

Bibliography

- [1] A. Adler, J. E. Coury, *The Theory of Numbers. A Text and the Source Book of Problems*, Jones and Barlett Publishers, Sudbury, 1995.
- [2] N. M. Adrianov, F. Pakovich, A. K. Zvonkin, *Davenport-Zannier Polynomials and Dessins d'Enfants*, American Mathematical Society, Providence, 2020.
- [3] N. Adžaga, *Automated conjecturing of Frobenius numbers via grammatical evolution*, *Experiment. Math.* **26** (2017), 247–252.
- [4] N. Adžaga, *On the size of Diophantine m -tuples in imaginary quadratic number rings*, *Bull. Math. Sci.*, to appear.
- [5] N. Adžaga, A. Dujella, D. Kreso, P. Tadić, *Triples which are $D(n)$ -sets for several n 's*, *J. Number Theory* **184** (2018), 330–341.
- [6] M. Aigner, G. M. Ziegler, *Proofs from The Book*, Springer, Berlin, 2018.
- [7] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, *Ann. of Math. (2)* **160** (2004), 781–793.
- [8] J. Aguirre, A. Dujella, M. Jukić Bokun, J. C. Peral, *High rank elliptic curves with prescribed torsion group over quadratic fields*, *Period. Math. Hungar.* **68** (2014), 222–230.
- [9] S. Alaca, K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, Cambridge, 2004.
- [10] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, *Ann. of Math. (2)* **139** (1994), 703–722.
- [11] T. Andreescu, D. Andrica, Z. Feng, *104 Number Theory Problems From the Training of the USA IMO Team*, Birkhäuser, Boston, 2007.
- [12] T. Andreescu, D. Andrica, *Number Theory. Structures, Examples, and Problems*, Birkhäuser, Boston, 2009.
- [13] J. Arkin, V. E. Hoggatt, E. G. Strauss, *On Euler's solution of a problem of Diophantus*, *Fibonacci Quart.* **17** (1979), 333–339.

- [14] A. O. L. Atkin, F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, *Math. Comp.* **60** (1993), 399–405.
- [15] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, *Math. Comp.* **61** (1993), 29–68.
- [16] R. M. Avanzi, C. Heuberger, H. Prodinger, *Scalar multiplication on Koblitz curves using the Frobenius endomorphism and its combination with point halving: extensions and mathematical analysis*, *Algorithmica* **46** (2006), 249–270.
- [17] E. Bach, J. Shallit, *Algorithmic Number Theory, Volume I: Efficient Algorithms*, MIT Press, Cambridge, 1996.
- [18] Lj. Bačić, A. Filipin, *A note on the number of $D(4)$ -quintuples*, *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.* **18** (2014), 7–13.
- [19] D. Badziahin, J. Schleisitz, *An improved bound in Wirsing’s problem*, *Trans. Amer. Math. Soc.* **374** (2021), 1847–1861.
- [20] T. Baigneres, P. Junod, Y. Lu, J. Monnerat, S. Vaudenay, *A Classical Introduction to Cryptography Exercise Book*, Springer, New York, 2006.
- [21] A. Baker, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers*, *Quart. J. Math. Oxford Ser. (2)* **15** (1964), 375–383.
- [22] A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1990.
- [23] A. Baker, *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, Cambridge, 1994.
- [24] A. Baker, *A Comprehensive Course in Number Theory*, Cambridge University Press, Cambridge, 2012.
- [25] A. Baker, H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$* , *Quart. J. Math. Oxford Ser. (2)* **20** (1969), 129–137.
- [26] A. Baker, G. Wüstholz, *Logarithmic forms and group varieties*, *J. Reine Angew. Math.* **442** (1993), 19–62.
- [27] A. Baker, G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, Cambridge University Press, Cambridge, 2008.
- [28] M. W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, *Elementary Number Theory, Cryptography and Codes*, Springer, Berlin, 2009.
- [29] E.J. Barbeau, *Pell’s Equation*, Springer, New York, 2003.
- [30] P. T. Bateman, H. G. Diamond, *Analytic Number Theory. An Introductory Course*, World Scientific, Singapore, 2004.

- [31] R. Becker, M. Ram Murty, *Diophantine m -tuples with the property $D(n)$* , Glas. Mat. Ser. III **54** (2019), 65–75.
- [32] A. H. Beiler, *Recreations in the Theory of Numbers*, Dover, New York, 1966.
- [33] M. A. Bennett, *Explicit lower bounds for rational approximation to algebraic numbers*, Proc. London Math. Soc. (3) **75** (1997), 63–78.
- [34] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. **498** (1998), 173–199.
- [35] M. A. Bennett, M. Cipu, M. Mignotte, R. Okazaki, *On the number of solutions of simultaneous Pell equations. II*, Acta Arith. **122** (2006), 407–417.
- [36] A. Bérczes, A. Dujella, L. Hajdu, F. Luca, *On the size of sets whose elements have perfect power n -shifted products*, Publ. Math. Debrecen **79** (2011), 325–339.
- [37] A. Bérczes, A. Dujella, L. Hajdu and S. Tengely, *Finiteness results for F -Diophantine sets*, Monatsh. Math. **180** (2016), 469–484.
- [38] V. Beresnevich, V. Bernik, F. Götze, *The distribution of close conjugate algebraic numbers*, Compos. Math. **146** (2010), 1165–1179.
- [39] D. J. Bernstein, T. Lange, *Faster addition and doubling on elliptic curves*, Lecture Notes in Comput. Sci. **4833**, Springer, Berlin, 2007, pp. 29–50.
- [40] N. M. Beskin, *Fascinating Fractions*, Mir Publishers, Moscow, 1986.
- [41] F. Beukers, C. L. Stewart, *Neighboring powers*, J. Number Theory **130** (2010), 660–679.
- [42] Yu. F. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér, R. F. Tichy, *Diophantine equations and Bernoulli polynomials*, with an appendix by A. Schinzel, Compos. Math. **131** (2002), 173–188.
- [43] Yu. F. Bilu, G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392.
- [44] Yu. F. Bilu, G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, with an appendix by M. Mignotte, J. Reine Angew. Math. **539** (2001), 75–122.
- [45] Yu. F. Bilu, R. F. Tichy, *The Diophantine equation $f(x) = g(y)$* , Acta Arith. **95** (2000), 261–288.
- [46] B. J. Birch, S. Chowla, M. Hall, Jr., A. Schinzel, *On the difference $x^3 - y^2$* , Norske Vid. Selsk. Forh. **38** (1965), 65–69.
- [47] B. J. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.

- [48] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, Cambridge, 1999.
- [49] M. Bliznac Trebješanin, A. Filipin, *Nonexistence of $D(4)$ -quintuples*, *J. Number Theory* **194** (2019), 170–217.
- [50] S. Bohniček, *Criteria for solvability of the Diophantine equation $t^2 - Dy^2 = -1$* , *Rad JAZU Matematičko-prirodoslovnog razreda* **97** (1920), 49–82 (in Croatian).
- [51] M. Bombardelli, A. Dujella, S. Slijepčević, *Mathematical Competitions of High-school Students*, HMD, Element, Zagreb, 1996 (in Croatian).
- [52] E. Bombieri, W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, Cambridge, 2006.
- [53] N. C. Bonciocat, M. Cipu, M. Mignotte, *There is no Diophantine $D(-1)$ -quadruple*, preprint, 2020.
- [54] O. Bordelles, *Arithmetic Tales*, Springer, London, 2012.
- [55] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1986.
- [56] J. Bosman, P. Bruin, A. Dujella, F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, *Int. Math. Res. Not. IMRN* **2014** (11) (2014), 2885–2923.
- [57] A. Bremner, *On perfect K -rational cuboids*, *Bull. Aust. Math. Soc.* **97** (2018), 26–32.
- [58] E. Brown, *Sets in which $xy + k$ is always a square*, *Math. Comp.* **45** (1985), 613–620.
- [59] N. Budarina, D. Dickinson, *Simultaneous Diophantine approximation in two metrics and the distance between conjugate algebraic numbers in $\mathbb{C} \times \mathbb{Q}_p$* , *Indag. Math. (N.S.)* **23** (2012), 32–41.
- [60] D. A. Buell, *Binary Quadratic Forms*, Springer-Verlag, New York, 1989.
- [61] Y. Bugeaud, *Approximation by Algebraic Numbers*, Cambridge University Press, Cambridge, 2004.
- [62] Y. Bugeaud, *Linear Forms in Logarithms and Applications*, IRMA Lectures in Mathematics and Theoretical Physics Vol. **28**, European Mathematical Society, Zürich, 2018.
- [63] Y. Bugeaud, *Effective simultaneous rational approximation to pairs of real quadratic numbers*, *Moscow J. Comb. Number Theory* **9** (2020), 353–360.
- [64] Y. Bugeaud, A. Dujella, *On a problem of Diophantus for higher powers*, *Math. Proc. Cambridge Philos. Soc.* **135** (2003), 1–10.

- [65] Y. Bugeaud, A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. **43** (2011), 1239–1244.
- [66] Y. Bugeaud, A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. **162** (2014), 393–403.
- [67] Y. Bugeaud, A. Dujella, W. Fang, T. Pejković, B. Salvy, *Absolute root separation*, Experiment. Math., to appear.
- [68] Y. Bugeaud, A. Dujella, T. Pejković, B. Salvy, *Absolute real root separation*, Amer. Math. Monthly **124** (2017), 930–936.
- [69] Y. Bugeaud, M. Mignotte, *Polynomial root separation*, Intern. J. Number Theory **6** (2010), 587–602.
- [70] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), 969–1018.
- [71] S. Bujačić, A. Filipin, *Linear forms in logarithms*, Diophantine Analysis: Course Notes from a Summer School (J. Steuding, Ed.), Birkhäuser, Basel, 2016, pp. 1–59.
- [72] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer-Verlag, Berlin, 2008.
- [73] R. D. Carmichael, *The Theory of Numbers and Diophantine Analysis*, Dover, New York, 1959.
- [74] J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, Cambridge, 1995.
- [75] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Berlin, 1997.
- [76] J. S. Chahal, *Topics in Number Theory*, Plenum Press, New York, 1988.
- [77] H. H. Chan, *Analytic Number Theory for Undergraduates*, World Scientific, Singapore, 2009.
- [78] M. Cipu, Y. Fujita, T. Miyazaki, *On the number of extensions of a Diophantine triple*, Int. J. Number Theory **14** (2018), 899–917.
- [79] M. Cipu, T. Trudgian, *Searching for Diophantine quintuples*, Acta Arith. **173** (2016), 365–382.
- [80] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York, 1993.
- [81] H. Cohen, *Number Theory. Volume I: Tools and Diophantine Equations*, Springer Verlag, Berlin, 2007.

- [82] H. Cohen, *Number Theory. Volume II: Analytic and Modern Tools*, Springer Verlag, Berlin, 2007.
- [83] H. Cohn, *Advanced Number Theory*, Dover, New York, 1980.
- [84] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28.
- [85] J. H. E. Cohn, *The length of the period of the simple continued fraction of $d^{1/2}$* , Pacific J. Math. **71** (1977), 21–32.
- [86] A. C. Cojocaru, M. Ram Murti, *An Introduction to Sieve Methods and Their Applications*, Cambridge University Press, Cambridge, 2005.
- [87] I. Connell, *Elliptic Curve Handbook*, McGill University, Montreal, 1999.
- [88] J. H. Conway, R. K. Guy, *The book of numbers*, Copernicus, New York, 1996.
- [89] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology **10** (1997), 233–260.
- [90] P. Corvaja, *Integral Points on Algebraic Varieties*, Springer, Singapore, 2016.
- [91] D. A. Cox, *Primes of the Form $x^2 + ny^2$* , John Wiley & Sons, New York, 1989.
- [92] D. A. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, New York, 2007.
- [93] R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, New York, 2005.
- [94] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1997.
- [95] T. W. Cusick, M. E. Flahive, *The Markoff and Lagrange Spectra*, American Mathematical Society, Providence, 1989.
- [96] H. Čavrak, *Enigma*, math.e **3** (2004) (in Croatian).
- [97] A. Das, *Computational Number Theory*, CRC Press, Boca Raton, 2013.
- [98] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York, 1980.
- [99] H. Davenport, K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 160–167.
- [100] J.-M. De Koninck, F. Luca, *Analytic Number Theory. Exploring the Anatomy of Integers*, American Mathematical Society, Providence, 2012.
- [101] J.-M. De Koninck, A. Mercier, *1001 Problems in Classical Number Theory*, American Mathematical Society, Providence, 2007.

- [102] C. A. Deavours, L. Kruh, *Machine Cryptography and Modern Cryptanalysis*, Artech House, Norwood, 1985.
- [103] M. N. Deshpande, *One interesting family of diophantine triplets*, *Internat. J. Math. Ed. Sci. Tech.* **33** (2002), 253–256.
- [104] E. Deza, M. M. Deza, *Figurate Numbers*, World Scientific, Singapore, 2012.
- [105] L. E. Dickson, *History of the Theory of Numbers, Volume 2: Diophantine analysis*, Chelsea, New York, 1966.
- [106] R. Dietmann, C. Elsholtz, *Sums of two squares and one biquadrate*, *Funct. Approx. Comment. Math.* **38** (2008), 233–234.
- [107] A. Dubickas, *Polynomial root separation in terms of the Remak height*, *Turkish J. Math.* **37** (2013), 747–761.
- [108] A. Dubickas, M. Sha, *Counting and testing dominant polynomials*, *Exp. Math.* **24** (2015), 312–325.
- [109] A. Dujella, *Generalization of a problem of Diophantus*, *Acta Arith.* **65** (1993), 15–27.
- [110] A. Dujella, *Pythagorean triples*, *Bilten seminara iz matematike za nastavnike mentore*, Crikvenica, 1994, pp. 1–10 (in Croatian).
- [111] A. Dujella, *Introduction to Number Theory, lecture notes*, University of Zagreb, 1999 (in Croatian).
- [112] A. Dujella, *Continued fractions and the problem of the calendar*, *Matematika i škola 1* (1999), no. 2, 74–77 (in Croatian).
- [113] A. Dujella, *Fibonacci Numbers*, HMD, Zagreb, 2000 (in Croatian).
- [114] A. Dujella, *A parametric family of elliptic curves*, *Acta Arith.* **94** (2000), 87–101.
- [115] A. Dujella, *Newton's formula and continued fraction expansion of \sqrt{d}* , *Experiment. Math.* **10** (2001), 125–131.
- [116] A. Dujella, *On the size of Diophantine m -tuples*, *Math. Proc. Cambridge Philos. Soc.* **132** (2002), 23–33.
- [117] A. Dujella, *There are only finitely many Diophantine quintuples*, *J. Reine Angew. Math.* **566** (2004), 183–214.
- [118] A. Dujella, *Bounds for the size of sets with the property $D(n)$* , *Glas. Mat. Ser. III* **39** (2004), 199–205.
- [119] A. Dujella, *Continued fractions and RSA with small secret exponent*, *Tatra Mt. Math. Publ.* **29** (2004), 101–112.

- [120] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42** (2007), 3–18.
- [121] A. Dujella, *On the number of Diophantine m -tuples*, Ramanujan J. **15** (2008), 37–46.
- [122] A. Dujella, *Algorithms for Elliptic Curves*, lecture notes, University of Zagreb, 2009 (in Croatian).
- [123] A. Dujella, *A variant of Wiener's attack on RSA*, Computing **85** (2009), 77–83.
- [124] A. Dujella, *On Hall's conjecture*, Acta Arith. **147** (2011), 397–402.
- [125] A. Dujella, *What is ... a Diophantine m -tuple?*, Notices Amer. Math. Soc. **63** (2016), 772–774.
- [126] A. Dujella, *Diophantine m -tuples*
<https://web.math.pmf.unizg.hr/~duje/dtuples.html>
- [127] A. Dujella, *High rank elliptic curves with prescribed torsion*
<https://web.math.pmf.unizg.hr/~duje/tors/tors.html>
- [128] A. Dujella, *History of elliptic curves rank records*
<https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html>
- [129] A. Dujella, A. Filipin, C. Fuchs, *Effective solution of the $D(-1)$ -quadruple conjecture*, Acta Arith. **128** (2007), 319–338.
- [130] A. Dujella, C. Fuchs, *Complete solution of the polynomial version of a problem of Diophantus*, J. Number Theory **106** (2004), 326–344.
- [131] A. Dujella, C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71** (2005), 33–52.
- [132] A. Dujella, I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. (Oxford) **57** (2006), 193–201.
- [133] A. Dujella, I. Gusić, *Decomposition of a recursive family of polynomials*, Monatsh. Math. **152** (2007), 97–104.
- [134] A. Dujella, B. Ibrahimpašić, *On Worley's theorem in Diophantine approximations*, Ann. Math. Inform. **35** (2008), 61–73.
- [135] A. Dujella, B. Jadrijević, *A parametric family of quartic Thue equations*, Acta Arith. **101** (2002), 159–170.
- [136] A. Dujella, B. Jadrijević, *A family of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.
- [137] A. Dujella, A. S. Janfada, S. Salami, *A search for high rank congruent number elliptic curves*, J. Integer Seq. **12** (2009), Article 09.5.8.

- [138] A. Dujella, M. Jukić Bokun, I. Soldo, *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** (2017), 1177–1185.
- [139] A. Dujella, A. Jurasić, *On the size of sets in a polynomial variant of a problem of Diophantus*, Int. J. Number Theory **6** (2010), 1449–1471.
- [140] A. Dujella, M. Kazalicki, *More on Diophantine sextuples*, Number Theory - Diophantine problems, uniform distribution and applications, Festschrift in honour of Robert F. Tichy's 60th birthday (C. Elsholtz, P. Grabner, Eds.), Springer-Verlag, Cham, 2017, pp. 227–235.
- [141] A. Dujella, M. Kazalicki, *Diophantine m -tuples in finite fields and modular forms*, Res. Number Theory **7** (2021), Article 3.
- [142] A. Dujella, M. Kazalicki, V. Petričević, *There are infinitely many rational Diophantine sextuples with square denominators*, J. Number Theory **205** (2019), 340–346.
- [143] A. Dujella, M. Kazalicki, V. Petričević, *Rational Diophantine sextuples containing two regular quadruples and one regular quintuple*, Acta Mathematica Spalatensia **1** (2020), 19–27.
- [144] A. Dujella, M. Kazalicki, V. Petričević, *$D(n)$ -quintuples with square elements*, preprint, 2020.
- [145] A. Dujella, M. Kazalicki, M. Mikić, M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN **2017** (2) (2017), 490–508.
- [146] A. Dujella, F. Luca, *Diophantine m -tuples for primes*, Int. Math. Res. Not. **47** (2005), 2913–2940.
- [147] A. Dujella, M. Maretić, *Cryptography*, Element, Zagreb, 2007 (in Croatian).
- [148] A. Dujella, M. Mikić, *On the torsion group of elliptic curves induced by $D(4)$ -triples*, An. Ştiinţ. Univ. “Ovidius” Constanţa Ser. Mat. **22** (2014), 79–90.
- [149] A. Dujella, F. Najman, *Elliptic curves with large torsion and positive rank over number fields of small degree and ECM factorization*, Period. Math. Hungar. **65** (2012), 193–203.
- [150] A. Dujella, M. Paganin, M. Sadek, *Strong rational Diophantine $D(q)$ -triples*, Indag. Math. (N.S.) **31** (2020), 505–511.
- [151] A. Dujella, T. Pejković, *Root separation for reducible monic quartics*, Rend. Semin. Mat. Univ. Padova **126** (2011), 63–72.
- [152] A. Dujella, J. C. Peral, *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** (2014), 282–288.

- [153] A. Dujella, J. C. Peral, *Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$* , Trends in Number Theory, Contemp. Math. **649** (2015), 47–62.
- [154] A. Dujella, J. C. Peral, *Elliptic curves induced by Diophantine triples*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **113** (2019), 791–806.
- [155] A. Dujella, J. C. Peral, *High rank elliptic curves induced by rational Diophantine triples*, Glas. Mat. Ser. III **55** (2020), 237–252.
- [156] A. Dujella, J. C. Peral, *Construction of high rank elliptic curves*, J. Geom. Anal., to appear.
- [157] A. Dujella, A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.
- [158] A. Dujella, A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), 321–335.
- [159] A. Dujella, V. Petričević, *Square roots with many good approximants*, Integers **5(3)** (2005), #A6. (13pp)
- [160] A. Dujella, V. Petričević, *Strong Diophantine triples*, Experiment. Math. **17** (2008), 83–89.
- [161] A. Dujella, V. Petričević, *Diophantine quadruples with the properties $D(n_1)$ and $D(n_2)$* , Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **114** (2020), Article 21.
- [162] A. Dujella, V. Petričević, *Doubly regular Diophantine quadruples*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **114** (2020), Article 189.
- [163] A. Dujella, A. M. S. Ramasamy, *Fibonacci numbers and sets with the property $D(4)$* , Bull. Belg. Math. Soc. Simon Stevin **12** (2005), 401–412.
- [164] A. Dujella, N. Saradha, *Diophantine m -tuples with elements in arithmetic progressions*, Indag. Math. (N.S.) **25** (2014), 131–136.
- [165] A. Dujella, R. F. Tichy, *Diophantine equations for second order recursive sequences of polynomials*, Quart. J. Math. Oxford Ser. (2) **52** (2001), 161–169.
- [166] H. M. Edwards, *Riemann's Zeta Function*, Academic Press, New York, 1974.
- [167] H. M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), 393–422.
- [168] N. Elezović, *A note on continued fractions of quadratic irrationals*, Math. Commun. **2** (1997), 27–33.
- [169] N. Elezović, *DisCont Mathematics 1*, Element, Zagreb, 2017 (in Croatian)
- [170] N. D. Elkies, *On $A^4 + B^4 + C^4 = D^4$* , Math. Comp. **51** (1988), 825–835.

- [171] N. D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction*, Lecture Notes in Comput. Sci. **1838**, Springer, Berlin, 2000, pp. 33–63.
- [172] N. D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, lecture notes, Oberwolfach, 2007.
- [173] N. D. Elkies, Z. Klagsbrun, *New rank records for elliptic curves having rational torsion*, Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Mathematical Sciences Publishers, Berkeley, 2020, pp. 233–250.
- [174] A. Enge, *Elliptic Curves and Their Applications to Cryptography. An Introduction*, Kluwer, Boston, 1999.
- [175] P. Erdős, *Beweis eines Satzes von Tschebyschef*, Acta Sci. Math. (Szeged) **5** (1930–1932), 194–198.
- [176] G. Everest, T. Ward, *An Introduction to Number Theory*, Springer-Verlag, London, 2005.
- [177] J.-H. Evertse, K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge University Press, Cambridge, 2015.
- [178] J.-H. Evertse, K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge University Press, Cambridge, 2017.
- [179] A. Filipin, *Application of LLL-algorithm in Solving Diophantine Equations*, Master Thesis, University of Zagreb, 2004 (in Croatian).
- [180] A. Filipin, *There does not exist a $D(4)$ -sextuple*, J. Number Theory **128** (2008), 1555–1565.
- [181] A. Filipin, *Linear forms in logarithms and Diophantine analysis*, lecture notes, Algorithms for Elliptic Curves, 2010 (in Croatian).
- [182] A. Filipin, Z. Franušić, *Diophantine sets*, lecture notes, University of Zagreb, 2020 (in Croatian).
- [183] A. Filipin, A. Jursić, *A polynomial variant of a problem of Diophantus and its consequences*, Glas. Mat. Ser. III **54** (2019), 21–52.
- [184] B. Fine, A. Gaglione, A. Moldenhauer, G. Rosenberger, D. Spellman, *Algebra and Number Theory. A Selection of Highlights*, De Gruyter, Berlin, 2017.
- [185] Z. Franušić, *Diophantine quadruples in $\mathbb{Z}[\sqrt{4k+3}]$* , Ramanujan J. **17** (2008), 77–88.
- [186] Z. Franušić, *A Diophantine problem in $\mathbb{Z}[(1+\sqrt{d})/2]$* , Studia Sci. Math. Hungar. **46** (2009), 103–112.
- [187] Z. Franušić, I. Soldo, *The problem of Diophantus for integers of $\mathbb{Q}(\sqrt{-3})$* , Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **18** (2014), 15–25.

- [188] Y. Fujita, T. Miyazaki, *The regularity of Diophantine quadruples*, Trans. Amer. Math. Soc. **370** (2018), 3803–3831.
- [189] I. Gaál, *Diophantine Equations and Power Integral Bases*, Birkhäuser, Boston, 2002.
- [190] I. Gaál, A. Pethő, M. Pohst, *On the resolution of index form equations in biquadratic number fields III. The bicyclic biquadratic case*, J. Number Theory **53** (1995), 100–114.
- [191] M. Gardner, *Mathematical Magic Show*, Alfred Knopf, New York, 1977.
- [192] J. Gebel, A. Pethő, H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.
- [193] J. Gebel, A. Pethő, H. G. Zimmer, *On Mordell's equation*, Compositio Math. **110** (1998), 335–367.
- [194] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.
- [195] P. Gibbs, *A survey of rational Diophantine sextuples of low height*, preprint, 2016.
- [196] F. Q. Gouvêa, *p -adic Numbers. An Introduction*, Springer, Berlin, 2003.
- [197] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics - A foundation for computer science*, Addison-Wesley, Reading, 1989.
- [198] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, CMS Conf. Proc. **20**, American Mathematical Society, Providence, 1997, pp. 253–276.
- [199] A. Granville, *Number Theory Revealed: A Masterclass*, American Mathematical Society, Providence, 2019.
- [200] Great Internet Mersenne Prime Search (GIMPS)
<https://www.mersenne.org/>
- [201] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), 481–547.
- [202] P. M. Gruber, C. G. Lekkerkerker, *Geometry of Numbers*, North Holland, Amsterdam, 1987.
- [203] I. Gusić, *Introduction to Arithmetic of Elliptic Curves*, lecture notes, University of Zagreb, 2008 (in Croatian).
- [204] I. Gusić, *On decomposition of polynomials over rings*, Glas. Mat. Ser. III **43** (2008), 7–12.
- [205] I. Gusić, P. Tadić, *A remark on the injectivity of the specialization homomorphism*, Glas. Mat. Ser. III **47** (2012), 265–275.

- [206] I. Gusić, P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory **148** (2015), 137–152.
- [207] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 2004.
- [208] K. Gyarmati, C. L. Stewart, *On powers in shifted products*, Glas. Mat. Ser. III **42** (2007), 273–279.
- [209] J. Hadamard, *Lessons in geometry. I. Plane geometry*, American Mathematical Society, Providence, 2008.
- [210] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, 2004.
- [211] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 2008.
- [212] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), 6665–6709.
- [213] T. L. Heath, *Diophantus of Alexandria: A study in the history of Greek Algebra*, Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003.
- [214] Y. Hellegouarch, *Invitation to the Mathematics of Fermat-Wiles*, Academic Press, San Diego, 2002.
- [215] D. Hensley, *Continued Fractions*, World Scientific, Singapore, 2006.
- [216] J. Herman, R. Kučera, J. Šimša, *Equations and Inequalities. Elementary Problems and Theorems in Algebra and Number Theory*, Springer, New York, 2000.
- [217] M. Hidry, J. H. Silverman, *Diophantine Geometry. An Introduction*, Springer-Verlag, New York, 2000.
- [218] M. J. Hinek, *Cryptanalysis of RSA and Its Variants*, CRC Press, Boca Raton, 2009.
- [219] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, New York, 2008.
- [220] V. E. Hoggatt, Jr., *Fibonacci and Lucas Numbers*, The Fibonacci Association, Santa Clara, 1979.
- [221] V. E. Hoggatt, G. E. Bergum, *A problem of Fermat and the Fibonacci sequence*, Fibonacci Quart. **15** (1977), 323–330.
- [222] A. F. Horadam, *Fibonacci number triples*, Amer. Math. Monthly **68** (1961), 751–753.
- [223] K. Horvatić, *Linear Algebra*, Golden Marketing - Tehnička knjiga, Zagreb, 2004 (in Croatian).

- [224] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
- [225] D. Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 2004.
- [226] B. Hutz, *An Experimental Introduction to Number Theory*, American Mathematical Society, Providence, 2018.
- [227] B. Ibrahimpašić, *Cryptography through Examples*, University of Bihać, 2011 (in Bosnian).
- [228] B. Ibrahimpašić, *Introduction to Number Theory*, University of Bihać, 2014 (in Bosnian).
- [229] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1998.
- [230] M. J. Jacobson, H. C. Williams, *Modular arithmetic on elements of small norm in quadratic fields*, *Des. Codes and Cryptogr.* **27** (2002), 93–110.
- [231] M. J. Jacobson, H. C. Williams, *Solving the Pell Equation*, Springer, New York, 2009.
- [232] B. Jadrijević, *A Two-parametric Family of Quartic Thue Equations*, Ph.D. Dissertation, University of Zagreb, 2001 (in Croatian).
- [233] B. Jadrijević, V. Ziegler, *A system of relative Pellian equations and a related family of relative Thue equations*, *Int. J. Number Theory* **2** (2006), 569–590.
- [234] G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
- [235] D. Jao, L. De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, *Post-quantum cryptography*, *Lecture Notes in Comput. Sci.* **7071**, Springer, Heidelberg, 2011, pp. 19–34.
- [236] B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, The Mathematical Association of America, New York, 1950.
- [237] B. W. Jones, *A variation on a problem of Davenport and Diophantus*, *Quart. J. Math. Oxford Ser. (2)* **27** (1976), 349–353.
- [238] A. Jurasić, *Diophantine Equations over Function Fields*, Master Thesis, University of Zagreb, 2006 (in Croatian).
- [239] D. Kahn, *The Codebreakers. The Story of Secret Writing*, Scribner, New York, 1996.
- [240] S. Kamienny, *Torsion points on elliptic curves and q -coefficients of modular forms*, *Invent. Math.* **109** (1992), 221–229.
- [241] M. Kazalicki, *Modular forms, lecture notes*, University of Zagreb, 2017 (in Croatian).
- [242] H. L. Keng, *Introduction to Number Theory*, Springer-Verlag, Berlin, 1982.

- [243] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
- [244] M. Kiseljak, Contributions to the theory of perfect numbers, Kr. zemaljska tiskara, Zagreb, 1911 (in Croatian).
- [245] A. Ya. Khinchin, Continued Fractions, Dover, New York, 1997.
- [246] A. Kihel, O. Kihel, *On the intersection and the extendibility of P_t -sets*, Far East J. Math. Sci. **3** (2001), 637–643.
- [247] Z. Klagsbrun, T. Sherman, J. Weigandt, *The Elkies curve has rank 28 subject only to GRH*, Math. Comp. **88** (2019), 837–846.
- [248] A. W. Knap, Elliptic Curves, Princeton University Press, Princeton, 1992.
- [249] D. Knuth, The Art of Computer Programming, Vol. 2, Seminumerical Algorithms, Addison-Wesley, Reading, 1981.
- [250] N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, New York, 1994.
- [251] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1996.
- [252] N. Koblitz, p -adic Numbers, p -adic Analysis, and Zeta Functions, Springer-Verlag, New York, 1996.
- [253] T. Koshy, Fibonacci and Lucas Numbers with Applications, Wiley, New York, 2001.
- [254] J. S. Kraft, L. C. Washington, An Introduction to Number Theory with Cryptography, CRC Press, Boca Raton, 2018.
- [255] H. Kraljević, Selected Topics of the Theory of Analytic Functions, lecture notes, University of Zagreb, 2010 (in Croatian).
- [256] H. Kraljević, S. Kurepa, Mathematical Analysis 4 - Functions of a Complex Variable, Tehnička knjiga, Zagreb, 1979 (in Croatian).
- [257] E. Kranakis, Primality and Cryptography, Teubner, Stuttgart; Wiley, Chichester, 1986.
- [258] D. Kreso, Rational function decomposition and Diophantine equations, Ph.D. Dissertation, Graz University of Technology, Graz, 2014.
- [259] D. Kreso, R. Tichy, *Functional composition of polynomials: indecomposability, Diophantine equations and lacunary polynomials*, Grazer Math. Ber. **363** (2015), 143-170.
- [260] M. Křížek, F. Luca, L. Somer, 17 Lectures on Fermat Numbers, Springer-Verlag, New York, 2001.

- [261] L. Kulesz, *Families of elliptic curves of high rank with nontrivial torsion group over \mathbb{Q}* , Acta Arith. **108** (2003), 339–356.
- [262] S. Kurepa, *Mathematical Analysis 2*, Školska knjiga, Zagreb, 1987 (in Croatian).
- [263] E. Landau, *Elementary Number Theory*, Chelsea, New York, 1966.
- [264] E. Landau, *Foundations of Analysis*, Chelsea, New York, 1966.
- [265] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, 1966.
- [266] S. Lang, *Elliptic Curves. Diophantine Analysis*, Springer-Verlag, Berlin, 1978.
- [267] S. Lang, *Algebra*, Springer-Verlag, New York, 2002.
- [268] L. Lasić, *Heights in Diophantine Geometry and Consequences of the abc-conjecture*, Master Thesis, University of Zagreb, 2009 (in Croatian).
- [269] O. Lecacheux, *Rang de courbes elliptiques sur \mathbb{Q} avec un groupe de torsion isomorphe à $\mathbb{Z}/5\mathbb{Z}$* , C. R. Acad. Sci. Paris Ser. I Math. **332** (2001), 1–6.
- [270] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer, Berlin, 2000.
- [271] A. K. Lenstra, H. W. Lenstra, Jr., L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
- [272] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673.
- [273] W. J. LeVeque, *Topics in Number Theory I, II*, Dover, New York, 1984.
- [274] W. J. LeVeque, *Fundamentals of Number Theory*, Dover, New York, 1996.
- [275] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials*, Longman, Essex, 1993.
- [276] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
- [277] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin, 1999.
- [278] W. Ljunggren, *On the Diophantine equation $x^2 + 4 = Ay^4$* , Norske Vid. Selsk. Forh. **24** (1951), 82–84.
- [279] L. Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*, SIAM, Philadelphia, 1986.
- [280] A. Lozano-Robledo, *Elliptic Curves, Modular Forms and their L -functions*, American Mathematical Society, Providence, 2011.

- [281] F. Luca, *On shifted products which are powers*, Glas. Mat. Ser. III **40** (2005), 13–20.
- [282] F. Luca, *Exponential Diophantine equations*, Notes from the International Autumn School on Computational Number Theory, Birkhäuser, Cham, 2019, pp. 267–309.
- [283] F. Luca, C. F. Osgood, P. G. Walsh, *Diophantine approximations and a problem from the 1988 IMO*, Rocky Mountain J. Math. **36** (2006), 637–648.
- [284] F. Luca, L. Szalay, *Fibonacci Diophantine triples*, Glas. Mat. Ser. III **43** (2008), 253–264.
- [285] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.
- [286] K. Mahler, *p -adic Numbers and Their Functions*, Cambridge University Press, Cambridge, 1981.
- [287] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.
- [288] S. Mardešić, *Mathematical Analysis 1*, Školska knjiga, Zagreb, 1988 (in Croatian).
- [289] A. I. Markushevich, *Theory of functions of a complex variable*. Vol. I, II, III, Translated and edited by R. A. Silverman, Prentice-Hall, Englewood Cliffs, 1965.
- [290] G. Martin, S. Sitar, *Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples*, Matematika **57** (2011), 1–29.
- [291] D. Masser, *Auxiliary Polynomials in Number Theory*, Cambridge University Press, Cambridge, 2016.
- [292] I. Matić, *Introduction to Number Theory*, Josip Juraj Strossmayer University of Osijek, Osijek, 2015 (in Croatian).
- [293] K. R. Matthews, J. P. Robertson, J. White, *On a Diophantine equation of Andrej Dujella*, Glas. Mat. Ser. III **48** (2013), 265–289.
- [294] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Math. **64** (2000), 1217–1269.
- [295] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
- [296] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

- [297] J. McKee, C. Smyth (Eds.), *Number Theory and Polynomials*, Cambridge University Press, Cambridge, 2008.
- [298] E. Mendelson, *Introduction to Mathematical Logic*, CRC Press, Boca Raton, 2015.
- [299] J.-F. Mestre, *Construction de courbes elliptiques sur \mathbb{Q} de rang = 12*, C. R. Acad. Sci. Paris Ser. I **295**, (1982), 643–644.
- [300] J.-F. Mestre, *Courbes elliptiques de rang ≥ 11 sur $\mathbb{Q}(t)$* , C. R. Acad. Sci. Paris Ser. I **313** (1991), 139–142.
- [301] M. Mignotte, *Some useful bounds*, Computer algebra (B. Buchberger, G. E. Collins, R. Loos, R. Albrecht, Eds.), Springer-Verlag, Vienna, 1983, pp. 259–263.
- [302] M. Mignotte, D. Stefanescu, *Polynomials. An Algorithmic Approach*, Springer-Verlag, Singapore, 1999.
- [303] M. Mihaljinec, *A contribution to Fermat's problem*, Glasnik mat.–fiz. i astr. **7** (1952), 12–18 (in Croatian).
- [304] M. Mikić, *On the Mordell-Weil group of elliptic curves induced by families of Diophantine triples*, Rocky Mountain J. Math. **45** (2015), 1565–1589.
- [305] J. Mikusiński, *Sur la méthode d'approximation de Newton*, Ann. Polon. Math. **1** (1954), 184–194.
- [306] J. S. Milne, *Elliptic Curves*, BookSurge Publishers, Charleston, 2006.
- [307] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, 1996.
- [308] H. L. Montgomery, R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge University Press, Cambridge, 2007.
- [309] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), 243–264.
- [310] V. K. Mootha, G. Berzsényi, *Characterizations and extendibility of P_t -sets*, Fibonacci Quart. **27** (1989), 287–288.
- [311] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.
- [312] J. Morgado, *Some remarks on an identity of Catalan concerning the Fibonacci numbers*, Portugaliae Math. **39** (1980), 341–348.
- [313] G. Muić, *Algebraic Curves*, lecture notes, University of Zagreb, 2016 (in Croatian).
- [314] K. Nagao, *An example of elliptic curve over \mathbb{Q} with rank = 20*, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), 291–293.
- [315] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1981.

- [316] F. Najman, *Integer points on two families of elliptic curves*, Publ. Math. Debrecen **75** (2009), 401–418.
- [317] F. Najman, *Compact representation of quadratic integers and integer points on some elliptic curves*, Rocky Mountain J. Math. **40** (2010), 1979–2002.
- [318] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory **130** (2010), 1964–1968.
- [319] F. Najman, *Elliptic curves over number fields*, lecture notes, University of Zagreb, 2013 (in Croatian).
- [320] F. Najman, *Some rank records for elliptic curves with prescribed torsion over quadratic fields*, An. Ştiinţ. Univ. “Ovidius” Constanţa Ser. Mat. **22** (2014), 215–220.
- [321] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$* , Math. Res. Letters **23** (2016), 245–272.
- [322] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw, 1974; Springer, Berlin, 2004.
- [323] W. Narkiewicz, *Classical Problems in Number Theory*, PWN, Warsaw, 1986.
- [324] B. Nathanson, *Additive Number Theory. The Classical Bases*, Springer-Verlag, New York, 1996.
- [325] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.
- [326] P. Q. Nguyen, B. Vallee (Eds.), *The LLL Algorithm. Survey and Applications*, Springer, Berlin, 2010.
- [327] I. Niven, *Diophantine Approximations*, Wiley, New York, 1963.
- [328] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, New York, 1991.
- [329] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q -series*, American Mathematical Society, Providence, 2004.
- [330] O. Ore, *Number Theory and Its History*, Dover, New York, 1988.
- [331] PARI Group, PARI/GP version 2.14.0, Bordeaux, 2021,
<http://pari.math.u-bordeaux.fr/>
- [332] J. Park, B. Poonen, J. Voight, M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), 2859–2903.
- [333] S. J. Patterson, *An Introduction to the Theory of the Riemann Zeta-Function*, Cambridge University Press, Cambridge, 1995.
- [334] B. Pavković, B. Dakić, *Polynomials*, Školska knjiga, Zagreb, 1990 (in Croatian).

- [335] B. Pavković, B. Dakić, P. Mladinić, Elementary Number Theory, HMD, Element, Zagreb, 1994 (in Croatian).
- [336] B. Pavković, D. Veljan, Elementary Mathematics 1, Tehnička knjiga, Zagreb, 1992 (in Croatian).
- [337] B. Pavković, D. Veljan, Elementary Mathematics 2, Školska knjiga, Zagreb, 1995 (in Croatian).
- [338] T. Pejšković, Irrational Numbers, HMD, Zagreb, 2001 (in Croatian).
- [339] T. Pejšković, Roth's Theorem, Graduation Thesis, University of Zagreb, 2005 (in Croatian).
- [340] T. Pejšković, *p-adic root separation for quadratic and cubic polynomials*, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **20** (2016), 9–18.
- [341] O. Perron, Die Lehre von den Kettenbrüchen I, II, Teubner, 1954.
- [342] A. Pethő, Algebraische Algorithmen, Vieweg, Braunschweig, 1999.
- [343] V. Petričević, Continued Fraction Convergents and Newton's Approximants for Quadratic Irrationalities, Ph.D. Dissertation, University of Zagreb, 2011 (in Croatian).
- [344] H. Pollard, H. G. Diamond, The Theory of Algebraic Numbers, Dover, New York, 1998.
- [345] V. V. Prasolov, Polynomials, Springer, Berlin, 2004.
- [346] M. Ram Murty, Problems in Analytic Number Theory, Springer, New York, 2008.
- [347] M. Ram Murty, J. Esmonde, Problems in Algebraic Number Theory, Springer, New York, 2005.
- [348] J. L. Ramirez Alfonsin, The Diophantine Frobenius Problem, Oxford University Press, Oxford, 2005.
- [349] P. Ribenboim, The Book of Prime Number Records, Springer-Verlag, New York, 1988.
- [350] J. H. Rickert, *Simultaneous rational approximations and related Diophantine equations*, Math. Proc. Cambridge Philos. Soc. **113** (1993), 461–472.
- [351] H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhäuser, Boston, 1994.
- [352] J. Roberts, Elementary Number Theory. A Problem Oriented Approach, MIT Press, Cambridge, 1977.
- [353] A. M. Rockett, P. Szusz, Continued Fractions, World Scientific, Singapore, 1992.

- [354] H. E. Rose, *A Course in Number Theory*, Oxford University Press, Oxford, 1995.
- [355] K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, 1993.
- [356] M. Sadek, N. El-Sissi, *On large F -Diophantine sets*, *Monatsh. Math.* **186** (2018), 703–710.
- [357] P. Samuel, *Algebraic Theory of Numbers*, Hermann, Paris, 1970.
- [358] A. Schinzel, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge, 2000.
- [359] W. M. Schmidt, *Diophantine Approximation*, Springer-Verlag, Berlin, 1996.
- [360] W. M. Schmidt, *Diophantine Approximation and Diophantine Equations*, Springer-Verlag, Berlin, 1996.
- [361] S. Schmitt, H. G. Zimmer, *Elliptic Curves. A Computational Approach*, de Gruyter, Berlin, 2003.
- [362] M. Schütt, T. Shioda, *Mordell-Weil Lattices*, Springer, Singapore, 2019.
- [363] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1996.
- [364] J. E. Shockley, *Introduction to Number Theory*, Holt, Rinehart and Winston, New York, 1967.
- [365] T. N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.
- [366] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, 2009.
- [367] I. E. Shparlinski, *Finite Fields: Theory and Computation. The Meeting Point of Number Theory, Computer Science, Coding Theory and Cryptography*, Kluwer, Dordrecht, 1999.
- [368] W. Sierpiński, *250 Problems in Elementary Number Theory*, PWN, Warsaw; Elsevier, New York, 1970.
- [369] W. Sierpiński, *Elementary Theory of Numbers*, PNW, Warsaw; North Holland, Amsterdam, 1987.
- [370] W. Sierpiński, *Pythagorean Triangles*, Dover, New York, 2003.
- [371] J. H. Silverman, *Computing heights on elliptic curves*, *Math. Comp.* **51** (1988), 339–358.
- [372] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

- [373] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Dordrecht, 2009.
- [374] J. H. Silverman, *Lifting and Elliptic Curve Discrete Logarithms*, Lecture Notes in Comput. Sci. **5381**, Springer, Berlin, 2009, pp. 82–102.
- [375] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer, Cham, 2015.
- [376] S. Singh, *The Code Book*, Fourth Estate, London, 1999.
- [377] J. L. Slater, *Generalized Hypergeometric Functions*, Cambridge University Press, Cambridge, 1966.
- [378] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, Cambridge, 1998.
- [379] N. P. Smart, *Cryptography. An Introduction*, McGraw-Hill, New York, 2002.
- [380] J. Solinas, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.
- [381] I. S. Sominski, *The Method of Mathematical Induction*, Mir Publishers, Moscow, 1975.
- [382] V. G. Sprindžuk, *Classical Diophantine Equations*, Springer, Berlin, 1993.
- [383] H. M. Stark, *An Introduction to Number Theory*, MIT Press, Cambridge, 1998.
- [384] H. M. Stark, *The Gauss class-number problems*, Analytic Number Theory. A Tribute to Gauss and Dirichlet (W. Duke, Y. Tschinkel, Eds.), American Mathematical Society, Providence, 2007.
- [385] J. Steuding, *Diophantine Analysis*, CRC Press, Boca Raton, 2005.
- [386] C. L. Stewart, *Linear Forms in Logarithms and Diophantine Equations*, lecture notes, University of Waterloo, 2005.
- [387] I. Stewart, D. Tall, *Algebraic Number Theory and Fermat’s Last Theorem*, A K Peters, Natick, 2002.
- [388] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.
- [389] D. R. Stinson, *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 2005.
- [390] M. Stoll, *Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational diophantine quintuples*, Acta Arith. **190** (2019), 239–261.
- [391] Th. Stoll, *Complete decomposition of Dickson-type polynomials and related Diophantine equations*, J. Number Theory **128** (2008), 1157–1181.

- [392] V. Stošić, *Mathematical Competitions of Primary School Students*, HMD, Element, Zagreb, 1994 (in Croatian).
- [393] R. J. Stroeker, N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, *Acta Arith.* **67** (1994), 177–196.
- [394] M. V. Subbarao, *On two congruences for primality*, *Pacific J. Math.* **52** (1974), 261–268.
- [395] Z. Šikić, Z. Šćekić, *Mathematics and Music*, Profil, Zagreb, 2013 (in Croatian).
- [396] B. Širola, *Distribution of primes and the Riemann zeta-function*, *math.e* **13** (2008) (in Croatian).
- [397] B. Širola, *Algebraic Structures*, lecture notes, University of Zagreb, 2008 (in Croatian).
- [398] R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory. Right Triangles, Sums of Squares, and Arithmetic*, Springer, Cham, 2018.
- [399] R. Tijdeman, *Diophantine equations and Diophantine approximations*, *Number theory and applications*, Kluwer, Dordrecht, 1989, pp. 215–243.
- [400] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Clarendon Press, Oxford, 1986.
- [401] A. Trbović, *Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$* , *Acta Arith.* **192** (2020), 141–153.
- [402] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight $3/2$* , *Invent. Math.* **72** (1983), 323–334.
- [403] N. Tzanakis, *Explicit solution of a class of quartic Thue equations*, *Acta Arith.* **64** (1993), 271–283.
- [404] N. Tzanakis, *Elliptic Diophantine Equations. A Concrete Approach Via the Elliptic Logarithm*, de Gruyter, Berlin, 2013.
- [405] D. Ugrin-Šparac, *A view on the contemporary number theory*, *Numbers*, Školska knjiga, Zagreb, 1985 (in Croatian).
- [406] Š. Ungar, *Mathematical Analysis 4*, lecture notes, University of Zagreb, 2008 (in Croatian).
- [407] S. Vajda, *Fibonacci & Lucas Numbers, and the Golden Section. Theory and Applications*, Ellis Horwood, Chichester, 1989.
- [408] I. Vidav, *Elliptic Curves and Elliptic Functions*, Society of mathematicians, physicists and astronomers of Slovenia, Ljubljana, 1991 (in Slovenian).
- [409] I. M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.

- [410] N. N. Vorobiev, *Fibonacci Numbers*, Birkhäuser, Basel, 2002.
- [411] P. M. Voutier, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers revisited*, *J. Théor. Nombres Bordeaux* **19** (2007), 263–288.
- [412] M. Vuković, *Mathematical Logic, Element*, Zagreb, 2009 (in Croatian).
- [413] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Springer-Verlag, Berlin, 2000.
- [414] D. D. Wall, *Fibonacci series modulo m* , *Amer. Math. Monthly* **67** (1960), 525–532.
- [415] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, 2008.
- [416] B. M. M. de Weger, *Algorithms for Diophantine Equations*, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.
- [417] S. H. Weintraub, *Factorization. Unique and Otherwise*, CMS, Ottawa; A K Peters, Wellesley, 2008.
- [418] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, *IEEE Trans. Inform. Theory* **36** (1990), 553–558.
- [419] H. Williams, *Solving the Pell equation*, *Number Theory for the Millennium III*, A K Peters, Natick, 2002, pp. 397–435.
- [420] R. T. Worley, *Estimating $|\alpha - p/q|$* , *Austral. Math. Soc. Ser. A* **31** (1981), 202–206.
- [421] D. Wright, *Mathematics and Music*, American Mathematical Society, Providence, 2009.
- [422] S. Y. Yan, *Quantum Attacks on Public-Key Cryptosystems*, Springer, New York, 2013.
- [423] U. Zannier, *On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's Existence Theorem*, *Acta Arith.* **71** (1995), 103–137.
- [424] U. Zannier, *Some applications of Diophantine Approximation to Diophantine Equations*, Forum Editrice, Udine, 2003.
- [425] Y. Zhang, G. Grossman, *On Diophantine triples and quadruples*, *Notes Number Theory Discrete Math.* **21** (2015), 6–16.
- [426] V. Zorich, *Mathematical Analysis I*, Springer Verlag, Berlin, 2015.

Notation Index

\mathbb{N}	set of positive integers
\mathbb{Z}	set of integers
\mathbb{Q}	set of rational numbers
\mathbb{R}	set of real numbers
\mathbb{C}	set of complex numbers
\square	symbol for the end of a proof
\diamond	symbol for the end of a solution
$n!$	factorial
$\binom{n}{k}$	binomial coefficient
L_n	n -th Lucas number
F_n	n -th Fibonacci number
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$a^k \parallel b$	a^k is the largest power of a dividing b
$\gcd(a, b)$	greatest common divisor of a and b
$\log_b(x)$	logarithm to the base b
$\ln(x)$	natural logarithm
$\text{lcm}(a, b)$	least common multiple of a and b
$\min(a, b)$	minimum of a and b
$\max(a, b)$	maximum of a and b
f_n	Fermat number $2^{2^n} + 1$
M_p	Mersenne number $2^p - 1$
$a \equiv b \pmod{m}$	a is congruent b modulo m
$a \not\equiv b \pmod{m}$	a is not congruent b modulo m
$\varphi(m)$	Euler function
$\text{ind}_g a$	index of a with respect to a primitive root g
$\text{psp}(b)$	pseudoprime to the base b
$\text{spsp}(b)$	strong pseudoprime to the base b
$\left(\frac{a}{p}\right)$	Legendre symbol

$ A $	number of elements of a finite set A
$\left(\frac{a}{Q}\right)$	Jacobi symbol
$\text{lpsp}(a, b)$	Lucas pseudoprime
A^T	transpose of a matrix A
$h(d)$	class number of the discriminant d
t_m	m -th triangular number
$\lfloor x \rfloor$	the largest integer $\leq x$
$\lceil x \rceil$	the smallest integer $\geq x$
$\{x\}$	fractional part of x
$\mu(n)$	Möbius function
$\sigma(n)$	sum of divisors of n
$\tau(n)$	number of divisors of n
$f(x) = O(g(x))$	$ f(x) \leq Cg(x)$ for a constant C
$f(x) = o(g(x))$	$\lim_{x \rightarrow \infty} f(x)/g(x) = 0$
$f(x) \ll g(x)$	$ f(x) \leq Cg(x)$ for a constant C
$g(x) \gg f(x)$	same as $f(x) \ll g(x)$
γ	Euler-Mascheroni constant
$f * g$	Dirichlet product
$\omega(n)$	number of prime divisors of n
$\pi(x)$	number of primes which are $\leq x$
$\text{li}(x)$	logarithmic integral function
$\Lambda(n)$	von Mangoldt function
$\psi(x)$	Chebyshev function ψ
$\vartheta(x)$	Chebyshev function ϑ
$\zeta(s)$	Riemann zeta function
$\text{Re}(s)$	real part of a complex number s
$\text{Im}(s)$	imaginary part of a complex number s
$\Gamma(s)$	gamma-function
B_n	n -th Bernoulli number
$\chi(n)$	Dirichlet character
$L(s, \chi)$	Dirichlet L -function
$\ \alpha\ $	distance from α to the nearest integer
\mathcal{F}_n	Farey sequence of order n
$[a_0, a_1, \dots, a_n]$	finite continued fraction
$[a_0, a_1, \dots]$	infinite continued fraction
$\frac{p_i}{q_i}$	i -th convergent of a continued fraction
$\frac{p_{n,r}}{q_{n,r}}$	secondary convergent of a continued fraction
$M(\alpha)$	Markov constant
$\ x\ $	$\max(x_1 , \dots, x_n)$, for $x = (x_1, \dots, x_n)$

$\lfloor x \rfloor$	nearest integer to a real number x
$g(a_1, \dots, a_n)$	Frobenius number
$\nu_p(x)$	p -adic valuation
$ x _p$	p -adic norm
$\left(\frac{\alpha, \beta}{p}\right)$	Hilbert symbol
$R[x]$	polynomial ring on R
$\text{cont}(f)$	content of a polynomial f
$\text{Res}(f, g)$	resultant of polynomials f and g
$\text{Disc}(f)$	discriminant of a polynomial f
$D_m(x, a)$	Dickson polynomial
$T_n(x)$	Chebyshev polynomial of the first kind
$U_n(x)$	Chebyshev polynomial of the second kind
$F_n(x)$	Fibonacci polynomial
$\sigma_k(x_1, \dots, x_n)$	elementary symmetric polynomials
\mathbb{K}	algebraic number field
$N(\alpha)$	norm of an algebraic number
$T(\alpha)$	trace of an algebraic number
$N_{\mathbb{K}/\mathbb{Q}}(\alpha)$	norm of α with respect to \mathbb{K}
$T_{\mathbb{K}/\mathbb{Q}}(\alpha)$	trace of α with respect to \mathbb{K}
$\mathcal{O}_{\mathbb{K}}$	set of all algebraic integers in \mathbb{K}
$\langle \alpha \rangle$	principal ideal generated by α
$N(\mathfrak{a})$	norm of an ideal \mathfrak{a}
$h(\mathbb{K})$	class number of a number field \mathbb{K}
$\zeta_{\mathbb{K}}(s)$	Dedekind zeta function
$F\left(\begin{smallmatrix} \alpha, \beta \\ \gamma \end{smallmatrix} \middle x\right)$	hypergeometric function
$H(P)$	height of a polynomial P
$M(P)$	Mahler measure of a polynomial P
$h(P)$	logarithmic Weil height of a polynomial P
$e(P)$	separation exponent of a polynomial P
c_k	k -th Catalan number
\overline{K}	algebraic closure of a field K
\wp	Weierstrass \wp -function
$E(\mathbb{Q})_{\text{tors}}$	torsion group of an elliptic curve E
$\text{rank}(E(\mathbb{Q}))$	rank of an elliptic curve E
\hat{h}	canonical height
$\langle P, Q \rangle$	Néron-Tate pairing
\mathbb{F}_q	finite field with q elements
$\text{rad}(f)$	radical of a polynomial f
$\text{rad}(m)$	radical of a positive integer m

Subject Index

- 2-Selmer rank, 512
- abc* conjecture, 576
- abc* theorem for polynomials, 574
- AKS algorithm, 548
- algebraic integer, 368
 - irreducible, 372, 393
 - prime, 372, 393
- algebraic number, 366
 - degree, 368
- algebraic number field, 378
- analytic rank, 516
- Artin's conjecture, 65
- Artin's constant, 65
- associated algebraic numbers, 392
- badly approximable numbers, 216
- Baker, Alan, 408
- Baker-Davenport reduction, 445
- Baker-Wüstholz theorem, 444
- Bernoulli numbers, 174
- Bernoulli, Jacob, 174
- Bertrand's postulate, 163
- binary quadratic form, 111
 - positive definite, 112
 - primitive, 116
 - principal, 111
 - reduced, 114
- Binet's formula, 17
- binomial coefficient, 8
- binomial theorem, 8
- Birch and Swinnerton-Dyer (BSD) conjecture, 515
- Blichfeldt's theorem, 235
- BSGS method, 532
- canonical decomposition, 32
- canonical height, 500
- Carmichael numbers, 75
- Carmichael's theorem, 104
- Cassini's identity, 15
- Catalan numbers, 426
- Chebyshev functions, 164
- Chebyshev polynomials
 - of the first kind, 352
 - of the second kind, 356
- Chebyshev, Pafnuti Lvovich, 159
- Chevalley-Waring theorem, 321
- Chinese remainder theorem (CRT), 51
- class number
 - of a number field, 396
 - of binary quadratic forms, 115
- compact set, 235
- complete residue system, 44
- completely multiplicative function, 140
- composite numbers, 31
- conductor, 485
- congruence, 42
- congruence method, 458
- congruent number, 556
- continued fraction
 - complete quotient, 205, 208
 - convergent, 205, 208
 - partial quotient, 205, 208
 - secondary convergent, 214

- continued fractions, 202
 - finite, 205
 - infinite, 208
 - periodic, 222
 - period length, 222
 - purely periodic, 222
- convex set, 235
- Coppersmith's theorem, 267
- coprime integers, 24
- cryptology, 250
- cryptosystem, 251
- cyclotomic field, 399

- $D(n)$ - m -tuple, 459
- Davenport's theorem, 575
- Davenport, Harold, 446
- Dedekind zeta function, 398
- Dickson polynomials, 352
- Diffie-Hellman key exchange protocol, 535
- Diffie-Hellman problem (DHP), 536
- Diophantine m -tuple, 454
- Diophantine quadruple
 - regular, 457
- Diophantine triple
 - regular, 457
- Diophantus of Alexandria, 455
- Dirichlet L -function, 181
- Dirichlet character, 177
- Dirichlet product, 152
- Dirichlet's theorem
 - on Diophantine approximations, 192
 - on primes in arithmetic progressions, 176
 - on simultaneous approximation, 234
 - on units, 393
- Dirichlet, Peter Gustav Lejeune, 177
- discrete logarithm, 535
- discrete logarithm problem (DLP), 535

- discriminant
 - of a polynomial, 346
 - of a quadratic form, 111
 - of an algebraic number field, 382
 - of an elliptic curve, 467
- divisor, 22, 336
- Doud's algorithm, 491

- ECDL, 540
- Edwards curves, 479
- Eisenstein's irreducibility criterion, 349
- elementary symmetric polynomials, 358
- ElGamal cryptosystem, 536
- elliptic curve, 466
 - anomalous, 531, 542
 - induced by a Diophantine triple, 578
 - supersingular, 531, 542
- elliptic functions, 471
- elliptic integrals, 470
- equivalent decompositions, 351
- equivalent numbers, 217
- equivalent quadratic forms, 112, 125
- Erdős, Paul, 162
- Erdős-Strauss conjecture, 140
- Euclid, 26
- Euclid's algorithm, 25
 - extended, 28
- Euclidean field, 373
- Euler function, 54
- Euler's criterion, 84
- Euler's product formula, 176
- Euler's theorem, 54
- Euler, Leonhard, 54
- Euler-Maclaurin formula, 168
- Euler-Mascheroni constant, 150

- factor basis, 538
- factorial, 8
- Farey sequence, 194
- Faulhaber's formula, 174
- Fermat numbers, 37
- Fermat's Last Theorem for polynomials, 575

- Fermat's little theorem, 55
- Fermat, Pierre de, 37
- Fibonacci numbers, 11
- Fibonacci polynomials, 356
- Fibonacci, Leonardo Pisano, 10
- field, 334
 - algebraically closed, 344
- formal derivative, 342
- fraction field, 348
- Frobenius automorphism, 521
- Frobenius endomorphism, 533
- Frobenius number, 273
- function
 - analytic, 172
 - ceiling, 136
 - differentiable, 172
 - fractional part, 136
 - greatest integer, 136
 - meromorphic, 173
- Fundamental theorem of arithmetic, 32
- Fundamental theorem of symmetric polynomials, 359
- fundamental unit, 371
- Galois extension, 378
- Galois, Évariste, 378
- gamma-function, 173
- Gauss hypergeometric function, 409
- Gauss sum, 525
- Gauss' lemma, 89
- Gauss' lemma for polynomials, 339
- Gauss' quadratic reciprocity law, 91
- Gauss, Carl Friedrich, 42
- Gaussian rationals, 369
- GCD-domain, 336
- genus of a curve, 472
- Goldbach's conjecture, 39
- good approximation, 215
- greatest common divisor, 23, 336
- group homomorphism, 178
- Hardy-Ramanujan number, 586
- Hasse's theorem, 527
- Hasse-Minkowski principle, 325
- Hasse-Minkowski theorem, 325
- height
 - of a polynomial, 422
 - of an algebraic number, 417
- height determinant, 505
- Hensel's lemma, 61
- Hilbert symbol, 326
 - product formula, 326
- Holzer's theorem, 313
- Hurwitz's theorem, 198
- Håstad's attack, 263
- ideal, 385
 - maximal, 387
 - norm, 390
 - prime, 387
 - principal, 385
 - totally ramified, 392
 - unramified, 392
- ideal class group, 395
- index, 66
- index calculus method, 538
- infinite product
 - absolutely convergent, 175
 - convergent, 175
- integral basis, 382
- integral domain, 334
 - characteristic, 343
- irreducible element, 336
- isogeny, 507
- j -invariant, 481
- Jacobi symbol, 96
- Jacobi's formula, 123
- Jacobian projective coordinates, 478
- Koblitz curves, 534
- Korselt's criterion, 75
- Kronecker symbol, 97
- Kronecker's algorithm, 348
- Kummer, Ernst Eduard, 384
- López-Dahab coordinates, 529
- Lagrange's four-square theorem, 121

- Lagrange's theorem
 - on the best approximations, 214
 - on the number of congruence solutions, 59
- Lagrange, Joseph-Louis, 121
- lattice, 240
 - basis, 240
- least common multiple, 33
- Legendre symbol, 84
- Legendre's theorem
 - on continued fractions, 210
 - on ternary equations, 309
- Legendre, Adrien-Marie, 84
- Lenstra's algorithm for factorization (ECM), 549
- Liouville numbers, 403
- Liouville's theorem, 402
- Liouville, Joseph, 402
- LLL algorithm, 243
- LLL-reduced basis, 241
- local-global principle, 325
- logarithmic integral function, 159
- logarithmic Weil height, 423
- Lucas numbers, 11
- Lucas pseudoprime (lpsp), 103
- Lucas sequences, 103
- Lucas, Edouard, 10
- Lucas-Lehmer algorithm, 545
- Lutz, Élisabeth, 488
- Lutz-Nagell theorem, 488

- Mahler measure, 423
- Mahler, Kurt, 422
- Markov constant, 219
- Matiyasevich's lemma, 106
- Mazur's bound, 517
- Menezes-Vanstone cryptosystem, 537
- Mersenne numbers, 38
- Mertens constant, 170
- Mestre polynomial method, 514
- Midy's theorem, 72
- Miller-Rabin primality test, 78
- minimal polynomial, 368
 - over integers, 368
- minimal Weierstrass equation, 483

- Minkowski's theorem
 - on convex bodies, 237
 - on linear forms, 238
- Minkowski, Hermann, 235
- Möbius function, 141
- Möbius inversion formula, 142
- Mordell's equation, 559
- Mordell, Louis Joel, 486
- Mordell-Weil basis, 505
- Mordell-Weil theorem, 486
- multiple, 22, 336
- multiplicative function, 55

- NAF representation, 530
- Nagell, Trygve, 488
- Néron-Tate pairing, 504
- Newton's approximant, 230
- Newton's formulas, 362
- Newton's method, 229
- Noetherian ring, 400
- norm
 - of an algebraic number, 379
- normal basis, 524

- optimal normal basis, 524
- order, 62

- p -adic integers, 324
- p -adic norm, 323
- p -adic numbers, 324
- p -adic valuation, 323
- pairwise coprime integers, 24
- parallelogram law, 500
- partial summation formula, 168
- Pascal's formula, 8
- Pell's equation, 284
 - fundamental solution, 286
- Pellian equation, 296
 - ambiguous class, 297
 - class of solutions, 297
- perfect numbers, 143
- perfect square, 33
- Pocklington's theorem, 544
- Pohlig-Hellman algorithm, 540
- Pollard's ρ -method, 541
- Pollard's $p - 1$ method, 548

- polynomial, 335
 - coefficients, 335
 - degree, 335
 - indecomposable, 351
 - irreducible, 347
 - monic, 335
 - primitive, 339
 - reducible, 347
 - symmetric, 358
 - total degree, 358
- polynomial basis, 523
- polynomial content, 339
- polynomial resultant, 345
- polynomial ring, 335
- power integral basis, 383
- prime number theorem (PNT), 159
- prime numbers, 31
- primitive prime divisor, 104
- primitive root, 63
- principal character, 178
- principal ideal domain, 397
- principle of mathematical induction, 4
- product of ideals, 385
- pseudoprime (psp), 74
- Pythagorean triple, 274
 - primitive, 274

- quadratic field, 368
 - imaginary, 370
 - real, 370
- quadratic form, 125
 - positive definite, 126
- quadratic irrationality, 222
 - reduced, 225
- quadratic nonresidue, 83
- quadratic residue, 83

- radical
 - of a polynomial, 574
 - of a positive integer, 576
- ramification index, 392
- rank of an elliptic curve, 486
- rational Diophantine m -tuple, 454
- reduced residue system, 54

- reduction
 - additive, 483
 - good, 483
 - multiplicative, 483
 - non-split, 483
 - split, 483
- regulator
 - of a number field, 394
 - of an elliptic curve, 505
- residuum, 173
- Riemann hypothesis (RH), 174
 - extended (ERH), 182
 - generalized (GRH), 183
- Riemann zeta function, 173
- Riemann, Bernhard, 172
- ring, 334
 - commutative with unity, 334
- root of a polynomial, 342
 - order (multiplicity), 342
- root of unity, 524
 - primitive, 524
- Roth's theorem, 404
- Roth, Klaus Friedrich, 404
- RSA cryptosystem, 254
 - rebalanced, 262

- Schmidt's subspace theorem, 406
- Schönemann's irreducibility criterion, 349
- Segre's theorem, 199
- Selberg's formula, 172
- separation exponent, 424
- Shanks-Mestre method, 532
- Siegel's identity, 569
- Sierpiński, Waclaw, 274
- sieve of Eratosthenes, 34
- signed digit representation, 530
- singularity, 172
 - essential, 172
 - isolated, 172
 - pole of order n , 172
 - removable, 172
- Sophie Germain primes, 38
- square-free integer, 33
- strong Diophantine m -tuple, 456

- strong pseudoprime (spsp), 75
- sum of ideals, 387
- sums of powers, 359
- Sun Tzu, 50
- Sylvester's theorem, 273
- symmetric set, 234

- Tate normal form, 494
- Tate, John, 494
- Taylor series, 172
- Taylor's formula, 344
- ternary quadratic form, 307
- Theorem of division with remainder, 23
 - for polynomials, 337
- Thue equation, 431
- Thue's theorem, 432
- Thue, Alex, 431
- torsion group, 486
- trace of an algebraic number, 379
- trace of Frobenius, 527
- transcendental numbers, 366
- triangular numbers, 131
- trinomial basis, 523
- Tunnell's theorem, 558

- twin primes, 38
- twist of an elliptic curve, 533

- unimodular matrices, 113
- unique factorization domain, 336
- unique factorization property, 373
- unit, 392

- Vandermonde matrix, 423
- Vinogradov, Ivan Matveevich, 86
- von Mangoldt function, 164

- Weierstrass form, 467
 - short, 467
- Weierstrass, Karl, 470
- Weierstrass \wp -function, 470
- Weil, André, 486
- Wiener's attack, 257
- Wilson's theorem, 57
- Wirsing's theorem, 417
- Worley's theorem, 212

- zero of a polynomial, 342
- zero polynomial, 335

Translator

Petra Švob

Lector

Maria Jurjevich

Cover by

Tanja Pružek Šimpović

Graphics preparation

Graphic-art redaction of Školska knjiga

Press

Grafički zavod Hrvatske, d.o.o., Zagreb

ISBN 978-953-0-30897-8

CIP copy is available in the catalogue of the National and University Library in Zagreb, under the number 001092040.