

Contents

Preface to the Croatian edition	i
Preface to the English edition	v
1 Introduction	1
1.1 Peano's axioms	1
1.2 Principle of mathematical induction	4
1.3 Fibonacci numbers	10
1.4 Exercises	18
2 Divisibility	22
2.1 Greatest common divisor	22
2.2 Euclid's algorithm	25
2.3 Prime numbers	31
2.4 Exercises	39
3 Congruences	42
3.1 Definition and properties of congruences	42
3.2 Tests of divisibility	45
3.3 Linear congruences	48
3.4 Chinese remainder theorem	50
3.5 Reduced residue system	54
3.6 Congruences with a prime modulus	57
3.7 Primitive roots and indices	62
3.8 Representations of rational numbers by decimals	68
3.9 Pseudoprimes	73
3.10 Exercises	79
4 Quadratic residues	83
4.1 Legendre symbol	83
4.2 Law of quadratic reciprocity	89

4.3	Computing square roots modulo p	94
4.4	Jacobi symbol	96
4.5	Divisibility of Fibonacci numbers	99
4.6	Exercises	104
5	Quadratic forms	107
5.1	Sums of two squares	107
5.2	Positive definite binary quadratic forms	111
5.3	Sums of four squares	121
5.4	Sums of three squares	125
5.5	Exercises	132
6	Arithmetical functions	136
6.1	Greatest integer function	136
6.2	Multiplicative functions	140
6.3	Asymptotic estimates for arithmetical functions	145
6.4	Dirichlet product	152
6.5	Exercises	155
7	Distribution of primes	159
7.1	Elementary estimates for the function $\pi(x)$	159
7.2	Chebyshev functions	164
7.3	The Riemann zeta function	172
7.4	Dirichlet characters	176
7.5	Primes in arithmetic progressions	183
7.6	Exercises	187
8	Diophantine approximation	191
8.1	Dirichlet's theorem	191
8.2	Farey sequences	194
8.3	Continued fractions	201
8.4	Continued fraction and approximations to irrational numbers	208
8.5	Equivalent numbers	217
8.6	Periodic continued fractions	222
8.7	Newton's approximants	229
8.8	Simultaneous approximations	233
8.9	LLL algorithm	240
8.10	Exercises	246

9	Applications of Diophantine approximation to cryptography	250
9.1	A very short introduction to cryptography	250
9.2	RSA cryptosystem	254
9.3	Wiener's attack on RSA	257
9.4	Attacks on RSA using the LLL algorithm	260
9.5	Coppersmith's theorem	264
9.6	Exercises	267
10	Diophantine equations I	270
10.1	Linear Diophantine equations	270
10.2	Pythagorean triangles	274
10.3	Pell's equation	284
10.4	Continued fractions and Pell's equation	293
10.5	Pellian equation	296
10.6	Squares in the Fibonacci sequence	302
10.7	Ternary quadratic forms	307
10.8	Local-global principle	320
10.9	Exercises	328
11	Polynomials	334
11.1	Divisibility of polynomials	334
11.2	Polynomial roots	342
11.3	Irreducibility of polynomials	347
11.4	Polynomial decomposition	350
11.5	Symmetric polynomials	358
11.6	Exercises	363
12	Algebraic numbers	366
12.1	Quadratic fields	366
12.2	Algebraic number fields	376
12.3	Algebraic integers	380
12.4	Ideals	384
12.5	Units and ideal classes	392
12.6	Exercises	399
13	Approximation of algebraic numbers	402
13.1	Liouville's theorem	402
13.2	Roth's theorem	404
13.3	The hypergeometric method	407
13.4	Approximation by quadratic irrationals	417

13.5	Polynomial root separation	422
13.6	Exercises	428
14	Diophantine equations II	431
14.1	Thue equations	431
14.2	Tzanakis' method	435
14.3	Linear forms in logarithms	440
14.4	Baker-Davenport reduction	445
14.5	LLL reduction	450
14.6	Diophantine m -tuples	454
14.7	Exercises	462
15	Elliptic curves	466
15.1	Introduction to elliptic curves	466
15.2	Equations of elliptic curves	473
15.3	Torsion group	486
15.4	Canonical height and Mordell-Weil theorem	499
15.5	Rank of elliptic curves	506
15.6	Finite fields	519
15.7	Elliptic curves over finite fields	526
15.8	Applications of elliptic curves in cryptography	535
15.9	Primality proving using elliptic curves	544
15.10	Elliptic curve factorization method	548
15.11	Exercises	552
16	Diophantine problems and elliptic curves	556
16.1	Congruent numbers	556
16.2	Mordell's equation	558
16.3	Applications of factorization in quadratic fields	560
16.4	Transformation of elliptic curves to Thue equations	565
16.5	Algorithm for solving Thue equations	568
16.6	abc conjecture	574
16.7	Diophantine m -tuples and elliptic curves	578
16.8	Exercises	586
	References	589
	Notation Index	613
	Subject Index	616