

Contents

<i>Preface</i>	<i>page</i> xi
<i>For Readers</i>	xii
<i>Table of Theorems</i>	xv
1 Divisibility	1
§1 Euclid’s spirit. Divisors. Multiples	1
§2 Deviation from being divisible. Division algorithm	3
§3 Euclid’s algorithm. Greatest common divisor. Coprimality	5
§4 Integral modules. Inclusion and divisibility	8
§5 Modular group. Group structure over the integers	10
§6 Coprimality and divisibility	13
§7 Greatest common divisor of many integers	14
§8 Integral linear indefinite equations. Chaotic behavior	17
§9 Canonical form of integral matrices. Free Abelian groups	21
§10 Prime numbers. Least common multiple	24
§11 Unique prime power decomposition. Euler product. Zeta-function	29
§12 Prime number theorem. Riemann’s paradigm and his hypothesis	35
§13 Sums over prime numbers. Summation by parts	44
§14 Least common multiple of many integers	49
§15 Arithmetic functions. Multiplicative functions. Dirichlet series	51
§16 Multiplicative convolution. Divisor problem	56
§17 Möbius inversion. Chebyshev’s logarithmic amplification	64
§18 Separating coprime integers	69
§19 Basic sieve identities. Two kinds of sieves	76
§20 Fractions. Rational approximation	84

§21	Euler–Lagrange theory of continued fractions. Convergents	88
§22	Infinite continued fractions. Extended Euclid’s algorithm	93
§23	Lagrange’s theorem on best rational approximation	96
§24	Legendre’s criterion for convergents	100
§25	Modular property of continued fractions	104
§26	Saga of the <i>Elements</i> . History of continued fractions	106
2	Congruences	116
§27	Moduli. Residues	116
§28	Reduced residues. Fermat’s theorem. Euler’s proofs	119
§29	Linear congruence equations	125
§30	Rings of residue classes. Structure of finite Abelian groups	129
§31	System of linear congruence equations	133
§32	Groups of reduced residue classes. Small set of generators	135
§33	Congruence equations. Severe premise on moduli	138
§34	Prime moduli. Fundamental theorem of Lagrange	141
§35	Wilson’s theorem proved in various ways	144
§36	Contraposition of Fermat’s theorem	146
§37	Integers resembling to prime numbers	148
§38	ρ - algorithm for factoring integers	151
§39	Order of reduced residue. Primitive roots	153
§40	Existence of primitive roots	155
§41	Primitive roots and primality test	159
§42	Reduced residue system modulo a prime power	161
§43	Criteria for power residues. A reciprocity issue	163
§44	Discrete logarithm	169
§45	Solving binomial congruences (part 1)	173
§46	Probabilistic primality test and factorization of integers	178
§47	Quantum factorization of integers (phase 1)	183
§48	Quantum factorization of integers (phase 2)	190
§49	Basic methods of integer factorization. Public key cryptosystems	193
3	Characters	199
§50	Additive characters	199
§51	Multiplicative characters. Characters of finite Abelian groups	202
§52	Dirichlet characters and L -functions	207
§53	Primitive characters. Generalized Riemann hypothesis	211
§54	Structure of primitive characters. Primitive real characters	214
§55	Fourier expansion of primitive characters. Gauss sums	217

Contents

ix

§56	Fourier expansion of arbitrary characters	221
§57	Quadratic residues and non-residues. Legendre symbol	225
§58	The quadratic reciprocity law. Gauss' 3 rd proof	227
§59	Reciprocity and automorphic structure. Gauss' 4 th proof	233
§60	Poisson's sum formula	235
§61	Digression related to Gauss sums and Jacobi sums	239
§62	Jacobi symbol. Contents of the reciprocity law	247
§63	Solving quadratic congruence	252
§64	Irreducibility of cyclotomic polynomials	256
§65	Quadratic decomposition of cyclotomic polynomials	262
§66	Gauss' 6 th proof. Extension of the notion of integers	267
§67	Gauss' 7 th and 8 th proofs. Algebraic extensions of finite fields	270
§68	Solving binomial congruences (part 2)	278
§69	Discovery of the reciprocity law. Legendre's efforts	281
§70	Prehistory of Gauss sums. Vandermonde resolvents	285
4	Quadratic Forms	296
§71	Integral binary quadratic forms. The representation problem	296
§72	Lagrange's principle. Matrix modules, orders, and ideals	304
§73	Kronecker symbol. Rôle of the reciprocity law	313
§74	Classification of quadratic forms modulo the modular group	319
§75	Ambiguous forms and classes	326
§76	Class number. Automorphisms and seed representations	329
§77	Definite forms. Fundamental domain of the modular group	334
§78	Sums of two squares	340
§79	The case of discriminant -20 . Dirichlet identity	348
§80	The case of discriminant -231 . Glimpse of genus groups	353
§81	Directly solving the representation problem (part 1)	356
§82	Indefinite forms. Periodic continued fractions. Closed geodesics	362
§83	Cycles of orbits. Parity of periods	369
§84	Lagrange's theorem on Pell equations	375
§85	Automorphism groups. Selberg's zeta-function (part 1)	387
§86	Cakravala algorithm	395
§87	Directly solving the representation problem (part 2)	400
§88	Intermezzo. Legendre's proof of the reciprocity law	409
§89	Diagonal ternary quadratic forms	416
§90	Gauss' composition of quadratic forms. Class group	423

§91	Genus theory. Genus characters. Gauss’ 2 nd proof of the reciprocity law	438
§92	Dirichlet’s class number formula	456
§93	Analytic approach to the theory of quadratic forms	470
5	Distribution of Prime Numbers	487
§94	Riemann’s article. Selberg’s zeta-function (part 2)	487
§95	The explicit formula of Riemann	505
§96	Bounding exponential sums	518
§97	Vinogradov’s prime number theorem	524
§98	Hoheisel scheme. Basic L^2 -inequalities	535
§99	Mean values of the Riemann zeta-function	548
§100	Huxley’s prime number theorem	562
§101	Exceptional Dirichlet characters. Siegel’s theorem	568
§102	Duality between Linnik’s and Selberg’s sieves	581
§103	Blending dual sieves (part 1)	591
§104	Sifting arithmetic progressions	602
§105	Bombieri’s prime number theorem	609
§106	Blending dual sieves (part 2). Linnik’s prime number theorem	622
§107	Detecting infinitely often bounded gaps between prime numbers	638
	<i>Bibliography</i>	653
	<i>Index</i>	676