Andrej Dujella

Diophantine m-tuples and Elliptic Curves

Springer Nature

Preface

This book provides an overview of the main historical and recent results and problems concerning Diophantine m-tuples and their various generalizations, with special emphasis on their connections with elliptic curves. A Diophantine m-tuple is a set of m positive integers with the property that the product of any two of its distinct elements plus 1 is a square. Fermat found the first Diophantine quadruple in integers $\{1, 3, 8, 120\}$. If a set of non-zero rationals has the same property, it is called a rational Diophantine m-tuple. The ancient Greek mathematician Diophantus found the first example of a rational Diophantine quadruple.

If we want to extend a Diophantine triple $\{a, b, c\}$ to a quadruple, we have to find an integer or rational x such that $ax+1$, $bx+1$ and $cx+1$ are all squares. By multiplying these three conditions, we obtain a single condition $y^2 = (ax + 1)(bx + 1)(cx + 1)$, which is, in fact, the equation of an elliptic curve (non-singular cubic curve with a rational point).

Diophantine m-tuples have a very long and exciting history, but it is also a very active research topic today. Some of the famous mathematicians of the past, like Diophantus, Fermat and Euler, as well as some modern ones like Fields Medalist Alan Baker, made important contributions to problems related to Diophantine m-tuples, but many problems remain open. The author's web page contains the full list of references related to Diophantine m-tuples. At the moment, it contains 518 references (38 references before 1990, 95 references before 2000, 245 references before 2010) of authors from all continents. The recent booklet *Wonderland of Families of Diophantine triples* by Deshpande covers a particular subtopic of regular Diophantine triples, and there are some books that treat some aspects of Diophantine m-tuples (e.g. Sections 14.6, 16.7 of *Number Theory* by Dujella, Chapter 6 of *Liczby Kwadratowe* by Nowicki). However, until now, no book systematically covered this topic.

Let us mention that the third edition of the well-known book *Unsolved Problems in Number Theory* by Richard Guy contains a new section (Section D29) devoted to Diophantine m-tuples. The problem of the existence of Diophantine quintuples was mentioned in 2001 by Michel Waldschmidt as one of the important problems at the end of the second millennium. A brief survey on Diophantine m-tuples and

their generalizations appeared in "What is . . . " column in the August 2016 issue of Notices of AMS.

The systematic study of connections between Diophantine m-tuples and elliptic curves started around the year 2000. It proved to be very fruitful in both directions: elliptic curves are used in solving some long-standing problems on Diophantine m-tuples, like the existence of infinite families of rational Diophantine sextuples, but also rational Diophantine m-tuples are used in the construction of elliptic curves with interesting Mordell-Weil groups, including some curves with the record (highest known) rank a for given torsion group.

Since it is impossible to cover all aspects appearing in more than 500 publications in one book, we think that focusing on aspects related to connections with elliptic curves is a good and attractive choice. Of course, this book contains fragments of the exciting history of Diophantine m-tuples, which might often have modern interpretations in terms of elliptic curves but which did not originally use this language, as it was unavailable at the time.

In Chapter 1, we present the contributions of Diophantus, Fermat and Euler on this topic, which served as motivation for further investigations. We state the main definitions, results and open problems which will be discussed in the book. We also mention here various generalizations of the notion of Diophantine m-tuples. Later in the book, we will concentrate on "ordinary" (integer or rational) Diophantine m-tuples and discuss only generalizations connected with elliptic curves.

Chapter 2 covers prerequisites on elliptic curves over $\mathbb{Q}$ needed later in the book. We discuss possible torsion groups of elliptic curves over $\mathbb{Q}$, with particular attention to those groups that can appear for curves induced by Diophantine triples. We present methods for computing the rank and constructing elliptic curves with high rank. General methods are illustrated on examples coming from Diophantine tuples. We also explain the functions related to elliptic curves, which are available in the software package PARI/GP.

Chapter 3 is the central part of the book. Here, we introduce elliptic curves induced by Diophantine triples and discuss their properties and applications. One of the main applications is the construction of infinite families of rational Diophantine sextuples (an open problem from the time when Euler found families of such quintuples). There are four known different constructions of such families, which all use elliptic curves in some form, and will be presented in this chapter. Another important application of elliptic curves induced by Diophantine triples comes in constructing high-rank elliptic curves with certain torsion groups. We present details on the construction of some record curves over $\mathbb{Q}(t)$ and $\mathbb{Q}$. We also discuss some other connections between Diophantine m-tuples and elliptic curves.

In Chapter 4, we explain general methods for finding integer points on elliptic curves (transformation to Thue equations, application of elliptic logarithms, solving systems of Pellian equations via linear forms in logarithms and the Baker-Davenport reduction). These methods are then applied to the problem of finding all integer points on elliptic curves induced by (integer) Diophantine triples. We present the proof of an absolute upper bound for the size of Diophantine tuples and sketch the

main steps in the results that lead to the proof of the non-existence of Diophantine quintuples.

In Chapter 5, we provide more details on one of the generalizations of the notion of Diophantine m-tuples, namely, that in which the condition that $ab+1$ is a square is replaced by $ab+n$ is a square for a fixed integer or rational number n. We discuss the problem of the existence of integer $D(n)$-quadruples and rational $D(n)$-quintuples. We will see that the last problem is related to the distribution of ranks in families of twists of certain elliptic curves. Finally, we consider sets which are $D(n)$-triples, quadruples and quintuples for several distinct values of n. Elliptic curves will also play an important role here, but their appearance will differ in those three problems.

The book's primary audience is expected to be researchers and graduate students working in Diophantine equations and elliptic curves. However, this book might be of interest to many other mathematicians interested in number theory and arithmetic geometry. If used as a textbook for a graduate course, the prerequisites would be on the level of a standard first course in elementary number theory (e.g. the Niven-Zuckerman-Montgomery textbook *An Introduction to the Theory of Numbers*, or other textbooks that cover the notions of divisibility, congruences and quadratic residues, like *A Concise Introduction to the Theory of Numbers* by Baker). All prerequisites on elliptic curves are provided here (mainly in Chapter 2). For a more systematic introduction to elliptic curves, we can recommend the textbook by Silverman and Tate *Rational Points on Elliptic Curves* (additional recommended books on elliptic curves are given at the beginning of Chapter 2). Most prerequisites related to Diophantine equations and Diophantine approximations are included in the introductory sections of Chapter 4, particularly in Section 4.1. Some books that systematically treat aspects of Diophantine equations relevant to this book are *Linear Forms in Logarithms and Applications* by Bugeuad, *Number Theory. Volume I: Tools and Diophantine Equations* by Cohen, *Diophantine Equations* by Mordell, and *The Algorithmic Resolution of Diophantine Equations* by Smart.

The author gave a course based on the preliminary version of this book in the academic year 2021/2022 for PhD students at the University of Zagreb. On the course web page, additional materials, like homework exercises (mostly included in the book in the exercise sections at the end of each chapter), seminar topics and links to relevant software, can be found. The book could be used as a textbook for a specialized graduate course, and it may also be suitable for a second reading supplement reference in any course on Diophantine equations and/or elliptic curves at the graduate or undergraduate level.

Let me give here some personal comments on how I got involved in Diophantine m-tuples and how they became my main research topic. Since high school mathematics competitions, I have been occupied and inspired by number theory. During my mathematics undergraduate studies, I did not have the opportunity to take courses in number theory. However, I acquired solid knowledge in various areas of mathematics and had the opportunity to listen to the lectures of prominent Croatian mathematicians. I deepened my interest in number theory through the literature I bought in a foreign literature bookstore in Zagreb (mainly Russian editions, accessible to the student pocket). In the last year of my undergraduate studies, I received a finan-

cially generous scholarship from the University of Zagreb. That was a very happy circumstance because, among other things, it made it possible for me to buy the proceedings from the 2nd Conference on Fibonacci numbers held in Greece, where in the two papers *On a problem of Diophantus* by Long and Bergum and *More on the problem of Diophantus* by Arkin and Bergum, I met for the first time a problem of Diophantus, which I later dealt with for the most part of my scientific career. As I mentioned, my interest in number theory started in high school and is closely related to my participation in math competitions. My PhD dissertation was from that area and contained published results in international journals. Nevertheless, I would say that my work in number theory was on a somewhat amateurish basis until, in July 1996, I participated at the 7th Conference on Fibonacci numbers, which was held in Graz, where I met Professor Attila Pethő. We immediately understood that we had a lot of common mathematical interests. He guided me from that moment with his advice on my scientific career. The results from two of our joint papers are described in Section 4.8. He is also "responsible" for suggesting that I study connections between Diophantine m-tuples and elliptic curves. This became a very fruitful research topic, as I hope this book shows.

I would like to thank all my coauthors, collaborators and PhD students. Most of my 13 PhD students had theses related to Diophantine m-tuples (and several of their PhD students, too). Their enthusiasm gave me a lot of inspiration during my research. Many joint results are included in some form in this book. I thank all colleagues who have read some versions of the manuscript of this book and suggested improvements to the text, in particular, Bill Allombert, Nicolae Bonciocat, Yann Bugeaud, Mihai Cipu, Jelena Dujella, Yasutsugu Fujita, Shubham Gupta, Seoyoung Kim, Matija Kazalicki, Franz Lemmermeyer, Takafumi Miyazaki, Filip Najman, Bartosz Naskrecki, Tomislav Pejković, Vinko Petričević, Ákos Pintér, Ivan Soldo, Gökhan Soydan, Maksym Voznyy, and Gary Walsh. Nicolae Bonciocat, Mihai Cipu and Tomislav Pejković read all the chapters carefully and provided many very helpful comments and corrections. I would like to thank the referees of this book for their very useful comments, remarks and suggestions. I am grateful to Remi Lodh, Senior Editor for Mathematics Books at Springer Nature, for his constant support and encouragement during the writing process.

I would also like to thank the PhD students at the Croatian Doctoral Program in Mathematics who attended my lectures on the course *Diophantine m-tuples and elliptic curves* in 2021/2022. Because of the situation in that period, most of the activities on the course appeared online, but they regularly attended my online lectures (they are available (in Croatian) on my YouTube channel), solved exercises and gave interesting seminar talks in the frame of our Seminar on Number Theory and Algebra (partly online and partly at the Department of Mathematics in Zagreb).

I also thank my family for their patience, support and understanding while writing this book.

Novigrad and Zagreb, January 2024 *Andrej Dujella*

Contents