
Contents

Preface	ix
Notations and Symbols	xv
Chapter 1. Evens, Odds, and Primes: A Taste of Number Theory	1
1.1. A first excursion into prime numbers	3
1.2. Even and odd integers	12
1.3. Calculating primes and the sieve of Eratosthenes	18
1.4. Division	23
1.5. Greatest common divisor	27
1.6. Statement of prime factorization	35
1.7*. Perfect numbers	39
1.8*. One of the Mersenne conjectures	40
1.9*. Twin primes: An excursion into the unknown	42
1.10*. Goldbach's conjecture	43
1.11. Hints and partial solutions for the exercises	45
Chapter 2. Mathematical Induction	49
2.1. Mathematical induction	50
2.2. Rates of growth of functions	62
2.3. Sums of powers of the first n positive integers	69
2.4. Strong mathematical induction	78
2.5. Fibonacci numbers	82
2.6. Recursive definitions	91
2.7. Arithmetic and algebraic equalities and inequalities	95
2.8. Hints and partial solutions for the exercises	99

Chapter 3. Logic: Implications, Contrapositives, Contradictions, and Quantifiers	107
3.1. The need for rigor	108
3.2. Statements	113
3.3. Truth teller and liar riddle: Asking the right question	115
3.4*. Logic puzzles	116
3.5. Logical connectives	120
3.6. Implications	128
3.7. Contrapositive	134
3.8. Proof by contradiction	138
3.9. Pythagorean triples	145
3.10. Quantifiers	150
3.11. Hints and partial solutions for the exercises	156
Chapter 4. The Euclidean Algorithm and Its Consequences	161
4.1. The Division Theorem	161
4.2. There are an infinite number of primes	171
4.3. The Euclidean algorithm	173
4.4. Consequences of the Division Theorem	176
4.5. Solving linear Diophantine equations	182
4.6. “Practical” applications of solving linear Diophantine equations (wink ☺)	187
4.7*. (Polynomial) Diophantine equations	188
4.8. The Fundamental Theorem of Arithmetic	190
4.9. The least common multiple	191
4.10. Residues modulo an odd prime	193
4.11. Appendix	194
4.12. Hints and partial solutions for the exercises	196
Chapter 5. Sets and Functions	203
5.1. Basics of set theory	204
5.2. Cartesian products of sets	214
5.3. Functions and their properties	225
5.4. Types of functions: Injections, surjections, and bijections	234
5.5. Arbitrary unions, intersections, and cartesian products	244
5.6*. Universal properties of surjections and injections	246
5.7. Hints and partial solutions for the exercises	247
Chapter 6. Modular Arithmetic	255
6.1. Multiples of 3 and 9 and the digits of a number in base 10	256
6.2. Congruence modulo m	257

6.3.	Inverses, coprimeness, and congruence	266
6.4.	Congruence and multiplicative cancellation	267
6.5*.	Fun congruence facts	269
6.6.	Solving linear congruence equations	270
6.7*.	The Chinese Remainder Theorem	278
6.8.	Quadratic residues	280
6.9.	Fermat's Little Theorem	284
6.10*.	Euler's totient function and Euler's Theorem	289
6.11*.	An application of Fermat's Little Theorem: The RSA algorithm	294
6.12*.	The Euclid–Euler Theorem characterizing even perfect numbers	295
6.13*.	Twin prime pairs	299
6.14.	Chameleons roaming around in a zoo	299
6.15.	Hints and partial solutions for the exercises	302
Chapter 7.	Counting Finite Sets	309
7.1.	The addition principle	309
7.2.	Cartesian products and the multiplication principle	312
7.3.	The inclusion-exclusion principle	314
7.4.	Binomial coefficients and the Binomial Theorem	322
7.5.	Counting functions	344
7.6.	Counting problems	350
7.7*.	Using the idea of a bijection	353
7.8.	Hints and partial solutions for the exercises	354
Chapter 8.	Congruence Class Arithmetic, Groups, and Fields	361
8.1.	Congruence classes modulo m	361
8.2.	Inverses of congruence classes	369
8.3.	Reprise of the proof of Fermat's Little Theorem	372
8.4.	Equivalence relations, equivalence classes, and partitions	374
8.5.	Elementary abstract algebra	380
8.6.	Rings, principal ideal domains, and all that	397
8.7.	Fields	400
8.8*.	Quadratic residues and the law of quadratic reciprocity	410
8.9.	Hints and partial solutions for the exercises	425
Bibliography		435
Index		437