

Contents

Foreword	i
1 Introduction	1
2 Divisibility	3
2.1 Basic properties	3
2.1.1 Divisibility and congruences	3
2.1.2 Divisibility and order relation	10
2.2 Induction and binomial coefficients	22
2.2.1 Proving divisibility by induction	22
2.2.2 Arithmetic of binomial coefficients	26
2.2.3 Derivatives and finite differences	34
2.2.4 The binomial formula	38
2.3 Euclidean division	43
2.3.1 The Euclidean division	43
2.3.2 Combinatorial arguments and complete residue systems	47
2.4 Problems for practice	56
3 GCD and LCM	63
3.1 Bézout's theorem and Gauss' lemma	63
3.1.1 Bézout's theorem and the Euclidean algorithm	63
3.1.2 Relatively prime numbers	68
3.1.3 Inverse modulo n and Gauss' lemma	72
3.2 Applications to diophantine equations and approximations . . .	80
3.2.1 Linear diophantine equations	80

3.2.2	Pythagorean triples	83
3.2.3	The rational root theorem	92
3.2.4	Farey fractions and Pell's equation	96
3.3	Least common multiple	113
3.4	Problems for practice	121
4	The fundamental theorem of arithmetic	129
4.1	Composite numbers	129
4.2	The fundamental theorem of arithmetic	134
4.2.1	The theorem and its first consequences	134
4.2.2	The smallest and largest prime divisor	144
4.2.3	Combinatorial number theory	149
4.3	Infinitude of primes	154
4.3.1	Looking for primes in classical sequences	155
4.3.2	Euclid's argument	160
4.3.3	Euler's and Borse's inequalities	171
4.4	Arithmetic functions	178
4.4.1	Classical arithmetic functions	178
4.4.2	Multiplicative functions	184
4.4.3	Euler's phi function	194
4.4.4	The Möbius function and its applications	206
4.4.5	Application to squarefree numbers	210
4.5	Problems for practice	216
5	Congruences involving prime numbers	225
5.1	Fermat's little theorem	225
5.1.1	Fermat's little theorem and (pseudo-)primality	225
5.1.2	Some concrete examples	230
5.1.3	Application to primes of the form $4k + 3$ and $3k + 2$	238
5.2	Wilson's theorem	244
5.2.1	Wilson's theorem as criterion of primality	244
5.2.2	Application to sums of two squares	252
5.3	Lagrange's theorem and applications	259
5.3.1	The number of solutions of polynomial congruences	259
5.3.2	The congruence $x^d \equiv 1 \pmod{p}$	266

5.3.3	The Chevalley-Waring theorem	272
5.4	Quadratic residues and quadratic reciprocity	278
5.4.1	Quadratic residues and Legendre's symbol	278
5.4.2	Points on spheres mod p and Gauss sums	286
5.4.3	The quadratic reciprocity law	297
5.5	Congruences involving rational numbers and binomial coefficients	304
5.5.1	Binomial coefficients modulo primes: Lucas' theorem	304
5.5.2	Congruences involving rational numbers	310
5.5.3	Higher congruences: Fleck, Morley, Wolstenholme,...	316
5.5.4	Hensel's lemma	324
5.6	Problems for practice	330
6	p-adic valuations and the distribution of primes	341
6.1	The yoga of p -adic valuations	341
6.1.1	The local-global principle	341
6.1.2	The strong triangle inequality	347
6.1.3	Lifting the exponent lemma	353
6.2	Legendre's formula	360
6.2.1	The p -adic valuation of $n!$: the exact formula	360
6.2.2	The p -adic valuation of $n!$: inequalities	363
6.2.3	Kummer's theorem	369
6.3	Estimates for binomial coefficients and the distribution of prime numbers	373
6.3.1	Central binomial coefficients and Erdős' inequality	373
6.3.2	Estimating $\pi(n)$	376
6.3.3	Bertrand's postulate	380
6.4	Problems for practice	386
7	Congruences for composite moduli	393
7.1	The Chinese remainder theorem	393
7.1.1	Proof of the theorem and first examples	393
7.1.2	The local-global principle	400
7.1.3	Covering systems of congruences	408
7.2	Euler's theorem	417

7.2.1	Reduced residue systems and Euler's theorem	417
7.2.2	Practicing Euler's theorem	421
7.3	Order modulo n	427
7.3.1	Elementary properties and examples	427
7.3.2	Practicing the notion of order modulo n	440
7.3.3	Primitive roots modulo n	448
7.4	Problems for practice	460
8	Solutions to practice problems	467
8.1	Divisibility	467
8.2	GCD and LCM	496
8.3	The fundamental theorem of arithmetic	523
8.4	Congruences involving prime numbers	568
8.5	p -adic valuations and the distribution of primes	620
8.6	Congruences for composite moduli	652
	Bibliography	683
	Other Books from XYZ Press	685