Contents

Preface *page* x
Preliminaries xiv

1 Basic properties of the integers 1
1.1 Divisibility and primality 1
1.2 Ideals and greatest common divisors 5
1.3 Some consequences of unique factorization 10

2 Congruences 15
2.1 Equivalence relations 15
2.2 Definitions and basic properties of congruences 16
2.3 Solving linear congruences 19
2.4 The Chinese remainder theorem 22
2.5 Residue classes 25
2.6 Euler's phi function 31
2.7 Euler's theorem and Fermat's little theorem 32
2.8 Quadratic residues 35
2.9 Summations over divisors 45

3 Computing with large integers 50
3.1 Asymptotic notation 50
3.2 Machine models and complexity theory 53
3.3 Basic integer arithmetic 55
3.4 Computing in $\mathbb{Z}_n$ 64
3.5 Faster integer arithmetic (*) 69
3.6 Notes 71

4 Euclid's algorithm 74
4.1 The basic Euclidean algorithm 74
4.2 The extended Euclidean algorithm 77
4.3 Computing modular inverses and Chinese remaindering 82

4.4 Speeding up algorithms via modular computation 84
4.5 An effective version of Fermat's two squares theorem 86
4.6 Rational reconstruction and applications 89
4.7 The RSA cryptosystem 99
4.8 Notes 102

5 The distribution of primes 104
5.1 Chebyshev's theorem on the density of primes 104
5.2 Bertrand's postulate 108
5.3 Mertens' theorem 110
5.4 The sieve of Eratosthenes 115
5.5 The prime number theorem . . . and beyond 116
5.6 Notes 124

6 Abelian groups 126
6.1 Definitions, basic properties, and examples 126
6.2 Subgroups 132
6.3 Cosets and quotient groups 137
6.4 Group homomorphisms and isomorphisms 142
6.5 Cyclic groups 153
6.6 The structure of finite abelian groups ($*$) 163

7 Rings 166
7.1 Definitions, basic properties, and examples 166
7.2 Polynomial rings 176
7.3 Ideals and quotient rings 185
7.4 Ring homomorphisms and isomorphisms 192
7.5 The structure of $\mathbb{Z}_n^*$ 203

8 Finite and discrete probability distributions 207
8.1 Basic definitions 207
8.2 Conditional probability and independence 213
8.3 Random variables 221
8.4 Expectation and variance 233
8.5 Some useful bounds 241
8.6 Balls and bins 245
8.7 Hash functions 252
8.8 Statistical distance 260
8.9 Measures of randomness and the leftover hash lemma ($*$) 266
8.10 Discrete probability distributions 270
8.11 Notes 275

9 Probabilistic algorithms 277
9.1 Basic definitions 278
9.2 Generating a random number from a given interval 285
9.3 The generate and test paradigm 287
9.4 Generating a random prime 292
9.5 Generating a random non-increasing sequence 295
9.6 Generating a random factored number 298
9.7 Some complexity theory 302
9.8 Notes 304

10 Probabilistic primality testing 306
10.1 Trial division 306
10.2 The Miller–Rabin test 307
10.3 Generating random primes using the Miller–Rabin test 311
10.4 Factoring and computing Euler's phi function 320
10.5 Notes 324

11 Finding generators and discrete logarithms in $\mathbb{Z}_p^*$ 327
11.1 Finding a generator for $\mathbb{Z}_p^*$ 327
11.2 Computing discrete logarithms in $\mathbb{Z}_p^*$ 329
11.3 The Diffie–Hellman key establishment protocol 334
11.4 Notes 340

12 Quadratic reciprocity and computing modular square roots 342
12.1 The Legendre symbol 342
12.2 The Jacobi symbol 346
12.3 Computing the Jacobi symbol 348
12.4 Testing quadratic residuosity 349
12.5 Computing modular square roots 350
12.6 The quadratic residuosity assumption 355
12.7 Notes 357

13 Modules and vector spaces 358
13.1 Definitions, basic properties, and examples 358
13.2 Submodules and quotient modules 360
13.3 Module homomorphisms and isomorphisms 363
13.4 Linear independence and bases 367
13.5 Vector spaces and dimension 370

14 Matrices 377
14.1 Basic definitions and properties 377
14.2 Matrices and linear maps 381
14.3 The inverse of a matrix 386

14.4 Gaussian elimination 388
14.5 Applications of Gaussian elimination 392
14.6 Notes 398

15 Subexponential-time discrete logarithms and factoring 399
15.1 Smooth numbers 399
15.2 An algorithm for discrete logarithms 400
15.3 An algorithm for factoring integers 407
15.4 Practical improvements 414
15.5 Notes 418

16 More rings 421
16.1 Algebras 421
16.2 The field of fractions of an integral domain 427
16.3 Unique factorization of polynomials 430
16.4 Polynomial congruences 435
16.5 Minimal polynomials 438
16.6 General properties of extension fields 440
16.7 Formal derivatives 444
16.8 Formal power series and Laurent series 446
16.9 Unique factorization domains (∗) 451
16.10 Notes 464

17 Polynomial arithmetic and applications 465
17.1 Basic arithmetic 465
17.2 Computing minimal polynomials in $F[X]/(f)$(I) 468
17.3 Euclid's algorithm 469
17.4 Computing modular inverses and Chinese remaindering 472
17.5 Rational function reconstruction and applications 474
17.6 Faster polynomial arithmetic (∗) 478
17.7 Notes 484

18 Linearly generated sequences and applications 486
18.1 Basic definitions and properties 486
18.2 Computing minimal polynomials: a special case 490
18.3 Computing minimal polynomials: a more general case 492
18.4 Solving sparse linear systems 497
18.5 Computing minimal polynomials in $F[X]/(f)$(II) 500
18.6 The algebra of linear transformations (∗) 501
18.7 Notes 508

19 Finite fields 509
19.1 Preliminaries 509

19.2 The existence of finite fields 511
19.3 The subfield structure and uniqueness of finite fields 515
19.4 Conjugates, norms and traces 516

20 Algorithms for finite fields 522
20.1 Tests for and constructing irreducible polynomials 522
20.2 Computing minimal polynomials in $F[X]/(f)$(III) 525
20.3 Factoring polynomials: square-free decomposition 526
20.4 Factoring polynomials: the Cantor–Zassenhaus algorithm 530
20.5 Factoring polynomials: Berlekamp's algorithm 538
20.6 Deterministic factorization algorithms ($*$) 544
20.7 Notes 546

21 Deterministic primality testing 548
21.1 The basic idea 548
21.2 The algorithm and its analysis 549
21.3 Notes 558

Appendix: Some useful facts 561
Bibliography 566
Index of notation 572
Index 574