Contents

Note: Chapters are divided into sections, and groups of sections form unified topics; this is indicated in the table of contents by indentation. Thus, for example, in Chapter 1, Sections 1 through 3 form a topic, as do Sections 4 and 5.

Preface to the Second Edition v

Preface to the First Edition vii

Preface to the English Translation ix

Facts Used Without Proof in the Book xvii

Chapter 1. Divisibility, the Fundamental Theorem of Number Theory .. 1

1. Perfect numbers, amicable numbers. **2.** Division with remainder. (Exercises **1–11.**) **3.** The four number theorem. (Exercises **13–14.**) 1

4. Divisibility properties. (Exercise **15.**) **5.** Further divisibility properties. (Exercises **16–18.**) 7

6. Prime and composite numbers, existence of prime divisors. The sequence of primes is infinite. (Exercises **19–20.**) **7.** Decomposition as a product of prime factors. (Exercises **21–23.**) **8.** Euclid's lemma. (Exercises **24–25.**) **9.** The prime property. 10

10. The uniqueness of decomposition into prime factors (fundamental theorem). The generalization of the four number theorem. **11.** The proof of the generalization. **12.** History of the fundamental theorem. (Exercises **26–33.**) **13.** Canonical decomposition. **14.** The divisors, multiples, and number of divisors of an integer. (Exercises **34–35.**) **15.** Common divisors of numbers, the distinguished common divisor. **16.** Common multiples, the distinguished common multiple. (Exercises **36–38.**) **17.** Relatively prime numbers and pairwise relatively prime numbers. **18.** The irrationality of the kth root. **19.** The canonical decomposition of factorials. **20.** Canonical decomposition of binomial coefficients, their prime power divisors. (Exercises **39–44.**) 13

21. Pythagorean triples. **22.** Squares of odd integers. **23–24.** Parametrization of Pythagorean triples, primitive triples. (Exercises **45–49.**) **25.** The divisors of the sum of two squares. (Exercises **50–53.**) 25

26. Two properties of the distinguished common divisor (without the use of the fundamental theorem). **27.** The Euclidean algorithm. (Exercises **54–57.**) **28.** Numbers with the prime property. (Exercise **58.**) A new proof of the fundamental theorem. (Exercises **59–60.**) **29.** Solubility of first-order Diophantine equations. **30.** All solutions of first-order Diophantine equations. (Exercises **61–65.**) 30

Chapter 2. Congruences 39

1. The concept of congruence. **2.** Fundamental properties. **3.** Rules for divisibility. **4.** Residue classes, operations with residue classes. **5.** The splitting of a residue class into residue classes for a multiple of the original modulus. **6.** Complete residue system. (Exercises **1–6.**) 39

7. Disjoint residue systems. **8.** Covering residue systems. (Exercises **7–10.**) **9*–10.** The sum of the reciprocals of the moduli. 45

11. Solubility of first-order congruences. (Exercises **11–13.**) **12.** A necessary and sufficient condition for the solution. **13.** Relation with first-order Diophantine equations. **14.** Simultaneous systems of congruences, a survey of solubility. **15.** How to determine one solution (in the case of relatively prime moduli). **16.** The Chinese remainder theorem. **17.** The general case. (Exercises **14–18.**) **18.** Improving the computational speed using parallel processing. **19.** "Reclusive primes." (Dirichlet's theorem on arithmetic progressions.) (Exercises **19–20.**) 49

20. Reduced residue systems, Euler's φ-function. **21.** A characterization of the function. **22.** A characterization of reduced residue systems. (Exercise **21.**) **23.** An application: the Euler–Fermat theorem. **24.** Fermat's theorem. **25.** An application to the solution of first-order congruences. **26.** A geometric proof of Fermat's theorem. **27.** Cryptography. **28.** A number-theoretic code. **29.** The code can be published. **30.** Verifying the identity of the sender. 58

31. The order of an element, modulo m. **32.** Factoring out a root of a polynomial, modulo m. **33.** The number of roots for a prime modulus. **34.** Wilson's theorem. **35.** Solubility of $c^2 \equiv -1 \pmod{p}$. (Exercises **22–26.**) **36.** The number of roots of $x^k - 1$, modulo m. (Exercises **27–28.**) **37.** Properties of the order of an element. **38.** The distribution of the order of elements for a prime modulus, primitive roots, index. (Exercises **29–31.**) **39.** The Euler function is multiplicative. 64

40. Second degree congruences, quadratic residues, quadratic character of a product. **41.** The Legendre symbol. **42.** The Euler lemma. **43.** An example; notes on how to arrive at a solution. **44.** The Gauss lemma. **45–47.** Examples to determine those primes for which a number can be a quadratic residue. **48–50.** Two general theorems to the previous question. **51.** The reciprocity theorem. (Exercises **32–38.**) 73

Chapter 3. Rational and Irrational Numbers. Approximation of Numbers by Rational Numbers (Diophantine Approximation) 85

1. The goal of the chapter. **2.** Rational numbers in decimal notation. **3.** The meaning of infinite decimals. **4.** The common fractional representation of periodic decimals (Exercises **1–3.**) **5–6.** Aperiodic decimals. (Exercise **4.**) **7.** Incommensurable distances, the irrationality of $\sqrt{m^2+1}$. **8.** A modification to the proof. (Exercises **5–6.**) **9.** An arithmetic proof of the irrationality of $\sqrt{2}$. **10.** A geometric proof that $\sqrt{m}$ either is an integer or is irrational. **11.** An arithmetic variation of the proof. 85

12. The irrationality of $\tan(\pi/m)$; a formula for $\tan m\alpha$. The case for m odd. **13.** The case for m even. **14*.** The irrationality of e. **15.** Transcendental numbers, results, problems. (Exercises **7–13.**) 95

16. Approximating real numbers well by rational numbers; the existence of infinitely many close rational numbers. The sequence of points of a circle arising by measuring off arc lengths. **17.** Finding approximating fractions. (Exercises **14–15.**) **18.** Liouville's theorem; Thue equations. **19.** Roth's theorem and limits to approximation. **20–22.** Related Diophantine equations, results, problems. 100

Chapter 4. Geometric Methods in Number Theory 109

1. A geometrical–combinatorial proof of Wilson's theorem. **2.** Related problems. (Exercises **1–4.**) **3.** Parallelogram lattices, lattice points. **4.** Lattice coordinates. Two fundamental properties **5.** Further lattice properties. **6.** Regular lattice polygons. **7.** Simultaneous regular lattice polygons. 109

8. Lattices arising from parallelograms. Parallelogram lattices that give rise to a given point lattice. 119

9. Determining the area of lattice polygons by the number of lattice points. Subpolygons of lattice polygons. **10.** Proving the theorem for lattice triangles. **11.** The extension to arbitrary lattice polygons. **12.** The existence of simple, interior diagonals in lattice polygons. (Exercises **5–19.**) 120

13. Lattice points close to lines. **14.** Sharpening of the result for lattice rays. **15.** An application. (Exercises **20–21.**) 127

16. Minkowski's theorem about convex regions. **17.** The proof of the theorem for regions of area greater than $4d$. **18.** The case of equality. **19.** The necessity of the hypotheses. **20.** A related problem. **21.** Three applications. **22–23.** The sharpness of the theorem; the existence of infinitely many lattice points satisfying the hypotheses. **24.** An application to the decomposition of a prime number as the sum of two squares. (Exercises **22–27.**) 130

25. The sharpness of the hypotheses of the theorem. **26–27.** The sharpness of the theorem relating to disks. **28.** Admissible lattices between the pair of hyperbolas. **29.** Proof of the theorem. **30.** The bound cannot be improved. **31.** An application to Diophantine approximation. **32.** A possible improvement of the theorem by decreasing the lattice circle. 139

33. Homogeneous and inhomogeneous lattices. The existence of divided cells. **34.** The theorem rediscovered; the 3-dimensional case. **35.** Obtaining all divided cells. **36.** An application of the theorem. **37.** An arithmetic conclusion to the proof. (Exercises **28–31.**) 150

Chapter 5. Properties of Prime Numbers 157

1. The role of prime numbers, their distribution. **2.** The differences among primes: results, problems. (Exercises **1–2.**) **3.** Sequences of pairwise relatively prime elements. **4.** An observation about primes not greater than x. (Exercises **3–4.**) **5.** A lower bound for $\pi(x)$. **6.** The sum of the reciprocals of the elements of a sequence. **7.** An indirect proof that the series of reciprocals of primes diverges. (Exercises **5–7.**) **8–9*.** A lower bound for the sum of the sequence of reciprocals of primes. 157

10. The order of magnitude of $\pi(x)$, a lower bound. **11.** An upper bound on the product of the primes less than x. **12.** Using the result to bound $\pi(x)$ from below. Sequences of density 0. **13.** The order of magnitude of the number of prime powers not greater than x. (Exercises **8–12.**) **14.** Primes between n and $2n$. **15.** A sharpening, the Sylvester–Schur theorem. (Exercises **13–16.**) **16.** A common thread to the proofs. The asymptotic value of $\pi(x)$. The Riemann zeta function. 166

17–18. Some primes in arithmetic progressions. **19.** Reduction to the proof of the existence of a prime. **20.** The special case of a satisfying infinite arithmetic sequence. **21.** The relation with primitive roots. **22.** The generalized scope of validity of the method. 177

Chapter 6. Sequences of Integers 181

1. Some examples from the preceding chapters. **2.** Pairs of numbers having a short Euclidean algorithm, Fibonacci and Fibonacci-type numbers. **3.** Divisors of Fibonacci numbers. **4.** Observations. (Exercises **1–8.**) **5.** Lower, upper, and asymptotic density of the sequence. (Exercises **9–10.**) 181

6. Sequences not containing the difference of two elements. **7.** The partition of all integers up to a given bound into such sequences. **8.** Fermat's last theorem in the congruence case. **9.** Fermat's last theorem. **10.** Remarks regarding the tests in Section 7. 186

11. The number of prime divisors of the sum of a given set of numbers. A lemma. **12.** The proof of the theorem. Results relating to the sum of elements from two sequences. **13.** The number of elements in a sequence not containing multiples of its elements. **14.** Proof by induction. **15.** Proof by examining parity. **16–17.** Results for infinite sequences. (Exercise **11.**) 190

18. The number of elements in sequences not containing arithmetic progressions of length k ($r_k(n)$), some results about $r_3(n)$. **19.** Some small values calculated. (Exercise **12.**) **20.** Some related results for arithmetic progressions. 196

21. Sequences with all pairwise two-element sums distinct (Sidon sequences). Upper bound on the number of elements. **22–23.** Further improvement of the bound. **24–25.** Sharpness of the bound. (Exercises **13–23.**) 199

Chapter 7. Diophantine Problems 205

1. Parametric representation of "Pythagorean n-tuples." **2.** The representation is essentially unique. (Exercises **1–3.**) **3.** Problems regarding the representation of integers as sums of squares. 205

4. Numbers which are the sum of squares of two integers. **5.** The sufficiency of the hypothesis. **6.** Numbers that cannot be written as the sum of three integers. **7.** Representation as the sum of four squares. Reduction to the case of primes. **8–9.** Proof of the special case. **10–11.** Proof of the lemmas. (Exercises **4–6.**) **12.** Further results and exercises. 208

13. Representation as the sum of fourth powers. **14.** Infinitely many numbers that are not the sum of 15 fourth powers. **15.** The functions $g(k)$ and $G(k)$ relating to the number of terms in a kth-power representation, known results, problems. (Exercises **7–9.**) 215

16. Representations as sums of kth powers with mixed signs, squares. **17.** Cubics. **18.** The number of terms is bounded in the case of arbitrary powers. (Exercises **10–11.**) 218

19. When can $(p-1)!+1$ be a power of p? **20.** Related results, problems. **21*–22*.** Binomial coefficients as perfect powers, a lower bound. **23*–24*.** Upper bound, completion of the proof. **25.** Further results, problems. (Exercises **12–26.**) 221

Chapter 8. Arithmetic Functions 231

1–2. Arithmetic functions, a new method of calculating the value of φ. **3.** Probabilistic background for the proof. (Exercises **1–5.**) **4.** The sum of the divisors ($\sigma(n)$). **5.** Representation of even perfect numbers. **6.** Mersenne primes; a criterion for their primality. **7.** The function σ is multiplicative. **8.** A formula for σ. (Exercises **6–13.**) **9.** Further examples of arithmetic functions, the determination of additive and multiplicative functions. (Exercises **14–17.**) **10.** Deficient and abundant numbers. **11*.** A theorem about odd perfect numbers, a grouping of the prime divisors. **12*.** A result arising from limits leads to a contradiction. **13*.** Extension of the theorem to primitive abundant numbers. **14.** Further results and problems. (Exercises **18–29.**) 231

15. Examples of the behavior of inequalities for number-theoretic functions. (Exercise **30.**) **16*.** The rhapsodic behavior of the number of divisors. **17*–18*.** Sequences of k consecutive integers with a small number of average divisors. **19.** Possible fine tuning of the proof. **20.** Further results, problems. **21*–22*.** The range of the Euler function is bounded above. **23.** Related results, problems. **24.** A sequence arising from the iteration of φ. **25.** Further results, problems. **26.** "Narrow valleys" in the graph of τ. **27.** A lower bound for $\tau(n)$. **28.** An upper bound for $\tau(n)$. 245

29. The average value of $\tau(n)$. **30.** Earlier results, the current situation. **31.** The average value of ω and Ω. **32.** Average values of additional functions; $\tau(n)$'s most frequent values and determination of its average values. 262

33. Only the logarithmic function is additive and monotone. **34.** Improvements, extending the tests. (Exercises **31–32.**) 265

Hints to the More Difficult Exercises 269

Bibliography 275

Index 283