

Contents

Introduction	1
1 Cyclohexane, cryptography, codes, and computer algebra	9
1.1 Cyclohexane conformations	9
1.2 The RSA cryptosystem	14
1.3 Distributed data structures	16
1.4 Computer algebra systems	17
I Euclid	21
2 Fundamental algorithms	27
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	43
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	67
4.1 Modular arithmetic	67
4.2 Modular inverses via Euclid	71
4.3 Repeated squaring	73
4.4 Modular inverses via Fermat	74

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

II	Newton	215
8	Fast multiplication	219
8.1	Karatsuba’s multiplication algorithm	220
8.2	The Discrete Fourier Transform and the Fast Fourier Transform	225
8.3	Schönhage and Strassen’s multiplication algorithm	235
8.4	Multiplication in $\mathbb{Z}[x]$ and $R[x, y]$	243
	Notes	244
	Exercises	245
9	Newton iteration	253
9.1	Division with remainder using Newton iteration	253
9.2	Generalized Taylor expansion and radix conversion	260
9.3	Formal derivatives and Taylor expansion	261
9.4	Solving polynomial equations via Newton iteration	263
9.5	Computing integer roots	267
9.6	Newton iteration, Julia sets, and fractals	269
9.7	Implementations of fast arithmetic	274
	Notes	282
	Exercises	283
10	Fast polynomial evaluation and interpolation	291
10.1	Fast multipoint evaluation	291
10.2	Fast interpolation	295
10.3	Fast Chinese remaindering	297
	Notes	302
	Exercises	302
11	Fast Euclidean Algorithm	309
11.1	A fast Euclidean Algorithm for polynomials	309
11.2	Subresultants via Euclid’s algorithm	320
	Notes	324
	Exercises	324
12	Fast linear algebra	327
12.1	Strassen’s matrix multiplication	327
12.2	Application: fast modular composition of polynomials	330
12.3	Linearly recurrent sequences	331
12.4	Wiedemann’s algorithm and black box linear algebra	337
	Notes	344
	Exercises	345

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

17 Applications of basis reduction	491
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	499
18 Primality testing	505
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	531
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	563
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

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

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

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/>