Teorija brojeva

Andrej Dujella

UDŽBENICI SVEUČILIŠTA U ZAGREBU

MANUALIA UNIVERSITATIS STUDIORUM ZAGRABIENSIS

---

akademik ANDREJ DUJELLA: TEORIJA BROJEVA

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

Za izdavača
dr. sc. Ante Žužul

Direktorica školskog programa
Matilda Bulić, prof.

Glavna urednica
Jelena Lončarić, dipl.ing.

Urednica
Tanja Djaković, prof.

Recenzenti
prof. dr. sc. Ivica Gusić
izv. prof. dr. sc. Matija Kazalicki
izv. prof. dr. sc. Filip Najman

Uporabu ovog sveučilišnog udžbenika odobrio je
Senat Sveučilišta u Zagrebu.
(Klasa: 032-01/19-01/11, Ur. broj: 390-061/117-19-5
od 16. travnja 2019.)

Objavljivanje ovog sveučilišnog udžbenika potpomoglo je
Ministarstvo znanosti i obrazovanja.

CIP zapis je dostupan u računalnome katalogu
Nacionalne i sveučilišne knjižnice u Zagrebu pod brojem 001037625.

ISBN 978-953-0-30894-7

Predgovor

Teorija brojeva grana je matematike koja se ponajprije bavi proučavanjem svojstava prirodnih brojeva kao što su djeljivost, rastav na proste faktore ili rješivost jednadžbi u prirodnim brojevima. Ona ima vrlo dugu i bogatu povijest, a važan su joj doprinos dali i neki od najvažnijih matematičara u povijesti poput Euklida, Eulera i Gaussa. Tijekom te duge povijesti teorija brojeva često se smatrala "najčišćom" granom matematike, u smislu da je bila najdalja od bilo kakvih konkretnih primjena. Međutim, sredinom 70-ih godina 20. stoljeća nastupa bitna promjena, tako da je danas teorija brojeva jedna od najvažnijih grana matematike za primjene u kriptografiji i sigurnoj razmjeni informacija.

Ova je knjiga nastala na osnovi nastavnih materijala (dostupnih na internetskoj stranici `https://web.math.pmf.unizg.hr/~duje/`) iz kolegija *Teorija brojeva* i *Elementarna teorija brojeva*, koji se predaju na preddiplomskim studijima na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu, te kolegija *Diofantske jednadžbe* i *Diofantske aproksimacije i primjene*, koji su se predavali na doktorskom studiju matematike na istom fakultetu. Knjiga potpuno pokriva sadržaj navedenih kolegija, ali sadržava i druge povezane teme poput eliptičkih krivulja kojima su posvećena zadnja dva poglavlja u knjizi. U knjizi su obrađene i neke teme koje su bile i jesu u središtu istraživačkog interesa autora knjige i ostalih članova hrvatske grupe iz teorije brojeva okupljene oko *Seminara za teoriju brojeva i algebru*.

Knjiga je ponajprije namijenjena studentima matematike i srodnih fakulteta na hrvatskim sveučilištima koji slušaju kolegije iz teorije brojeva i njezinih primjena, potom naprednim srednjoškolcima koji se pripremaju za matematička natjecanja u kojima na svim razinama, od školske do međunarodne, teorija brojeva uvijek zauzima važno mjesto, te doktorskim studentima i znanstvenicima koji se bave teorijom brojeva, algebrom i kriptografijom.

Pri pisanju ove knjige korišteni su brojni izvori. Osnovna literatura za svako (pot)poglavlje navedena je na odgovarajućim mjestima u knjizi. Istaknimo ovdje da su kod pisanja prve verzije skripata [73] osnovna literatura bile knjige A. Baker: *A Concise Introduction to the Theory of Numbers* [14] i I. Niven, H. S. Zuckerman, H. L. Montgomery: *An Introduction to the Theory of Numbers* [229]. Veliki dio korištene literature dostupan je u Središnjoj matematičkoj knjižnici na Matematičkom odsjeku PMF-a, a znatnim dijelom je nabavljen iz sredstava znanstvenih projekata kojima sam bio voditelj ili član (projekti Ministarstva znanosti i obrazovanja, potpore Sveučilišta u Zagrebu, projekti Hrvatske zaklade za znanost, Znanstveni centar izvrsnosti QuantiXLie).

Kao što je već rečeno, knjiga potpuno pokriva sadržaj kolegija *Teorija brojeva* (Poglavlja 2, 3.1–3.7, 4, 5.2, 5.3, 6.2, 6.3, 7.2, 8.1, 8.3, 8.4, 8.6, 10.1–10.4, 12.1), *Elementarna teorija brojeva* (Poglavlja 2, 3.1–3.7, 4, 5.1, 5.3, 6.1, 6.2, 7.1, 10.1–10.4, 9.1, 9.2), *Diofantske jednadžbe* (Poglavlja 10.3–10.8, 13.1–13.3, 8.8, 8.9, 14, 16.2–16.5, 15.1, 15.5), *Diofantske aproksimacije i primjene* (Poglavlja 8.1–8.6, 10.4, 10.5, 8.8, 8.9, 9, 13.1, 13.2, 14.1, 14.2, 13.4, 13.5).

Gore navedena poglavlja iz kolegija *Teorija brojeva* i *Elementarna teorija brojeva* ujedno su i poglavlja (uz dodatak uvodnog Poglavlja 1) koja se preporučaju čitatelju zainteresiranom za sadržaj koji se obično naziva elementarna teorija brojeva. Poglavlje 12 se može shvatiti kao kratki uvod u algebarsku teoriju brojeva, a Poglavlje 7 isto tako kao kratki uvod u analitičku teoriju brojeva. Svakako treba naglasiti da opseg knjige (a i znanje autora) ne omogućavaju da knjiga uključi sve ono što bi sustavna obrada tema iz algebarske i analitičke teorije brojeva obuhvaćala. Poglavlje 11 koje obrađuje temu polinoma može se shvatiti i kao priprema za Poglavlje 12. Eliptičkim krivuljama su posvećena zadnja dva Poglavlja 15 i 16, ali to naravno ne obuhvaća sve što bi se o toj temi moglo reći (kao što piše u uvodu knjige [193], "o eliptičkim krivuljama se može pisati beskrajno"), posebice se to odnosi na vezu eliptičkih krivulja s modularnim formama i algebarskom geometrijom, pa čitatelja koji će poželjeti dodatne informacije o toj temi upućujemo na skripte na hrvatskom jeziku [84, 141, 172, 217, 220]. Ostala postojeća literatura na hrvatskom jeziku odnosi se ponajprije na neke dijelove elementarne teorije brojeva [121, 209, 235, 237], a spomenimo i knjižicu *Brojevi* koja sadržava zanimljiv pregled i viđenje teorije brojeva [291]. Teme iz elementarne teorije brojeva dobro su zastupljene i u člancima u hrvatskim stručno-metodičkim i znanstveno-popularizacijskim časopisima: *Matematika*, *Matematičko-fizički list*, *Matka*, *Poučak*, *math.e*, *Matematika i*

škola, *Osječki matematički list*, *Acta mathematica Spalatensia Series didactica*. U ovoj knjizi dotiče se i tema primjene teorije brojeva u kriptografiji (Poglavlja 9 i 15.8), o čemu zainteresirani čitatelj može dodatne informacije naći u knjizi [105]. Spomenimo još i da se kroz više poglavlja (osobito Potpoglavlja 1.3, 4.5 i 10.6) provlače Fibonaccijevi brojevi kao zanimljiv matematički objekt s pomoću kojeg se ilustriraju neke od obrađenih tema. Pritom je korišten materijal iz knjižice [75].

Neke od specifičnih tema koje su u knjigu uključene zbog autorovih afiniteta, a neće se uobičajeno naći u knjigama i udžbenicima iz teorije brojeva, dane su u Potpoglavljima 8.7, 9.3, 11.4, 13.5, 14.2, 14.6 i 16.7. S jedne strane to znači da ih čitatelj slobodno može preskočiti u prvom čitanju, a s druge strane nadam se da će ipak biti čitatelja kojima će biti zanimljivo u kratkim crtama pročitati što je autor knjige sa svojim suradnicima znanstveno radio u zadnjih 25 godina.

Na kraju svakog poglavlja nalaze se (neriješeni) zadatci koji jednim dijelom mogu poslužiti studentima i natjecateljima za vježbu, a katkad su dopuna osnovnog teksta. Izvori zadataka su različiti. S jedne strane su to zadatci s kolokvija, pismenih ispita i zadaća na preddiplomskom i doktorskom studiju te zadatci s priprema natjecatelja, a s druge strane je dio zadataka preuzet iz literature, primjerice iz [1, 8, 9, 22, 30, 66, 105, 138, 159, 160, 161, 246, 247, 251, 253, 254, 264, 265, 282, 295], u kojoj zainteresirani čitatelj može pronaći mnogo dodatnih zadataka.

Zahvaljujem svima koji su čitali različite verzije rukopisa ove knjige te me upozorili na pogreške i sugerirali poboljšanja teksta. Tu posebno ističem kolegu Ivicu Gusića, koji mi je pomogao brojnim savjetima oko različitih nedoumica koje sam imao prilikom pisanja knjige, kolegu Tomislava Pejkovića, koji je pomno pročitao cijeli rukopis knjige te me upozorio na mnoge manje ili veće pogreške i nepreciznosti, te kolege Nikolu Adžagu, Mariju Bliznac Trebješanin, Bernadina Ibrahimpašića, Borku Jadrijević, Anu Jurasić, Matiju Kazalickog, Dijanu Kreso, Marcela Maretića, Miljena Mikića, Gorana Muića, Filipa Najmana, Vinka Petričevića, Valentinu Pribanić, Ivana Soldu, Borisa Širolu i Mladena Vukovića, koji su mi slali svoje komentare i sugestije na pojedina poglavlja ili na cijeli rukopis prethodne verzije knjige.

Zahvaljujem i generacijama studenata Matematičkog odsjeka PMF-a koji su svojim interesom za kolegij, koji je najprije pod naslovom *Uvod u teoriju brojeva* uveden kao izborni kolegij, omogućili da poslije uđe u program studija kao obvezni kolegij *Teorija brojeva* na tzv. inženjerskom smjeru te *Elementarna teorija brojeva* na nastavničkom smjeru preddiplomskog studija matematike. Posebno zahvaljujem studentima kojima sam bio mentor

diplomskih radova (do sada ih je bilo 189, a priličan dio tema tih radova odnosi se na teoriju brojeva i njezine primjene u kriptografiji). Imao sam sreću da su i moja predavanja na kolegijima na doktorskom studiju matematike bila dosta dobro posjećena, pa zahvaljujem i doktorskim studentima te ostalim članovima Seminara za teoriju brojeva i algebru koji su često davali korisne komentare na radne materijale iz tih kolegija. Petnaest godina sam bio član državnog povjerenstva za natjecanja iz matematike, a i poslije sam povremeno sudjelovao u pripremama darovitih učenika za međunarodna natjecanja. Dio materijala i zadataka koje sam pripremao za tu svrhu također je uključen u knjigu. Prvi ozbiljniji susret autora ove knjige s teorijom brojeva došao je upravo preko matematičkih natjecanja, pa i ovom prilikom zahvaljujem svom srednjoškolskom profesoru Petru Vranjkoviću uz čiju sam se pomoć pripremao za ta natjecanja uključujući i matematičku olimpijadu u Pragu 1984. godine. Zahvaljujem i mentoru svog diplomskog i magistarskog rada Zvonku Čerinu te mentorima doktorske disertacije Dragutinu Svrtanu i Dimitriju Ugrin-Šparcu na uvođenju u znanstveni rad. Posebna zahvala ide Attili Pethőu, profesoru sa Sveučilišta u Debrecinu i članu Mađarske akademije znanosti, koji je, od našeg prvog susreta 1996. godine pa sve do danas, svojim brojnim, vrlo korisnim savjetima usmjeravao moju znanstvenu i nastavnu karijeru. Kao što je već naglašeno, neka od potpoglavlja u knjizi govore o osobnim znanstvenim interesima autora, pa zahvaljujem svim svojim brojnim koautorima znanstvenih radova na inspirativnoj znanstvenoj suradnji. Zahvaljujem i svojoj obitelji na strpljenju, potpori i razumijevanju tijekom pisanja ove knjige.

Novigrad i Zagreb, 2018. – 2019. akad. Andrej Dujella

Sadržaj

Bibliografija

[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. Adžaga, *Automated conjecturing of Frobenius numbers via grammatical evolution*, Experiment. Math. **26** (2017), 247–252.

[3] N. Adžaga, *On the size of Diophantine m-tuples in imaginary quadratic number rings*, Bull. Math. Sci., to appear.

[4] 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.

[5] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Ann. of Math. **160** (2004), 781–793.

[6] 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.

[7] S. Alaca, K. S. Williams, Introductory Algebraic Number Theory, Cambridge University Press, Cambridge, 2004.

[8] T. Andreescu, D. Andrica, Z. Feng, 104 Number Theory Problems From the Training of the USA IMO Team, Birkhäuser, Boston, 2007.

[9] T. Andreescu, D. Andrica: Number Theory. Structures, Examples, and Problems, Birkhäuser, Boston, 2009.

[10] E. Bach, J. Shallit, Algorithmic Number Theory, Volume I: Efficient Algorithms, MIT Press, Cambridge, 1996.

[11] Lj. Baćić, A. Filipin, *A note on the number of $D(4)$-quintuples*, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **18** (2014), 7–13.

[12] A. Baker, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers*, Quart. J. Math. Oxford Ser. (2) **15** (1964), 375–383.

[13] A. Baker, Transcendental Number Theory, Cambridge University Press, Cambridge, 1990.

[14] A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1994.

[15] A. Baker, A Comprehensive Course in Number Theory, Cambridge University Press, Cambridge, 2012.

[16] 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.

[17] A. Baker, G. Wüstholz, Logarithmic Forms and Diophantine Geometry, Cambridge University Press, Cambridge, 2008.

[18] M. W. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo, Elementary Number Theory, Cryptography and Codes, Springer, Berlin, 2009.

[19] E. J. Barbeau, Pell's Equation, Springer, New York, 2003.

[20] P. T. Bateman, H. G. Diamond, Analytic Number Theory. An Introductory Course, World Scientific, Singapore, 2004.

[21] R. Becker, M. Ram Murty, *Diophantine m-tuples with the property $D(n)$*, Glas. Mat. Ser. III **54** (2019), 65–75.

[22] A. H. Beiler, Recreations in the Theory of Numbers, Dover, New York, 1966.

[23] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. **498** (1998), 173–199.

[24] 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.

[25] D. J. Bernstein, T. Lange, *Faster addition and doubling on elliptic curves*, Lecture Notes in Comput. Sci. **4833**, Springer, Berlin, 2007, pp. 29–50.

[26] Y. Bilu, R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

[27] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, Cambridge University Press, Cambridge, 1999.

[28] M. Bliznac Trebješanin, A. Filipin, *Nonexistence of $D(4)$-quintuples*, J. Number Theory **194** (2019), 170–217.

[29] S. Bohniček, *Kriteriji za rješivost diofantske jednadžbe $t^2 - Dy^2 = -1$*, Rad JAZU Matematičko-prirodoslovnog razreda **97** (1920), 49–82.

[30] M. Bombardelli, A. Dujella, S. Slijepčević, Matematička natjecanja učenika srednjih škola, HMD, Element, Zagreb, 1996.

[31] E. Bombieri, W. Gubler, Heights in Diophantine Geometry, Cambridge University Press, Cambridge, 2006.

[32] O. Bordelles, Arithmetic Tales, Springer, London, 2012.

[33] Z. I. Borevich, I. R. Shafarevich, Number Theory, Academic Press, New York, 1986.

[34] 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.

[35] E. Brown, *Sets in which $xy + k$ is always a square*, Math. Comp. **45** (1985), 613–620.

[36] D. A. Buell, Binary Quadratic Forms, Springer-Verlag, New York, 1989.

[37] Y. Bugeaud, Approximation by Algebraic Numbers, Cambridge University Press, Cambridge, 2004.

[38] Y. Bugeaud, Linear Forms in Logarithms and Applications, IRMA Lectures in Mathematics and Theoretical Physics Vol. **28**, European Mathematical Society, Zürich, 2018.

[39] Y. Bugeaud, A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. **135** (2003), 1–10.

[40] Y. Bugeaud, A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. **43** (2011), 1239–1244.

[41] Y. Bugeaud, A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. **162** (2014), 393–403.

[42] Y. Bugeaud, A. Dujella, T. Pejković, B. Salvy, *Absolute real root separation*, Amer. Math. Monthly **124** (2017), 930–936.

[43] Y. Bugeaud, M. Mignotte, *Polynomial root separation*, Intern. J. Number Theory **6** (2010), 587–602.

[44] 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.

[45] 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.

[46] P. Bundschuh, Einführung in die Zahlentheorie, Springer-Verlag, Berlin, 2008.

[47] R. D. Carmichael, The Theory of Numbers and Diophantine Analysis, Dover, New York, 1959.

[48] J. W. Cassels, An Introduction to the Geometry of Numbers, Springer-Verlag, Berlin, 1997.

[49] H. H. Chan, Analytic Number Theory for Undergraduates, World Scientific, Singapore, 2009.

[50] M. Cipu, Y. Fujita, T. Miyazaki, *On the number of extensions of a Diophantine triple*, Int. J. Number Theory **14** (2018), 899–917.

[51] H. Cohen, Number Theory. Volume I: Tools and Diophantine Equations, Springer Verlag, Berlin, 2007.

[52] H. Cohen, Number Theory. Volume II: Analytic and Modern Tools, Springer Verlag, Berlin, 2007.

[53] H. Cohn, Advanced Number Theory, Dover, New York, 1980.

[54] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28.

[55] A. C. Cojocaru, M. Ram Murti, An Introduction to Sieve Methods and Their Applications, Cambridge University Press, Cambridge, 2005.

[56] I. Connell, Elliptic Curve Handbook, McGill University, Montreal, 1999.

[57] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology **10** (1997), 233–260.

[58] D. A. Cox, Primes of the Form $x^2 + ny^2$, John Wiley & Sons, New York, 1989.

[59] R. Crandall, C. Pomerance, Prime Numbers: A Computational Perspective, Springer, New York, 2005.

[60] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1997.

[61] T. W. Cusick, M. E. Flahive, The Markoff and Lagrange Spectra, American Mathematical Society, Providence, 1989.

[62] H. Čavrak, *Enigma*, Hrvatski matematički elektronički časopis math.e **3** (2004).

[63] A. Das, Computational Number Theory, CRC Press, Boca Raton, 2013.

[64] H. Davenport, Multiplicative Number Theory, Springer-Verlag, New York, 1980.

[65] J.-M. De Koninck, F. Luca, Analytic Number Theory. Exploring the Anatomy of Integers, American Mathematical Society, Providence, 2012.

[66] J.-M. De Koninck, A. Mercier, 1001 Problems in Classical Number Theory, American Mathematical Society, Providence, 2007.

[67] C. A. Deavours, L. Kruh, Machine Cryptography and Modern Cryptanalysis, Artech House, Norwood, 1985.

[68] E. Deza, M. M. Deza, Figurate Numbers, World Scientific, Singapore, 2012.

[69] L. E. Dickson, History of the Theory of Numbers, Volume 2: Diophantine analysis, Chelsea, New York, 1966.

[70] R. Dietmann, C. Elsholtz, *Sums of two squares and one biquadrate*, Funct. Approx. Comment. Math. **38** (2008), 233–234.

[71] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

[72] A. Dujella, *Pitagorine trojke*, Bilten seminara iz matematike za nastavnike mentore, Crikvenica, 1994, pp. 1–10.

[73] A. Dujella, Uvod u teoriju brojeva, skripta, Sveučilište u Zagrebu, 1999.

[74] A. Dujella, *Verižni razlomci i problem kalendara*, Matematika i škola 1 (1999), no. 2, 74–77.

[75] A. Dujella, Fibonaccijevi brojevi, HMD, Zagreb, 2000.

[76] A. Dujella, *A parametric family of elliptic curves*, Acta Arith. **94** (2000), 87–101.

[77] A. Dujella, *Newton's formula and continued fraction expansion of* $\sqrt{d}$, Experiment. Math. **10** (2001), 125–131.

[78] A. Dujella, *On the size of Diophantine* m*-tuples*, Math. Proc. Cambridge Philos. Soc. **132** (2002), 23–33.

[79] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[80] A. Dujella, *Bounds for the size of sets with the property* $D(n)$, Glas. Mat. Ser. III **39** (2004), 199–205.

[81] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

[82] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42** (2007), 3–18.

[83] A. Dujella, *On the number of Diophantine* m*-tuples*, Ramanujan J. **15** (2008), 37–46.

[84] A. Dujella, Algoritmi za eliptičke krivulje, skripta, Sveučilište u Zagrebu, 2009.

[85] A. Dujella, *A variant of Wiener's attack on RSA*, Computing **85** (2009), 77–83.

[86] A. Dujella, *On Hall's conjecture*, Acta Arith. **147** (2011), 397–402.

[87] A. Dujella, *What is ... a Diophantine m-tuple?*, Notices Amer. Math. Soc. **63** (2016), 772–774.

[88] A. Dujella, *Diophantine m-tuples*
https://web.math.pmf.unizg.hr/∼duje/dtuples.html

[89] A. Dujella, *High rank elliptic curves with prescribed torsion*
https://web.math.pmf.unizg.hr/∼duje/tors/tors.html

[90] A. Dujella, *History of elliptic curves rank records*
https://web.math.pmf.unizg.hr/∼duje/tors/rankhist.html

[91] A. Dujella, A. Filipin, C. Fuchs, *Effective solution of the $D(-1)$-quadruple conjecture*, Acta Arith. **128** (2007), 319–338.

[92] A. Dujella, C. Fuchs, *Complete solution of the polynomial version of a problem of Diophantus*, J. Number Theory **106** (2004), 326–344.

[93] A. Dujella, C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71** (2005), 33–52.

[94] A. Dujella, I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. (Oxford) **57** (2006), 193–201.

[95] A. Dujella, I. Gusić, *Decomposition of a recursive family of polynomials*, Monatsh. Math. **152** (2007), 97–104.

[96] A. Dujella, B. Ibrahimpašić, *On Worley's theorem in Diophantine approximations*, Ann. Math. Inform. **35** (2008), 61–73.

[97] A. Dujella, B. Jadrijević, *A parametric family of quartic Thue equations*, Acta Arith. **101** (2002), 159–170.

[98] A. Dujella, B. Jadrijević, *A family of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.

[99] 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.

[100] 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.

[101] 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.

[102] 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, Berlin, 2017, pp. 227–235.

[103] 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.

[104] A. Dujella, F. Luca, *Diophantine m-tuples for primes*, Int. Math. Res. Not. **47** (2005), 2913–2940.

[105] A. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007.

[106] 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.

[107] 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.

[108] 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.

[109] 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.

[110] 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.

[111] A. Dujella, A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.

[112] A. Dujella, A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), 321–335.

[113] A. Dujella, V. Petričević, *Square roots with many good approximants*, Integers **5(3)** (2005), #A6. (13pp)

[114] A. Dujella, V. Petričević, *Strong Diophantine triples*, Experiment. Math. **17** (2008), 83–89.

[115] A Dujella, V. Petričević, *Diophantine quadruples with the properties $D(n_1)$ and $D(n_2)$*, preprint, 2019.

[116] A. Dujella, N. Saradha, *Diophantine m-tuples with elements in arithmetic progressions*, Indag. Math. (N.S.) **25** (2014), 131–136.

[117] A. Dujella, R. F. Tichy, *Diophantine equations for second order recursive sequences of polynomials*, Quart. J. Math. Oxford Ser. (2) **52** (2001), 161–169.

[118] H. M. Edwards, Riemann's Zeta Function, Academic Press, New York, 1974.

[119] H. M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), 393–422.

[120] N. Elezović, *A note on continued fractions of quadratic irrationals*, Math. Commun. **2** (1997), 27–33.

[121] N. Elezović, Diskontna matematika 1, Element, 2017.

[122] G. Everest, T. Ward, An Introduction to Number Theory, Springer-Verlag, London, 2005.

[123] J.-H. Evertse, K. Győry, Unit Equations in Diophantine Number Theory, Cambridge University Press, Cambridge, 2015.

[124] J.-H. Evertse, K. Győry, Discriminant Equations in Diophantine Number Theory, Cambridge University Press, Cambridge, 2017.

[125] A. Filipin, Primjena LLL-algoritma u rješavanju diofantskih jednadžbi, magistarski rad, Sveučilište u Zagrebu, 2004.

[126] A. Filipin, *There does not exist a $D(4)$-sextuple*, J. Number Theory **128** (2008), 1555–1565.

[127] A. Filipin, Linearne forme u logaritmima i diofantska analiza, skripta, Sveučilište u Zagrebu, 2010.

[128] A. Filipin, A. Jurasić, *A polynomial variant of a problem of Diophantus and its consequences*, Glas. Mat. Ser. III **54** (2019), 21–52.

[129] B. Fine, A. Gaglione, A. Moldenhauer, G. Rosenberger, D.Spellman, Algebra and Number Theory. A Selection of Highlights, De Gruyter, Berlin, 2017.

[130] Z. Franušić, *Diophantine quadruples in* $\mathbb{Z}[\sqrt{4k+3}]$, Ramanujan J. **17** (2008), 77–88.

[131] Z. Franušić, *A Diophantine problem in* $\mathbb{Z}[(1+\sqrt{d})/2]$, Studia Sci. Math. Hungar. **46** (2009), 103–112.

[132] 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.

[133] Y. Fujita, T. Miyazaki, *The regularity of Diophantine quadruples*, Trans. Amer. Math. Soc. **370** (2018), 3803–3831.

[134] I. Gaál, Diophantine Equations and Power Integral Bases, Birkhäuser, Boston, 2002.

[135] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.

[136] P. E. Gibbs, *A survey of rational Diophantine sextuples of low height*, preprint, 2016.

[137] F. Q. Gouvêa, p-adic Numbers. An Introduction, Springer, Berlin, 2003.

[138] R. L. Graham, D. E. Knuth, O. Patashnik, Concrete Mathematics - A foundation for computer science, Addison-Wesley, Reading, 1989.

[139] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167** (2008), 481–547.

[140] P. M. Gruber, C. G. Lekkerkerker, Geometry of Numbers, North Holland, Amsterdam, 1987.

[141] I. Gusić, Uvod u aritmetiku eliptičkih krivulja, skripta, Sveučilište u Zagrebu, 2008.

[142] I. Gusić, *On decomposition of polynomials over rings*, Glas. Mat. Ser. III **43** (2008), 7–12.

[143] I. Gusić, P. Tadić, *A remark on the injectivity of the specialization homomorphism*, Glas. Mat. Ser. III **47** (2012), 265–275.

[144] I. Gusić, P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory **148** (2015), 137–152.

[145] R. K. Guy, Unsolved Problems in Number Theory, Springer, New York, 2004.

[146] K. Gyarmati, C. L. Stewart, *On powers in shifted products*, Glas. Mat. Ser. III **42** (2007), 273–279.

[147] D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag, New York, 2004.

[148] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, Oxford, 2008.

[149] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), 6665–6709.

[150] T. L. Heath, Diophantus of Alexandria: A study in the history of Greek Algebra, Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003.

[151] D. Hensley, Continued Fractions, World Scientific, Singapore, 2006.

[152] M. Hidry, J. H. Silverman, Diophantine Geometry. An Introduction, Springer-Verlag, New York, 2000.

[153] M. J. Hinek, Cryptanalysis of RSA and Its Variants, CRC Press, Boca Raton, 2009.

[154] J. Hoffstein, J. Pipher, J. H. Silverman, An Introduction to Mathematical Cryptography, Springer, New York, 2008.

[155] V. E. Hoggatt, Jr., Fibonacci and Lucas Numbers, The Fibonacci Association, Santa Clara, 1979.

[156] K. Horvatić, Linearna algebra, Golden Marketing - Tehnička knjiga, Zagreb, 2004.

[157] T. W. Hungerford, Algebra, Springer-Verlag, New York, 1974.

[158] D. Husemöller, Elliptic Curves, Springer-Verlag, New York, 2004.

[159] B. Hutz, An Experimental Introduction to Number Theory, American Mathematical Society, Providence, 2018.

[160] B. Ibrahimpašić, Kriptografija kroz primjere, Pedagoški fakultet Bihać, Bihać, 2011.

[161] B. Ibrahimpašić, Uvod u teoriju brojeva, Pedagoški fakultet Bihać, Bihać, 2014.

[162] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1998.

[163] M. J. Jacobson, H. C. Williams, *Modular arithmetic on elements of small norm in quadratic fields*, Des. Codes and Cryptogr. **27** (2002), 93–110.

[164] M. J. Jacobson, H. C. Williams, Solving the Pell Equation, Springer, New York, 2009.

[165] B. Jadrijević, Dvoparametarska familija Thueovih jednadžbi četvrtog stupnja, Disertacija, Sveučilište u Zagrebu, 2001.

[166] 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.

[167] G. J. Janusz, Algebraic Number Fields, Academic Press, New York, 1973.

[168] 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.

[169] B. W. Jones, The Arithmetic Theory of Quadratic Forms, The Mathematical Association of America, New York, 1950.

[170] A. Jurasić, Diofantske jednadžbe nad funkcijskim poljima, magistarski rad, Sveučilište u Zagrebu, 2006.

[171] D. Kahn, The Codebreakers. The Story of Secret Writing, Scribner, New York, 1996. (hrvatski prijevod: Šifranti protiv špijuna, Centar za informacije i publicitet, Zagreb, 1979.)

[172] M. Kazalicki, Modularne forme, skripta, Sveučilište u Zagrebu, 2017.

[173] H. L. Keng, Introduction to Number Theory, Springer-Verlag, Berlin, 1982.

[174] M. Kiseljak, Prilozi za teoriju savršenih brojeva, Kr. zemaljska tiskara, Zagreb, 1911.

[175] A. Ya. Khinchin, Continued Fractions, Dover, New York, 1997.

[176] A. W. Knapp, Elliptic Curves, Princeton University Press, Princeton, 1992.

[177] D. Knuth, The Art of Computer Programming, Vol. 2, Seminumerical Algorithms, Addison-Wesley, Reading, 1981.

[178] N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, New York, 1994.

[179] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1996.

[180] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta Functions, Springer-Verlag, New York, 1996.

[181] T. Koshy, Fibonacci and Lucas Numbers with Applications, Wiley, New York, 2001.

[182] J. S. Kraft, L. C. Washington, An Introduction to Number Theory with Cryptography, CRC Press, Boca Raton, 2018.

[183] H. Kraljević, Odabrana poglavlja teorije analitičkih funkcija, skripta, Sveučilište u Zagrebu, 2010.

[184] H. Kraljević, S. Kurepa, Matematička analiza 4 - Funkcije kompleksne varijable, Tehnička knjiga, Zagreb, 1979.

[185] E. Kranakis, Primality and Cryptography, Teubner, Stuttgart; Wiley, Chichester, 1986.

[186] D. Kreso, Rational function decomposition and Diophantine equations, Disertacija, Graz University of Technology, Graz, 2014.

[187] D. Kreso, R. Tichy, *Functional composition of polynomials: indecomposability, Diophantine equations and lacunary polynomials*, Grazer Math. Ber. **363** (2015), 143-170.

[188] M. Křížek, F. Luca, L. Somer, 17 Lectures on Fermat Numbers, Springer-Verlag, New York, 2001.

[189] S. Kurepa, Matematička analiza 2, Školska knjiga, Zagreb, 1987.

[190] E. Landau, Elementary Number Theory, Chelsea, New York, 1966.

[191] E. Landau, Foundations of Analysis, Chelsea, New York, 1966.

[192] S. Lang, Introduction to Diophantine Approximations, Addison-Wesley, Reading, 1966.

[193] S. Lang, Elliptic Curves. Diophantine Analysis, Springer-Verlag, Berlin, 1978.

[194] S. Lang, Algebra, Springer-Verlag, New York, 2002.

[195] L. Lasić, Visine u diofantskoj geometriji i posljedice abc-slutnje, magistarski rad, Sveučilište u Zagrebu, 2009.

[196] F. Lemmermeyer, Reciprocity Laws. From Euler to Eisenstein, Springer, Berlin, 2000.

[197] W. J. LeVeque, Topics in Number Theory I, II, Dover, New York, 1984.

[198] W. J. LeVeque, Fundamentals of Number Theory, Dover, New York, 1996.

[199] R. Lidl, G. L. Mullen, G. Turnwald, Dickson Polynomials, Longman, Essex, 1993.

[200] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.

[201] J. H. van Lint, Introduction to Coding Theory, Springer-Verlag, Berlin, 1999.

[202] A. Lozano-Robledo, Elliptic Curves, Modular Forms and their L-functions, American Mathematical Society, Providence, 2011.

[203] F. Luca, *On shifted products which are powers*, Glas. Mat. Ser. III **40** (2005), 13–20.

[204] F. Luca, L. Szalay, *Fibonacci Diophantine triples*, Glas. Mat. Ser. III **43** (2008), 253–264.

[205] K. Mahler, p-adic Numbers and Their Functions, Cambridge Univesity Press, Cambridge, 1981.

[206] D. A. Marcus, Number Fields, Springer-Verlag, New York, 1977.

[207] S. Mardešić, Matematička analiza 1, Školska knjiga, Zagreb, 1988.

[208] G. Martin, S. Sitar, *Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples*, Mathematika **57** (2011), 1–29.

[209] I. Matić, Uvod u teoriju brojeva, Sveučilište Josipa Jurja Strossmayera, Osijek, 2015.

[210] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[211] M. Mignotte, D. Stefanescu, Polynomials. An Algorithmic Approach, Springer-Verlag, Singapore, 1999.

[212] M. Mihaljinec, *Prilog Fermatovom problemu*, Glasnik mat.–fiz. i astr. **7** (1952), 12–18.

[213] M. Mikić, *On the Mordell-Weil group of elliptic curves induced by families of Diophantine triples*, Rocky Mountain J. Math. **45** (2015), 1565–1589.

[214] R. A. Mollin, Quadratics, CRC Press, Boca Raton, 1996.

[215] H. L. Montgomery, R. C. Vaughan, Multiplicative Number Theory I. Classical Theory, Cambridge University Press, Cambridge, 2007.

[216] L. J. Mordell, Diophantine Equations, Academic Press, New York, 1969.

[217] G. Muić, Algebarske krivulje, skripta, Sveučilište u Zagrebu, 2016.

[218] T. Nagell, Introduction to Number Theory, Chelsea, New York, 1981.

[219] F. Najman, *Integer points on two families of elliptic curves*, Publ. Math. Debrecen **75** (2009), 401–418.

[220] F. Najman, Eliptičke krivulje nad poljima algebarskih brojeva, skripta, Sveučilište u Zagrebu, 2013.

[221] 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.

[222] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Letters **23** (2016), 245–272.

[223] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers, Warszawa, 1974; Springer, Berlin, 2004.

[224] W. Narkiewicz, Classical Problems in Number Theory, PWN, Warszawa, 1986.

[225] B. Nathanson, Additive Number Theory. The Classical Bases, Springer-Verlag, New York, 1996.

[226] J. Neukirch, Algebraic Number Theory, Springer-Verlag, Berlin, 1999.

[227] P. Q. Nguyen, B. Vallee (Eds.), The LLL Algorithm. Survey and Applications, Springer, Berlin, 2010.

[228] I. Niven, Diophantine Approximations, Wiley, New York, 1963.

[229] I. Niven, H. S. Zuckerman, H. L. Montgomery, An Introduction to the Theory of Numbers, Wiley, New York, 1991.

[230] O. Ore, Number Theory and Its History, Dover, New York, 1988.

[231] PARI Group, PARI/GP version 2.11.0, Bordeaux, 2018, `http://pari.math.u-bordeaux.fr/`

[232] J. Park, B. Poonen, J. Voight, M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS), to appear.

[233] S. J. Patterson, An Introduction to the Theory of the Riemann Zeta-Function, Cambridge University Press, Cambridge, 1995.

[234] B. Pavković, B. Dakić, Polinomi, Školska knjiga, Zagreb, 1990.

[235] B. Pavković, B. Dakić, P. Mladinić, Elementarna teorija brojeva, HMD, Element, Zagreb, 1994.

[236] B. Pavković, D. Veljan, Elementarna matematika 1, Tehnička knjiga, Zagreb, 1992.

[237] B. Pavković, D. Veljan, Elementarna matematika 2, Školska knjiga, Zagreb, 1995.

[238] T. Pejković, Iracionalni brojevi, HMD, Zagreb, 2001.

[239] T. Pejković, Rothov teorem, diplomski rad, Sveučilište u Zagrebu, 2005.

[240] T. Pejković, *P-adic root separation for quadratic and cubic polynomials*, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **20** (2016), 9–18.

[241] O. Perron, Die Lehre von den Kettenbruchen I, II, Teubner, 1954.

[242] A. Pethő, Algebraische Algorithmen, Vieweg, Braunschweig, 1999.

[243] V. Petričević, Konvergente verižnih razlomaka i Newtonovi aproksimanti za kvadratne iracionalnosti, Disertacija, Sveučilište u Zagrebu, 2011.

[244] H. Pollard, H.G. Diamond, The Theory of Algebraic Numbers, Dover, New York, 1998.

[245] V. V. Prasolov, Polynomials, Springer, Berlin, 2004.

[246] M. Ram Murty, Problems in Analytic Number Theory, Springer, New York, 2008.

[247] M. Ram Murty, J. Esmonde, Problems in Algebraic Number Theory, Springer, New York, 2005.

[248] J. L. Ramirez Alfonsin, The Diophantine Frobenius Problem, Oxford University Press, Oxford, 2005.

[249] P. Ribenboim, The Book of Prime Number Records, Springer-Verlag, New York, 1988.

[250] H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhäuser, Boston, 1994.

[251] J. Roberts, Elementary Number Theory. A Problem Oriented Approach, MIT Press, Cambridge, 1977.

[252] A. M. Rockett, P. Szusz, Continued Fractions, World Scientific, Singapore, 1992.

[253] H. E. Rose, A Course in Number Theory, Oxford University Press, Oxford, 1995.

[254] K. H. Rosen, Elementary Number Theory and Its Applications, Addison-Wesley, Reading, 1993.

[255] P. Samuel, Algebraic Theory of Numbers, Hermann, Paris, 1970.

[256] A. Schinzel, Polynomials with special regard to reducibility, Cambridge University Press, Cambridge, 2000.

[257] W. M. Schmidt, Diophantine Approximation, Springer-Verlag, Berlin, 1996.

[258] W. M. Schmidt, Diophantine Approximation and Diophantine Equations, Springer-Verlag, Berlin, 1996.

[259] S. Schmitt, H. G. Zimmer, Elliptic Curves. A Computational Approach, de Gruyter, Berlin, 2003.

[260] J.-P. Serre, A Course in Arithmetic, Springer-Verlag, New York, 1996.

[261] J. E. Shockley, Introduction to Number Theory, Holt, Rinehart and Winston, New York, 1967.

[262] T. N. Shorey, R. Tijdeman, Exponential Diophantine Equations, Cambridge University Press, Cambridge, 1986.

[263] W. Sierpiński: Pythagorean Triangles, Dover, New York, 2003.

[264] W. Sierpiński: 250 Problems in Elementary Number Theory, PWN, Warszawa; Elsevier, New York, 1970.

[265] W. Sierpiński, Elementary Theory of Numbers, PNW, Warszawa; North Holland, Amsterdam, 1987.

[266] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer, Dordrecht, 2009.

[267] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, New York, 2015.

[268] J. H. Silverman, J. Tate, Rational Points on Elliptic Curves, Springer, Cham, 2015.

[269] S. Singh, The Code Book, Fourth Estate, London, 1999. (hrvatski prijevod: Šifre. Kratka povijest kriptografije, Mozaik knjiga, Zagreb, 2003.)

[270] J. L. Slater, Generalized Hypergeometric Functions, Cambridge University Press, Cambridge, 1966.

[271] N. P. Smart, The Algorithmic Resolution of Diophantine Equations, Cambridge University Press, Cambridge, 1998.

[272] N. P. Smart, Cryptography. An Introduction, McGraw-Hill, New York, 2002.

[273] I. S. Sominski, The Method of Mathematical Induction, Mir Publishers, Moskva, 1975.

[274] V. G. Sprindzuk, Classical Diophantine Equations, Springer, Berlin, 1993.

[275] H. M. Stark, An Introduction to Number Theory, MIT Press, Cambridge, 1998.

[276] J. Steudings, Diophantine Analysis, CRC Press, Boca Raton, 2005.

[277] C. L. Stewart, Linear Forms in Logarithms and Diophantine Equations, Lecture notes, University of Waterloo, 2005.

[278] I. Stewart, D. Tall, Algebraic Number Theory and Fermat's Last Theorem, A K Peters, Natick, 2002.

[279] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

[280] D. R. Stinson, Cryptography. Theory and Practice, CRC Press, Boca Raton, 2005.

[281] M. Stoll, *Diagonal genus* 5 *curves, elliptic curves over* $\mathbb{Q}(t)$*, and rational diophantine quintuples*, Acta Arith., to appear.

[282] V. Stošić, Matematička natjecanja učenika osnovnih škola, HMD, Element, Zagreb, 1994.

[283] Z. Šikić, Z. Šćekić, Matematika i muzika, Profil, Zagreb, 2013.

[284] B. Širola, *Distribucija prim brojeva i Riemannova zeta-funkcija*, Hrvatski matematički elektronički časopis math.e **13** (2008).

[285] B. Širola, Algebarske strukture, skripta, Sveučilište u Zagrebu, 2008.

[286] R. Takloo-Bighash, A Pythagorean Introduction to Number Theory. Right Triangles, Sums of Squares, and Arithmetic, Springer, Cham, 2018.

[287] E. C. Titchmarsh, The Theory of the Riemann Zeta-Function, Claredon Press, Oxford, 1986.

[288] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* $3/2$, Invent. Math. **72** (1983), 323–334.

[289] N. Tzanakis, *Explicit solution of a class of quartic Thue equations*, Acta Arith. **64** (1993), 271–283.

[290] N. Tzanakis, Elliptic Diophantine Equations. A Concrete Approach Via the Elliptic Logarithm, de Gruyter, Berlin, 2013.

[291] D. Ugrin-Šparac, *Jedno viđenje suvremene teorije brojeva*, Brojevi, Školska knjiga, Zagreb, 1985.

[292] Š. Ungar, Matematička analiza 4, skripta, Sveučilište u Zagrebu, 2008.

[293] S. Vajda, Fibonacci & Lucas Numbers, and the Golden Section, theory and applications, Ellis Horwood, Chichester, 1989.

[294] I. Vidav, Eliptične krivulje in eliptične funkcije, Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana, 1991.

[295] I. M. Vinogradov, Elements of Number Theory, Dover, New York, 1954.

[296] N. V. Vorobiev, Fibonacci Numbers, Birkhäuser, Basel, 2002.

[297] M. Vuković, Matematička logika, Element, Zagreb, 2009.

[298] M. Waldschmidt, Diophantine Approximation on Linear Algebraic Groups, Springer-Verlag, Berlin, 2000.

[299] D. D. Wall, *Fibonacci series modulo* m, Amer. Math. Monthly **67** (1960), 525–532.

[300] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, Boca Raton, 2008.

[301] B. M. M. de Weger, Algorithms for Diophantine Equations, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[302] S. H. Weintraub, Factorization. Unique and Otherwise, CMS, Ottawa; A K Peters, Wellesley, 2008.

[303] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), 553–558.

[304] R. T. Worley, *Estimating* $|\alpha - p/q|$, Austral. Math. Soc. Ser. A **31** (1981), 202–206.

[305] S. Y. Yan, Quantum Attacks on Public-Key Cryptosystems, Springer, New York, 2013.

Indeks oznaka

$\mathbb{N}$	skup prirodnih brojeva
$\mathbb{Z}$	skup cijelih brojeva
$\mathbb{Q}$	skup racionalnih brojeva
$\mathbb{R}$	skup realnih brojeva
$\mathbb{C}$	skup kompleksnih brojeva
$\square$	oznaka za kraj dokaza
$\diamondsuit$	oznaka za kraj rješenja
$n!$	faktorijel
$\binom{n}{k}$	binomni koeficijent
L_n	n-ti Lucasov broj
F_n	n-ti Fibonaccijev broj
$a \mid b$	a dijeli b
$a \nmid b$	a ne dijeli b
$a^k \parallel b$	a^k je najveća potencija od a koja dijeli b
$\mathrm{nzd}(a, b)$	najveći zajednički djelitelj brojeva a i b
$\log_b(x)$	logaritam po bazi b
$\ln(x)$	prirodni logaritam
$\mathrm{nzv}(a, b)$	najmanji zajednički višekratnik brojeva a i b
$\min(a, b)$	minimum brojeva a i b
$\max(a, b)$	maksimum brojeva a i b
f_n	Fermatov broj $2^{2^n} + 1$
M_p	Mersenneov broj $2^p - 1$
$a \equiv b \pmod{m}$	a je kongruentan b modulo m
$a \not\equiv b \pmod{m}$	a nije kongruentan b modulo m
$\varphi(m)$	Eulerova funkcija
$\mathrm{ind}_g\, a$	indeks od a u odnosu na primitivni korijen g
$\mathrm{psp}(b)$	pseudoprosti broj u bazi b
$\mathrm{spsp}(b)$	jaki pseudoprosti broj u bazi b
$(\frac{a}{p})$	Legendreov simbol

$\lvert A\rvert$	broj elemenata konačnog skupa A
$(\frac{a}{Q})$	Jacobijev simbol
$\mathrm{lpsp}(a,b)$	Lucasov pseudoprosti broj
A^τ	transponirana matrica matrice A
$h(d)$	broj reduciranih formi s diskriminantom d
t_m	m-ti trokutasti broj
$\lfloor x\rfloor$	najveći cijeli broj $\leq x$
$\lceil x\rceil$	najmanji cijeli broj $\geq x$
$\{x\}$	razlomljeni dio od x
$\mu(n)$	Möbiusova funkcija
$\sigma(n)$	suma djelitelja broja n
$\tau(n)$	broj djelitelja broja n
$f(x)=O(g(x))$	$\lvert f(x)\rvert \leq Cg(x)$ za neku konstantu C
$f(x)=o(g(x))$	$\lim_{x\to\infty} f(x)/g(x)=0$
$f(x)\ll g(x)$	$\lvert f(x)\rvert \leq Cg(x)$ za neku konstantu C
$g(x)\gg f(x)$	isto kao $f(x)\ll g(x)$
γ	Eulerova konstanta
$f*g$	Dirichletov produkt
$\omega(n)$	broj prostih djelitelja broja n
$\pi(x)$	broj prostih brojeva koji su $\leq x$
$\mathrm{li}(x)$	logaritamsko-integralna funkcija
$\Lambda(n)$	Von Mangoldtova funkcija
$\psi(x)$	Čebiševljeva funkcija ψ
$\vartheta(x)$	Čebiševljeva funkcija ϑ
$\zeta(s)$	Riemannova zeta-funkcija
$\mathrm{Re}(s)$	realni dio kompleksnog broja s
$\mathrm{Im}(s)$	imaginarni dio kompleksnog broja s
$\Gamma(s)$	gama-funkcija
B_n	n-ti Bernoullijev broj
$\chi(n)$	Dirichletov karakter
$L(s,\chi)$	Dirichletova L-funkcija
$\lVert\alpha\rVert$	udaljenost od α do najbližeg cijelog broja
$\mathcal{F}_n$	Fareyjev niz reda n
$[a_0,a_1,\ldots,a_n]$	konačni verižni razlomak
$[a_0,a_1,\ldots]$	beskonačni verižni razlomak
$\frac{p_i}{q_i}$	i-ta konvergenta verižnog razlomka
$\frac{p_{n,r}}{q_{n,r}}$	sekundarna konvergenta verižnog razlomka
$M(\alpha)$	Markovljeva konstanta
$\lVert x\rVert$	$\max(\lvert x_1\rvert,\ldots,\lvert x_n\rvert)$, za $x=(x_1,\ldots,x_n)$

$\lfloor x \rceil$	najbliži cijeli broj realnom broju x
$g(a_1, \ldots, a_n)$	Frobeniusov broj
$\nu_p(x)$	p-adska valuacija
$\lvert x \rvert_p$	p-adska norma
$(\frac{\alpha,\beta}{p})$	Hilbertov simbol
$R[x]$	prsten polinoma nad R
$\mathrm{cont}(f)$	sadržaj polinoma f
$\mathrm{Res}(f, g)$	rezultanta polinoma f i g
$\mathrm{Disc}(f)$	diskriminanta polinoma f
$D_m(x, a)$	Dicksonov polinom
$T_n(x)$	Čebiševljev polinom prve vrste
$U_n(x)$	Čebiševljev polinom druge vrste
$F_n(x)$	Fibonaccijev polinom
$\sigma_k(x_1, \ldots, x_n)$	elementarni simetrični polinomi
$N(\alpha)$	norma algebarskog broja
$T(\alpha)$	trag algebarskog broja
$N_{\mathbb{K}/\mathbb{Q}}(\alpha)$	norma od α s obzirom na $\mathbb{K}$
$T_{\mathbb{K}/\mathbb{Q}}(\alpha)$	trag od α s obzirom na $\mathbb{K}$
$\mathcal{O}_{\mathbb{K}}$	skup svih algebarskih cijelih brojeva iz $\mathbb{K}$
$<\alpha>$	glavni ideal generiran s α
$N(\mathfrak{a})$	norma ideala $\mathfrak{a}$
$h(\mathbb{K})$	broj klasa polja brojeva $\mathbb{K}$
$\zeta_{\mathbb{K}}(s)$	Dedekindova zeta-funkcija
$F(\overset{\alpha,\beta}{\gamma}\lvert x)$	hipergeometrijska funkcija
$H(P)$	visina polinoma P
$M(P)$	Mahlerova mjera polinoma P
$e(P)$	eksponent separacije polinoma P
$\overline{K}$	algebarsko zatvorenje polja K
$\wp$	Weierstrassova $\wp$-funkcija
$E(\mathbb{Q})_{\mathrm{tors}}$	torzijska grupa eliptičke krivulje
$\mathrm{rank}(E(\mathbb{Q}))$	rang eliptičke krivulje
$\hat{h}$	kanonska visina
$\langle P, Q \rangle$	Néron-Tateovo sparivanje
$\mathbb{F}_q$	konačno polje s q elemenata
$\mathrm{rad}(f)$	radikal polinoma f
$\mathrm{rad}(m)$	radikal prirodnog broja m

Indeks pojmova

Lektorica
Silvija Legin, prof.

Korektor
doc. dr. sc. Tomislav Pejković

Naslovnicu opremio
Marijan Zafron

Grafička priprema
Grafičko-likovna redakcija Školske knjige

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