Introduction

The book is intended to serve several purposes; being a

(A) Theoretical textbook for teaching number theory at universities and colleges, mostly for majors in mathematics, applied mathematics, mathematics education, and computer science.

(B) Collection of exercises and problems for the above audience.

(C) Handbook for those interested in more detail in some chapters of number theory beyond the compulsory and elective courses and/or writing a thesis in this subject.

(D) Manual summarizing the most important chapters of (elementary) number theory for mathematicians and mathematics teachers.

Structure of the book

To achieve the above goals, the discussion starts at an absolutely basic level and the first two chapters are based solely on high school mathematics. This part uses elementary and non-abstract tools, and instead of overly compact reasoning, detailed explanations facilitate better understanding for beginners. On the other hand, we lay stress on presenting theorems illustrating the deeper coherence of the material and on proofs containing nice and difficult ideas.

The subsequent chapters enter more and more deeply into the discussion of various topics in number theory. We strive to present a wide panorama of this extremely multi-colored world (including many old but still unsolved problems) and to discuss many methods elaborated through many centuries to treat these questions. Where possible, the newest results of number theory are inserted. Several parts apply some results and methods from other fields of mathematics too, mostly from (classical, linear, and abstract) algebra, analysis, and combinatorics.

The book is structured to systemize the material and to provide a close relation between the individual chapters as much as possible.

As a general guideline, the notions and statements are thoroughly illuminated from various aspects beyond the formal phrasing, they are illustrated by examples and connections to the previous material. Their essential features are strongly emphasized pointing out the complications and analyzing the motives for introducing a given notion. Careful attention is paid to start from the concrete where possible and to proceed towards the general only afterwards. We try to give a broad perspective about the strong and colorful relations of number theory to other branches of mathematics.

Exercises

Each section in every chapter is followed by exercises. They serve several purposes: some of them check the comprehension of the notions, theorems, and methods, and give a deeper understanding; others present new examples, relations, and applications; again others study further problems related to the topic. They often include also theorems disguised as exercises revealing some interesting aspects or more remote connections not treated in the text in detail.

Exercises vary in quantity and in difficulty within fairly large limits depending on the topic, size, and depth of the material. The hard and extra-hard exercises (in our judgement) are marked with one and two asterisks, resp. (The difficulty of an exercise is always relative, of course: besides the abilities, interests, and preliminary general knowledge of the solver, it depends strongly also on the exercises already solved.)

Answers and/or some hints to nearly all exercises can be found in the chapter Answers and Hints. To some (mostly harder) problems detailed solutions are presented in an online chapter available at `www.ams.org/bookpages/amstext-48`. These exercises are marked with a letter **S** in the text.

The reader is advised to consult a hint or solution only if an exercise turns out to be absolutely unmanageable, or to return to the same problem later, or to solve first some special case of it.

It is important to unravel the message and background of an exercise, its position and role in the mathematical environment. Also a generalization or raising new problems are very useful (even if it is not clear how to solve them).

Short overview of the individual chapters

The first two chapters are introductory, discussing the divisibility of integers, the greatest common divisor, unique prime factorization, and elementary facts about congruences. A firm mastery of this material is indispensable for understanding the later chapters.

In Chapters 3 and 4 we continue to develop the theory of congruences.

Chapter 5 deals with prime numbers. This simply defined set is one of the most mysterious objects in mathematics. We discuss Euclid's theorems (more than two thousand years old) and the sensational discovery of the last decades, the public key cryptosystems based on the contrast of quick primality testing and awfully slow prime factorization. In this chapter we rely both on previously acquired knowledge in number theory and the results and methods of elementary analysis.

In Chapter 6 we study arithmetic functions. Besides investigating some concrete important functions, we present several general constructions and applications.

Chapter 7 is about Diophantine equations. After discussing the simplest types (linear equations, Pythagorean triples), we look at Waring's problem and prove the special cases of Fermat's Last Theorem for exponents three and four. The methods require the theory of Gaussian and Eulerian integers that will be generalized in Chapters 10 and 11.

The topic of Chapter 8 is Diophantine approximation that is important for certain applications. We briefly consider also the connection with the geometry of numbers and continued fractions.

Chapters 9–11 are closely related to each other. The basic properties of algebraic numbers and algebraic integers from Chapter 9 are essential for understanding the next two chapters. Chapter 10 studies field extensions, focusing on the arithmetic properties of algebraic integers in a simple extension of the rational field by an algebraic number. Here, an intensive use is made of the notions and theorems of elementary linear algebra. Finally, in Chapter 11 the arithmetic aspects of ideals are investigated. On the one hand, ideals constitute a fine tool for exhibiting some necessary and sufficient, or useful sufficient, conditions for the validity of unique prime factorization in general rings, and on the other hand, the validity of unique prime factorization for ideals of algebraic integers (though in general not for the algebraic integers themselves) plays an important role in studying algebraic number fields.

In Chapter 12 several interesting problems from combinatorial number theory are presented. Some of these can be discussed even at a high school study circle, whereas others require deeper methods from various branches of mathematics. We hope that the selection gives an idea also about the fundamental role of Paul Erdős in the progress of this field with thrilling questions and ingenious proofs.

Throughout the text, we often refer to interesting aspects of the history of number theory and this purpose is served also by the short Historical Notes at the end of the book.

As is clear also from the above description, the different subfields of number theory are closely interrelated to each other and to other branches of mathematics. This causes a serious difficulty since, on the one hand, it is important to emphasize this tight connection during the discussion of the individual topics, but, on the other hand, it is desirable that every chapter be self-contained and complete. We tried to achieve a balance that makes it possible to get a gradually growing full picture of a mathematical field rich in problems and ideas for continuous readers, but allows those who just pick a few chapters to acquire interesting, substantial, and useful knowledge.

Technical details

The chapters are divided into sections. Definitions, theorems, and formulas are numbered as $k.m.n$ where k refers to the chapter, m to the section, and n is the serial number within the given section. Definitions and theorems have a common list, thus, for example, Definition 6.2.1 is followed by Theorem 6.2.2. Examples, exercises, etc. are numbered with a single number restarting in each section. The statement of a definition or theorem is closed by a ♣ sign and the end of a proof is denoted by □.

The search for notations, notions, and theorems can be facilitated by the very detailed Index at the end of the book.

We distinguish the floor and ceiling of (real) numbers, denoted by $\lfloor\ \rfloor$ and $\lceil\ \rceil$, resp., thus e.g. $\lfloor\pi\rfloor = 3$, $\lceil\pi\rceil = 4$ (we do not use the notation $[\pi]$). The fractional part is denoted by $\{\ \}$, i.e. $\{c\} = c - \lfloor c\rfloor$. Divisibility, greatest common divisor, and least common multiple are denoted as usual, so e.g. $7 \mid 42$, $(9, 15) = 3$, and $[9, 15] = 45$. Square brackets $[\ ]$ can mean a least common multiple, a closed interval, or just a replacement for (round) parentheses (this latter function occurs frequently in Chapter 11 where round parentheses $(\ )$ stand for an ideal; to avoid confusion, the greatest common divisor is denoted here by $\gcd\{a, b\}$).

Polynomials and functions are denoted generally without indicating the argument: f, g, etc. but sometimes also $f(x)$, $g(x)$, etc. can occur. The degree of a polynomial is denoted by "deg," so e.g., $\deg(x^3 + x) = 3$. As usual, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ stand for the rational, real, and complex numbers. $\mathbf{Z}$, $\mathbf{Z}_m$, and $F[x]$ mean the integers, the modulo m residue classes, and the polynomials over F. At field extensions, $\mathbf{Q}(\vartheta)$ and $I(\vartheta)$ denote the simple extension of the rationals by ϑ and (in case ϑ is algebraic) the ring of algebraic integers in this extension. The letter p denotes nearly exclusively a (positive) prime and the log (without a lower index) stands for natural logarithm (of base e). For (finite and infinite) products and sums we often use the signs $\prod$ and $\sum$, e.g.

$$\prod_{i=1}^{r} p_i^{\alpha_i}, \qquad \prod_{p\le n} p, \qquad \sum_{p} \frac{1}{p^2}$$

mean the product $p_1^{\alpha_1} \dots p_r^{\alpha_r}$, the product of primes not greater than n, and the sum of reciprocals of squares of primes.

Commemoration

The book is dedicated to the memory of Paul Turán, Paul Erdős, and Tibor Gallai (who were close friends and collaborators).

Both authors enjoyed the privilege to be in touch with two giants of 20th century number theory, Paul Turán and Paul Erdős.

We were educated in Paul Turán's legendary seminars where we learned how to explore, elaborate, and explain to others the essential components of a mathematical problem. Turán taught us that connecting seemingly remote areas can often result in new, efficient methods.

Edit Gyarmati wrote a number theory textbook (in Hungarian) some fifty years ago using Turán's lectures among several other sources that can be considered as a predecessor of this book in a certain sense. The experiences of our lectures, the students' broadening preliminary knowledge (e.g. in linear algebra), and the new scientific achievements in this field during the past decades necessitated the creation of a new book instead of a long-due revision. The spirit and structure of the two books show several similar features, of course.

Both of us were largely influenced by the mathematical and human greatness of Paul Erdős sharing his enthusiastic devotion towards "nice" mathematical problems and proofs, talking about these (and many more things) equally naturally and openly with great scientists or just interested beginners. Róbert Freud owes many adventures in doing joint mathematics and a great deal of his professional progress to Erdős.

Edit Gyarmati's choosing mathematics as a profession is mostly due to her unforgettable high school teacher, Tibor Gallai, who was a world-famous expert in graph theory. Gallai was a brilliant personality whose wonderful classes both in high school and at universities helped to start mathematical research for the best students, and offered the joy of understanding and creation for all pupils.

Acknowledgements

We are very thankful for the great job the reviewers Imre Ruzsa (Chapter 12), András Sárközy (Chapters 1–12), and Mihály Szalay (Chapters 1–11) did. All three of them checked the manuscript with extreme thoroughness and suggested many general, concrete, and stylistic improvements nearly all of which were accepted by us. The conceptual remarks of András Sárközy helped us in unifying some notions, homogenizing the structure, and mentioning several further results. Mihály Szalay checked every tiny detail carefully, solved all the exercises without a solution given in the book, noted even the smallest inaccuracies, and his concretely worded suggestions made it possible to correct many lesser or greater errors and discrepancies. Imre Ruzsa added many valuable observations on Chapter 12.

In spite of all the efforts of the authors (and reviewers) there probably remain errors and imperfections in the book. Any comments or suggestions are gratefully accepted.

The book in its present form is an English translation and an improved and corrected version of the two Hungarian editions used by all universities of science in Hungary. Edit Gyarmati, who was not only my coauthor but also my wonderful wife for many decades, passed away in 2014, and could not participate in preparing this manuscript. I devote this work to her memory.

Budapest, February 2019

Róbert Freud
Institute of Mathematics, University Eötvös Loránd
1117 Budapest, Pázmány Péter sétány 1c, Hungary
freud@caesar.elte.hu