

# Contents

<b>Introduction</b>	<b>1</b>
<b>1 Cyclohexane, cryptography, codes, and computer algebra</b>	<b>9</b>
1.1 Cyclohexane conformations . . . . .	9
1.2 The RSA cryptosystem . . . . .	14
1.3 Distributed data structures . . . . .	16
1.4 Computer algebra systems . . . . .	17
<b>I Euclid</b>	<b>21</b>
<b>2 Fundamental algorithms</b>	<b>27</b>
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
<b>3 The Euclidean Algorithm</b>	<b>43</b>
3.1 ✓ Euclidean domains . . . . .	43
3.2 ✓ The Extended Euclidean Algorithm . . . . .	46
3.3 Cost analysis for $\mathbb{Z}$ and $F[x]$ . . . . .	50
Notes . . . . .	55
Exercises . . . . .	57
<b>4 Applications of the Euclidean Algorithm</b>	<b>63</b>
4.1 \ Modular arithmetic . . . . .	63
4.2 \ Modular inverses via Euclid . . . . .	67
4.3 \ Repeated squaring . . . . .	69
4.4 \ Modular inverses via Fermat . . . . .	70
4.5 ✓ Linear Diophantine equations . . . . .	71

4.6	✓ Continued fractions and Diophantine approximation . . . . .	73
4.7	Calendars . . . . .	77
4.8	Musical scales . . . . .	78
	Notes . . . . .	81
	Exercises . . . . .	84
<b>5</b>	<b>Modular algorithms and interpolation</b>	<b>89</b>
5.1	Change of representation . . . . .	92
5.2	Evaluation and interpolation . . . . .	93
5.3	Application: Secret sharing . . . . .	95
5.4	The Chinese Remainder Algorithm . . . . .	96
5.5	Modular determinant computation . . . . .	101
5.6	Hermite interpolation . . . . .	105
5.7	Rational function reconstruction . . . . .	106
5.8	Cauchy interpolation . . . . .	110
5.9	Padé approximation . . . . .	112
5.10	Rational number reconstruction . . . . .	116
5.11	Partial fraction decomposition . . . . .	119
	Notes . . . . .	122
	Exercises . . . . .	123
<b>6</b>	<b>The resultant and gcd computation</b>	<b>131</b>
6.1	Coefficient growth in the Euclidean Algorithm . . . . .	131
6.2	Gauß' lemma . . . . .	137
6.3	The resultant . . . . .	142
6.4	Modular gcd algorithms . . . . .	148
6.5	Modular gcd algorithm in $F[x, y]$ . . . . .	151
6.6	Mignotte's factor bound and a modular gcd algorithm in $\mathbb{Z}[x]$ . . . . .	153
6.7	Small primes modular gcd algorithms . . . . .	157
6.8	Application: intersecting plane curves . . . . .	161
6.9	Nonzero preservation and the gcd of several polynomials . . . . .	165
6.10	Subresultants . . . . .	167
6.11	Modular Extended Euclidean Algorithms . . . . .	172
6.12	Pseudo-division and primitive Euclidean Algorithms . . . . .	180
6.13	Implementations . . . . .	182
	Notes . . . . .	185
	Exercises . . . . .	188
<b>7</b>	<b>Application: Decoding BCH codes</b>	<b>197</b>
	Notes . . . . .	203
	Exercises . . . . .	203

<b>II</b>	<b>Newton</b>	<b>205</b>
<b>8</b>	<b>Fast multiplication</b>	<b>209</b>
8.1	Karatsuba's multiplication algorithm . . . . .	210
8.2	The Discrete Fourier Transform and the Fast Fourier Transform . . . . .	215
8.3	Schönhage and Strassen's multiplication algorithm . . . . .	225
8.4	Multiplication in $\mathbb{Z}[x]$ and $\mathbb{R}[x, y]$ . . . . .	233
	Notes . . . . .	234
	Exercises . . . . .	235
<b>9</b>	<b>Newton iteration</b>	<b>243</b>
9.1	Division with remainder using Newton iteration . . . . .	243
9.2	Generalized Taylor expansion and radix conversion . . . . .	250
9.3	Formal derivatives and Taylor expansion . . . . .	251
9.4	Solving polynomial equations via Newton iteration . . . . .	253
9.5	Computing integer roots . . . . .	257
9.6	Valuations, Newton iteration, and Julia sets . . . . .	259
9.7	Implementations of fast arithmetic . . . . .	263
	Notes . . . . .	272
	Exercises . . . . .	272
<b>10</b>	<b>Fast polynomial evaluation and interpolation</b>	<b>279</b>
10.1	Fast multipoint evaluation . . . . .	279
10.2	Fast interpolation . . . . .	283
10.3	Fast Chinese remaindering . . . . .	285
	Notes . . . . .	290
	Exercises . . . . .	290
<b>11</b>	<b>Fast Euclidean Algorithm</b>	<b>295</b>
11.1	A fast Euclidean Algorithm for polynomials . . . . .	295
11.2	Subresultants via Euclid's algorithm . . . . .	306
	Notes . . . . .	310
	Exercises . . . . .	310
<b>12</b>	<b>Fast linear algebra</b>	<b>313</b>
12.1	Strassen's matrix multiplication . . . . .	313
12.2	Application: fast modular composition of polynomials . . . . .	316
12.3	Linearly recurrent sequences . . . . .	317
12.4	Wiedemann's algorithm and black box linear algebra . . . . .	323
	Notes . . . . .	330
	Exercises . . . . .	331

<b>13</b>	<b>Fourier Transform and image compression</b>	<b>335</b>
13.1	The Continuous and the Discrete Fourier Transform . . . . .	335
13.2	Audio and video compression . . . . .	339
	Notes . . . . .	344
	Exercises . . . . .	344
<b>III</b>	<b>Gauß</b>	<b>347</b>
<b>14</b>	<b>Factoring polynomials over finite fields</b>	<b>353</b>
14.1	Factorization of polynomials . . . . .	353
14.2	Distinct-degree factorization . . . . .	356
14.3	Equal-degree factorization: Cantor and Zassenhaus' algorithm . . . . .	358
14.4	A complete factoring algorithm . . . . .	365
14.5	Application: root finding . . . . .	368
14.6	Squarefree factorization . . . . .	369
14.7	The iterated Frobenius algorithm . . . . .	373
14.8	Algorithms based on linear algebra . . . . .	377
14.9	Testing irreducibility and constructing irreducible polynomials . . . . .	382
14.10	Cyclotomic polynomials and constructing BCH codes . . . . .	387
	Notes . . . . .	393
	Exercises . . . . .	397
<b>15</b>	<b>Hensel lifting and factoring polynomials</b>	<b>407</b>
15.1	Factoring in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ : the basic idea . . . . .	407
15.2	A factoring algorithm . . . . .	409
15.3	Frobenius' and Chebotarev's density theorems . . . . .	415
15.4	Hensel lifting . . . . .	418
15.5	Multifactor Hensel lifting . . . . .	424
15.6	Factoring using Hensel lifting: Zassenhaus' algorithm . . . . .	427
15.7	Implementations . . . . .	435
	Notes . . . . .	440
	Exercises . . . . .	441
<b>16</b>	<b>Short vectors in lattices</b>	<b>447</b>
16.1	Lattices . . . . .	447
16.2	Lenstra, Lenstra and Lovász' basis reduction algorithm . . . . .	449
16.3	Cost estimate for basis reduction . . . . .	454
16.4	From short vectors to factors . . . . .	461
16.5	A polynomial-time factoring algorithm for $\mathbb{Q}[x]$ . . . . .	463
16.6	Factoring multivariate polynomials . . . . .	467
	Notes . . . . .	470
	Exercises . . . . .	472

<b>17 Applications of basis reduction</b>	<b>477</b>
17.1 Breaking knapsack-type cryptosystems . . . . .	477
17.2 Pseudorandom numbers . . . . .	479
17.3 Simultaneous Diophantine approximation . . . . .	479
17.4 Disproof of Mertens' conjecture . . . . .	482
Notes . . . . .	483
Exercises . . . . .	483
<b>IV Fermat</b>	<b>485</b>
<b>18 Primality testing</b>	<b>491</b>
18.1 Multiplicative order of integers . . . . .	491
18.2 The Fermat test . . . . .	493
18.3 The strong pseudoprimality test . . . . .	494
18.4 Finding primes . . . . .	497
18.5 The Solovay and Strassen test . . . . .	503
18.6 The complexity of primality testing . . . . .	504
Notes . . . . .	506
Exercises . . . . .	509
<b>19 Factoring integers</b>	<b>515</b>
19.1 Factorization challenges . . . . .	515
19.2 Trial division . . . . .	518
19.3 Pollard's and Strassen's method . . . . .	518
19.4 Pollard's rho method . . . . .	519
19.5 Dixon's random squares method . . . . .	523
19.6 Pollard's $p - 1$ method . . . . .	531
19.7 Lenstra's elliptic curve method . . . . .	531
Notes . . . . .	541
Exercises . . . . .	543
<b>20 Application: Public key cryptography</b>	<b>547</b>
20.1 Cryptosystems . . . . .	547
20.2 The RSA cryptosystem . . . . .	550
20.3 The Diffie–Hellman key exchange protocol . . . . .	552
20.4 The ElGamal cryptosystem . . . . .	553
20.5 Rabin's cryptosystem . . . . .	553
20.6 Elliptic curve systems . . . . .	554
20.7 Short vector cryptosystems . . . . .	554
Notes . . . . .	555
Exercises . . . . .	555

<b>V Hilbert</b>	<b>559</b>
<b>21 Gröbner bases</b>	<b>565</b>
21.1 Polynomial ideals . . . . .	565
21.2 Monomial orders and multivariate division with remainder . . . . .	570
21.3 Monomial ideals and Hilbert's basis theorem . . . . .	575
21.4 Gröbner bases and S-polynomials . . . . .	579
21.5 Buchberger's algorithm . . . . .	582
21.6 Geometric applications . . . . .	586
21.7 The complexity of computing Gröbner bases . . . . .	589
Notes . . . . .	591
Exercises . . . . .	593
<b>22 Symbolic integration</b>	<b>597</b>
22.1 Differential algebra . . . . .	597
22.2 Hermite's method . . . . .	599
22.3 The method of Rothstein and Trager . . . . .	601
Notes . . . . .	606
Exercises . . . . .	606
<b>23 Symbolic summation</b>	<b>609</b>
23.1 Polynomial summation . . . . .	609
23.2 Harmonic numbers . . . . .	614
23.3 Greatest factorial factorization . . . . .	617
23.4 Hypergeometric summation: Gosper's algorithm . . . . .	622
Notes . . . . .	633
Exercises . . . . .	635
<b>24 Applications</b>	<b>641</b>
24.1 Gröbner proof systems . . . . .	641
24.2 Petri nets . . . . .	643
24.3 Proving identities and analysis of algorithms . . . . .	645
24.4 Cyclohexane revisited . . . . .	649
Notes . . . . .	661
Exercises . . . . .	662
<b>Appendix</b>	<b>665</b>
<b>25 Fundamental concepts</b>	<b>667</b>
25.1 Groups . . . . .	667
25.2 Rings . . . . .	669
25.3 Polynomials and fields . . . . .	672

25.4	Finite fields . . . . .	675
25.5	Linear algebra . . . . .	677
25.6	Finite probability spaces . . . . .	681
25.7	“Big Oh” notation . . . . .	684
25.8	Complexity theory . . . . .	685
	Notes . . . . .	688
	Sources of illustrations . . . . .	689
	Sources of quotations . . . . .	689
	List of algorithms . . . . .	694
	List of figures and tables . . . . .	696
	References . . . . .	698
	List of notation . . . . .	728
	Index . . . . .	729

### 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.uni-paderborn.de/mca/>