

---

# Contents

Introduction	1
Structure of the book	1
Exercises	2
Short overview of the individual chapters	2
Technical details	4
Commemoration	4
Acknowledgements	5
Chapter 1. Basic Notions	7
1.1. Divisibility	7
Exercises 1.1	9
1.2. Division Algorithm	11
Exercises 1.2	13
1.3. Greatest Common Divisor	15
Exercises 1.3	19
1.4. Irreducible and Prime Numbers	21
Exercises 1.4	23
1.5. The Fundamental Theorem of Arithmetic	24
Exercises 1.5	27
1.6. Standard Form	28
Exercises 1.6	33
Chapter 2. Congruences	37
2.1. Elementary Properties	37
Exercises 2.1	40

---

2.2. Residue Systems and Residue Classes	41
Exercises 2.2	44
2.3. Euler's Function $\varphi$	46
Exercises 2.3	49
2.4. The Euler–Fermat Theorem	50
Exercises 2.4	51
2.5. Linear Congruences	52
Exercises 2.5	57
2.6. Simultaneous Systems of Congruences	58
Exercises 2.6	64
2.7. Wilson's Theorem	66
Exercises 2.7	67
2.8. Operations with Residue Classes	68
Exercises 2.8	70
Chapter 3. Congruences of Higher Degree	73
3.1. Number of Solutions and Reduction	73
Exercises 3.1	75
3.2. Order	76
Exercises 3.2	78
3.3. Primitive Roots	80
Exercises 3.3	84
3.4. Discrete Logarithm (Index)	86
Exercises 3.4	87
3.5. Binomial Congruences	88
Exercises 3.5	90
3.6. Chevalley's Theorem, Kőnig–Rados Theorem	91
Exercises 3.6	95
3.7. Congruences with Prime Power Moduli	96
Exercises 3.7	98
Chapter 4. Legendre and Jacobi Symbols	101
4.1. Quadratic Congruences	101
Exercises 4.1	103
4.2. Quadratic Reciprocity	104
Exercises 4.2	108
4.3. Jacobi Symbol	109
Exercises 4.3	111

---

Chapter 5. Prime Numbers	113
5.1. Classical Problems	113
Exercises 5.1	117
5.2. Fermat and Mersenne Primes	118
Exercises 5.2	124
5.3. Primes in Arithmetic Progressions	125
Exercises 5.3	127
5.4. How Big Is $\pi(x)$ ?	128
Exercises 5.4	133
5.5. Gaps between Consecutive Primes	134
Exercises 5.5	139
5.6. The Sum of Reciprocals of Primes	140
Exercises 5.6	147
5.7. Primality Tests	149
Exercises 5.7	157
5.8. Cryptography	160
Exercises 5.8	163
Chapter 6. Arithmetic Functions	165
6.1. Multiplicative and Additive Functions	165
Exercises 6.1	167
6.2. Some Important Functions	170
Exercises 6.2	173
6.3. Perfect Numbers	175
Exercises 6.3	177
6.4. Behavior of $d(n)$	178
Exercises 6.4	185
6.5. Summation and Inversion Functions	186
Exercises 6.5	189
6.6. Convolution	190
Exercises 6.6	193
6.7. Mean Value	195
Exercises 6.7	206
6.8. Characterization of Additive Functions	207
Exercises 6.8	209
Chapter 7. Diophantine Equations	211
7.1. Linear Diophantine Equation	212
Exercises 7.1	214

---

7.2. Pythagorean Triples	215
Exercises 7.2	217
7.3. Some Elementary Methods	218
Exercises 7.3	221
7.4. Gaussian Integers	223
Exercises 7.4	229
7.5. Sums of Squares	230
Exercises 7.5	235
7.6. Waring's Problem	236
Exercises 7.6	240
7.7. Fermat's Last Theorem	241
Exercises 7.7	249
7.8. Pell's Equation	251
Exercises 7.8	255
7.9. Partitions	256
Exercises 7.9	261
Chapter 8. Diophantine Approximation	263
8.1. Approximation of Irrational Numbers	263
Exercises 8.1	268
8.2. Minkowski's Theorem	270
Exercises 8.2	274
8.3. Continued Fractions	275
Exercises 8.3	280
8.4. Distribution of Fractional Parts	281
Exercises 8.4	283
Chapter 9. Algebraic and Transcendental Numbers	285
9.1. Algebraic Numbers	285
Exercises 9.1	288
9.2. Minimal Polynomial and Degree	288
Exercises 9.2	290
9.3. Operations with Algebraic Numbers	291
Exercises 9.3	294
9.4. Approximation of Algebraic Numbers	296
Exercises 9.4	300
9.5. Transcendence of $e$	301
Exercises 9.5	306
9.6. Algebraic Integers	306

---

Exercises 9.6	308
Chapter 10. Algebraic Number Fields	311
10.1. Field Extensions	311
Exercises 10.1	314
10.2. Simple Algebraic Extensions	315
Exercises 10.2	319
10.3. Quadratic Fields	320
Exercises 10.3	330
10.4. Norm	331
Exercises 10.4	334
10.5. Integral Basis	335
Exercises 10.5	340
Chapter 11. Ideals	341
11.1. Ideals and Factor Rings	341
Exercises 11.1	345
11.2. Elementary Connections to Number Theory	347
Exercises 11.2	350
11.3. Unique Factorization, Principal Ideal Domains, and Euclidean Rings	350
Exercises 11.3	355
11.4. Divisibility of Ideals	357
Exercises 11.4	361
11.5. Dedekind Rings	363
Exercises 11.5	372
11.6. Class Number	373
Exercises 11.6	376
Chapter 12. Combinatorial Number Theory	377
12.1. All Sums Are Distinct	377
Exercises 12.1	384
12.2. Sidon Sets	386
Exercises 12.2	393
12.3. Sumsets	394
Exercises 12.3	402
12.4. Schur's Theorem	403
Exercises 12.4	407
12.5. Covering Congruences	408
Exercises 12.5	412

---

12.6. Additive Complements	412
Exercises 12.6	418
Answers and Hints	421
A.1. Basic Notions	421
A.2. Congruences	431
A.3. Congruences of Higher Degree	442
A.4. Legendre and Jacobi Symbols	452
A.5. Prime Numbers	455
A.6. Arithmetic Functions	467
A.7. Diophantine Equations	483
A.8. Diophantine Approximation	501
A.9. Algebraic and Transcendental Numbers	505
A.10. Algebraic Number Fields	510
A.11. Ideals	516
A.12. Combinatorial Number Theory	521
Historical Notes	531
Tables	537
Primes 2–1733	538
Primes 1741–3907	539
Prime Factorization	540
Mersenne Numbers	541
Fermat Numbers	542
Index	543