

Henri Cohen

A Course in Computational Algebraic Number Theory

Springer-Verlag Berlin Heidelberg GmbH

Henri Cohen
U.F.R. de Mathématiques et Informatique
Université Bordeaux I
351 Cours de la Libération
F-33405 Talence Cedex, France

Editorial Board

J. H. Ewing
Department of Mathematics
Indiana University
Bloomington, IN 47405, USA

F. W. Gehring
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109, USA

P. R. Halmos
Department of Mathematics
Santa Clara University
Santa Clara, CA 95053, USA

With 1 Figure

Mathematics Subject Classification (1991): 11Y05, 11Y11, 11Y16,
11Y40, 11A51, 11C08, 11C20, 11R09, 11R11, 11R29

ISBN 978-3-642-08142-2

Library of Congress Cataloging-in-Publication Data

Cohen, Henri. A course in computational algebraic number theory / Henri Cohen. p. cm.
(Graduate texts in mathematics; 138) Includes bibliographical references and index.

ISBN 978-3-642-08142-2 ISBN 978-3-662-02945-9 (eBook)

DOI 10.1007/978-3-662-02945-9

I. Algebraic number theory—Data processing. I. Title. II. Series.

QA247.C55 1993 512'.74/028551—dc20 93-3701

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1993

Originally published by Springer-Verlag Berlin Heidelberg New York in 1993

Softcover reprint of the hardcover 1st edition 1993

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready copy by author using AmsT_EX and LamsT_EX

41/3140 – 5 4 3 2 1 0 – Printed on acid-free paper

Contents

Chapter 1. Fundamental Number-Theoretic Algorithms	1
1.1. Introduction	1
1.1.1. Algorithms	1
1.1.2. Multi-precision	2
1.1.3. Base Fields and Rings	5
1.1.4. Notations	6
1.2. The Powering Algorithms	8
1.3. Euclid's Algorithms	12
1.3.1. Euclid's and Lehmer's Algorithms	12
1.3.2. Euclid's Extended Algorithms	16
1.3.3. The Chinese Remainder Theorem	19
1.3.4. Continued Fraction Expansions of Real Numbers	21
1.4. The Legendre Symbol	24
1.4.1. The Groups $(\mathbb{Z}/n\mathbb{Z})^*$	24
1.4.2. The Legendre-Jacobi-Kronecker Symbol	27
1.5. Computing Square Roots Modulo p	31
1.5.1. The Algorithm of Tonelli and Shanks	32
1.5.2. The Algorithm of Cornacchia	34
1.6. Solving Polynomial Equations Modulo p	36
1.7. Power Detection	38
1.7.1. Integer Square Roots	38
1.7.2. Square Detection	39
1.7.3. Prime Power Detection	41
1.8. Exercises for Chapter 1	42
 Chapter 2. Algorithms for Linear Algebra and Lattices	 45
2.1. Introduction	45
2.2. Linear Algebra Algorithms on Square Matrices	46
2.2.1. Generalities on Linear Algebra Algorithms	46
2.2.2. Gaussian Elimination and Solving Linear Systems	47
2.2.3. Computing Determinants	49
2.2.4. Computing the Characteristic Polynomial	52
2.3. Linear Algebra on General Matrices	56
2.3.1. Kernel and Image	56
2.3.2. Inverse Image and Supplement	59

2.3.3. Operations on Subspaces	61
2.3.4. Remarks on Modules	63
2.4. $\mathbb{Z}$ -Modules and the Hermite and Smith Normal Forms	65
2.4.1. Introduction to $\mathbb{Z}$ -Modules	65
2.4.2. The Hermite Normal Form	66
2.4.3. Applications of the Hermite Normal Form	72
2.4.4. The Smith Normal Form and Applications	74
2.5. Generalities on Lattices	78
2.5.1. Lattices and Quadratic Forms	78
2.5.2. The Gram-Schmidt Orthogonalization Procedure	81
2.6. Lattice Reduction Algorithms	83
2.6.1. The LLL Algorithm	83
2.6.2. The LLL Algorithm with Deep Insertions	89
2.6.3. The Integral LLL Algorithm	91
2.6.4. LLL Algorithms for Linearly Dependent Vectors	94
2.7. Applications of the LLL Algorithm	96
2.7.1. Computing the Integer Kernel and Image of a Matrix	96
2.7.2. Linear and Algebraic Dependence Using LLL	99
2.7.3. Finding Small Vectors in Lattices	102
2.8. Exercises for Chapter 2	105
Chapter 3. Algorithms on Polynomials	108
3.1. Basic Algorithms	108
3.1.1. Representation of Polynomials	108
3.1.2. Multiplication of Polynomials	109
3.1.3. Division of Polynomials	110
3.2. Euclid's Algorithms for Polynomials	112
3.2.1. Polynomials over a Field	112
3.2.2. Unique Factorization Domains (UFD's)	113
3.2.3. Polynomials over Unique Factorization Domains	115
3.2.4. Euclid's Algorithm for Polynomials over a UFD	116
3.3. The Sub-Resultant Algorithm	117
3.3.1. Description of the Algorithm	117
3.3.2. Resultants and Discriminants	118
3.3.3. Resultants over a Non-Exact Domain	122
3.4. Factorization of Polynomials Modulo p	123
3.4.1. General Strategy	123
3.4.2. Squarefree Factorization	124
3.4.3. Distinct Degree Factorization	125
3.4.4. Final Splitting	126
3.5. Factorization of Polynomials over $\mathbb{Z}$ or $\mathbb{Q}$	132
3.5.1. Bounds on Polynomial Factors	133
3.5.2. A First Approach to Factoring over $\mathbb{Z}$	134
3.5.3. Factorization Modulo p^e : Hensel's Lemma	136
3.5.4. Factorization of Polynomials over $\mathbb{Z}$	138

3.5.5. Discussion	140
3.6. Additional Polynomial Algorithms	141
3.6.1. Modular Methods for Computing GCD's in $\mathbb{Z}[X]$	141
3.6.2. Factorization of Polynomials over a Number Field	142
3.6.3. A Root Finding Algorithm over $\mathbb{C}$	145
3.7. Exercises for Chapter 3	147
 Chapter 4. Algorithms for Algebraic Number Theory I	151
4.1. Algebraic Numbers and Number Fields	151
4.1.1. Basic Definitions and Properties of Algebraic Numbers	151
4.1.2. Number Fields	152
4.2. Representation and Operations on Algebraic Numbers	156
4.2.1. Algebraic Numbers as Roots of their Minimal Polynomial	156
4.2.2. The Standard Representation of an Algebraic Number	157
4.2.3. The Matrix (or Regular) Representation of an Algebraic Number	158
4.2.4. The Conjugate Vector Representation of an Algebraic Number	159
4.3. Trace, Norm and Characteristic Polynomial	160
4.4. Discriminants, Integral Bases and Polynomial Reduction	163
4.4.1. Discriminants and Integral Bases	163
4.4.2. The Polynomial Reduction Algorithm	166
4.5. The Subfield Problem and Applications	172
4.5.1. The Subfield Problem Using the LLL Algorithm	172
4.5.2. The Subfield Problem Using Linear Algebra over $\mathbb{C}$	173
4.5.3. The Subfield Problem Using Algebraic Algorithms	175
4.5.4. Applications of the Solutions to the Subfield Problem	177
4.6. Orders and Ideals	179
4.6.1. Basic Definitions	179
4.6.2. Ideals of $\mathbb{Z}_K$	184
4.7. Representation of Modules and Ideals	186
4.7.1. Modules and the Hermite Normal Form	186
4.7.2. Representation of Ideals	188
4.8. Decomposition of Prime Numbers I	193
4.8.1. Definitions and Main Results	194
4.8.2. A Simple Algorithm for the Decomposition of Primes	196
4.8.3. Computing Valuations	198
4.8.4. Ideal Inversion and the Different	202
4.9. Units and Ideal Classes	205
4.9.1. The Class Group	205
4.9.2. Units and the Regulator	206
4.9.3. Conclusion: the Main Computational Tasks of Algebraic Number Theory	214
4.10. Exercises for Chapter 4	215

Chapter 5. Algorithms for Quadratic Fields	218
5.1. Discriminant, Integral Basis and Decomposition of Primes	218
5.2. Ideals and Quadratic Forms	220
5.3. Class Numbers of Imaginary Quadratic Fields	226
5.3.1. Computing Class Numbers Using Reduced Forms	226
5.3.2. Computing Class Numbers Using Modular Forms	229
5.3.3. Computing Class Numbers Using Analytic Formulas	232
5.4. Class Groups of Imaginary Quadratic Fields	235
5.4.1. Shanks's Baby Step Giant Step Method	235
5.4.2. Reduction and Composition of Quadratic Forms	238
5.4.3. Class Groups Using Shanks's Method	245
5.5. McCurley's Sub-exponential Algorithm	247
5.5.1. Outline of the Algorithm	247
5.5.2. Detailed Description of the Algorithm	250
5.5.3. Atkin's Variant	255
5.6. Class Groups of Real Quadratic Fields	257
5.6.1. Computing Class Numbers Using Reduced Forms	257
5.6.2. Computing Class Numbers Using Analytic Formulas	261
5.6.3. A Heuristic Method of Shanks	263
5.7. Computation of the Fundamental Unit and of the Regulator	264
5.7.1. Description of the Algorithms	264
5.7.2. Analysis of the Continued Fraction Algorithm	266
5.7.3. Computation of the Regulator	273
5.8. The Infrastructure Method of Shanks	274
5.8.1. The Distance Function	274
5.8.2. Description of the Algorithm	278
5.8.3. Compact Representation of the Fundamental Unit	280
5.8.4. Other Application and Generalization of the Distance Function	282
5.9. Buchmann's Sub-exponential Algorithm	283
5.9.1. Outline of the Algorithm	284
5.9.2. Detailed Description of Buchmann's Sub-exponential Algorithm	286
5.10. The Cohen-Lenstra Heuristics	289
5.10.1. Results and Heuristics for Imaginary Quadratic Fields	290
5.10.2. Results and Heuristics for Real Quadratic Fields	292
5.11. Exercises for Chapter 5	293
 Chapter 6. Algorithms for Algebraic Number Theory II	 297
6.1. Computing the Maximal Order	297
6.1.1. The Pohst-Zassenhaus Theorem	297
6.1.2. The Dedekind Criterion	299
6.1.3. Outline of the Round 2 Algorithm	302
6.1.4. Detailed Description of the Round 2 Algorithm	305
6.2. Decomposition of Prime Numbers II	306
6.2.1. Newton Polygons	307
6.2.2. Theoretical Description of the Buchmann-Lenstra Method	309

6.2.3. Multiplying and Dividing Ideals Modulo p	311
6.2.4. Splitting of Separable Algebras over $\mathbb{F}_p$	312
6.2.5. Detailed Description of the Algorithm for Prime Decomposition	314
6.3. Computing Galois Groups	316
6.3.1. The Resolvent Method	316
6.3.2. Degree 3	319
6.3.3. Degree 4	319
6.3.4. Degree 5	322
6.3.5. Degree 6	323
6.3.6. Degree 7	325
6.3.7. A List of Test Polynomials	327
6.4. Examples of Families of Number Fields	328
6.4.1. Making Tables of Number Fields	328
6.4.2. Cyclic Cubic Fields	330
6.4.3. Pure Cubic Fields	337
6.4.4. Decomposition of Primes in Pure Cubic Fields	341
6.4.5. General Cubic Fields	345
6.5. Computing the Class Group, Regulator and Fundamental Units	346
6.5.1. Ideal Reduction	346
6.5.2. Computing the Relation Matrix	348
6.5.3. Computing the Regulator and a System of Fundamental Units	351
6.5.4. The General Class Group and Unit Algorithm	352
6.5.5. The Principal Ideal Problem	354
6.6. Exercises for Chapter 6	356
Chapter 7. Introduction to Elliptic Curves	360
7.1. Basic Definitions	360
7.1.1. Introduction	360
7.1.2. Elliptic Integrals and Elliptic Functions	360
7.1.3. Elliptic Curves over a Field	362
7.1.4. Points on Elliptic Curves	365
7.2. Complex Multiplication and Class Numbers	369
7.2.1. Maps Between Complex Elliptic Curves	370
7.2.2. Isogenies	372
7.2.3. Complex Multiplication	374
7.2.4. Complex Multiplication and Hilbert Class Fields	377
7.2.5. Modular Equations	378
7.3. Rank and L -functions	379
7.3.1. The Zeta Function of a Variety	380
7.3.2. L -functions of Elliptic Curves	381
7.3.3. The Taniyama-Weil Conjecture	383
7.3.4. The Birch and Swinnerton-Dyer Conjecture	385
7.4. Algorithms for Elliptic Curves	387
7.4.1. Algorithms for Elliptic Curves over $\mathbb{C}$	387
7.4.2. Algorithm for Reducing a General Cubic	392

7.4.3. Algorithms for Elliptic Curves over $\mathbb{F}_p$	396
7.5. Algorithms for Elliptic Curves over $\mathbb{Q}$	399
7.5.1. Tate's algorithm	399
7.5.2. Computing rational points	402
7.5.3. Algorithms for computing the L -function	405
7.6. Algorithms for Elliptic Curves with Complex Multiplication	407
7.6.1. Computing the Complex Values of $j(\tau)$	407
7.6.2. Computing the Hilbert Class Polynomials	408
7.6.3. Computing Weber Class Polynomials	408
7.7. Exercises for Chapter 7	409
Chapter 8. Factoring in the Dark Ages	412
8.1. Factoring and Primality Testing	412
8.2. Compositeness Tests	414
8.3. Primality Tests	416
8.3.1. The Pocklington-Lehmer $N - 1$ Test	416
8.3.2. Briefly, Other Tests	417
8.4. Lehmann's Method	418
8.5. Pollard's ρ Method	419
8.5.1. Outline of the Method	419
8.5.2. Methods for Detecting Periodicity	420
8.5.3. Brent's Modified Algorithm	422
8.5.4. Analysis of the Algorithm	423
8.6. Shanks's Class Group Method	426
8.7. Shanks's SQUFOF	427
8.8. The $p - 1$ -method	431
8.8.1. The First Stage	432
8.8.2. The Second Stage	433
8.8.3. Other Algorithms of the Same Type	434
8.9. Exercises for Chapter 8	435
Chapter 9. Modern Primality Tests	437
9.1. The Jacobi Sum Test	438
9.1.1. Group Rings of Cyclotomic Extensions	438
9.1.2. Characters, Gauss Sums and Jacobi Sums	440
9.1.3. The Basic Test	442
9.1.4. Checking Condition $\mathcal{L}_p$	447
9.1.5. The Use of Jacobi Sums	449
9.1.6. Detailed Description of the Algorithm	455
9.1.7. Discussion	457
9.2. The Elliptic Curve Test	459
9.2.1. The Goldwasser-Kilian Test	459
9.2.2. Atkin's Test	463
9.3. Exercises for Chapter 9	467

Chapter 10. Modern Factoring Methods	469
10.1. The Continued Fraction Method	469
10.2. The Class Group Method	473
10.2.1. Sketch of the Method	473
10.2.2. The Schnorr-Lenstra Factoring Method	474
10.3. The Elliptic Curve Method	476
10.3.1. Sketch of the Method	476
10.3.2. Elliptic Curves Modulo N	477
10.3.3. The ECM Factoring Method of Lenstra	479
10.3.4. Practical Considerations	481
10.4. The Multiple Polynomial Quadratic Sieve	482
10.4.1. The Basic Quadratic Sieve Algorithm	483
10.4.2. The Multiple Polynomial Quadratic Sieve	484
10.4.3. Improvements to the MPQS Algorithm	486
10.5. The Number Field Sieve	487
10.5.1. Introduction	487
10.5.2. Description of the Special NFS when $h(K) = 1$	488
10.5.3. Description of the Special NFS when $h(K) > 1$	492
10.5.4. Description of the General NFS	493
10.5.5. Miscellaneous Improvements to the Number Field Sieve	495
10.6. Exercises for Chapter 10	496
Appendix A. Packages for Number Theory	498
Appendix B. Some Useful Tables	503
B.1. Table of Class Numbers of Complex Quadratic Fields	503
B.2. Table of Class Numbers and Units of Real Quadratic Fields	505
B.3. Table of Class Numbers and Units of Complex Cubic Fields	509
B.4. Table of Class Numbers and Units of Totally Real Cubic Fields	511
B.5. Table of Elliptic Curves	514
Bibliography	517
Index	529