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 financially 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

References

1. Adédji, K.N, He, B., Pintér, Á, Togbé, A.: On the Diophantine pair $\{a, 3a\}$. J. Number Theory **227**, 330–351 (2021)
2. Adžaga, N.: On the size of Diophantine m-tuples in imaginary quadratic number rings. Bull. Math. Sci. **11(1)**, Paper No. 1950020 (2021)
3. Adžaga, N., Dražić, G., Dujella, A., Pethő, A.: Asymptotics of $D(q)$-pairs and triples via L-functions of Dirichlet characters, preprint (2023) arXiv: 2304.01775
4. Adžaga, N., Dujella, A., Kreso, D., Tadić, P.: Triples which are $D(n)$-sets for several n's. J. Number Theory **184**, 330–341 (2018)
5. Aguirre, J., Dujella, A., Jukić Bokun, M., Peral, J.C.: High rank elliptic curves with prescribed torsion group over quadratic fields. Period. Math. Hungar. **68**, 222–230 (2014)
6. Aguirre, J., Dujella, A., Peral, J.C.: On the rank of elliptic curves coming from rational Diophantine triples. Rocky Mountain J. Math. **42**, 1759–1776 (2012)
7. Aguirre, J., Lozano-Robledo, Á., Peral, J.C.: Elliptic curves of maximal rank. In: Proceedings of the Segundas Jornadas de Teoria de Numeros, pp. 1–28. Bibl. Rev. Mat. Iberoamericana, Madrid (2008)
8. Alaca, S., Williams, K.S.: Introductory Algebraic Number Theory. Cambridge University Press, Cambridge (2004)
9. Aleksentsev, Y.M.: The Hilbert polynomial and linear forms in the logarithms of algebraic numbers. Izv. Math. **72**, 1063–1110 (2008)
10. Alp, M., Irmak, N., Szalay, L.: Reduced diophantine quadruples with the binary recurrence $G_n = AG_{n-1} - G_{n-2}$. An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. **23**, 23–31 (2015)
11. Andreescu, T., Andrica, D.: Quadratic Diophantine Equations. Springer, New York (2015)
12. Arkin, J., Bergum, G.E.: More on the problem of Diophantus. In: Philippou, A.N., Horadam, A.F., Bergum, G.E. (eds.) Application of Fibonacci Numbers, Vol. **2**, pp. 177–181. Kluwer, Dordrecht (1988)
13. Arkin, J., Hoggatt, V.E., Strauss, E.G.: On Euler's solution of a problem of Diophantus. Fibonacci Quart. **17**, 333–339 (1979)
14. Artin, M., Rodriguez-Villegas, F., Tate, J.: On the Jacobians of plane cubics. Adv. Math. **198** 366–382 (2005)
15. Atkin, A.O.L., Morain, F.: Finding suitable curves for the elliptic curve method of factorization. Math. Comp. **60**, 399–405 (1993)
16. Baćić, Lj., Filipin, A.: On the extendibility of $D(4)$-pair $\{k-2, k+2\}$. J. Comb. Number Theory **5**, 181–197 (2013)
17. Baker, A.: Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers. Quart. J. Math. Oxford Ser. (2) **15**, 375–383 (1964)
18. Baker, A.: Simultaneous rational approximations to certain algebraic numbers. Proc. Cambridge Philos. Soc. **63**, 693–702 (1967)

19. Baker, A.: Linear forms in the logarithms of algebraic numbers. IV. Mathematika **15**, 204–216 (1968)
20. Baker, A.: The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. J. London Math. Soc. **43**, 1–9 (1968)
21. Baker, A.: Transcendental Number Theory. Cambridge University Press, Cambridge (1990)
22. Baker, A.: A Concise Introduction to the Theory of Numbers. Cambridge University Press, Cambridge (1994)
23. Baker, A.: A Comprehensive Course in Number Theory. Cambridge University Press, Cambridge (2012)
24. Baker, A., Davenport, H.: The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. Quart. J. Math. Oxford Ser. (2) **20**, 129–137 (1969)
25. Baker, A., Wüstholz, G.: Logarithmic forms and group varieties. J. Reine Angew. Math. **442**, 19–62 (1993)
26. Baker, A., Wüstholz, G.: Logarithmic Forms and Diophantine Geometry. Cambridge University Press, Cambridge (2008)
27. Barbeau, E.J.: Pell's Equation, Springer, New York (2003)
28. Bashmakova, I.G.: Diophantus of Alexandria. Arithmetica and the Book of Polygonal Numbers. Introduction and Comments. Nauka, Moscow (1974), (in Russian)
29. Becker, R., Murty, M.R.: Diophantine m-tuples with the property $D(n)$. Glas. Mat. Ser. III **54**, 65–75 (2019)
30. Bennett, M.A.: On the number of solutions of simultaneous Pell equations. J. Reine Angew. Math. **498**, 173–199 (1998)
31. Bérczes, A., Dujella, A., Hajdu, L., Luca, F.: On the size of sets whose elements have perfect power n-shifted products. Publ. Math. Debrecen **79**, 325–339 (2011)
32. Bérczes, A., Dujella, A., Hajdu, L., Tengely, S.: Finiteness results for F-Diophantine sets. Monatsh. Math. **180**, 469–484 (2016)
33. Bérczes, A., Luca, F., Pink, I., Ziegler, V.: Finiteness results for Diophantine triples with repdigit values. Acta Arith. **172**, 133–148 (2016)
34. Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Lecture Notes in Comput. Sci. **4833**, pp. 29–50. Springer, Berlin (2007)
35. Bhargava, M., Shankar, A,: The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1. preprint (2013) arXiv: 1312.7859
36. Bhattacharjee, S., Dixit, A.B., Saikia, D.: An effective bound on generalized Diophantine m-tuples. Bull. Aust. Math. Soc., to appear.
37. Bilu, Yu.F., Hanrot, G.: Solving Thue equations of high degree. J. Number Theory **60**, 373–392 (1996)
38. Birch, B.J.: Elliptic curves and modular functions. In: Symposia Mathematica, Vol. IV, pp. 27–32. Academic Press, London (1970)
39. Birch, B.J., Swinnerton-Dyer, H.P.F.: Notes on elliptic curves. I. J. Reine Angew. Math. **212**, 7–25 (1963)
40. Blake, I., Seroussi, G., Smart, N.: Elliptic Curves in Cryptography. Cambridge University Press, Cambridge (1999)
41. Bliznac Trebješanin, M., Filipin, A.: Nonexistence of $D(4)$-quintuples, J. Number Theory **194**, 170–217 (2019)
42. Bober, J.W.: Conditionally bounding analytic ranks of elliptic curves. In: ANTS X – Proceedings of the Tenth Algorithmic Number Theory Symposium, pp. 135–144. Mathematical Sciences Publishers, Berkeley (2013)
43. Bombieri, E., Gubler, W.: Heights in Diophantine Geometry. Cambridge University Press, Cambridge (2006)
44. Bonciocat, N.C., Cipu, M., Mignotte, M.: There is no Diophantine $D(-1)$-quadruple. J. London Math. Soc. **105**, 63–99 (2022)
45. Bosma, W., Cannon, J.J., Fieker, C., Steel, A.: Handbook of Magma functions, Edition 2.28 (2023).
46. Bosman, J., Bruin, P., Dujella, A., Najman, F.: Ranks of elliptic curves with prescribed torsion over number fields. Int. Math. Res. Not. IMRN **2014**, 2885–2923 (2014)

47. Brown, E.: Sets in which $xy + k$ is always a square. Math. Comp. **45**, 613–620 (1985)
48. Bugeaud, Y.: Linear Forms in Logarithms and Applications. IRMA Lectures in Mathematics and Theoretical Physics Vol. **28**, European Mathematical Society, Zürich (2018)
49. Bugeaud, Y., Dujella, A.: On a problem of Diophantus for higher powers. Math. Proc. Cambridge Philos. Soc. **135**, 1–10 (2003)
50. Bugeaud, Y., Dujella, A., Mignotte, M.: On the family of Diophantine triples $\{k-1, k+1, 16k^3-4k\}$. Glasgow Math. J. **49**, 333–344 (2007)
51. Bugeaud, Y., Mignotte, M., Siksek, S.: Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers, Ann. of Math. (2) **163**, 969–1018 (2006)
52. Bundschuh, P.: Einführung in die Zahlentheorie. Springer-Verlag, Berlin (2008)
53. Caporaso, L., Harris, J., Mazur, B.: Uniformity of rational points. J. Amer. Math. Soc. **10**, 1–35 (1997)
54. Carmichael, R.D.: Diophantine Analysis. Dover, New York (1959)
55. Cassels, J.W.S.: Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups. Proc. London Math. Soc. (3) **12**, 259–296 (1962)
56. Cassels, J.W.S.: Lectures on Elliptic Curves. Cambridge University Press, Cambridge (1995)
57. Chahal, J.S.: Topics in Number Theory. Plenum Press, New York (1988)
58. Chakraborty, K., Gupta, S., Hoque, A.: Diophantine triples with the property $D(n)$ for distinct n's. Mediterr. J. Math. **20**, Article 31 (2023)
59. Chakraborty, K., Gupta, S., Hoque, A.: On a conjecture of Franušić and Jadrijević: Counter-examples. Results Math. **78**, Article 18 (2023)
60. Chebyshev, P.L., Sur les formes quadratiques. J. Math. Pures Appl. **16**, 257–282 (1851)
61. Cipu, M.: Further remarks on Diophantine quintuples. Acta Arith. **168**, 201–219 (2015)
62. Cipu, M., Dujella, A., Fujita, Y.: Extensions of a Diophantine triple by adjoining smaller elements. Mediterr. J. Math. **19**, Article 187 (2022)
63. Cipu, M., Filipin, A., Fujita, Y.: Bounds for Diophantine quintuples II. Publ. Math. Debrecen **88**, 59–78 (2016)
64. Cipu, M., Fujita, Y.: Bounds for Diophantine quintuples. Glas. Mat. Ser. III **50**, 25–34 (2015)
65. Cipu, M., Fujita, Y.: On the length of $D(\pm 1)$-tuples in imaginary quadratic rings. Bull. Lond. Math. Soc. **56**, 274–287 (2024)
66. Cipu, M., Fujita, Y., Miyazaki, T.: On the number of extensions of a Diophantine triple. Int. J. Number Theory **14**, 899–917 (2018)
67. Cipu, M., Trudgian, T.: Searching for Diophantine quintuples. Acta Arith. **173**, 365–382 (2016)
68. Cohen, H.: A Course in Computational Algebraic Number Theory. Springer-Verlag, Berlin (1993)
69. Cohen, H.: Number Theory. Volume I: Tools and Diophantine Equations. Springer, New York (2007)
70. Cohn, J.H.E.: Lucas and Fibonacci numbers and some Diophantine equations, Proc. Glasgow Math. Assoc. **7**, 24–28 (1965)
71. Cohn, J.H.E.: The length of the period of the simple continued fraction of $d^{1/2}$. Pacific J. Math. **71**, 21–32 (1977)
72. Connell, I.: Elliptic Curve Handbook. McGill University, Montreal (1999)
73. Cremona, J.E.: Algorithms for Modular Elliptic Curves. Cambridge University Press, Cambridge (1997)
74. Cremona, J.E.: Elliptic Curve Data (2020) `http://johncremona.github.io/ecdata/`
75. Christianidis, J., Oaks, J.: The Arithmetica of Diophantus. A Complete Translation and Commentary. Routledge, London, 2023.
76. Davenport, H., Roth, K.F.: Rational approximations to algebraic numbers. Mathematika **2**, 160–167 (1955)
77. David, S.: Minorations de formes linéaires de logarithmes elliptiques. Mém. Soc. Math. France (N.S.) **62**, 1–143 (1995)

78. Denton, A.D.: A holiday brain teaser. The Sunday Times, 4th August 1957, 18th August 1957
79. Deshpande, M.N.: One interesting family of diophantine triplets, Internat. J. Math. Ed. Sci. Tech. **33**, 253–256 (2002)
80. Deshpande, M.N.: Wonderland of Families of Diophantine triples. Nagpur (2022)
81. Deshpande, M.N, Dujella, A.: An interesting property of a reccurence related to the Fibonacci sequence. Fibonacci Quart. **40**, 157–160 (2002)
82. Dickson, L.E.: History of the Theory of Numbers, Volume 2: Diophantine analysis. Chelsea, New York (1966)
83. Dixit, A.B., Kim, S., Murty, M.R.: Generalized Diophantine m-tuples. Proc. Amer. Math. Soc. **150**, 1455–1465 (2022)
84. Dörge, K.: Über die Seltenheit der reduziblen Polynome und der Normalgleichungen. Math. Ann. **95**, 247–256 (1926)
85. Dražić, G.: Rational $D(q)$-quintuples. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **116**, Article 9 (2022)
86. Dražić, G., Kazalicki, M.: Rational $D(q)$-quadruples. Indag. Math. (N.S.) **33**, 440–449 (2022)
87. Dujella, A.: Generalization of a problem of Diophantus. Acta Arith. **65**, 15–27 (1993)
88. Dujella, A.: Diophantine quadruples for squares of Fibonacci and Lucas numbers. Portugaliae Math. **52**, 305–318 (1995)
89. Dujella, A.: Generalized Fibonacci numbers and the problem of Diophantus. Fibonacci Quart. **34**, 164–175 (1996)
90. Dujella, A.: Some polynomial formulas for Diophantine quadruples. Grazer Math. Ber. **328**, 25–30 (1996)
91. Dujella, A.: On Diophantine quintuples. Acta Arith. **81**, 69–79 (1997)
92. Dujella, A.: The problem of the extension of a parametric family of Diophantine triples. Publ. Math. Debrecen **51**, 311–322 (1997)
93. Dujella, A.: Some estimates of the number of Diophantine quadruples. Publ. Math. Debrecen **53**, 177–189 (1998)
94. Dujella, A.: A problem of Diophantus and Pell numbers. In: Bergum, G.E., Philippou, A.N., Horadam, A.F. (eds.) Application of Fibonacci Numbers, Vol. **7**, pp. 61–68. Kluwer, Dordrecht (1998)
95. Dujella, A.: A problem of Diophantus and Dickson's conjecture. In: Győry, K., Pethő, A., Sós, V.T. (eds.) Number Theory, Diophantine, Computational and Algebraic Aspects, pp. 147–156. Walter de Gruyter, Berlin (1998)
96. Dujella, A.: An extension of an old problem of Diophantus and Euler. Fibonacci Quart. **37**, 312–314 (1999)
97. Dujella, A.: A proof of the Hoggatt-Bergum conjecture. Proc. Amer. Math. Soc. **127**, 1999–2005 (1999)
98. Dujella, A.: Diophantine triples and construction of high-rank elliptic curves over $\mathbb{Q}$ with three non-trivial 2-torsion points. Rocky Mountain J. Math. **30**, 157–164 (2000)
99. Dujella, A.: A note on Diophantine quintuples. In: Halter-Koch, F., Tichy, R.F. (eds.) Algebraic Number Theory and Diophantine Analysis, pp. 123–127. Walter de Gruyter, Berlin (2000)
100. Dujella, A.: A parametric family of elliptic curves. Acta Arith. **94**, 87–101 (2000)
101. Dujella, A.: Irregular Diophantine m-tuples and elliptic curves of high rank. Proc. Japan Acad. Ser. A Math. Sci. **76**, 66–67 (2000)
102. Dujella, A.: Diophantine m-tuples and elliptic curves. J. Théor. Nombres Bordeaux **13**, 111–124 (2001)
103. Dujella, A.: An absolute bound for the size of Diophantine m-tuples. J. Number Theory **89**, 126–150 (2001)
104. Dujella, A.: An extension of an old problem of Diophantus and Euler. II. Fibonacci Quart. **40**, 118–123 (2002)
105. Dujella, A.: On the size of Diophantine m-tuples. Math. Proc. Cambridge Philos. Soc. **132**, 23–33 (2002)

106. Dujella, A.: There are only finitely many Diophantine quintuples. J. Reine Angew. Math. **566**, 183–214 (2004)
107. Dujella, A.: Bounds for the size of sets with the property $D(n)$. Glas. Mat. Ser. III **39**, 199–205 (2004)
108. Dujella, A.: Continued fractions and RSA with small secret exponent. Tatra Mt. Math. Publ. **29**, 101–112 (2004)
109. Dujella, A.: On Mordell-Weil groups of elliptic curves induced by Diophantine triples. Glas. Mat. Ser. III **42**, 3–18 (2007)
110. Dujella, A.: Conjectures and results on the size and number of Diophantine tuples. In: Komatsu, T. (ed.) Diophantine Analysis and Related Fields (DARF 2007/2008), AIP Conf. Proc. **976**, pp. 58–61, Amer. Inst. Phys., Melville, (2008)
111. Dujella, A.: On the number of Diophantine m-tuples, Ramanujan J. **15**, 37–46 (2008)
112. Dujella, A.: Rational Diophantine sextuples with mixed signs. Proc. Japan Acad. Ser. A Math. Sci. **85**, 27–30 (2009)
113. Dujella, A.: What is ... a Diophantine m-tuple?. Notices Amer. Math. Soc. **63**, 772–774 (2016)
114. Dujella, A.: History of elliptic curves rank records (2020) `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`
115. Dujella, A.: Number Theory. Školska knjiga, Zagreb (2021)
116. Dujella, A.: Diophantine m-tuples and elliptic curves. Course webpage (2022) `https://web.math.pmf.unizg.hr/~duje/diophell.html`
117. Dujella, A.: High rank elliptic curves with prescribed torsion (2022) `https://web.math.pmf.unizg.hr/~duje/tors/tors.html`
118. Dujella, A.: High rank elliptic curves with prescribed torsion over quadratic fields (2023) `https://web.math.pmf.unizg.hr/~duje/tors/torsquad.html`
119. Dujella, A.: Infinite families of elliptic curves with high rank and prescribed torsion (2023) `https://web.math.pmf.unizg.hr/~duje/tors/generic.html`
120. Dujella, A.: Diophantine m-tuples page (2023) `https://web.math.pmf.unizg.hr/~duje/dtuples.html`
121. Dujella, A., Gusić, I., Petričević, V., Tadić, P.: Strong Eulerian triples. Glas. Mat. Ser. III **53**, 33–42 (2018)
122. Dujella, A., Filipin, A., Fuchs, C.: Effective solution of the $D(-1)$-quadruple conjecture. Acta Arith. **128**, 319–338 (2007)
123. Dujella, A., Fuchs, C.: Complete solution of the polynomial version of a problem of Diophantus. J. Number Theory **106**, 326–344 (2004)
124. Dujella, A., Fuchs, C.: Complete solution of a problem of Diophantus and Euler. J. London Math. Soc. **71**, 33–52 (2005)
125. Dujella, A., Fuchs, C.: On a problem of Diophantus for rationals. J. Number Theory **132**, 2075–2083 (2012)
126. Dujella, A., Fuchs, C., Luca, F.: A polynomial variant of a problem of Diophantus for pure powers. Int. J. Number Theory **4**, 57–71 (2008)
127. Dujella, A., Fuchs, C., Tichy, R.F.: Diophantine m-tuples for linear polynomials. Period. Math. Hungar. **45**, 21–33 (2002)
128. Dujella, A., Fuchs, C., Walsh, P.G.: Diophantine m-tuples for linear polynomials. II. Equal degrees, J. Number Theory **120**, 213–228 (2006)
129. Dujella, A., Gusić, I., Lasić, L.: On quadratic twists of elliptic curves $y^2 = x(x-1)(x-\lambda)$. Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **18**, 27–34 (2014)
130. Dujella, A., Jadrijević, B.: A family of quartic Thue inequalities. Acta Arith. **111**, 61–76 (2004)
131. Dujella, A., Jukić Bokun, M., Soldo, I.: On the torsion group of elliptic curves induced by Diophantine triples over quadratic fields. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **111**, 1177–1185 (2017)
132. Dujella, A., Jurasić, A.: On the size of sets in a polynomial variant of a problem of Diophantus. Int. J. Number Theory **6**, 1449–1471 (2010)

133. Dujella, A., Jurasić, A.: Some Diophantine triples and quadruples for quadratic polynomials. J. Comb. Number Theory **3(2)**, 123–141 (2011)
134. Dujella, A., Kazalicki, M.: More on Diophantine sextuples. In: Elsholtz, C., Grabner, P. (eds.) Number Theory - Diophantine problems, uniform distribution and applications, Festschrift in honour of Robert F. Tichy's 60th birthday, pp. 227–235. Springer, Cham (2017)
135. Dujella, A., Kazalicki, M.: Diophantine m-tuples in finite fields and modular forms. Res. Number Theory **7**, Article 3 (2021)
136. Dujella, A., Kazalicki, M., Mikić, M., Szikszai, M.: There are infinitely many rational Diophantine sextuples. Int. Math. Res. Not. IMRN **2017(2)**, 490–508 (2017)
137. Dujella, A., Kazalicki, M., Peral, J.C.: Elliptic curves with torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **115**, Article 169 (2021)
138. Dujella, A., Kazalicki, M., Petričević, V.: Rational Diophantine sextuples with square denominators. J. Number Theory **205**, 340–346 (2019)
139. Dujella, A., Kazalicki, M., Petričević, V.: Rational Diophantine sextuples containing two regular quadruples and one regular quintuple. Acta Mathematica Spalatensia **1**, 19–27 (2021)
140. Dujella, A., Kazalicki, M., Petričević, V.: $D(n)$-quintuples with square elements. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **115**, Article 172 (2021)
141. Dujella, A., Luca, F.: Diophantine m-tuples for primes. Int. Math. Res. Not. **47**, 2913–2940 (2005)
142. Dujella, A., Luca, F.: On a problem of Diophantus with polynomials. Rocky Mountain J. Math. **37**, 131–157 (2007)
143. Dujella, A., Mikić, M.: On the torsion group of elliptic curves induced by $D(4)$-triples, An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. **22**, 79–90 (2014)
144. Dujella, A., Mikić, M.: Rank zero elliptic curves induced by rational Diophantine triples. Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **24**, 29–37 (2020)
145. Dujella, A., Paganin, M., Sadek, M.: Strong rational Diophantine $D(q)$-triples. Indag. Math. (N.S.) **31**, 505–511 (2020)
146. Dujella, A., Peral, J.C.: High rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples. LMS J. Comput. Math. **17**, 282–288 (2014)
147. Dujella, A., Peral, J.C.: Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. In: Trends in Number Theory, Contemp. Math. **649**, 47–62 (2015)
148. Dujella, A., Peral, J.C.: Elliptic curves induced by Diophantine triples. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **113**, 791–806 (2019)
149. Dujella, A., Peral, J.C.: High rank elliptic curves induced by rational Diophantine triples. Glas. Mat. Ser. III **55**, 237–252 (2020)
150. Dujella, A., Peral, J.C.: Construction of high rank elliptic curves. J. Geom. Anal. **31**, 6698–6724 (2021)
151. Dujella, A., Pethő, A.: A generalization of a theorem of Baker and Davenport. Quart. J. Math. Oxford Ser. (2) **49**, 291–306 (1998)
152. Dujella, A., Pethő, A.: Integer points on a family of elliptic curves. Publ. Math. Debrecen **56**, 321–335 (2000)
153. Dujella, A., Petričević, V.: Strong Diophantine triples. Experiment. Math. **17**, 83–89 (2008)
154. Dujella, A., Petričević, V.: On the largest element in $D(n)$-quadruples. Indag. Math. (N.S.) **30**, 1079–1086 (2019)
155. Dujella, A., Petričević, V.: Diophantine quadruples with the properties $D(n_1)$ and $D(n_2)$. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **114**, Article 21 (2020)
156. Dujella, A., Petričević, V.: Doubly regular Diophantine quadruples. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **114**, Article 189 (2020)
157. Dujella, A., Saradha, N.: Diophantine m-tuples with elements in arithmetic progressions, Indag. Math. (N.S.) **25**, 131–136 (2014)
158. Dujella, A., Soydan, G.: On elliptic curves induced by rational Diophantine quadruples. Proc. Japan Acad. Ser. A Math. Sci. **98**, 1–6 (2022)
159. Edwards, H.M.: A normal form for elliptic curves. Bull. Amer. Math. Soc. (N.S.) **44**, 393–422 (2007)

160. Elkies, N.D.: $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc. Number Theory Listserver (2006) https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;99f4e7cd.0605
161. Elkies, N.D.: Three lectures on elliptic surfaces and curves of high rank. Lecture notes, Oberwolfach (2007) arXiv: 0709.2908
162. Elkies, N.D., Klagsbrun, Z.: New rank records for elliptic curves having rational torsion. In: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, pp. 233–250. Mathematical Sciences Publishers, Berkeley (2020)
163. Elsholtz, C., Filipin, A., Fujita, Y.: On Diophantine quintuples and $D(-1)$-quadruples. Monatsh. Math. **175**, 227–239 (2014)
164. Eroshkin, Y.G.: Personal communication (2008, 2009)
165. Fermigier, S.: Exemples de courbes elliptiques de grand rang sur $\mathbb{Q}(t)$ et sur $\mathbb{Q}$ possédant des points d'ordre 2. C. R. Acad. Sci. Paris Sér. I **332**, 949–952 (1996)
166. Filipin, A., Fujita, Y.: The number of Diophantine quintuples II. Publ. Math. Debrecen **82**, 293–308 (2013)
167. Filipin, A., Jurasić, A.: A polynomial variant of a problem of Diophantus and its consequences. Glas. Mat. Ser. III **54**, 21–52 (2019)
168. Filipin, A., Szalay, L.: Triangular Diophantine tuples from $\{1, 2\}$. Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **27**, 55–70 (2023)
169. Fisher, T.: Higher descents on an elliptic curve with a rational 2-torsion point. Math. Comp. **86**, 2493–2518 (2017)
170. Fisher, T.: A formula for the Jacobian of a genus one curve of arbitrary degree. Algebra Number Theory **12**, 2123–2150 (2018)
171. Fisher, T.: On binary quartics and the Cassels-Tate pairing. Res. Number Theory **8**, Paper No. 74 (2022)
172. Franušić, Z.: Diophantine quadruples in $\mathbb{Z}[\sqrt{4k+3}]$. Ramanujan J. **17**, 77–88 (2008)
173. Franušić, Z.: A Diophantine problem in $\mathbb{Z}[(1+\sqrt{d})/2]$. Studia Sci. Math. Hungar. **46**, 103–112 (2009)
174. Franušić, Z.: Diophantine quadruples in the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$. Miskolc Math. Notes **14**, 893–903 (2013)
175. Franušić, Z., Jadrijević, B.: $D(n)$-quadruples in the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, Math. Slovaca **69**, 1263-1278 (2019)
176. Franušić, Z., Soldo, I.: The problem of Diophantus for integers of $\mathbb{Q}(\sqrt{-3})$. Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **18**, 15–25 (2014)
177. Friedl, S.: An elementary proof of the group law for elliptic curves. Groups Complex. Cryptol. **9**, 117–123 (2017)
178. Fuchs, C., Heintze, S.: A polynomial variant of Diophantine triples in linear recurrences. Period. Math. Hungar. **86**, 289–299 (2023)
179. Fuchs, C., Hutle, C., Luca, F.: Diophantine triples in linear recurrence sequences of Pisot type. Res. Number Theory **4**, Paper No. 29 (2018)
180. Fuchs, C., Hutle, C., Luca, F., Szalay, L.: Diophantine triples and k-generalized Fibonacci sequences. Bull. Malays. Math. Sci. Soc. (2) **41**, 1449–1465 (2018)
181. Fuchs, C., Luca, F., Szalay, L.: Diophantine triples with values in binary recurrences. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **7**, 579–608 (2008)
182. Fujita, Y.: The extensibility of $D(-1)$-triples $\{1, b, c\}$. Publ. Math. Debrecen **70**, 103–117 (2007)
183. Fujita, Y.: The extensibility of Diophantine pairs $\{k-1, k+1\}$. J. Number Theory **128**, 322–353 (2008)
184. Fujita, Y.: Any Diophantine quintuple contains a regular Diophantine quadruple. J. Number Theory **129**, 1678–1697 (2009)
185. Fujita, Y.: The number of Diophantine quintuples. Glas. Mat. Ser. III **45**, 15–29 (2010)
186. Fujita, Y., Miyazaki, T.: The regularity of Diophantine quadruples. Trans. Amer. Math. Soc. **370**, 3803–3831 (2018)
187. Gaál, I.: Diophantine Equations and Power Integral Bases. Theory and Algorithms. Birkhäuser, Boston (2019)

188. Gallagher, P.X.: A larger sieve. Acta Arith. **18**, 77–81 (1971)
189. Gardner, M.: Mathematical games. Scientific American **216** (1967), March 1967, p. 124; April 1967, p. 119.
190. Gardner, M.: Mathematical Magic Show. Alfred Knopf, New York (1977), pp. 210, 221–222
191. Gebel, J., Pethő, A., Zimmer, H.G.: Computing integral points on elliptic curves. Acta Arith. **68**, 171–192 (1994)
192. Gibbs, P.E.: Computer Bulletin **17**, 16-16 (1978)
193. Gibbs, P.E.: A generalised Stern-Brocot tree from regular Diophantine quadruples. preprint (1999) arXiv: math.NT/9903035.
194. Gibbs, P.E.: Some rational Diophantine sextuples. Glas. Mat. Ser. III **41**, 195–203 (2006)
195. Gibbs, P.E.: Regular rational Diophantine sextuples. preprint (2016) doi: 10.13140/RG.2.2.36449.51040
196. Gibbs, P.E.: A survey of rational Diophantine sextuples of low height. preprint (2016) doi: 10.13140/RG.2.2.29253.65761
197. Gouvêa, F., Mazur, B.: The square-free sieve and the rank of elliptic curves. J. Amer. Math. Soc. **4**, 1–23 (1991)
198. Gross, B.H., Zagier, D.B.: Heegner points and derivatives of L-series. Invent. Math. **84** 225–320 (1986)
199. Gupta, H., Singh, K.: On k-triad sequences. Internat. J. Math. Math. Sci. **5**, 799–804 (1985)
200. Gupta, S.: $D(-1)$ tuples in imaginary quadratic fields. Acta Math. Hungar. **164**, 556–569 (2021)
201. Gusić, I., Tadić, P.: A remark on the injectivity of the specialization homomorphism. Glas. Mat. Ser. III **47**, 265–275 (2012)
202. Gusić, I., Tadić, P.: Injectivity of the specialization homomorphism of elliptic curves. J. Number Theory **148**, 137–152 (2015)
203. Guy, R.K.: Unsolved Problems in Number Theory. Springer, New York (2004)
204. Gyarmati. K.: On a problem of Diophantus. Acta Arith. **97**, 53–65 (2001)
205. Gyarmati, K., Stewart, C.L.: On powers in shifted products. Glas. Mat. Ser. III **42**, 273–279 (2007)
206. Hajdu, L., Herendi, T.: Explicit bounds for the solutions of elliptic equations with rational coefficients. J. Symbolic Computation **25**, 361–366 (1998)
207. Hammonds, T., Kim, S., Miller, S.J., Nigam, A., Onghai, K., Saikia, D., Sharma, L.M.: k-Diophantine m-tuples in finite fields. Int. J. Number Theory **19**, 891–912 (2023)
208. Hankerson, D., Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer-Verlag, New York (2004)
209. He, B., Luca, F., Togbé, A.: Diophantine triples of Fibonacci numbers. Acta Arith. **175**, 57–70 (2016)
210. He, B., Togbé, A.: On the $D(-1)$-triple $\{1, k^2+1, k^2+2k+2\}$ and its unique $D(1)$-extension. J. Number Theory **131**, 120–137 (2011)
211. He, B., Togbé, A., Ziegler, V.: There is no Diophantine quintuple. Trans. Amer. Math. Soc. **371**, 6665–6709 (2019)
212. Heath, T.L.: Diophantus of Alexandria: A study in the history of Greek Algebra. Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center (2003)
213. Heichelheim, P.: The study of positive integers (a, b) such that $ab+1$ is a square. Fibonacci Quart. **17**, 269–274 (1979)
214. Herrmann, E., Pethő, A., Zimmer, H.G.: On Fermat's quadruple equations. Abh. Math. Sem. Univ. Hamburg **69**, 283–291 (1999)
215. Hindry, M., Silverman, J.H.: Diophantine Geometry. An Introduction. Springer-Verlag, New York (2000)
216. Hoggatt, V.E. Jr.: Fibonacci and Lucas Numbers. The Fibonacci Association, Santa Clara (1979)
217. Hoggatt, V.E., Bergum, G.E.: A problem of Fermat and the Fibonacci sequence. Fibonacci Quart. **15**, 323–330 (1977)
218. Horadam, A.F.: Generalization of a result of Morgado. Portugaliae Math. **44**, 131–136 (1987)

219. Hungerford, T.W.: Algebra. Springer-Verlag, New York (1974)
220. Husemöller, D.: Elliptic Curves. Springer-Verlag, New York (2004)
221. Irmak, N., Szalay, L.: Diophantine triples and reduced quadruples with the Lucas sequence of recurrence $u_n = Au_{n-1} - u_{n-2}$. Glas. Mat. Ser. III **49**, 303–312 (2014)
222. Jacobson, M.J. Jr., Williams, H.C.: Modular arithmetic on elements of small norm in quadratic fields. Des. Codes and Cryptogr. **27**, 93–110 (2002)
223. Jacobson, M.J. Jr., Williams, H.C.: Solving the Pell Equation. Springer, New York (2009)
224. Jones, B.W.: A second variation on a problem of Diophantus and Davenport. Fibonacci Quart. **16**, 155–165 (1978)
225. Jurasić, A.: Diophantine m-tuples for quadratic polynomials. Glas. Mat. Ser. III **46**, 283–309 (2011)
226. Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. **109**, 221–229 (1992)
227. Kanagasabapathy, P., Ponnudurai, T.: The simultaneous Diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$. Quart. J. Math. Oxford Ser. (2) **26**, 275–278 (1975)
228. Kazalicki, M., Naskrecki, B. (with an appendix by Lasić, L.): Diophantine triples and $K3$ surfaces. J. Number Theory **236**, 41–70 (2022)
229. Kazalicki, M., Vlah, D.: Ranks of elliptic curves and deep neural networks. Res. Number Theory **9**, Article 53 (2023)
230. Kedlaya, K.S.: When is $(xy+1)(yz+1)(zx+1)$ a square?. Math. Mag. **71**, 61–63 (1998)
231. Kedlaya, K.S.: Solving constrained Pell equations. Math. Comp. **67**, 833–842 (1998)
232. Kenku, M.A., Momose, F.: Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. **109**, 125–149 (1988)
233. Khinchin, A.Ya.: Continued Fractions. Dover, New York (1997)
234. Kihara, S.: On an elliptic curve over $\mathbb{Q}(t)$ of rank $\geq$ 14. Proc. Japan. Acad. Ser. A Math. Sci. **77**, 50–51 (2001)
235. Kihel, A., Kihel, O.: On the intersection and the extendability of P_t sets. Far East J. Math. Sci. **3**, 637–643 (2001)
236. Kim, S., Murty, M.R. (with an appendix by Sutherland, A.V.): From the Birch and Swinnerton-Dyer conjecture to Nagao's conjecture. Math. Comp. **92**, 385–408 (2023)
237. Kim, S., Yip, C.H., Yoo, S.: Diophantine tuples and multiplicative structure of shifted multiplicative subgroups. preprint (2023) arXiv: 2309.09124
238. Klagsbrun, Z., Sherman, T., Weigandt, J.: The Elkies curve has rank 28 subject only to GRH. Math. Comp. **88**, 837–846 (2019)
239. Knapp, A.W.: Elliptic Curves. Princeton University Press, Princeton (1992)
240. Koblitz, N.: A Course in Number Theory and Cryptography. Springer-Verlag, New York (1994)
241. Kolyvagin, V.: Finiteness of $E(\mathbb{Q})$ and $\mathrm{CH}(E, \mathbb{Q})$ for a class of Weil curves. Math. USSR-Izv. **32**, 523–541 (1989)
242. Koshy, T.: Fibonacci and Lucas Numbers with Applications. Wiley, New York (2001)
243. Kulesz, L.: Families of elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$. Acta Arith. **108**, 339–356 (2003)
244. Kwon, S.: Torsion subgroups of elliptic curves over quadratic extensions. J. Number Theory **62**, 144–162 (1997)
245. Lang, S.: Algebra. Springer-Verlag, New York (2002)
246. Laurent, M.: Linear forms in two logarithms and interpolation determinants II. Acta Arith. **133**, 25–348 (2008)
247. Laurent, M., Mignotte, M., Nesterenko, Y.: Formes linéaires en deux logarithmes et déterminants d'interpolation. J. Number Theory **55**, 285–321 (1995)
248. Le, M., Srinivasan, A.: A note on Dujella's unicity conjecture. Glas. Mat. Ser. III **58**, 59–65 (2023)
249. Lecacheux, O.: Rang de courbes elliptiques sur $\mathbb{Q}$ avec un groupe de torsion isomorphe á $\mathbb{Z}/5\mathbb{Z}$. C. R. Acad. Sci. Paris Sér. I Math. **332**, 1–6 (2001)
250. Lecacheux, O.: Rang de courbes elliptiques avec groupe de torsion non trivial, J. Théor. Nombres Bordeaux **15**, 231–247 (2003)

251. Lecacheux, O.: Rang de courbes elliptiques dont le groupe de torsion est non trivial. Ann. Sci. Math. Québec **28**, 145–151 (2004)
252. Lenstra, A.K., Lenstra, H.W. Jr., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**, 515–534 (1982)
253. Lenstra, H.W. Jr.: Factoring integers with elliptic curves. Ann. of Math. **126**, 649–673 (1987)
254. LeVeque, W.J.: Topics in Number Theory I, II. Dover, New York (1984)
255. van Lint, J.H.: On a set of diophantine equations. T. H.-Report 68 - WSK-03, Department of Mathematics, Technological University Eindhoven, Eindhoven (1968)
256. Ljunggren, W.: On the Diophantine equation $x^2 + 4 = Ay^4$. Norske Vid. Selsk. Forh. **24**, 82–84 (1951).
257. LMFDB Collaboration: The L-functions and modular forms database (2023) `https://www.lmfdb.org`
258. Long, C., Bergum, G.E.: On a problem of Diophantus. In: Philippou, A.N., Horadam, A.F., Bergum, G.E. (eds.) Application of Fibonacci Numbers, Vol. **2**, pp. 183–191. Kluwer, Dordrecht (1988)
259. Lozano-Robledo, Á.: Elliptic Curves, Modular Forms and their L-functions. American Mathematical Society, Providence (2011)
260. Luca, F.: On shifted products which are powers. Glas. Mat. Ser. III **40**, 13–20 (2005)
261. Luca, F., Fujita, Y.: On Diophantine quadruples of Fibonacci numbers. Glas. Mat. Ser. III **52**, 221–234 (2017)
262. Luca, F., Fujita, Y.: There are no Diophantine quadruples of Fibonacci numbers. Acta Arith. **185**, 19–38 (2018)
263. Luca, F., Szalay, L.: Fibonacci Diophantine triples. Glas. Mat. Ser. III **43**, 253–264 (2008)
264. Luca, F., Szalay, L.: Lucas Diophantine triples. Integers **9**, 441–457 (2009)
265. Luca, F., Osgood, C.F., Walsh, P.G.: Diophantine approximations and a problem from the 1988 IMO. Rocky Mountain J. Math. **36**, 637–648 (2006)
266. van Luijk, R.: On Perfect Cuboids. Thesis, Universiteit Utrecht (2000)
267. Mani, N., Rubinstein-Salzedo, S.: Diophantine tuples over $\mathbb{Z}_p$. Acta Arith. **197**, 331–351 (2021)
268. Martin, G., Sitar, S.: Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples. Mathematika **57**, 1–29 (2011)
269. Matthews, K.R., Robertson, J.P., White, J.: On a diophantine equation of Andrej Dujella. Glas. Mat. Ser. III **48**, 265–289 (2013)
270. Matveev, E.M.: An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. Izv. Math. **64**, 1217–1269 (2000)
271. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. **18**, 183–266 (1972)
272. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. **47**, 33–186 (1977)
273. Mazur, B. (with an appendix by D. Goldfeld): Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
274. Mestre, J.-F.: Construction d'une courbe elliptique de rang $\geq$ 12. C. R. Acad. Sci. Paris Sér. I **295**, 643–644 (1982)
275. Mestre, J.-F.: Formules explicites et minorations de conducteurs de variétés algébriques. Compositio Math. **58**, 209–232 (1986)
276. Mestre, J.-F.: Courbes elliptiques de rang $\geq$ 11 sur $\mathbb{Q}(t)$. C. R. Acad. Sci. Paris Sér. I **313**, 139–142 (1991)
277. Mestre, J.-F.: Courbes elliptiques de rang $\geq$ 12 sur $\mathbb{Q}(t)$. C. R. Acad. Sci. Paris Sér. I **313**, 171–174 (1991)
278. Mignotte, M.: A kit on linear forms in three logarithms. preprint (2008)
279. Mignotte, M., Voutier, P. (with an appendix by Laurent, M.): A kit for linear forms in three logarithms. Math. Comp., to appear.
280. Mikić, M.: On the Mordell-Weil group of elliptic curves induced by the families of Diophantine triples. Rocky Mountain J. Math. **45**, 1565–1589 (2015)

281. Milne, J.S. Elliptic Curves. BookSurge Publishers, Charleston (2006)
282. Mohanty, S.P., Ramasamy, A.M.S.: On $P_{r,k}$ sequences. Fibonacci Quart. **23**, 36–44 (1985)
283. Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization. Math. Comp. **48**, 243–264 (1987)
284. Mootha, V.K.: On the set of numbers $\{14, 22, 30, 42, 90\}$. Acta Arith. **71**, 259–263 (1995)
285. Mootha, V.K., Berzsenyi, G.: Characterizations and extendibility of P_t-sets, Fibonacci Quart. **27**, 287–288 (1989)
286. Mordell, L.J.: Diophantine Equations. Academic Press, New York (1969)
287. Morgado, J.: Generalization of a result of Hoggatt and Bergum on Fibonacci numbers. Portugaliae Math. **42**, 441–445 (1983–1984)
288. Morgado, J.: Note on some results of A. F. Horadam and A. G. Shannon concerning a Catalan's identity on Fibonacci numbers. Portugaliae Math. **44**, 243–252 (1987)
289. Morgado, J.: Note on a Shannon's theorem concerning the Fibonacci numbers and Diophantine quadruples. Portugaliae Math. **48**, 429–439 (1991)
290. Morgado, J.: Note on the Chebyshev polynomials and applications to the Fibonacci numbers. Portugaliae Math. **52**, 363–378 (1995)
291. Nagao, K.: An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20. Proc. Japan Acad. Ser. A Math. Sci. **69**, 291–293 (1993)
292. Nagao, K.: An example of elliptic curve over $\mathbb{Q}(T)$ with rank ≥ 13, Proc. Japan Acad. Ser. A Math. Sci. **70**, 152–153 (1994)
293. Nagao, K.: Construction of high-rank elliptic curves with a nontrivial torsion point. Math. Comp. **66**, 411–415 (1997)
294. Nagell, T.: Introduction to Number Theory. Chelsea, New York (1981)
295. Najman, F.: Integer points on two families of elliptic curves. Publ. Math. Debrecen **75**, 401–418 (2009)
296. Najman, F.: Compact representation of quadratic integers and integer points on some elliptic curves. Rocky Mountain J. Math. **40**, 1979–2002 (2010)
297. Najman, F.: Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. Math. Res. Letters **23**, 245–272 (2016)
298. Nguyen, P.Q., Stehlé, D.: An LLL algorithm with quadratic complexity. SIAM J. Comput. **39**, 874–903, (2009)
299. Nguyen, P.G., Vallee, B. (Eds.): The LLL Algorithm. Survey and Applications. Springer, Berlin (2010)
300. Niven, I., Zuckerman, H.S., Montgomery, H.L.: An Introduction to the Theory of Numbers. Wiley, New York (1991)
301. Nowicki, A.: Liczby Kwadratowe. Podróżze po Imperium Liczb 03. Olsztyn, Toruń (2011)
302. Ono, K.: Euler's concordant forms. Acta Arith. **78**, 101–123 (1996)
303. PARI Group, PARI/GP version 2.15.4. Bordeaux (2023) `http://pari.math.u-bordeaux.fr/`
304. Park, J., Poonen, B., Voight, J., Wood, M.M.: A heuristic for boundedness of ranks of elliptic curves, J. Eur. Math. Soc. (JEMS) **21**, 2859–2903 (2019)
305. Perron, O.: Die Lehre von den Kettenbruchen I, II. Teubner, Stuttgart (1954)
306. Petričević, V.: Personal communication (2019, 2022, 2023)
307. Piezas, T.: Extending rational Diophantine triples to sextuples. `http://mathoverflow.net/questions/233538/extending-rational-diophantine-triples-to-sextuples`
308. Rathbun, R.: Personal communication (2003)
309. Rickert, J.H.: Simultaneous rational approximations and related diophantine equations. Math. Proc. Cambridge Philos. Soc. **113**, 461–472 (1993)
310. Rihane, S.E., Luca, F., Togbé, A.: There are no Diophantine quadruples of Pell numbers. Int. J. Number Theory **18**, 27–45 (2022)
311. Rockett, A.M., Szusz, P.: Continued Fractions. World Scientific, Singapore (1992)
312. Rosser, J.B., Schoenfeld, L.: Approximate formulas for some functions of prime numbers. Illinois J. Math. **6**, 64–94 (1962)

313. Sadek, M., El-Sissi, N.: On large F-Diophantine sets. Monatsh. Math. **186**, 703–710 (2018)
314. Sadek, M., Yesin, T.: Divisibility by 2 on quartic models of elliptic curves and rational Diophantine $D(q)$-quintuples. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **116**, Article 139 (2022)
315. Sansone, G.: Il sistema diofanteo $N + 1 = x^2$, $3N + 1 = y^2$, $8N + 1 = z^2$, Ann. Mat. Pura Appl. (4) **111**, 125–151 (1976)
316. Schinzel, A.: Selected Topics on Polynomials. University of Michigan Press, Ann Arbor (1982)
317. Schinzel, A.: Polynomials with special regard to reducibility. Cambridge University Press, Cambridge (2000)
318. Schmidt, W.M.: Integer points on curves of genus 1. Compositio Math. **81**, 33–59 (1992)
319. Schmidt, W.M.: Diophantine Approximation. Springer-Verlag, Berlin (1996)
320. Schmidt, W.M.: Diophantine Approximation and Diophantine Equations. Springer-Verlag, Berlin (1996)
321. Schmitt, S., Zimmer, H.G.: Elliptic Curves. A Computational Approach. de Gruyter, Berlin (2003)
322. Schütt, M., Shioda, T.: Mordell-Weil Lattices. Springer, Singapore (2019)
323. Serre, J.-P.: A Course in Arithmetic. Springer-Verlag, New York (1996)
324. Shannon, A.G.: Fibonacci numbers and Diophantine quadruples: Generalizations of results of Morgado and Horadam. Portugaliae Math. **45**, 165-169 (1988)
325. Shockley, J.E.: Introduction to Number Theory. Holt, Rinehart and Winston, New York (1967)
326. Shorey, T.N.: Linear forms in the logarithms of algebraic numbers with small coefficients I, II. J. Indian Math. Soc. **38**, 271–292 (1974)
327. Shparlinski, I.E.: On the number of Diophantine m-tuples in finite fields. Finite Fields Appl. **90**, Paper No. 102241 (2023)
328. Silverman, J.H.: Computing heights on elliptic curves. Math. Comp. **51**, 339–358 (1988)
329. Silverman, J.H.: The difference between the Weil height and the canonical height on elliptic curves. Math. Comp. **55**, 723–743 (1990)
330. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves. Springer-Verlag, New York (1994)
331. Silverman, J.H.: The Arithmetic of Elliptic Curves. Springer, Dordrecht (2009)
332. Silverman, J.H., Tate, J.: Rational Points on Elliptic Curves. Springer, Cham (2015)
333. Skolem, T: Diophantische Gleichungen. Chelsea, New York (1950)
334. Smart, N.P.: The Algorithmic Resolution of Diophantine Equations. Cambridge University Press, Cambridge (1998)
335. Soldo, I.: On the existence of Diophantine quadruples in $\mathbb{Z}[\sqrt{-2}]$. Miskolc Math. Notes **14**, 265–277 (2013)
336. Srinivasan, A.: $D(-1)$-quadruples and products of two primes. Glas. Mat. Ser. III **50**, 261–268 (2015)
337. Stewart, C.L.: On sets of integers whose shifted products are powers. J. Combin. Theory Ser. A **115**, 662–673 (2008)
338. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer-Verlag, Berlin (1993)
339. Stoll, M.: On the average number of rational points on curves of genus 2. preprint (2009) arXiv: 0902.4165
340. Stoll, M.: Documentation for the ratpoints program. preprint (2013) arXiv: 0803.3165
341. Stoll, M.: Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational diophantine quintuples. Acta Arith. **190**, 239–261 (2019)
342. Stroeker, R.J., Tzanakis, N.: Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. Acta Arith. **67**, 177–196 (1994)
343. Tijdeman, R.: Diophantine equations and Diophantine approximations. In: Number theory and applications, pp. 215–243. Kluwer, Dordrecht (1989)
344. Trudgian, T.: Bounds on the number of Diophantine quintuples. J. Number Theory **157**, 233–249 (2015)

345. Tzanakis, N.: Explicit solution of a class of quartic Thue equations. Acta Arith. **64**, 271–283 (1993)
346. Tzanakis, N.: Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. Acta Arith. **75**, 165–190 (1996)
347. Tzanakis, N.: Elliptic Diophantine Equations. A Concrete Approach Via the Elliptic Logarithm. de Gruyter, Berlin (2013)
348. Udrea, Gh.: A note on the sequence (W_n) of A. F. Horadam. Portugaliae Math. **53**, 143–155 (1996)
349. Udrea, Gh.: A problem of Diophantus-Fermat and Chebyshev polynomials of the first kind. Rev. Roumaine Math. Pures Appl. **45**, 531–535 (2000)
350. Vajda, S.: Fibonacci & Lucas Numbers, and the Golden Section. Theory and Applications. Ellis Horwood, Chichester (1989)
351. Vellupillai, M.: The equations $z^2 - 3y^2 = -2$ and $z^2 - 6x^2 = -5$. In: Hoggatt, V.E., Bicknell-Johnson, M. (eds.) A Collection of Manuscripts Related to the Fibonacci Sequence, pp. 71–75. The Fibonacci Association, Santa Clara (1980)
352. Vinogradov, I.M.: Elements of Number Theory. Nauka, Moscow (1972) (in Russian)
353. Vorobiev, N.N.: Fibonacci Numbers. Birkhäuser, Basel (2002)
354. Voznyy, M.: Personal communication (2021, 2023)
355. Waldschmidt, M.: Open Diophantine problems. Moscow Math. J. **4**, 245–305 (2004)
356. Washington, L.C.: Elliptic Curves: Number Theory and Cryptography. CRC Press, Boca Raton (2008)
357. de Weger, B.M.M.: Algorithms for Diophantine Equations. Centrum voor Wiskunde en Informatica, Amsterdam (1989)
358. Weil, A: Number Theory: An Approach through History from Hammurapi to Legendre. Birkhäuser, Boston (1987)
359. Weintraub, S.H.: Factorization. Unique and Otherwise. CMS, Ottawa; A K Peters, Wellesley (2008)
360. Worley, R.T.: Estimating $|\alpha - p/q|$. Austral. Math. Soc. Ser. A **31**, 202–206 (1981)
361. Yip, C.H.: Multiplicatively reducible subsets of shifted perfect k-th powers and bipartite Diophantine tuples. preprint (2023) arXiv: 2312.14450
362. Zannier, U.: Some applications of Diophantine Approximation to Diophantine Equations. Forum Editrice, Udine (2003)
363. Zhang, Y., Grossman, G.: On Diophantine triples and quadruples. Notes Number Theory Discrete Math. **21(4)**, 6–16 (2015)
364. Zwegers, S.: On the associativity of the addition on elliptic curves. preprint (2024) arXiv: 2401.02346

Index