Modern Computer Algebra

Computer algebra systems are gaining more and more importance in all areas of science and engineering. This textbook gives a thorough introduction to the algorithmic basis of the mathematical engine in computer algebra systems.

It is designed to accompany one- or two-semester courses for advanced undergraduate or graduate students in computer science or mathematics. Its comprehensiveness and authority make it also an essential reference for professionals in the area.

Special features include: detailed study of algorithms including time analysis; implementation reports on several topics; complete proofs of the mathematical underpinnings; a wide variety of applications (among others, in chemistry, coding theory, cryptography, computational logic, and the design of calendars and musical scales). Finally, a great deal of historical information and illustration enlivens the text.

Joachim von zur Gathen has a PhD from Universität Zürich, taught at University of Toronto from 1981 to 1994, and is now at Universität Paderborn.

Jürgen Gerhard has a PhD from Universität Paderborn, and is now working at Maplesoft.
Modern Computer Algebra
Second Edition

JOACHIM VON ZUR GATHEN
Universität Paderborn

JÜRGEN GERHARD
Maplesoft, Waterloo
To Dorothea, Rafaela, Désirée
For endless patience

To Mercedes Cappuccino
# Contents

## Introduction

1 Cyclohexane, cryptography, codes, and computer algebra 
   1.1 Cyclohexane conformations ........................................... 9
   1.2 The RSA cryptosystem .................................................. 14
   1.3 Distributed data structures ........................................... 16
   1.4 Computer algebra systems ............................................. 17

1 Euclid

2 Fundamental algorithms
   2.1 Representation and addition of numbers .......................... 27
   2.2 Representation and addition of polynomials ....................... 30
   2.3 Multiplication .......................................................... 32
   2.4 Division with remainder ............................................... 35
       Notes ................................................................. 39
       Exercises ......................................................... 39

3 The Euclidean Algorithm
   3.1 Euclidean domains .................................................... 43
   3.2 The Extended Euclidean Algorithm ................................ 45
   3.3 Cost analysis for $\mathbb{Z}$ and $F[x]$ ............................. 49
   3.4 (Non-)Uniqueness of the gcd ........................................ 53
       Notes ................................................................. 59
       Exercises ......................................................... 60

4 Applications of the Euclidean Algorithm
   4.1 Modular arithmetic .................................................... 67
   4.2 Modular inverses via Euclid ......................................... 71
   4.3 Repeated squaring .................................................... 73
   4.4 Modular inverses via Fermat ....................................... 74
## Contents

4.5 Linear Diophantine equations .................................. 75
4.6 Continued fractions and Diophantine approximation .......... 77
4.7 Calendars ....................................................... 81
4.8 Musical scales .................................................. 82
Notes ............................................................... 86
Exercises ........................................................... 89

5 Modular algorithms and interpolation .......................... 95
5.1 Change of representation ........................................ 98
5.2 Evaluation and interpolation .................................... 99
5.3 Application: Secret sharing .................................... 101
5.4 The Chinese Remainder Algorithm ............................ 102
5.5 Modular determinant computation ............................. 107
5.6 Hermite interpolation .......................................... 111
5.7 Rational function reconstruction .............................. 113
5.8 Cauchy interpolation .......................................... 116
5.9 Padé approximation ........................................... 119
5.10 Rational number reconstruction .............................. 122
5.11 Partial fraction decomposition ............................... 126
Notes ............................................................... 129
Exercises ........................................................... 130

6 The resultant and gcd computation ........................... 139
6.1 Coefficient growth in the Euclidean Algorithm ................ 139
6.2 Gauß’ lemma ................................................. 145
6.3 The resultant ................................................. 150
6.4 Modular gcd algorithms ...................................... 156
6.5 Modular gcd algorithm in $F[x,y]$ ............................ 159
6.6 Mignotte’s factor bound and a modular gcd algorithm in $\mathbb{Z}[x]$ 162
6.7 Small primes modular gcd algorithms ...................... 166
6.8 Application: intersecting plane curves ...................... 169
6.9 Nonzero preservation and the gcd of several polynomials . 174
6.10 Subresultants ............................................... 176
6.11 Modular Extended Euclidean Algorithms .................. 181
6.12 Pseudodivision and primitive Euclidean Algorithms ........ 189
6.13 Implementations ............................................. 191
Notes ............................................................... 195
Exercises ........................................................... 197

7 Application: Decoding BCH codes ......................... 207
Notes ............................................................... 213
Exercises ........................................................... 213
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td>Newton</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Fast multiplication</td>
<td>215</td>
</tr>
<tr>
<td>8.1</td>
<td>Karatsuba’s multiplication algorithm</td>
<td>219</td>
</tr>
<tr>
<td>8.2</td>
<td>The Discrete Fourier Transform and the Fast Fourier Transform</td>
<td>220</td>
</tr>
<tr>
<td>8.3</td>
<td>Schönhage and Strassen’s multiplication algorithm</td>
<td>225</td>
</tr>
<tr>
<td>8.4</td>
<td>Multiplication in ( \mathbb{Z}[x] ) and ( R[x,y] )</td>
<td>235</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>243</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>244</td>
</tr>
<tr>
<td>9</td>
<td>Newton iteration</td>
<td>253</td>
</tr>
<tr>
<td>9.1</td>
<td>Division with remainder using Newton iteration</td>
<td>253</td>
</tr>
<tr>
<td>9.2</td>
<td>Generalized Taylor expansion and radix conversion</td>
<td>260</td>
</tr>
<tr>
<td>9.3</td>
<td>Formal derivatives and Taylor expansion</td>
<td>261</td>
</tr>
<tr>
<td>9.4</td>
<td>Solving polynomial equations via Newton iteration</td>
<td>263</td>
</tr>
<tr>
<td>9.5</td>
<td>Computing integer roots</td>
<td>267</td>
</tr>
<tr>
<td>9.6</td>
<td>Newton iteration, Julia sets, and fractals</td>
<td>269</td>
</tr>
<tr>
<td>9.7</td>
<td>Implementations of fast arithmetic</td>
<td>274</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>282</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>283</td>
</tr>
<tr>
<td>10</td>
<td>Fast polynomial evaluation and interpolation</td>
<td>291</td>
</tr>
<tr>
<td>10.1</td>
<td>Fast multipoint evaluation</td>
<td>291</td>
</tr>
<tr>
<td>10.2</td>
<td>Fast interpolation</td>
<td>295</td>
</tr>
<tr>
<td>10.3</td>
<td>Fast Chinese remaindering</td>
<td>297</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>302</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>302</td>
</tr>
<tr>
<td>11</td>
<td>Fast Euclidean Algorithm</td>
<td>309</td>
</tr>
<tr>
<td>11.1</td>
<td>A fast Euclidean Algorithm for polynomials</td>
<td>309</td>
</tr>
<tr>
<td>11.2</td>
<td>Subresultants via Euclid’s algorithm</td>
<td>320</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>324</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>324</td>
</tr>
<tr>
<td>12</td>
<td>Fast linear algebra</td>
<td>327</td>
</tr>
<tr>
<td>12.1</td>
<td>Strassen’s matrix multiplication</td>
<td>327</td>
</tr>
<tr>
<td>12.2</td>
<td>Application: fast modular composition of polynomials</td>
<td>330</td>
</tr>
<tr>
<td>12.3</td>
<td>Linearly recurrent sequences</td>
<td>331</td>
</tr>
<tr>
<td>12.4</td>
<td>Wiedemann’s algorithm and black box linear algebra</td>
<td>337</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>344</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>345</td>
</tr>
</tbody>
</table>
Contents

13 Fourier Transform and image compression 349
  13.1 The Continuous and the Discrete Fourier Transform 349
  13.2 Audio and video compression 353
  Notes 358
  Exercises 358

III Gauß 361

14 Factoring polynomials over finite fields 367
  14.1 Factorization of polynomials 367
  14.2 Distinct-degree factorization 370
  14.3 Equal-degree factorization: Cantor and Zassenhaus’ algorithm 372
  14.4 A complete factoring algorithm 379
  14.5 Application: root finding 382
  14.6 Squarefree factorization 383
  14.7 The iterated Frobenius algorithm 387
  14.8 Algorithms based on linear algebra 391
  14.9 Testing irreducibility and constructing irreducible polynomials 396
  14.10 Cyclotomic polynomials and constructing BCH codes 402
     Notes 407
     Exercises 411

15 Hensel lifting and factoring polynomials 421
  15.1 Factoring in \( \mathbb{Z}[x] \) and \( \mathbb{Q}[x] \): the basic idea 421
  15.2 A factoring algorithm 423
  15.3 Frobenius’ and Chebotarev’s density theorems 429
  15.4 Hensel lifting 432
  15.5 Multifactor Hensel lifting 438
  15.6 Factoring using Hensel lifting: Zassenhaus’ algorithm 441
  15.7 Implementations 449
     Notes 453
     Exercises 455

16 Short vectors in lattices 461
  16.1 Lattices 461
  16.2 Lenstra, Lenstra and Lovász’ basis reduction algorithm 463
  16.3 Cost estimate for basis reduction 468
  16.4 From short vectors to factors 475
  16.5 A polynomial-time factoring algorithm for \( \mathbb{Z}[x] \) 477
  16.6 Factoring multivariate polynomials 481
     Notes 484
     Exercises 486
## Contents

### 17 Applications of basis reduction

17.1 Breaking knapsack-type cryptosystems ........................................ 491
17.2 Pseudorandom numbers ............................................................ 493
17.3 Simultaneous Diophantine approximation ................................. 493
17.4 Disproof of Mertens’ conjecture .............................................. 496
   Notes ................................................................. 497
   Exercises ............................................................ 497

### IV Fermat

18 Primality testing

18.1 Multiplicative order of integers ............................................. 505
18.2 The Fermat test ............................................................... 507
18.3 The strong pseudoprimality test ............................................ 508
18.4 Finding primes ............................................................... 511
18.5 The Solovay and Strassen test ............................................. 517
18.6 The complexity of primality testing ...................................... 518
   Notes ................................................................. 520
   Exercises ............................................................ 523

### 19 Factoring integers

19.1 Factorization challenges ..................................................... 531
19.2 Trial division ............................................................... 533
19.3 Pollard’s and Strassen’s method ........................................... 534
19.4 Pollard’s rho method ....................................................... 535
19.5 Dixon’s random squares method ......................................... 539
19.6 Pollard’s \( p - 1 \) method ................................................ 547
19.7 Lenstra’s elliptic curve method ............................................ 547
   Notes ................................................................. 557
   Exercises ............................................................ 559

### 20 Application: Public key cryptography

20.1 Cryptosystems ............................................................... 563
20.2 The RSA cryptosystem ...................................................... 566
20.3 The Diffie–Hellman key exchange protocol ............................. 568
20.4 The ElGamal cryptosystem ................................................ 569
20.5 Rabin’s cryptosystem ....................................................... 569
20.6 Elliptic curve systems ....................................................... 570
   Notes ................................................................. 570
   Exercises ............................................................ 571
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
<td>Hilbert</td>
<td>575</td>
</tr>
<tr>
<td>21</td>
<td>Gröbner bases</td>
<td>581</td>
</tr>
<tr>
<td>21.1</td>
<td>Polynomial ideals</td>
<td>581</td>
</tr>
<tr>
<td>21.2</td>
<td>Monomial orders and multivariate division with remainder</td>
<td>585</td>
</tr>
<tr>
<td>21.3</td>
<td>Monomial ideals and Hilbert’s basis theorem</td>
<td>591</td>
</tr>
<tr>
<td>21.4</td>
<td>Gröbner bases and S-polynomials</td>
<td>594</td>
</tr>
<tr>
<td>21.5</td>
<td>Buchberger’s algorithm</td>
<td>598</td>
</tr>
<tr>
<td>21.6</td>
<td>Geometric applications</td>
<td>602</td>
</tr>
<tr>
<td>21.7</td>
<td>The complexity of computing Gröbner bases</td>
<td>606</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>607</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>609</td>
</tr>
<tr>
<td>22</td>
<td>Symbolic integration</td>
<td>613</td>
</tr>
<tr>
<td>22.1</td>
<td>Differential algebra</td>
<td>613</td>
</tr>
<tr>
<td>22.2</td>
<td>Hermite’s method</td>
<td>615</td>
</tr>
<tr>
<td>22.3</td>
<td>The method of Lazard, Rioboo, Rothstein, and Trager</td>
<td>617</td>
</tr>
<tr>
<td>22.4</td>
<td>Hyperexponential integration: Almkvist &amp; Zeilberger’s algorithm</td>
<td>622</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>630</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>631</td>
</tr>
<tr>
<td>23</td>
<td>Symbolic summation</td>
<td>635</td>
</tr>
<tr>
<td>23.1</td>
<td>Polynomial summation</td>
<td>635</td>
</tr>
<tr>
<td>23.2</td>
<td>Harmonic numbers</td>
<td>640</td>
</tr>
<tr>
<td>23.3</td>
<td>Greatest factorial factorization</td>
<td>643</td>
</tr>
<tr>
<td>23.4</td>
<td>Hypergeometric summation: Gosper’s algorithm</td>
<td>648</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>659</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>661</td>
</tr>
<tr>
<td>24</td>
<td>Applications</td>
<td>667</td>
</tr>
<tr>
<td>24.1</td>
<td>Gröbner proof systems</td>
<td>667</td>
</tr>
<tr>
<td>24.2</td>
<td>Petri nets</td>
<td>669</td>
</tr>
<tr>
<td>24.3</td>
<td>Proving identities and analysis of algorithms</td>
<td>671</td>
</tr>
<tr>
<td>24.4</td>
<td>Cyclohexane revisited</td>
<td>675</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
<td>687</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
<td>688</td>
</tr>
<tr>
<td>Appendix</td>
<td>691</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Fundamental concepts</td>
<td>693</td>
</tr>
<tr>
<td>25.1</td>
<td>Groups</td>
<td>693</td>
</tr>
<tr>
<td>25.2</td>
<td>Rings</td>
<td>695</td>
</tr>
</tbody>
</table>
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.3 Polynomials and fields</td>
<td>698</td>
</tr>
<tr>
<td>25.4 Finite fields</td>
<td>701</td>
</tr>
<tr>
<td>25.5 Linear algebra</td>
<td>703</td>
</tr>
<tr>
<td>25.6 Finite probability spaces</td>
<td>707</td>
</tr>
<tr>
<td>25.7 “Big Oh” notation</td>
<td>710</td>
</tr>
<tr>
<td>25.8 Complexity theory</td>
<td>711</td>
</tr>
<tr>
<td>Notes</td>
<td>714</td>
</tr>
<tr>
<td>Sources of illustrations</td>
<td>715</td>
</tr>
<tr>
<td>Sources of quotations</td>
<td>715</td>
</tr>
<tr>
<td>List of algorithms</td>
<td>720</td>
</tr>
<tr>
<td>List of figures and tables</td>
<td>722</td>
</tr>
<tr>
<td>References</td>
<td>724</td>
</tr>
<tr>
<td>List of notation</td>
<td>758</td>
</tr>
<tr>
<td>Index</td>
<td>759</td>
</tr>
</tbody>
</table>

---

**Keeping up to date**

Addenda and corrigenda, comments, solutions to selected exercises, and ordering information can be found on the book's web page:

[http://www.math.upb.de/mca/](http://www.math.upb.de/mca/)
A Beggar’s Book Out-worths a Noble’s Blood.¹

William Shakespeare (1613)

Some books are to be tasted, others to be swallowed, and some few to be chewed and digested.

Francis Bacon (1597)

Les plus grands analystes eux-mêmes ont bien rarement dédaigné de se tenir à la portée de la classe moyenne des lecteurs; elle est en effet la plus nombreuse, et celle qui a le plus à profiter dans leurs écrits.²

Anonymous referee (1825)

It is true, we have already a great many Books of Algebra, and one might even furnish a moderate Library purely with Authors on that Subject.

Isaac Newton (1728)

فرمت هذا الكتاب وجمعته فيه جميع ما يحتاج إليه الحاسب محترزا عن أشباع ممل واختصار معنی

Ghiyāth al-Dīn Jamshīd bin Masrūd bin Maḥmūd al-Kāshī (1427)

¹ The sources for the quotations are given on pages 715–719.
² The greatest analysts [mathematicians] themselves have rarely shied away from keeping within the reach of the average class of readers; this is in fact the most numerous one, and the one that stands to profit most from their writing.
³ I wrote this book and compiled in it everything that is necessary for the computer, avoiding both boring verbosity and misleading brevity.