# Contents

*Preface*  
*Preliminaries*  

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

## 2 Congruences  
2.1 Equivalence relations  
2.2 Definitions and basic properties of congruences  
2.3 Solving linear congruences  
2.4 The Chinese remainder theorem  
2.5 Residue classes  
2.6 Euler’s phi function  
2.7 Euler’s theorem and Fermat’s little theorem  
2.8 Quadratic residues  
2.9 Summations over divisors  

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

## 4 Euclid’s algorithm  
4.1 The basic Euclidean algorithm  
4.2 The extended Euclidean algorithm  
4.3 Computing modular inverses and Chinese remaindering
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
  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
  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 $\mathbb{Z}_p^*$
  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
  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
  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
  14.1 Basic definitions and properties 377
  14.2 Matrices and linear maps 381
  14.3 The inverse of a matrix 386
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.4</td>
<td></td>
<td>Gaussian elimination</td>
<td>388</td>
</tr>
<tr>
<td>14.5</td>
<td></td>
<td>Applications of Gaussian elimination</td>
<td>392</td>
</tr>
<tr>
<td>14.6</td>
<td></td>
<td>Notes</td>
<td>398</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>Subexponential-time discrete logarithms and factoring</td>
<td>399</td>
</tr>
<tr>
<td>15.1</td>
<td>Smooth numbers</td>
<td>399</td>
<td></td>
</tr>
<tr>
<td>15.2</td>
<td>An algorithm for discrete logarithms</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>15.3</td>
<td>An algorithm for factoring integers</td>
<td>407</td>
<td></td>
</tr>
<tr>
<td>15.4</td>
<td>Practical improvements</td>
<td>414</td>
<td></td>
</tr>
<tr>
<td>15.5</td>
<td>Notes</td>
<td>418</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>More rings</td>
<td>421</td>
</tr>
<tr>
<td>16.1</td>
<td>Algebras</td>
<td>421</td>
<td></td>
</tr>
<tr>
<td>16.2</td>
<td>The field of fractions of an integral domain</td>
<td>427</td>
<td></td>
</tr>
<tr>
<td>16.3</td>
<td>Unique factorization of polynomials</td>
<td>430</td>
<td></td>
</tr>
<tr>
<td>16.4</td>
<td>Polynomial congruences</td>
<td>435</td>
<td></td>
</tr>
<tr>
<td>16.5</td>
<td>Minimal polynomials</td>
<td>438</td>
<td></td>
</tr>
<tr>
<td>16.6</td>
<td>General properties of extension fields</td>
<td>440</td>
<td></td>
</tr>
<tr>
<td>16.7</td>
<td>Formal derivatives</td>
<td>444</td>
<td></td>
</tr>
<tr>
<td>16.8</td>
<td>Formal power series and Laurent series</td>
<td>446</td>
<td></td>
</tr>
<tr>
<td>16.9</td>
<td>Unique factorization domains (∗)</td>
<td>451</td>
<td></td>
</tr>
<tr>
<td>16.10</td>
<td>Notes</td>
<td>464</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Polynomial arithmetic and applications</td>
<td>465</td>
</tr>
<tr>
<td>17.1</td>
<td>Basic arithmetic</td>
<td>465</td>
<td></td>
</tr>
<tr>
<td>17.2</td>
<td>Computing minimal polynomials in $F[X]/(f)(I)$</td>
<td>468</td>
<td></td>
</tr>
<tr>
<td>17.3</td>
<td>Euclid’s algorithm</td>
<td>469</td>
<td></td>
</tr>
<tr>
<td>17.4</td>
<td>Computing modular inverses and Chinese remaindering</td>
<td>472</td>
<td></td>
</tr>
<tr>
<td>17.5</td>
<td>Rational function reconstruction and applications</td>
<td>474</td>
<td></td>
</tr>
<tr>
<td>17.6</td>
<td>Faster polynomial arithmetic (∗)</td>
<td>478</td>
<td></td>
</tr>
<tr>
<td>17.7</td>
<td>Notes</td>
<td>484</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>Linearly generated sequences and applications</td>
<td>486</td>
</tr>
<tr>
<td>18.1</td>
<td>Basic definitions and properties</td>
<td>486</td>
<td></td>
</tr>
<tr>
<td>18.2</td>
<td>Computing minimal polynomials: a special case</td>
<td>490</td>
<td></td>
</tr>
<tr>
<td>18.3</td>
<td>Computing minimal polynomials: a more general case</td>
<td>492</td>
<td></td>
</tr>
<tr>
<td>18.4</td>
<td>Solving sparse linear systems</td>
<td>497</td>
<td></td>
</tr>
<tr>
<td>18.5</td>
<td>Computing minimal polynomials in $F[X]/(f)(II)$</td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>18.6</td>
<td>The algebra of linear transformations (∗)</td>
<td>501</td>
<td></td>
</tr>
<tr>
<td>18.7</td>
<td>Notes</td>
<td>508</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td>Finite fields</td>
<td>509</td>
</tr>
<tr>
<td>19.1</td>
<td>Preliminaries</td>
<td>509</td>
<td></td>
</tr>
</tbody>
</table>
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 \( F[X]/(f)(\text{III}) \) 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