0-521-64176-4/hbk]

As indicated in the Introduction, the aim of the authors of this book is triple: give rather complete information on the mathematical tools and results used, analyze the asymptotic cost of the algorithms and propose asymptotically fast methods. They reach completely this triple objective. This fact distinguishes this book from the preceding ones in the same domain which either focus on the mathematical point of view, or are mainly user-oriented.
This book contains more than seven hundred pages and five main sections, each section is given the name of a famous mathematician: Euclid, Newton, Fermat, Gauss and Hilbert. Of course, the part "Euclid" contains the Euclidean algorithm and also a very detailed study of modular calculus and its applications, resultant computation, and application for decoding BCH codes. The section "Newton" contains the presentation of fast algorithms for the elementary arithmetical operations, the fast Fourier transform algorithm (FFT), interpolation, ... The elementary arithmetics: primality tests, factorization of integers, applications to cryptography (RSA method) is the part "Fermat". The chapters linked to Gauss are: factorization of polynomials over finite fields, Hensel lifting lemma and factoring polynomials with integer coefficients, search of small vectors in lattices (LLL method) and applications. The last part, "Hilbert", contains the study of Groebner bases, symbolic summation, symbolic integration, and applications. There is also an Appendix on fundamental concepts such as elementary algebraic structures, linear algebra, finite fields, finite probability spaces and complexity theory.
Each chapter contains numerous examples which are very instructive, the pseudocode of the algorithms, exercises and very complete and interesting historical notes. The cost of the algorithms is studied in great detail and the authors give comments on the efficiency of these algorithms and their present practical limits.
The style is very clear. The arguments are very precise. In my opinion, the level of presentation is convenient for graduate students, some parts are quite readable for good undergraduate students. The typography and the quality of illustration of this Cambridge book are splendid.
To conclude, I find the quality of this book really exceptional, this is certainly an excellent source on the state of the art in Computer Algebra, just before 2000.

Maurice Mignotte (Strasbourg)

Keywords : computer algebra; asymptotic cost of algorithms; asymptotically fast methods; Euclidean algorithm; modular calculus; resultant computation; fast Fourier transform algorithm; interpolation; primality tests; factorization of integers; cryptography; RSA method; factorization of polynomials over finite fields; Hensel lifting lemma; LLL method; Groebner bases; symbolic summation; symbolic integration; complexity

Classification:

- 11Yxx Computational number theory
- 68W30 Symbolic computation and algebraic computation
- 68-01 Textbooks (computer science)
- 13P05 Polynomials, factorization
- 11Y16 Algorithms
- 12Y05 Computational aspects of field theory and polynomials
- 11Y05 Factorization
- 11Y11 Primality