Number Theory

Andrej Dujella

TEXTBOOKS OF THE UNIVERSITY OF ZAGREB

MANUALIA UNIVERSITATIS STUDIORUM ZAGRABIENSIS

ANDREJ DUJELLA: NUMBER THEORY

Publisher
Školska knjiga, d. d.
Zagreb, Masarykova 28

For the publisher
Ante Žužul

Director of school program
Matilda Bulić

Editor-in-Chief
Jelena Lončarić

Editor
Tanja Djaković

Creative director
Ana Marija Žužul

Art director
Tea Pavić

Reviewers
Ivica Gusić
Matija Kazalicki
Filip Najman

The use of this university textbook has been approved by the Senate of the University of Zagreb.
(class no. 032-01/19-01/11, reg. no. 390-061/117-19-5 of April 2, 2019)

The publication of this book was supported by the Ministry of Science and Education of the Republic of Croatia.

Preface to the Croatian edition

Number theory is a branch of mathematics that is primarily focused on the study of positive integers, or natural numbers, and their properties such as divisibility, prime factorization, or solvability of equations in integers. Number theory has a very long and diverse history, and some of the greatest mathematicians of all time, such as Euclid, Euler and Gauss, have made significant contributions to it. Throughout its long history, number theory has often been considered as the "purest" branch of mathematics in the sense that it was the furthest from any concrete application. However, a significant change took place in the mid-1970s, and nowadays, number theory is one of the most important branches of mathematics for applications in cryptography and secure information exchange.

This book is based on teaching materials (available on the author's website) from the courses *Number Theory* and *Elementary Number Theory*, which are taught at the undergraduate level studies at the Department of Mathematics, Faculty of Science, University of Zagreb, and the courses *Diophantine Equations* and *Diophantine Approximations and Applications*, which were taught at the doctoral program of mathematics at that faculty. The book thoroughly covers the content of these courses, but it also contains other related topics such as elliptic curves, which are the subject of the last two chapters in the book. The book also provides an insight into subjects that were and are at the centre of research interest of the author of the book and other members of the Croatian research group in number theory, gathered around the *Seminar on Number Theory and Algebra*.

This book is primarily intended for students of mathematics and related faculties at Croatian universities who attend courses in number theory and its applications. However, it can also be useful to advanced high school students who are preparing for mathematics competitions in which at all levels, from the school level to international competitions, number theory has a significant role, and for doctoral students and scientists in the fields of number theory, algebra and cryptography.

Numerous sources have been used while writing this book. The primary literature for each chapter is listed in the appropriate places in the book. It should also be emphasized here that when writing the first version of the lecture notes [111], the primary literature were the books A. Baker: *A Concise Introduction to the Theory of Numbers* [23] and I. Niven, H. S. Zuckerman, H. L. Montgomery: *An Introduction to the Theory of Numbers* [328]. Much of the literature is available in the Central Mathematical Library at

the Department of Mathematics of the Faculty of Science, and is in large part obtained from scientific projects of which I was a leader or member (projects of the Ministry of Science and Education, supports of the University of Zagreb, projects of the Croatian Foundation for Science, QuantiXLie Science Center of Excellence).

As already mentioned, this book covers in full, the content of the courses *Number Theory* (Chapters 2, 3.1–3.7, 4, 5.2, 5.3, 6.2, 6.3, 7.2, 8.1, 8.3, 8.4, 8.6, 10.1–10.4, 12.1), *Elementary Number Theory* (Chapters 2, 3.1–3.7, 4, 5.1, 5.3, 6.1, 6.2, 7.1, 10.1–10.4, 9.1, 9.2), *Diophantine Equations* (Chapters 10.3–10.8, 13.1–13.3, 8.8, 8.9, 14, 16.2–16.5, 15.1, 15.5) and *Diophantine Approximations and Applications* (Chapters 8.1–8.6, 10.4, 10.5, 8.8, 8.9, 9, 13.1, 13.2, 14.1, 14.2, 13.4, 13.5).

The above chapters from the courses *Number Theory* and *Elementary Number Theory* are also chapters (with the addition of the introductory Chapter 1) that are recommended to the reader interested in the subject that is usually referred to as elementary number theory. Chapter 12 can be understood as a brief introduction to algebraic number theory, and Chapter 7 as a brief introduction to analytic number theory. It should be emphasized that the scope of the book (and the knowledge of the author) does not allow the book to include everything that a systematic approach to the topics from algebraic and analytic number theory would cover. Chapter 11, which deals with the topic of polynomials, can also be understood as a preparation for Chapter 12. The last two chapters are devoted to elliptic curves; although this, of course, does not cover everything that could be said about that topic (as written in the introduction to the book [266], "it is possible to write endlessly on elliptic curves"); this especially concerns the connection of elliptic curves with modular forms and algebraic geometry, so readers who want additional information on this topic are referred to notes in the Croatian language [122, 203, 241, 313, 319]. Other existing literature in the Croatian language refers primarily to some parts of elementary number theory [169, 292, 335, 337]. We should also mention the booklet *Brojevi (Numbers)*, which contains an interesting overview of number theory [405]. Topics from elementary number theory are well represented in papers in Croatian professional-methodological and scientific popularization journals: *Matematika*, *Matematičko-fizički list*, *Matka*, *Poučak*, *math.e*, *Matematika i škola*, *Osječki matematički list*, *Acta mathematica Spalatensia Series didactica*. This book also touches upon the application of number theory in cryptography (Chapters 9 and 15.8), on which the interested reader can find additional information in the book [147]. Let us also mention that

Fibonacci numbers are discussed through several chapters (especially Chapters 1.3, 4.5 and 10.6) as an interesting mathematical object used to illustrate the topics dealt with in the book. The material from the booklet [113] was used there.

Some specific topics included in the book due to the author's affinities, as those would otherwise not be commonly found in number theory textbooks, are given in Chapters 8.7, 9.3, 11.4, 13.5, 14.2, 14.6 and 16.7. On the one hand, this means that the reader can skip them in the first reading, and on the other hand, I hope that there will still be readers who will find it interesting to read briefly what the author and his collaborators have done scientifically in the last 25 years.

At the end of each chapter, there are (unsolved) exercises that can be used in one part by students and competitors for practice and preparations, and sometimes they are a supplement to the basic text. The sources of the exercises are different. Some of these are taken from written exams and assignments in undergraduate and doctoral studies, as well as assignments from the preparation of competitors, while others are exercises taken from literature, for example from [1, 11, 12, 32, 51, 101, 147, 197, 226, 227, 228, 346, 347, 352, 354, 355, 368, 369, 392, 409], in which the interested reader can find many additional exercises.

I wish to thank everyone who has read the different versions of the manuscript of this book and warned me of mistakes and suggested improvements to the text. I would like to emphasize my thanks to Ivica Gusić, who helped me with countless advice on various dilemmas I had while writing the book, and to Tomislav Pejković, who carefully read the entire manuscript of the book and warned me of many minor or major errors and inaccuracies, as well as to Nikola Adžaga, Marija Bliznac Trebješanin, Bernadin Ibrahimpašić, Borka Jadrijević, Ana Jurasić, Matija Kazalicki, Dijana Kreso, Marcel Maretić, Miljen Mikić, Goran Muić, Filip Najman, Vinko Petričević, Valentina Pribanić, Ivan Soldo, Boris Širola and Mladen Vuković, who sent me their comments and suggestions on individual chapters or the entire manuscript of the previous version of the book.

I would also like to thank the generations of students in the Department of Mathematics who, with their interest in the course *Introduction to Number Theory*, which was first introduced as an elective course, enabled it to become later a part of the study program as a compulsory course *Number Theory* for the so-called engineering specialization and *Elementary Number Theory* for the teaching specialization of the undergraduate study of mathematics. I especially thank the students to whom I was the supervisor for

their graduation theses (there have been 189 so far, and a considerable share of the topics of these theses relates to the number theory and its application in cryptography). I was lucky that my lectures in doctoral program in mathematics were well attended, so I also thank the PhD students and other members of the Seminar on Number Theory and Algebra who often gave useful comments on the preliminary lecture notes for these courses. For fifteen years, I was a member of the State Commission for Mathematical Competitions, and after that, I occasionally participated in the preparation of gifted students for international mathematical competitions. Some materials and assignments I prepared for this purpose are also included in the book. The first serious encounter between the author of this book and number theory came through mathematical competitions, and I would like to take this opportunity to thank my high school professor Petar Vranjković, with whose help I prepared for these competitions, including the 1984 International Mathematical Olympiad in Prague. I would also like to thank the supervisor of my diploma and master's thesis, Zvonko Čerin, and the supervisors of my doctoral dissertation, Dragutin Svrtan and Dimitrije Ugrin-Šparac, for introducing me to scientific work. Special thanks go to Attila Pethő, a professor at the University of Debrecen and a member of the Hungarian Academy of Sciences, who, from our first meeting in 1996 until today, has guided my scientific and teaching career with his numerous and very useful advice. As already pointed out, some of the chapters in the book talk about the personal scientific interests of the author, so I thank all my coauthors of scientific papers for inspiring scientific collaboration. I also thank my family for their patience, support and understanding during the writing of this book.

Novigrad and Zagreb, 2018 – 2019 Andrej Dujella

Preface to the English edition

After the publication of the Croatian edition of this book in October 2019, several colleagues encouraged me to think about an English edition. Especially encouraging were the nice talks of the speakers at the presentations of the book in Zagreb and Zadar, in particular, those of Ivica Gusić and Filip Najman. As was the case many times before in my scientific career, the greatest support and encouragement came from Attila Pethő, whose very kind comments on the Croatian edition of the book were crucial in my decision to try to arrange an English translation of the book.

I am grateful to the publisher Školska knjiga Zagreb and their mathematical editor Tanja Djaković for organizing all the details concerning the translation and also to the translator Petra Švob for a good job on the translation.

In the English edition, there are only minor changes compared with the Croatian version. Several misprints noticed by the author and the readers were corrected. Some information and references were updated, in particular, those related to elliptic curves rank records and new constructions of families of rational Diophantine sextuples from joint works with Matija Kazalicki and Vinko Petričević. At just a few places in the Croatian version of the book only the references to literature in Croatian were given; these references were expanded in the English edition with the appropriate recommendations of literature in English. The list of references has been expanded to include some recent books and papers, as well as some references which were mentioned in the text of the Croatian edition but were not included in the list of references. Apart from the undergraduate and graduate courses mentioned in the preface to the Croatian edition, in the intervening time, this book was used as a textbook also for the graduate course *Diophantine Sets* [182] given by Alan Filipin and Zrinka Franušić.

I would like to thank all the colleagues who read some versions of this book and provided useful comments and corrections, in particular, Bill Allombert, Marija Bliznac Trebješanin, Yann Bugeaud, Sanda Bujačić Babić, Mihai Cipu, Jelena Dujella, Zrinka Franušić, Ivica Gusić, Kalman Győry, Lajos Hajdu, Matija Kazalicki, Dijana Kreso, Ivan Krijan, Miljen Mikić, Filip Najman, Tomislav Pejković, Vinko Petričević, Ivan Soldo, Gökhan Soydan, Szabolcs Tengely, Antonela Trbović, Paul Voutier, Mladen Vuković and Gary Walsh, and all my coauthors and collaborators as well as, of course, my family.

Novigrad and Zagreb, 2020 Andrej Dujella

Contents