

Victor Shoup

A Computational  
Introduction

to  
and **Number Theory**  
**Algebra**

CAMBRIDGE

# Contents

<i>Preface</i>	<i>page</i> x
<i>Preliminaries</i>	xiv
<b>1 Basic properties of the integers</b>	<b>1</b>
1.1 Divisibility and primality	1
1.2 Ideals and greatest common divisors	4
1.3 Some consequences of unique factorization	8
<b>2 Congruences</b>	<b>13</b>
2.1 Definitions and basic properties	13
2.2 Solving linear congruences	15
2.3 Residue classes	20
2.4 Euler's phi function	24
2.5 Fermat's little theorem	25
2.6 Arithmetic functions and Möbius inversion	28
<b>3 Computing with large integers</b>	<b>33</b>
3.1 Asymptotic notation	33
3.2 Machine models and complexity theory	36
3.3 Basic integer arithmetic	39
3.4 Computing in $\mathbb{Z}_n$	48
3.5 Faster integer arithmetic (*)	51
3.6 Notes	52
<b>4 Euclid's algorithm</b>	<b>55</b>
4.1 The basic Euclidean algorithm	55
4.2 The extended Euclidean algorithm	58
4.3 Computing modular inverses and Chinese remaindering	62
4.4 Speeding up algorithms via modular computation	63
4.5 Rational reconstruction and applications	66
4.6 Notes	73

<b>5</b>	<b>The distribution of primes</b>	74
5.1	Chebyshev's theorem on the density of primes	74
5.2	Bertrand's postulate	78
5.3	Mertens' theorem	81
5.4	The sieve of Eratosthenes	85
5.5	The prime number theorem ... and beyond	86
5.6	Notes	94
<b>6</b>	<b>Finite and discrete probability distributions</b>	96
6.1	Finite probability distributions: basic definitions	96
6.2	Conditional probability and independence	99
6.3	Random variables	104
6.4	Expectation and variance	111
6.5	Some useful bounds	117
6.6	The birthday paradox	121
6.7	Hash functions	125
6.8	Statistical distance	130
6.9	Measures of randomness and the leftover hash lemma (*)	136
6.10	Discrete probability distributions	141
6.11	Notes	147
<b>7</b>	<b>Probabilistic algorithms</b>	148
7.1	Basic definitions	148
7.2	Approximation of functions	155
7.3	Flipping a coin until a head appears	158
7.4	Generating a random number from a given interval	159
7.5	Generating a random prime	162
7.6	Generating a random non-increasing sequence	167
7.7	Generating a random factored number	170
7.8	The RSA cryptosystem	174
7.9	Notes	179
<b>8</b>	<b>Abelian groups</b>	180
8.1	Definitions, basic properties, and examples	180
8.2	Subgroups	185
8.3	Cosets and quotient groups	190
8.4	Group homomorphisms and isomorphisms	194
8.5	Cyclic groups	202
8.6	The structure of finite abelian groups (*)	208
<b>9</b>	<b>Rings</b>	211
9.1	Definitions, basic properties, and examples	211
9.2	Polynomial rings	220

9.3	Ideals and quotient rings	231
9.4	Ring homomorphisms and isomorphisms	236
<b>10</b>	<b>Probabilistic primality testing</b>	<b>244</b>
10.1	Trial division	244
10.2	The structure of $\mathbb{Z}_n^*$	245
10.3	The Miller–Rabin test	247
10.4	Generating random primes using the Miller–Rabin test	252
10.5	Perfect power testing and prime power factoring	261
10.6	Factoring and computing Euler’s phi function	262
10.7	Notes	266
<b>11</b>	<b>Finding generators and discrete logarithms in <math>\mathbb{Z}_p^*</math></b>	<b>268</b>
11.1	Finding a generator for $\mathbb{Z}_p^*$	268
11.2	Computing discrete logarithms $\mathbb{Z}_p^*$	270
11.3	The Diffie–Hellman key establishment protocol	275
11.4	Notes	281
<b>12</b>	<b>Quadratic residues and quadratic reciprocity</b>	<b>283</b>
12.1	Quadratic residues	283
12.2	The Legendre symbol	285
12.3	The Jacobi symbol	287
12.4	Notes	289
<b>13</b>	<b>Computational problems related to quadratic residues</b>	<b>290</b>
13.1	Computing the Jacobi symbol	290
13.2	Testing quadratic residuosity	291
13.3	Computing modular square roots	292
13.4	The quadratic residuosity assumption	297
13.5	Notes	298
<b>14</b>	<b>Modules and vector spaces</b>	<b>299</b>
14.1	Definitions, basic properties, and examples	299
14.2	Submodules and quotient modules	301
14.3	Module homomorphisms and isomorphisms	303
14.4	Linear independence and bases	306
14.5	Vector spaces and dimension	309
<b>15</b>	<b>Matrices</b>	<b>316</b>
15.1	Basic definitions and properties	316
15.2	Matrices and linear maps	320
15.3	The inverse of a matrix	323
15.4	Gaussian elimination	324
15.5	Applications of Gaussian elimination	328

15.6	Notes	334
<b>16</b>	<b>Subexponential-time discrete logarithms and factoring</b>	<b>336</b>
16.1	Smooth numbers	336
16.2	An algorithm for discrete logarithms	337
16.3	An algorithm for factoring integers	344
16.4	Practical improvements	352
16.5	Notes	356
<b>17</b>	<b>More rings</b>	<b>359</b>
17.1	Algebras	359
17.2	The field of fractions of an integral domain	363
17.3	Unique factorization of polynomials	366
17.4	Polynomial congruences	371
17.5	Polynomial quotient algebras	374
17.6	General properties of extension fields	376
17.7	Formal power series and Laurent series	378
17.8	Unique factorization domains (*)	383
17.9	Notes	397
<b>18</b>	<b>Polynomial arithmetic and applications</b>	<b>398</b>
18.1	Basic arithmetic	398
18.2	Computing minimal polynomials in $F[X]/(f)$ (I)	401
18.3	Euclid's algorithm	402
18.4	Computing modular inverses and Chinese remaindering	405
18.5	Rational function reconstruction and applications	410
18.6	Faster polynomial arithmetic (*)	415
18.7	Notes	421
<b>19</b>	<b>Linearly generated sequences and applications</b>	<b>423</b>
19.1	Basic definitions and properties	423
19.2	Computing minimal polynomials: a special case	428
19.3	Computing minimal polynomials: a more general case	429
19.4	Solving sparse linear systems	435
19.5	Computing minimal polynomials in $F[X]/(f)$ (II)	438
19.6	The algebra of linear transformations (*)	440
19.7	Notes	447
<b>20</b>	<b>Finite fields</b>	<b>448</b>
20.1	Preliminaries	448
20.2	The existence of finite fields	450
20.3	The subfield structure and uniqueness of finite fields	454
20.4	Conjugates, norms and traces	456

<b>21</b>	<b>Algorithms for finite fields</b>	462
21.1	Testing and constructing irreducible polynomials	462
21.2	Computing minimal polynomials in $F[X]/(f)$ (III)	465
21.3	Factoring polynomials: the Cantor–Zassenhaus algorithm	467
21.4	Factoring polynomials: Berlekamp’s algorithm	475
21.5	Deterministic factorization algorithms (*)	483
21.6	Faster square-free decomposition (*)	485
21.7	Notes	487
<b>22</b>	<b>Deterministic primality testing</b>	489
22.1	The basic idea	489
22.2	The algorithm and its analysis	490
22.3	Notes	500
	<i>Appendix: Some useful facts</i>	501
	<i>Bibliography</i>	504
	<i>Index of notation</i>	510
	<i>Index</i>	512