

Contents

Introduction	1
1 Cyclohexane, cryptography, codes, and computer algebra	11
1.1 Cyclohexane conformations	11
1.2 The RSA cryptosystem	16
1.3 Distributed data structures	18
1.4 Computer algebra systems	19
I Euclid	23
2 Fundamental algorithms	29
2.1 Representation and addition of numbers	29
2.2 Representation and addition of polynomials	32
2.3 Multiplication	34
2.4 Division with remainder	37
Notes	41
Exercises	41
3 The Euclidean Algorithm	45
3.1 Euclidean domains	45
3.2 The Extended Euclidean Algorithm	47
3.3 Cost analysis for \mathbb{Z} and $F[x]$	51
3.4 (Non-)Uniqueness of the gcd	55
Notes	61
Exercises	62
4 Applications of the Euclidean Algorithm	69
4.1 Modular arithmetic	69
4.2 Modular inverses via Euclid	73
4.3 Repeated squaring	75
4.4 Modular inverses via Fermat	76

4.5	Linear Diophantine equations	77
4.6	Continued fractions and Diophantine approximation	79
4.7	Calendars	83
4.8	Musical scales	84
	Notes	88
	Exercises	91
5	Modular algorithms and interpolation	97
5.1	Change of representation	100
5.2	Evaluation and interpolation	101
5.3	Application: Secret sharing	103
5.4	The Chinese Remainder Algorithm	104
5.5	Modular determinant computation	109
5.6	Hermite interpolation	113
5.7	Rational function reconstruction	115
5.8	Cauchy interpolation	118
5.9	Padé approximation	121
5.10	Rational number reconstruction	124
5.11	Partial fraction decomposition	128
	Notes	131
	Exercises	132
6	The resultant and gcd computation	141
6.1	Coefficient growth in the Euclidean Algorithm	141
6.2	Gauß' lemma	147
6.3	The resultant	152
6.4	Modular gcd algorithms	158
6.5	Modular gcd algorithm in $F[x, y]$	161
6.6	Mignotte's factor bound and a modular gcd algorithm in $\mathbb{Z}[x]$	164
6.7	Small primes modular gcd algorithms	168
6.8	Application: intersecting plane curves	171
6.9	Nonzero preservation and the gcd of several polynomials	176
6.10	Subresultants	178
6.11	Modular Extended Euclidean Algorithms	183
6.12	Pseudodivision and primitive Euclidean Algorithms	190
6.13	Implementations	193
	Notes	197
	Exercises	199
7	Application: Decoding BCH codes	209
	Notes	215
	Exercises	215

II	Newton	217
8	Fast multiplication	221
8.1	Karatsuba's multiplication algorithm	222
8.2	The Discrete Fourier Transform and the Fast Fourier Transform	227
8.3	Schönhage and Strassen's multiplication algorithm	238
8.4	Multiplication in $\mathbb{Z}[x]$ and $R[x, y]$	245
	Notes	247
	Exercises	248
9	Newton iteration	257
9.1	Division with remainder using Newton iteration	257
9.2	Generalized Taylor expansion and radix conversion	264
9.3	Formal derivatives and Taylor expansion	265
9.4	Solving polynomial equations via Newton iteration	267
9.5	Computing integer roots	271
9.6	Newton iteration, Julia sets, and fractals	273
9.7	Implementations of fast arithmetic	278
	Notes	286
	Exercises	287
10	Fast polynomial evaluation and interpolation	295
10.1	Fast multipoint evaluation	295
10.2	Fast interpolation	299
10.3	Fast Chinese remaindering	301
	Notes	306
	Exercises	306
11	Fast Euclidean Algorithm	313
11.1	A fast Euclidean Algorithm for polynomials	313
11.2	Subresultants via Euclid's algorithm	327
	Notes	332
	Exercises	332
12	Fast linear algebra	335
12.1	Strassen's matrix multiplication	335
12.2	Application: fast modular composition of polynomials	338
12.3	Linearly recurrent sequences	340
12.4	Wiedemann's algorithm and black box linear algebra	346
	Notes	352
	Exercises	353

13	Fourier Transform and image compression	359
13.1	The Continuous and the Discrete Fourier Transform	359
13.2	Audio and video compression	363
	Notes	368
	Exercises	368
III	Gauß	371
14	Factoring polynomials over finite fields	377
14.1	Factorization of polynomials	377
14.2	Distinct-degree factorization	380
14.3	Equal-degree factorization: Cantor and Zassenhaus' algorithm	382
14.4	A complete factoring algorithm	389
14.5	Application: root finding	392
14.6	Squarefree factorization	393
14.7	The iterated Frobenius algorithm	398
14.8	Algorithms based on linear algebra	401
14.9	Testing irreducibility and constructing irreducible polynomials	406
14.10	Cyclotomic polynomials and constructing BCH codes	412
	Notes	417
	Exercises	422
15	Hensel lifting and factoring polynomials	433
15.1	Factoring in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$: the basic idea	433
15.2	A factoring algorithm	435
15.3	Frobenius' and Chebotarev's density theorems	441
15.4	Hensel lifting	444
15.5	Multifactor Hensel lifting	450
15.6	Factoring using Hensel lifting: Zassenhaus' algorithm	453
15.7	Implementations	461
	Notes	465
	Exercises	467
16	Short vectors in lattices	473
16.1	Lattices	473
16.2	Lenstra, Lenstra and Lovász' basis reduction algorithm	475
16.3	Cost estimate for basis reduction	480
16.4	From short vectors to factors	487
16.5	A polynomial-time factoring algorithm for $\mathbb{Z}[x]$	489
16.6	Factoring multivariate polynomials	493
	Notes	496
	Exercises	498

17 Applications of basis reduction	503
17.1 Breaking knapsack-type cryptosystems	503
17.2 Pseudorandom numbers	505
17.3 Simultaneous Diophantine approximation	505
17.4 Disproof of Mertens' conjecture	508
Notes	509
Exercises	509
IV Fermat	511
18 Primality testing	517
18.1 Multiplicative order of integers	517
18.2 The Fermat test	519
18.3 The strong pseudoprimality test	520
18.4 Finding primes	523
18.5 The Solovay and Strassen test	529
18.6 Primality tests for special numbers	530
Notes	531
Exercises	534
19 Factoring integers	541
19.1 Factorization challenges	541
19.2 Trial division	543
19.3 Pollard's and Strassen's method	544
19.4 Pollard's rho method	545
19.5 Dixon's random squares method	549
19.6 Pollard's $p - 1$ method	557
19.7 Lenstra's elliptic curve method	557
Notes	567
Exercises	569
20 Application: Public key cryptography	573
20.1 Cryptosystems	573
20.2 The RSA cryptosystem	576
20.3 The Diffie–Hellman key exchange protocol	578
20.4 The ElGamal cryptosystem	579
20.5 Rabin's cryptosystem	579
20.6 Elliptic curve systems	580
Notes	580
Exercises	580

V Hilbert	585
21 Gröbner bases	591
21.1 Polynomial ideals	591
21.2 Monomial orders and multivariate division with remainder	595
21.3 Monomial ideals and Hilbert's basis theorem	601
21.4 Gröbner bases and S-polynomials	604
21.5 Buchberger's algorithm	608
21.6 Geometric applications	612
21.7 The complexity of computing Gröbner bases	616
Notes	617
Exercises	619
22 Symbolic integration	623
22.1 Differential algebra	623
22.2 Hermite's method	625
22.3 The method of Lazard, Rioboo, Rothstein, and Trager	627
22.4 Hyperexponential integration: Almkvist & Zeilberger's algorithm	632
Notes	640
Exercises	641
23 Symbolic summation	645
23.1 Polynomial summation	645
23.2 Harmonic numbers	650
23.3 Greatest factorial factorization	653
23.4 Hypergeometric summation: Gosper's algorithm	658
Notes	669
Exercises	671
24 Applications	677
24.1 Gröbner proof systems	677
24.2 Petri nets	679
24.3 Proving identities and analysis of algorithms	681
24.4 Cyclohexane revisited	685
Notes	697
Exercises	698
Appendix	701
25 Fundamental concepts	703
25.1 Groups	703
25.2 Rings	705

Contents

xiii

25.3	Polynomials and fields	708
25.4	Finite fields	711
25.5	Linear algebra	713
25.6	Finite probability spaces	717
25.7	“Big Oh” notation	720
25.8	Complexity theory	721
	Notes	724
	Sources of illustrations	725
	Sources of quotations	725
	List of algorithms	730
	List of figures and tables	732
	References	734
	List of notation	768
	Index	769

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://cosec.bit.uni-bonn.de/science/mca/>