UNIVERSIDAD NACIONAL DE ENTRE RIOS
FACULTAD DE INGENIERIA
CENTRO DE MEDIOS
BIBLIOTECA
9975

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 46

2.1 Introduction . . . 46

2.2 Linear Algebra Algorithms on Square Matrices . . . 47

2.2.1 Generalities on Linear Algebra Algorithms . . . 47

2.2.2 Gaussian Elimination and Solving Linear Systems . . . 48

2.2.3 Computing Determinants . . . 50

2.2.4 Computing the Characteristic Polynomial . . . 53

2.3 Linear Algebra on General Matrices . . . 57

2.3.1 Kernel and Image . . . 57

2.3.2 Inverse Image and Supplement . . . 60

2.3.3 Operations on Subspaces . . . 62

2.3.4 Remarks on Modules . . . 64

2.4 ℤ-Modules and the Hermite and Smith Normal Forms . . 66

2.4.1 Introduction to ℤ-Modules . . . 66

2.4.2 The Hermite Normal Form . . . 67

2.4.3 Applications of the Hermite Normal Form . . . 73

2.4.4 The Smith Normal Form and Applications . . . 75

2.5 Generalities on Lattices . . . 79

2.5.1 Lattices and Quadratic Forms . . . 79

2.5.2 The Gram-Schmidt Orthogonalization Procedure . . . 82

2.6 Lattice Reduction Algorithms . . . 84

2.6.1 The LLL Algorithm . . . 84

2.6.2 The LLL Algorithm with Deep Insertions . . . 90

2.6.3 The Integral LLL Algorithm . . . 92

2.6.4 LLL Algorithms for Linearly Dependent Vectors . . . 95

2.7 Applications of the LLL Algorithm . . . 97

2.7.1 Computing the Integer Kernel and Image of a Matrix . . . 97

2.7.2 Linear and Algebraic Dependence Using LLL . . . 100

2.7.3 Finding Small Vectors in Lattices . . . 103

2.8 Exercises for Chapter 2 . . . 106

Chapter 3 Algorithms on Polynomials . . . 109

3.1 Basic Algorithms . . . 109

3.1.1 Representation of Polynomials . . . 109

3.1.2 Multiplication of Polynomials . . . 110

3.1.3 Division of Polynomials . . . 111

3.2 Euclid's Algorithms for Polynomials . . . 113

3.2.1 Polynomials over a Field . . . 113

3.2.2 Unique Factorization Domains (UFD's) . . . 114

3.2.3 Polynomials over Unique Factorization Domains . . . 116

3.2.4 Euclid's Algorithm for Polynomials over a UFD 117

3.3 The Sub-Resultant Algorithm 118

3.3.1 Description of the Algorithm 118

3.3.2 Resultants and Discriminants 119

3.3.3 Resultants over a Non-Exact Domain 123

3.4 Factorization of Polynomials Modulo p 124

3.4.1 General Strategy 124

3.4.2 Squarefree Factorization 125

3.4.3 Distinct Degree Factorization 126

3.4.4 Final Splitting 127

3.5 Factorization of Polynomials over $\mathbb{Z}$ or $\mathbb{Q}$ 133

3.5.1 Bounds on Polynomial Factors 134

3.5.2 A First Approach to Factoring over $\mathbb{Z}$ 135

3.5.3 Factorization Modulo p^e: Hensel's Lemma 137

3.5.4 Factorization of Polynomials over $\mathbb{Z}$ 139

3.5.5 Discussion 141

3.6 Additional Polynomial Algorithms 142

3.6.1 Modular Methods for Computing GCD's in $\mathbb{Z}[X]$ 142

3.6.2 Factorization of Polynomials over a Number Field 143

3.6.3 A Root Finding Algorithm over $\mathbb{C}$ 146

3.7 Exercises for Chapter 3 148

Chapter 4 Algorithms for Algebraic Number Theory I 153

4.1 Algebraic Numbers and Number Fields 153

4.1.1 Basic Definitions and Properties of Algebraic Numbers 153

4.1.2 Number Fields 154

4.2 Representation and Operations on Algebraic Numbers . . 158

4.2.1 Algebraic Numbers as Roots of their Minimal Polynomial 158

4.2.2 The Standard Representation of an Algebraic Number 159

4.2.3 The Matrix (or Regular) Representation of an Algebraic Number . 160

4.2.4 The Conjugate Vector Representation of an Algebraic Number . . 161

4.3 Trace, Norm and Characteristic Polynomial 162

4.4 Discriminants, Integral Bases and Polynomial Reduction . 165

4.4.1 Discriminants and Integral Bases 165

4.4.2 The Polynomial Reduction Algorithm 168

4.5 The Subfield Problem and Applications 174

4.5.1 The Subfield Problem Using the LLL Algorithm 174

4.5.2 The Subfield Problem Using Linear Algebra over $\mathbb{C}$ 175

4.5.3 The Subfield Problem Using Algebraic Algorithms 177

4.5.4 Applications of the Solutions to the Subfield Problem 179

4.6 Orders and Ideals . . . 181
4.6.1 Basic Definitions . . . 181
4.6.2 Ideals of $\mathbb{Z}_K$ . . . 186

4.7 Representation of Modules and Ideals . . . 188
4.7.1 Modules and the Hermite Normal Form . . . 188
4.7.2 Representation of Ideals . . . 190

4.8 Decomposition of Prime Numbers I . . . 196
4.8.1 Definitions and Main Results . . . 196
4.8.2 A Simple Algorithm for the Decomposition of Primes . . . 199
4.8.3 Computing Valuations . . . 201
4.8.4 Ideal Inversion and the Different . . . 204

4.9 Units and Ideal Classes . . . 207
4.9.1 The Class Group . . . 207
4.9.2 Units and the Regulator . . . 209
4.9.3 Conclusion: the Main Computational Tasks of Algebraic Number Theory . . . 217

4.10 Exercises for Chapter 4 . . . 217

Chapter 5 Algorithms for Quadratic Fields . . . 223

5.1 Discriminant, Integral Basis and Decomposition of Primes 223

5.2 Ideals and Quadratic Forms . . . 225

5.3 Class Numbers of Imaginary Quadratic Fields . . . 231
5.3.1 Computing Class Numbers Using Reduced Forms . . . 231
5.3.2 Computing Class Numbers Using Modular Forms . . . 234
5.3.3 Computing Class Numbers Using Analytic Formulas . . . 237

5.4 Class Groups of Imaginary Quadratic Fields . . . 240
5.4.1 Shanks's Baby Step Giant Step Method . . . 240
5.4.2 Reduction and Composition of Quadratic Forms . . . 243
5.4.3 Class Groups Using Shanks's Method . . . 250

5.5 McCurley's Sub-exponential Algorithm . . . 252
5.5.1 Outline of the Algorithm . . . 252
5.5.2 Detailed Description of the Algorithm . . . 255
5.5.3 Atkin's Variant . . . 260

5.6 Class Groups of Real Quadratic Fields . . . 262
5.6.1 Computing Class Numbers Using Reduced Forms . . . 262
5.6.2 Computing Class Numbers Using Analytic Formulas . . . 266
5.6.3 A Heuristic Method of Shanks . . . 268

5.7 Computation of the Fundamental Unit and of the Regulator . . . 269
5.7.1 Description of the Algorithms . . . 269
5.7.2 Analysis of the Continued Fraction Algorithm . . . 271
5.7.3 Computation of the Regulator . . . 278

5.8 The Infrastructure Method of Shanks . . . 279
5.8.1 The Distance Function . . . 279
5.8.2 Description of the Algorithm . . . 283
5.8.3 Compact Representation of the Fundamental Unit . . . 285
5.8.4 Other Application and Generalization of the Distance Function . 287

5.9 Buchmann's Sub-exponential Algorithm . . . 288
5.9.1 Outline of the Algorithm . . . 289
5.9.2 Detailed Description of Buchmann's Sub-exponential Algorithm . 291

5.10 The Cohen-Lenstra Heuristics . . . 295
5.10.1 Results and Heuristics for Imaginary Quadratic Fields . . . 295
5.10.2 Results and Heuristics for Real Quadratic Fields . . . 297

5.11 Exercises for Chapter 5 . . . 298

Chapter 6 Algorithms for Algebraic Number Theory II 303

6.1 Computing the Maximal Order . . . 303
6.1.1 The Pohst-Zassenhaus Theorem . . . 303
6.1.2 The Dedekind Criterion . . . 305
6.1.3 Outline of the Round 2 Algorithm . . . 308
6.1.4 Detailed Description of the Round 2 Algorithm . . . 311

6.2 Decomposition of Prime Numbers II . . . 312
6.2.1 Newton Polygons . . . 313
6.2.2 Theoretical Description of the Buchmann-Lenstra Method . . . 315
6.2.3 Multiplying and Dividing Ideals Modulo p . . . 317
6.2.4 Splitting of Separable Algebras over $\mathbb{F}_p$ . . . 318
6.2.5 Detailed Description of the Algorithm for Prime Decomposition . 320

6.3 Computing Galois Groups . . . 322
6.3.1 The Resolvent Method . . . 322
6.3.2 Degree 3 . . . 325
6.3.3 Degree 4 . . . 325
6.3.4 Degree 5 . . . 328
6.3.5 Degree 6 . . . 329
6.3.6 Degree 7 . . . 331
6.3.7 A List of Test Polynomials . . . 333

6.4 Examples of Families of Number Fields . . . 334
6.4.1 Making Tables of Number Fields . . . 334
6.4.2 Cyclic Cubic Fields . . . 336

6.4.3 Pure Cubic Fields . . . 343
6.4.4 Decomposition of Primes in Pure Cubic Fields . . . 347
6.4.5 General Cubic Fields . . . 351

6.5 Computing the Class Group, Regulator and Fundamental Units . . . 352

6.5.1 Ideal Reduction . . . 352
6.5.2 Computing the Relation Matrix . . . 354
6.5.3 Computing the Regulator and a System of Fundamental Units . . . 357
6.5.4 The General Class Group and Unit Algorithm . . . 358
6.5.5 The Principal Ideal Problem . . . 360

6.6 Exercises for Chapter 6 . . . 362

Chapter 7 Introduction to Elliptic Curves . . . 367

7.1 Basic Definitions . . . 367

7.1.1 Introduction . . . 367
7.1.2 Elliptic Integrals and Elliptic Functions . . . 367
7.1.3 Elliptic Curves over a Field . . . 369
7.1.4 Points on Elliptic Curves . . . 372

7.2 Complex Multiplication and Class Numbers . . . 376

7.2.1 Maps Between Complex Elliptic Curves . . . 377
7.2.2 Isogenies . . . 379
7.2.3 Complex Multiplication . . . 381
7.2.4 Complex Multiplication and Hilbert Class Fields . . . 384
7.2.5 Modular Equations . . . 385

7.3 Rank and L-functions . . . 386

7.3.1 The Zeta Function of a Variety . . . 387
7.3.2 L-functions of Elliptic Curves . . . 388
7.3.3 The Taniyama-Weil Conjecture . . . 390
7.3.4 The Birch and Swinnerton-Dyer Conjecture . . . 392

7.4 Algorithms for Elliptic Curves . . . 394

7.4.1 Algorithms for Elliptic Curves over $\mathbb{C}$ . . . 394
7.4.2 Algorithm for Reducing a General Cubic . . . 399
7.4.3 Algorithms for Elliptic Curves over $\mathbb{F}_p$ . . . 403

7.5 Algorithms for Elliptic Curves over $\mathbb{Q}$ . . . 406

7.5.1 Tate's algorithm . . . 406
7.5.2 Computing rational points . . . 410
7.5.3 Algorithms for computing the L-function . . . 413

7.6 Algorithms for Elliptic Curves with Complex Multiplication . . . 414

7.6.1 Computing the Complex Values of $j(\tau)$ . . . 414
7.6.2 Computing the Hilbert Class Polynomials . . . 415

7.6.3 Computing Weber Class Polynomials 416

7.7 Exercises for Chapter 7 417

Chapter 8 Factoring in the Dark Ages 419

8.1 Factoring and Primality Testing 419

8.2 Compositeness Tests 421

8.3 Primality Tests 423

8.3.1 The Pocklington-Lehmer $N - 1$ Test 423

8.3.2 Briefly, Other Tests 424

8.4 Lehman's Method 425

8.5 Pollard's ρ Method 426

8.5.1 Outline of the Method 426

8.5.2 Methods for Detecting Periodicity 427

8.5.3 Brent's Modified Algorithm 429

8.5.4 Analysis of the Algorithm 430

8.6 Shanks's Class Group Method 433

8.7 Shanks's SQUFOF 434

8.8 The $p - 1$-method 438

8.8.1 The First Stage 439

8.8.2 The Second Stage 440

8.8.3 Other Algorithms of the Same Type 441

8.9 Exercises for Chapter 8 442

Chapter 9 Modern Primality Tests 445

9.1 The Jacobi Sum Test 446

9.1.1 Group Rings of Cyclotomic Extensions 446

9.1.2 Characters, Gauss Sums and Jacobi Sums 448

9.1.3 The Basic Test 450

9.1.4 Checking Condition $\mathcal{L}_p$ 455

9.1.5 The Use of Jacobi Sums 457

9.1.6 Detailed Description of the Algorithm 463

9.1.7 Discussion 465

9.2 The Elliptic Curve Test 467

9.2.1 The Goldwasser-Kilian Test 467

9.2.2 Atkin's Test 471

9.3 Exercises for Chapter 9 475

7.6.3 Computing Weber Class Polynomials . . . 416

7.7 Exercises for Chapter 7 . . . 417

Chapter 8 Factoring in the Dark Ages . . . 419

8.1 Factoring and Primality Testing . . . 419

8.2 Compositeness Tests . . . 421

8.3 Primality Tests . . . 423

8.3.1 The Pocklington-Lehmer $N-1$ Test . . . 423

8.3.2 Briefly, Other Tests . . . 424

8.4 Lehman's Method . . . 425

8.5 Pollard's ρ Method . . . 426

8.5.1 Outline of the Method . . . 426

8.5.2 Methods for Detecting Periodicity . . . 427

8.5.3 Brent's Modified Algorithm . . . 429

8.5.4 Analysis of the Algorithm . . . 430

8.6 Shanks's Class Group Method . . . 433

8.7 Shanks's SQUFOF . . . 434

8.8 The $p-1$-method . . . 438

8.8.1 The First Stage . . . 439

8.8.2 The Second Stage . . . 440

8.8.3 Other Algorithms of the Same Type . . . 441

8.9 Exercises for Chapter 8 . . . 442

Chapter 9 Modern Primality Tests . . . 445

9.1 The Jacobi Sum Test . . . 446

9.1.1 Group Rings of Cyclotomic Extensions . . . 446

9.1.2 Characters, Gauss Sums and Jacobi Sums . . . 448

9.1.3 The Basic Test . . . 450

9.1.4 Checking Condition $\mathcal{L}_p$ . . . 455

9.1.5 The Use of Jacobi Sums . . . 457

9.1.6 Detailed Description of the Algorithm . . . 463

9.1.7 Discussion . . . 465

9.2 The Elliptic Curve Test . . . 467

9.2.1 The Goldwasser-Kilian Test . . . 467

9.2.2 Atkin's Test . . . 471

9.3 Exercises for Chapter 9 . . . 475

Chapter 10 Modern Factoring Methods 477

10.1 The Continued Fraction Method 477

10.2 The Class Group Method 481

10.2.1 Sketch of the Method 481

10.2.2 The Schnorr-Lenstra Factoring Method 482

10.3 The Elliptic Curve Method 484

10.3.1 Sketch of the Method 484

10.3.2 Elliptic Curves Modulo N 485

10.3.3 The ECM Factoring Method of Lenstra 487

10.3.4 Practical Considerations 489

10.4 The Multiple Polynomial Quadratic Sieve 490

10.4.1 The Basic Quadratic Sieve Algorithm 491

10.4.2 The Multiple Polynomial Quadratic Sieve 492

10.4.3 Improvements to the MPQS Algorithm 494

10.5 The Number Field Sieve 495

10.5.1 Introduction 495

10.5.2 Description of the Special NFS when $h(K) = 1$ 496

10.5.3 Description of the Special NFS when $h(K) > 1$ 500

10.5.4 Description of the General NFS 501

10.5.5 Miscellaneous Improvements to the Number Field Sieve 503

10.6 Exercises for Chapter 10 504

Appendix A Packages for Number Theory 507

Appendix B Some Useful Tables 513

B.1 Table of Class Numbers of Complex Quadratic Fields . . 513

B.2 Table of Class Numbers and Units of Real Quadratic Fields 515

B.3 Table of Class Numbers and Units of Complex Cubic Fields 519

B.4 Table of Class Numbers and Units of Totally Real Cubic Fields 521

B.5 Table of Elliptic Curves 524

Bibliography 527

Index 540