

UDŽBENICI SVEUČILIŠTA U ZAGREBU
MANUALIA UNIVERSITATIS STUDIORUM ZAGRABIENSIS



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.

© ŠKOLSKA KNJIGA, d. d., Zagreb, 2019.

Nijedan dio ovog udžbenika ne smije se umnožavati,
fotokopirati ni na bilo koji način reproducirati
bez nakladnikova pismenog dopuštenja.

akademik Andrej Dujella

Teorija brojeva

drugo popravljeno izdanje

Zagreb, 2024.

Školska knjiga

Predgovor prvom izdanju

Teorija brojeva grana je matematike koja se ponajprije bavi proučavanjem svojstava prirodnih brojeva kao što su djeljivost, rastav na proste faktore ili rješivost jednažbi 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 jednažbe* 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 [78] 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* [246]. 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 [210], “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 [89, 156, 188, 234, 237]. Ostala postojeća literatura na hrvatskom jeziku odnosi se ponajprije na neke dijelove elementarne teorije brojeva [135, 226, 252, 254], a spomenimo i knjižicu *Brojevi* koja sadržava zanimljiv pregled i viđenje teorije brojeva [309]. 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 (Poglavljja 9 i 15.8), o čemu zainteresirani čitatelj može dodatne informacije naći u knjizi [115]. Spomenimo još i da se kroz više poglavlja (osobito Potpoglavljja 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 [80].

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, 71, 115, 153, 174, 175, 176, 263, 264, 268, 270, 271, 282, 283, 300, 313], 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 Jursić, 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

Predgovor drugom izdanju

Prvo izdanje *Teorije brojeva*, objavljeno na hrvatskom jeziku 2019. godine, rasprodano je u roku od samo četiri godine. Očito veliko zanimanje za tu knjigu pridonijelo je njezinu ponovnom izdavanju. Ta je prilika iskorištena za to da se u tekst unesu ispravci i sitnija objašnjenja za koja je nakon objave prvog izdanja uočeno da su potrebna te da se na nekim mjestima tekst ažurira novim informacijama i referencama. To se posebno odnosi na poglavlja knjige koja obrađuju teme ranga eliptičkih krivulja i Diofantovih m -torki što su vrlo aktivna istraživačka područja u kojima su u međuvremenu postignuti važni rezultati, a oni zavrjeđuju da se spomenu u knjizi. Pritom se pazilo na to da numeracija definicija, teorema i sl. ostane nepromijenjena u odnosu prema prvom izdanju s obzirom na to da je ono već citirano u mnogobrojnim člancima te seminarskim i diplomskim radovima.

Hvala svima koji su me upozorili na veće ili manje potrebne ispravke u prvom izdanju. To su, abecednim redom, Alejandra Alvarado, Sunben Chiu, Mihai Cipu, Lovro Čupić, Zrinka Franušić, Clemens Fuchs, Ivica Gusić, Lajos Hajdu, Tomislav Pejković, Attila Pethő, Johannes Schleisnitz, Lovro Sindičić, Boris Širola, Jagor Tambača, Antonela Trbović i Marin Varivoda. Dio sugestija dali su kolege koji su čitali neku od verzija engleskog izdanja knjige koje je pod naslovom *Number Theory* objavljeno 2021. godine u izdanju Školske knjige. Engleski prijevod ove knjige imao je dobar međunarodni odjek i uvršten je u knjižni fond stotinjak sveučilišnih knjižnica širom svijeta. Sugestije i ispravci skupljani su i redovito objavljeni na mrežnoj stranici knjige. Svi su uneseni u ovo drugo izdanje te su ažurirani podatci na odgovarajućim mjestima u knjizi. Dopunjen je i popis literature uključujući i nedavno objavljenu zbirku zadataka iz teorije brojeva na hrvatskom jeziku [185]. Hvala svima koji su kupili prvo izdanje knjige te tako pridonijeli tomu da se tiska drugo izdanje. Zahvaljujem i uredništvu Školske knjige na susretljivosti u organiziranju pripreme drugog izdanja.

Novigrad i Zagreb, prosinac 2023.

akad. Andrej Dujella

Sadržaj

Predgovor prvom izdanju	i
Predgovor drugom izdanju	v
1 Uvod	1
1.1 Peanovi aksiomi	1
1.2 Princip matematičke indukcije	4
1.3 Fibonaccijevi brojevi	9
1.4 Zadatci	17
2 Djeljivost	21
2.1 Najveći zajednički djelitelj	21
2.2 Euklidov algoritam	24
2.3 Prosti brojevi	29
2.4 Zadatci	37
3 Kongruencije	40
3.1 Definicija i svojstva kongruencija	40
3.2 Pravila za djeljivost	43
3.3 Linearne kongruencije	46
3.4 Kineski teorem o ostacima	48
3.5 Reducirani sustav ostataka	51
3.6 Kongruencije po prostom modulu	55
3.7 Primitivni korijeni i indeksi	60
3.8 Decimalni zapis racionalnog broja	65
3.9 Pseudoprosti brojevi	69
3.10 Zadatci	75
4 Kvadratni ostatci	79
4.1 Legendreov simbol	79

4.2	Kvadratni zakon reciprociteta	85
4.3	Računanje kvadratnog korijena modulo p	89
4.4	Jacobijev simbol	91
4.5	Djeljivost Fibonaccijevih brojeva	94
4.6	Zadatci	99
5	Kvadratne forme	102
5.1	Sume dvaju kvadrata	102
5.2	Pozitivno definitne kvadratne forme	106
5.3	Sume četiriju kvadrata	115
5.4	Sume triju kvadrata	119
5.5	Zadatci	127
6	Aritmetičke funkcije	130
6.1	Funkcija najveće cijelo	130
6.2	Multiplikativne funkcije	134
6.3	Asimptotske ocjene za aritmetičke funkcije	139
6.4	Dirichletov produkt	145
6.5	Zadatci	148
7	Distribucija prostih brojeva	152
7.1	Elementarne ocjene za funkciju $\pi(x)$	152
7.2	Čebiševljeve funkcije	157
7.3	Riemannova zeta-funkcija	165
7.4	Dirichletovi karakteri	169
7.5	Prosti brojevi u aritmetičkom nizu	176
7.6	Zadatci	180
8	Diofantske aproksimacije	184
8.1	Dirichletov teorem	184
8.2	Fareyjevi nizovi	187
8.3	Verižni razlomci	194
8.4	Verižni razlomci i aproksimacija iracionalnih brojeva	201
8.5	Ekvivalentni brojevi	210
8.6	Periodski verižni razlomci	215
8.7	Newtonovi aproksimanti	221
8.8	Simultane aproksimacije	225
8.9	LLL-algoritam	232
8.10	Zadatci	239

9	Primjena diofantskih aproksimacija u kriptografiji	243
9.1	Vrlo kratki uvod u kriptografiju	243
9.2	Kriptosustav RSA	247
9.3	Wienerov napad na kriptosustav RSA	250
9.4	Napadi na RSA koji se koriste LLL-algoritmom	253
9.5	Coppersmithov teorem	256
9.6	Zadatci	259
10	Diofantske jednadžbe I	263
10.1	Linearne diofantske jednadžbe	263
10.2	Pitagorine trojke	267
10.3	Pellova jednadžba	277
10.4	Verižni razlomci i Pellova jednadžba	285
10.5	Pelovska jednadžba	289
10.6	Kvadrati u Fibonaccijevu nizu	294
10.7	Ternarne kvadratne forme	298
10.8	Lokalno-globalni princip	311
10.9	Zadatci	319
11	Polinomi	324
11.1	Djeljivost polinoma	324
11.2	Korijeni polinoma	331
11.3	Ireducibilnost polinoma	337
11.4	Dekompozicija polinoma	340
11.5	Simetrični polinomi	347
11.6	Zadatci	352
12	Algebarski brojevi	355
12.1	Kvadratna polja	355
12.2	Polja algebarskih brojeva	365
12.3	Algebarski cijeli brojevi	369
12.4	Ideali	373
12.5	Jedinice i klase ideala	380
12.6	Zadatci	387
13	Aproksimacija algebarskih brojeva	389
13.1	Liouvilleov teorem	389
13.2	Rothov teorem	391
13.3	Hipergeometrijska metoda	394
13.4	Aproksimacija kvadratnim iracionalnostima	403

13.5	Separacija korijena polinoma	408
13.6	Zadatci	414
14	Diofantske jednadžbe II	417
14.1	Thueova jednadžba	417
14.2	Tzanakisova metoda	421
14.3	Linearne forme u logaritmima	426
14.4	Baker-Davenportova redukcija	431
14.5	LLL-redukcija	436
14.6	Diofantove m -torke	440
14.7	Zadatci	448
15	Eliptičke krivulje	451
15.1	Uvod u eliptičke krivulje	451
15.2	Jednadžbe eliptičke krivulje	458
15.3	Torzijska grupa	471
15.4	Kanonska visina i Mordell-Weilov teorem	483
15.5	Rang eliptičke krivulje	490
15.6	Konačna polja	504
15.7	Eliptičke krivulje nad konačnim poljima	510
15.8	Primjena eliptičkih krivulja u kriptografiji	519
15.9	Dokazivanje prostosti s pomoću eliptičkih krivulja	527
15.10	Faktorizacija s pomoću eliptičkih krivulja	531
15.11	Zadatci	535
16	Diofantski problemi i eliptičke krivulje	540
16.1	Kongruentni brojevi	540
16.2	Mordellova jednadžba	542
16.3	Primjena faktorizacije u kvadratnim poljima	544
16.4	Transformacija eliptičkih krivulja u Thueove jednadžbe	549
16.5	Algoritam za rješavanje Thueove jednadžbe	551
16.6	abc slutnja	557
16.7	Diofantove m -torke i eliptičke krivulje	561
16.8	Zadatci	569
	Bibliografija	572
	Indeks oznaka	593
	Indeks pojmova	596

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.* **11**(1) (2021), 1950020.
- [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. Bačić, A. Filipin, *A note on the number of $D(4)$ -quintuples*, *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.* **18** (2014), 7–13.

BIBLIOGRAFIJA

- [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] N. C. Bonciocat, M. Cipu, M. Mignotte, *There is no Diophantine $D(-1)$ -quadruple*, J. London Math. Soc. **105** (2022), 63–99.
- [33] O. Bordelles, *Arithmetic Tales*, Springer, London, 2012.
- [34] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1986.
- [35] 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.
- [36] E. Brown, *Sets in which $xy + k$ is always a square*, Math. Comp. **45** (1985), 613–620.
- [37] D. A. Buell, *Binary Quadratic Forms*, Springer-Verlag, New York, 1989.
- [38] Y. Bugeaud, *Approximation by Algebraic Numbers*, Cambridge University Press, Cambridge, 2004.
- [39] Y. Bugeaud, *Linear Forms in Logarithms and Applications*, IRMA Lectures in Mathematics and Theoretical Physics Vol. **28**, European Mathematical Society, Zürich, 2018.
- [40] Y. Bugeaud, A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. **135** (2003), 1–10.
- [41] Y. Bugeaud, A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. **43** (2011), 1239–1244.
- [42] Y. Bugeaud, A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. **162** (2014), 393–403.
- [43] Y. Bugeaud, A. Dujella, W. Fang, T. Pejković, B. Salvy, *Absolute root separation*, Experiment. Math. **31** (2022), 806–813.

BIBLIOGRAFIJA

- [44] Y. Bugeaud, A. Dujella, T. Pejković, B. Salvy, *Absolute real root separation*, Amer. Math. Monthly **124** (2017), 930–936.
- [45] Y. Bugeaud, M. Mignotte, *Polynomial root separation*, Intern. J. Number Theory **6** (2010), 587–602.
- [46] 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.
- [47] 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.
- [48] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer-Verlag, Berlin, 2008.
- [49] R. D. Carmichael, *The Theory of Numbers and Diophantine Analysis*, Dover, New York, 1959.
- [50] J. W. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Berlin, 1997.
- [51] W. Castryck, T. Decru, *An efficient key recovery attack on SIDH*, Lecture Notes in Comput. Sci. **14008**, Springer, Cham, 2023, pp. 423–447.
- [52] K. Chakraborty, S. Gupta, A. Hoque, *On a conjecture of Franušić and Jadrijević: Counter-examples*, Results Math. **78** (2023), Article 18.
- [53] H. H. Chan, *Analytic Number Theory for Undergraduates*, World Scientific, Singapore, 2009.
- [54] M. Cipu, Y. Fujita, *On the length of $D(\pm 1)$ -tuples in imaginary quadratic rings*, Bull. Lond. Math. Soc., to appear.
- [55] M. Cipu, Y. Fujita, T. Miyazaki, *On the number of extensions of a Diophantine triple*, Int. J. Number Theory **14** (2018), 899–917.
- [56] H. Cohen, *Number Theory. Volume I: Tools and Diophantine Equations*, Springer Verlag, Berlin, 2007.
- [57] H. Cohen, *Number Theory. Volume II: Analytic and Modern Tools*, Springer Verlag, Berlin, 2007.
- [58] H. Cohn, *Advanced Number Theory*, Dover, New York, 1980.

- [59] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28.
- [60] A. C. Cojocaru, M. Ram Murti, *An Introduction to Sieve Methods and Their Applications*, Cambridge University Press, Cambridge, 2005.
- [61] I. Connell, *Elliptic Curve Handbook*, McGill University, Montreal, 1999.
- [62] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology **10** (1997), 233–260.
- [63] D. A. Cox, *Primes of the Form $x^2 + ny^2$* , John Wiley & Sons, New York, 1989.
- [64] R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, New York, 2005.
- [65] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1997.
- [66] T. W. Cusick, M. E. Flahive, *The Markoff and Lagrange Spectra*, American Mathematical Society, Providence, 1989.
- [67] H. Čavrak, *Enigma*, Hrvatski matematički elektronički časopis math.e **3** (2004).
- [68] A. Das, *Computational Number Theory*, CRC Press, Boca Raton, 2013.
- [69] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York, 1980.
- [70] J.-M. De Koninck, F. Luca, *Analytic Number Theory. Exploring the Anatomy of Integers*, American Mathematical Society, Providence, 2012.
- [71] J.-M. De Koninck, A. Mercier, *1001 Problems in Classical Number Theory*, American Mathematical Society, Providence, 2007.
- [72] C. A. Deavours, L. Kruh, *Machine Cryptography and Modern Cryptanalysis*, Artech House, Norwood, 1985.
- [73] E. Deza, M. M. Deza, *Figurate Numbers*, World Scientific, Singapore, 2012.
- [74] L. E. Dickson, *History of the Theory of Numbers, Volume 2: Diophantine analysis*, Chelsea, New York, 1966.

BIBLIOGRAFIJA

- [75] R. Dietmann, C. Elsholtz, *Sums of two squares and one biquadrate*, *Funct. Approx. Comment. Math.* **38** (2008), 233–234.
- [76] A. Dujella, *Generalization of a problem of Diophantus*, *Acta Arith.* **65** (1993), 15–27.
- [77] A. Dujella, *Pitagorine trojke*, Bilten seminara iz matematike za nastavnike mentore, Crikvenica, 1994, pp. 1–10.
- [78] A. Dujella, *Uvod u teoriju brojeva*, skripta, Sveučilište u Zagrebu, 1999.
- [79] A. Dujella, *Verižni razlomci i problem kalendara*, *Matematika i škola* 1 (1999), no. 2, 74–77.
- [80] A. Dujella, *Fibonaccijevi brojevi*, HMD, Zagreb, 2000.
- [81] A. Dujella, *A parametric family of elliptic curves*, *Acta Arith.* **94** (2000), 87–101.
- [82] A. Dujella, *Newton's formula and continued fraction expansion of \sqrt{d}* , *Experiment. Math.* **10** (2001), 125–131.
- [83] A. Dujella, *On the size of Diophantine m -tuples*, *Math. Proc. Cambridge Philos. Soc.* **132** (2002), 23–33.
- [84] A. Dujella, *There are only finitely many Diophantine quintuples*, *J. Reine Angew. Math.* **566** (2004), 183–214.
- [85] A. Dujella, *Bounds for the size of sets with the property $D(n)$* , *Glas. Mat. Ser. III* **39** (2004), 199–205.
- [86] A. Dujella, *Continued fractions and RSA with small secret exponent*, *Tatra Mt. Math. Publ.* **29** (2004), 101–112.
- [87] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, *Glas. Mat. Ser. III* **42** (2007), 3–18.
- [88] A. Dujella, *On the number of Diophantine m -tuples*, *Ramanujan J.* **15** (2008), 37–46.
- [89] A. Dujella, *Algoritmi za eliptičke krivulje*, skripta, Sveučilište u Zagrebu, 2009.
- [90] A. Dujella, *A variant of Wiener's attack on RSA*, *Computing* **85** (2009), 77–83.
- [91] A. Dujella, *On Hall's conjecture*, *Acta Arith.* **147** (2011), 397–402.

- [92] A. Dujella, *What is ... a Diophantine m -tuple?*, Notices Amer. Math. Soc. **63** (2016), 772–774.
- [93] A. Dujella, *Diophantine m -tuples*
<https://web.math.pmf.unizg.hr/~duje/dtuples.html>
- [94] A. Dujella, *High rank elliptic curves with prescribed torsion*
<https://web.math.pmf.unizg.hr/~duje/tors/tors.html>
- [95] A. Dujella, *History of elliptic curves rank records*
<https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html>
- [96] A. Dujella, *High rank elliptic curves with prescribed torsion over quadratic fields*
<https://web.math.pmf.unizg.hr/~duje/tors/torsquad.html>
- [97] A. Dujella, A. Filipin, C. Fuchs, *Effective solution of the $D(-1)$ -quadruple conjecture*, Acta Arith. **128** (2007), 319–338.
- [98] A. Dujella, C. Fuchs, *Complete solution of the polynomial version of a problem of Diophantus*, J. Number Theory **106** (2004), 326–344.
- [99] A. Dujella, C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71** (2005), 33–52.
- [100] A. Dujella, I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. (Oxford) **57** (2006), 193–201.
- [101] A. Dujella, I. Gusić, *Decomposition of a recursive family of polynomials*, Monatsh. Math. **152** (2007), 97–104.
- [102] A. Dujella, B. Ibrahimpašić, *On Worley's theorem in Diophantine approximations*, Ann. Math. Inform. **35** (2008), 61–73.
- [103] A. Dujella, B. Jadrijević, *A parametric family of quartic Thue equations*, Acta Arith. **101** (2002), 159–170.
- [104] A. Dujella, B. Jadrijević, *A family of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.
- [105] 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.
- [106] 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.

BIBLIOGRAFIJA

- [107] 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.
- [108] 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.
- [109] 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.
- [110] A. Dujella, M. Kazalicki, J. C. Peral, *Elliptic curves with torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$* , Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **115** (2021), Article 169.
- [111] A. Dujella, M. Kazalicki, V. Petričević, *Rational Diophantine sextuples with square denominators*, J. Number Theory **205** (2019), 340–346.
- [112] A. Dujella, M. Kazalicki, V. Petričević, *Rational Diophantine sextuples containing two regular quadruples and one regular quintuple*, Acta Mathematica Spalatensia **1** (2021), 19–27.
- [113] A. Dujella, M. Kazalicki, V. Petričević, *$D(n)$ -quintuples with square elements*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **115** (2021), Article 172.
- [114] A. Dujella, F. Luca, *Diophantine m -tuples for primes*, Int. Math. Res. Not. **47** (2005), 2913–2940.
- [115] A. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007.
- [116] 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.
- [117] 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.
- [118] A. Dujella, T. Pejković, *Root separation for reducible monic quartics*, Rend. Semin. Mat. Univ. Padova **126** (2011), 63–72.
- [119] 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.

- [120] 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.
- [121] 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.
- [122] A. Dujella, J. C. Peral, *High rank elliptic curves induced by rational Diophantine triples*, Glas. Mat. Ser. III **55** (2020), 237–252.
- [123] A. Dujella, J. C. Peral, *Construction of high rank elliptic curves*, J. Geom. Anal. **31** (2021), 6698–6724.
- [124] A. Dujella, A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.
- [125] A. Dujella, A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), 321–335.
- [126] A. Dujella, V. Petričević, *Square roots with many good approximants*, Integers **5(3)** (2005), #A6. (13pp)
- [127] A. Dujella, V. Petričević, *Strong Diophantine triples*, Experiment. Math. **17** (2008), 83–89.
- [128] 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.
- [129] A. Dujella, V. Petričević, *Doubly regular Diophantine quadruples*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **114** (2020), Article 189.
- [130] A. Dujella, N. Saradha, *Diophantine m -tuples with elements in arithmetic progressions*, Indag. Math. (N.S.) **25** (2014), 131–136.
- [131] A. Dujella, R. F. Tichy, *Diophantine equations for second order recursive sequences of polynomials*, Quart. J. Math. Oxford Ser. (2) **52** (2001), 161–169.
- [132] H. M. Edwards, *Riemann's Zeta Function*, Academic Press, New York, 1974.
- [133] H. M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), 393–422.

BIBLIOGRAFIJA

- [134] N. Elezović, *A note on continued fractions of quadratic irrationals*, Math. Commun. **2** (1997), 27–33.
- [135] N. Elezović, *Diskontna matematika 1*, Element, Zagreb, 2017.
- [136] 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.
- [137] G. Everest, T. Ward, *An Introduction to Number Theory*, Springer-Verlag, London, 2005.
- [138] J.-H. Evertse, K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge University Press, Cambridge, 2015.
- [139] J.-H. Evertse, K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge University Press, Cambridge, 2017.
- [140] A. Filipin, *Primjena LLL-algoritma u rješavanju diofantskih jednadžbi*, magistarski rad, Sveučilište u Zagrebu, 2004.
- [141] A. Filipin, *There does not exist a $D(4)$ -sextuple*, J. Number Theory **128** (2008), 1555–1565.
- [142] A. Filipin, *Linearne forme u logaritmima i diofantska analiza*, skripta, Sveučilište u Zagrebu, 2010.
- [143] A. Filipin, A. Jurasić, *A polynomial variant of a problem of Diophantus and its consequences*, Glas. Mat. Ser. III **54** (2019), 21–52.
- [144] B. Fine, A. Gaglione, A. Moldenhauer, G. Rosenberger, D. Spellman, *Algebra and Number Theory. A Selection of Highlights*, De Gruyter, Berlin, 2017.
- [145] Z. Franušić, *Diophantine quadruples in $\mathbb{Z}[\sqrt{4k+3}]$* , Ramanujan J. **17** (2008), 77–88.
- [146] Z. Franušić, *A Diophantine problem in $\mathbb{Z}[(1+\sqrt{d})/2]$* , Studia Sci. Math. Hungar. **46** (2009), 103–112.
- [147] 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.
- [148] Y. Fujita, T. Miyazaki, *The regularity of Diophantine quadruples*, Trans. Amer. Math. Soc. **370** (2018), 3803–3831.

- [149] I. Gaál, *Diophantine Equations and Power Integral Bases*, Birkhäuser, Boston, 2002.
- [150] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.
- [151] P. E. Gibbs, *A survey of rational Diophantine sextuples of low height*, preprint, 2016.
- [152] F. Q. Gouvêa, *p -adic Numbers. An Introduction*, Springer, Berlin, 2003.
- [153] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics - A foundation for computer science*, Addison-Wesley, Reading, 1989.
- [154] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167** (2008), 481–547.
- [155] P. M. Gruber, C. G. Lekkerkerker, *Geometry of Numbers*, North Holland, Amsterdam, 1987.
- [156] I. Gusić, *Uvod u aritmetiku eliptičkih krivulja*, skripta, Sveučilište u Zagrebu, 2008.
- [157] I. Gusić, *On decomposition of polynomials over rings*, Glas. Mat. Ser. III **43** (2008), 7–12.
- [158] I. Gusić, P. Tadić, *A remark on the injectivity of the specialization homomorphism*, Glas. Mat. Ser. III **47** (2012), 265–275.
- [159] I. Gusić, P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory **148** (2015), 137–152.
- [160] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 2004.
- [161] K. Gyarmati, C. L. Stewart, *On powers in shifted products*, Glas. Mat. Ser. III **42** (2007), 273–279.
- [162] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, 2004.
- [163] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 2008.
- [164] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), 6665–6709.

BIBLIOGRAFIJA

- [165] T. L. Heath, *Diophantus of Alexandria: A study in the history of Greek Algebra*, Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003.
- [166] D. Hensley, *Continued Fractions*, World Scientific, Singapore, 2006.
- [167] M. Hindry, J. H. Silverman, *Diophantine Geometry. An Introduction*, Springer-Verlag, New York, 2000.
- [168] M. J. Hinek, *Cryptanalysis of RSA and Its Variants*, CRC Press, Boca Raton, 2009.
- [169] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, New York, 2008.
- [170] V. E. Hoggatt, Jr., *Fibonacci and Lucas Numbers*, The Fibonacci Association, Santa Clara, 1979.
- [171] K. Horvatić, *Linearna algebra*, Golden Marketing - Tehnička knjiga, Zagreb, 2004.
- [172] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
- [173] D. Husemüller, *Elliptic Curves*, Springer-Verlag, New York, 2004.
- [174] B. Hutz, *An Experimental Introduction to Number Theory*, American Mathematical Society, Providence, 2018.
- [175] B. Ibrahimpašić, *Kriptografija kroz primjere*, Pedagoški fakultet Bihać, Bihać, 2011.
- [176] B. Ibrahimpašić, *Uvod u teoriju brojeva*, Pedagoški fakultet Bihać, Bihać, 2014.
- [177] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1998.
- [178] M. J. Jacobson, H. C. Williams, *Modular arithmetic on elements of small norm in quadratic fields*, *Des. Codes and Cryptogr.* **27** (2002), 93–110.
- [179] M. J. Jacobson, H. C. Williams, *Solving the Pell Equation*, Springer, New York, 2009.
- [180] B. Jadrijević, *Dvoparametarska familija Thueovih jednadžbi četvrtog stupnja*, Disertacija, Sveučilište u Zagrebu, 2001.

- [181] 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.
- [182] G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
- [183] 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.
- [184] B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, The Mathematical Association of America, New York, 1950.
- [185] M. Jukić Bokun, I. Soldo, *Zbirka zadataka iz teorije brojeva*, Fakultet primijenjene matematike i informatike, Sveučilište Josipa Jurja Strossmayera u Osijeku, 2023.
- [186] A. Jurasić, *Diofantske jednadžbe nad funkcijskim poljima*, magistarski rad, Sveučilište u Zagrebu, 2006.
- [187] 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.)
- [188] M. Kazalicki, *Modularne forme*, skripta, Sveučilište u Zagrebu, 2017.
- [189] M. Kazalicki, B. Naskrecki (with an appendix by L. Lasić), *Diophantine triples and $K3$ surfaces*, *J. Number Theory* **236** (2022), 41–70.
- [190] H. L. Keng, *Introduction to Number Theory*, Springer-Verlag, Berlin, 1982.
- [191] M. Kiseljak, *Prilozi za teoriju savršenih brojeva*, Kr. zemaljska tiskara, Zagreb, 1911.
- [192] A. Ya. Khinchin, *Continued Fractions*, Dover, New York, 1997.
- [193] A. W. Knap, *Elliptic Curves*, Princeton University Press, Princeton, 1992.
- [194] D. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms*, Addison-Wesley, Reading, 1981.
- [195] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.

BIBLIOGRAFIJA

- [196] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1996.
- [197] N. Koblitz, p -adic Numbers, p -adic Analysis, and Zeta Functions, Springer-Verlag, New York, 1996.
- [198] T. Koshy, Fibonacci and Lucas Numbers with Applications, Wiley, New York, 2001.
- [199] J. S. Kraft, L. C. Washington, An Introduction to Number Theory with Cryptography, CRC Press, Boca Raton, 2018.
- [200] H. Kraljević, Odabrana poglavlja teorije analitičkih funkcija, skripta, Sveučilište u Zagrebu, 2010.
- [201] H. Kraljević, S. Kurepa, Matematička analiza 4 - Funkcije kompleksne varijable, Tehnička knjiga, Zagreb, 1979.
- [202] E. Kranakis, Primality and Cryptography, Teubner, Stuttgart; Wiley, Chichester, 1986.
- [203] D. Kreso, Rational function decomposition and Diophantine equations, Disertacija, Graz University of Technology, Graz, 2014.
- [204] D. Kreso, R. Tichy, *Functional composition of polynomials: indecomposability, Diophantine equations and lacunary polynomials*, Grazer Math. Ber. **363** (2015), 143-170.
- [205] M. Křížek, F. Luca, L. Somer, 17 Lectures on Fermat Numbers, Springer-Verlag, New York, 2001.
- [206] S. Kurepa, Matematička analiza 2, Školska knjiga, Zagreb, 1987.
- [207] E. Landau, Elementary Number Theory, Chelsea, New York, 1966.
- [208] E. Landau, Foundations of Analysis, Chelsea, New York, 1966.
- [209] S. Lang, Introduction to Diophantine Approximations, Addison-Wesley, Reading, 1966.
- [210] S. Lang, Elliptic Curves. Diophantine Analysis, Springer-Verlag, Berlin, 1978.
- [211] S. Lang, Algebra, Springer-Verlag, New York, 2002.
- [212] L. Lasić, Visine u diofantskoj geometriji i posljedice abc -slutnje, magistarski rad, Sveučilište u Zagrebu, 2009.

- [213] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer, Berlin, 2000.
- [214] W. J. LeVeque, *Topics in Number Theory I, II*, Dover, New York, 1984.
- [215] W. J. LeVeque, *Fundamentals of Number Theory*, Dover, New York, 1996.
- [216] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials*, Longman, Essex, 1993.
- [217] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
- [218] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin, 1999.
- [219] A. Lozano-Robledo, *Elliptic Curves, Modular Forms and their L -functions*, American Mathematical Society, Providence, 2011.
- [220] F. Luca, *On shifted products which are powers*, *Glas. Mat. Ser. III* **40** (2005), 13–20.
- [221] F. Luca, L. Szalay, *Fibonacci Diophantine triples*, *Glas. Mat. Ser. III* **43** (2008), 253–264.
- [222] K. Mahler, *p -adic Numbers and Their Functions*, Cambridge University Press, Cambridge, 1981.
- [223] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.
- [224] S. Mardešić, *Matematička analiza 1, Školska knjiga*, Zagreb, 1988.
- [225] G. Martin, S. Sitar, *Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples*, *Matematika* **57** (2011), 1–29.
- [226] I. Matić, *Uvod u teoriju brojeva*, Sveučilište Josipa Jurja Strossmayera, Osijek, 2015.
- [227] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, *Invent. Math.* **18** (1972), 183–266.
- [228] M. Mignotte, D. Stefanescu, *Polynomials. An Algorithmic Approach*, Springer-Verlag, Singapore, 1999.
- [229] M. Mihaljinec, *Prilog Fermatovom problemu*, *Glasnik mat.–fiz. i astr.* **7** (1952), 12–18.

BIBLIOGRAFIJA

- [230] M. Mikić, *On the Mordell-Weil group of elliptic curves induced by families of Diophantine triples*, Rocky Mountain J. Math. **45** (2015), 1565–1589.
- [231] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, 1996.
- [232] H. L. Montgomery, R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge University Press, Cambridge, 2007.
- [233] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.
- [234] G. Muić, *Algebarske krivulje*, skripta, Sveučilište u Zagrebu, 2016.
- [235] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1981.
- [236] F. Najman, *Integer points on two families of elliptic curves*, Publ. Math. Debrecen **75** (2009), 401–418.
- [237] F. Najman, *Eliptičke krivulje nad poljima algebarskih brojeva*, skripta, Sveučilište u Zagrebu, 2013.
- [238] 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.
- [239] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$* , Math. Res. Letters **23** (2016), 245–272.
- [240] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warszawa, 1974; Springer, Berlin, 2004.
- [241] W. Narkiewicz, *Classical Problems in Number Theory*, PWN, Warszawa, 1986.
- [242] B. Nathanson, *Additive Number Theory. The Classical Bases*, Springer-Verlag, New York, 1996.
- [243] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.
- [244] P. Q. Nguyen, B. Vallee (Eds.), *The LLL Algorithm. Survey and Applications*, Springer, Berlin, 2010.
- [245] I. Niven, *Diophantine Approximations*, Wiley, New York, 1963.
- [246] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, New York, 1991.

- [247] O. Ore, *Number Theory and Its History*, Dover, New York, 1988.
- [248] PARI Group, PARI/GP version 2.15.4, Bordeaux, 2023,
<http://pari.math.u-bordeaux.fr/>
- [249] 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.
- [250] S. J. Patterson, *An Introduction to the Theory of the Riemann Zeta-Function*, Cambridge University Press, Cambridge, 1995.
- [251] B. Pavković, B. Dakić, *Polinomi*, Školska knjiga, Zagreb, 1990.
- [252] B. Pavković, B. Dakić, P. Mladinić, *Elementarna teorija brojeva*, HMD, Element, Zagreb, 1994.
- [253] B. Pavković, D. Veljan, *Elementarna matematika 1*, Tehnička knjiga, Zagreb, 1992.
- [254] B. Pavković, D. Veljan, *Elementarna matematika 2*, Školska knjiga, Zagreb, 1995.
- [255] T. Pejšković, *Iracionalni brojevi*, HMD, Zagreb, 2001.
- [256] T. Pejšković, *Rothov teorem*, diplomski rad, Sveučilište u Zagrebu, 2005.
- [257] T. Pejšković, *P -adic root separation for quadratic and cubic polynomials*, *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.* **20** (2016), 9–18.
- [258] O. Perron, *Die Lehre von den Kettenbrüchen I, II*, Teubner, 1954.
- [259] A. Pethő, *Algebraische Algorithmen*, Vieweg, Braunschweig, 1999.
- [260] V. Petričević, *Konvergente verižnih razlomaka i Newtonovi aproksimanti za kvadratne iracionalnosti*, Disertacija, Sveučilište u Zagrebu, 2011.
- [261] H. Pollard, H.G. Diamond, *The Theory of Algebraic Numbers*, Dover, New York, 1998.
- [262] V. V. Prasolov, *Polynomials*, Springer, Berlin, 2004.
- [263] M. Ram Murty, *Problems in Analytic Number Theory*, Springer, New York, 2008.
- [264] M. Ram Murty, J. Esmonde, *Problems in Algebraic Number Theory*, Springer, New York, 2005.

BIBLIOGRAFIJA

- [265] J. L. Ramirez Alfonsin, *The Diophantine Frobenius Problem*, Oxford University Press, Oxford, 2005.
- [266] P. Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, New York, 1988.
- [267] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1994.
- [268] J. Roberts, *Elementary Number Theory. A Problem Oriented Approach*, MIT Press, Cambridge, 1977.
- [269] A. M. Rockett, P. Szusz, *Continued Fractions*, World Scientific, Singapore, 1992.
- [270] H. E. Rose, *A Course in Number Theory*, Oxford University Press, Oxford, 1995.
- [271] K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, 1993.
- [272] P. Samuel, *Algebraic Theory of Numbers*, Hermann, Paris, 1970.
- [273] A. Schinzel, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge, 2000.
- [274] J. Schleischitz, *Diophantine approximation in prescribed degree*, *Mosc. Math. J.* **18** (2018), 491–516.
- [275] W. M. Schmidt, *Diophantine Approximation*, Springer-Verlag, Berlin, 1996.
- [276] W. M. Schmidt, *Diophantine Approximation and Diophantine Equations*, Springer-Verlag, Berlin, 1996.
- [277] S. Schmitt, H. G. Zimmer, *Elliptic Curves. A Computational Approach*, de Gruyter, Berlin, 2003.
- [278] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1996.
- [279] J. E. Shockley, *Introduction to Number Theory*, Holt, Rinehart and Winston, New York, 1967.
- [280] T. N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.
- [281] W. Sierpiński: *Pythagorean Triangles*, Dover, New York, 2003.

- [282] W. Sierpiński: 250 Problems in Elementary Number Theory, PWN, Warszawa; Elsevier, New York, 1970.
- [283] W. Sierpiński, Elementary Theory of Numbers, PNW, Warszawa; North Holland, Amsterdam, 1987.
- [284] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer, Dordrecht, 2009.
- [285] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, New York, 2015.
- [286] J. H. Silverman, J. Tate, Rational Points on Elliptic Curves, Springer, Cham, 2015.
- [287] S. Singh, The Code Book, Fourth Estate, London, 1999. (hrvatski prijevod: Šifre. Kratka povijest kriptografije, Mozaik knjiga, Zagreb, 2003.)
- [288] J. L. Slater, Generalized Hypergeometric Functions, Cambridge University Press, Cambridge, 1966.
- [289] N. P. Smart, The Algorithmic Resolution of Diophantine Equations, Cambridge University Press, Cambridge, 1998.
- [290] N. P. Smart, Cryptography. An Introduction, McGraw-Hill, New York, 2002.
- [291] I. S. Sominski, The Method of Mathematical Induction, Mir Publishers, Moskva, 1975.
- [292] V. G. Sprindzuk, Classical Diophantine Equations, Springer, Berlin, 1993.
- [293] H. M. Stark, An Introduction to Number Theory, MIT Press, Cambridge, 1998.
- [294] J. Steuding, Diophantine Analysis, CRC Press, Boca Raton, 2005.
- [295] C. L. Stewart, Linear Forms in Logarithms and Diophantine Equations, Lecture notes, University of Waterloo, 2005.
- [296] I. Stewart, D. Tall, Algebraic Number Theory and Fermat's Last Theorem, A K Peters, Natick, 2002.
- [297] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

BIBLIOGRAFIJA

- [298] D. R. Stinson, *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 2005.
- [299] M. Stoll, *Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational diophantine quintuples*, *Acta Arith.* **190** (2019), 239–261.
- [300] V. Stošić, *Matematička natjecanja učenika osnovnih škola*, HMD, Element, Zagreb, 1994.
- [301] Z. Šikić, Z. Ščekić, *Matematika i muzika*, Profil, Zagreb, 2013.
- [302] B. Širola, *Distribucija prim brojeva i Riemannova zeta-funkcija*, *Hrvatski matematički elektronički časopis math.e* **13** (2008).
- [303] B. Širola, *Algebarske strukture*, skripta, Sveučilište u Zagrebu, 2008.
- [304] R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory. Right Triangles, Sums of Squares, and Arithmetic*, Springer, Cham, 2018.
- [305] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Clarendon Press, Oxford, 1986.
- [306] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight $3/2$* , *Invent. Math.* **72** (1983), 323–334.
- [307] N. Tzanakis, *Explicit solution of a class of quartic Thue equations*, *Acta Arith.* **64** (1993), 271–283.
- [308] N. Tzanakis, *Elliptic Diophantine Equations. A Concrete Approach Via the Elliptic Logarithm*, de Gruyter, Berlin, 2013.
- [309] D. Ugrin-Šparac, *Jedno viđenje suvremene teorije brojeva*, Brojevi, Školska knjiga, Zagreb, 1985.
- [310] Š. Ungar, *Matematička analiza 4*, skripta, Sveučilište u Zagrebu, 2008.
- [311] S. Vajda, *Fibonacci & Lucas Numbers, and the Golden Section, theory and applications*, Ellis Horwood, Chichester, 1989.
- [312] I. Vidav, *Eliptične krivulje in eliptične funkcije*, Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana, 1991.
- [313] I. M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.
- [314] N. N. Vorobiev, *Fibonacci Numbers*, Birkhäuser, Basel, 2002.

- [315] M. Vuković, *Matematička logika*, Element, Zagreb, 2009.
- [316] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Springer-Verlag, Berlin, 2000.
- [317] D. D. Wall, *Fibonacci series modulo m* , *Amer. Math. Monthly* **67** (1960), 525–532.
- [318] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, 2008.
- [319] B. M. M. de Weger, *Algorithms for Diophantine Equations*, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.
- [320] S. H. Weintraub, *Factorization. Unique and Otherwise*, CMS, Ottawa; A K Peters, Wellesley, 2008.
- [321] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, *IEEE Trans. Inform. Theory* **36** (1990), 553–558.
- [322] R. T. Worley, *Estimating $|\alpha - p/q|$* , *Austral. Math. Soc. Ser. A* **31** (1981), 202–206.
- [323] 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
\diamond	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
$\text{nzd}(a, b)$	najveći zajednički djelitelj brojeva a i b
$\log_b(x)$	logaritam po bazi b
$\ln(x)$	prirodni logaritam
$\text{nzv}(a, b)$	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
$\text{ind}_g a$	indeks od a u odnosu na primitivni korijen g
$\text{psp}(b)$	pseudoprosti broj u bazi b
$\text{spsp}(b)$	jaki pseudoprosti broj u bazi b

$\left(\frac{a}{p}\right)$	Legendreov simbol
$ A $	broj elemenata konačnog skupa A
$\left(\frac{a}{Q}\right)$	Jacobijev simbol
$\text{lpsp}(a, b)$	Lucasov pseudoprosti broj
A^T	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
$f(x) = O(g(x))$	$ f(x) \leq Cg(x)$ za neku konstantu 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)$ 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 $\leq x$
$\text{li}(x)$	logaritamsko-integralna funkcija
$\Lambda(n)$	Von Mangoldtova funkcija
$\psi(x)$	Čebiševljeva funkcija ψ
$\vartheta(x)$	Čebiševljeva funkcija ϑ
$\zeta(s)$	Riemannova zeta-funkcija
$\text{Re}(s)$	realni dio kompleksnog broja s
$\text{Im}(s)$	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
$\ \alpha\ $	udaljenost od α do najbližeg cijelog broja
\mathcal{F}_n	Fareyjev niz reda n
$[a_0, a_1, \dots, a_n]$	konačni verižni razlomak
$[a_0, a_1, \dots]$	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

INDEKS OZNAKA

$\ x\ $	$\max(x_1 , \dots, x_n)$, za $x = (x_1, \dots, x_n)$
$\lfloor x \rfloor$	najbliži cijeli broj realnom broju x
$g(a_1, \dots, a_n)$	Frobeniusov broj
$\nu_p(x)$	p -adska valuacija
$ x _p$	p -adska norma
$\left(\frac{\alpha, \beta}{p}\right)$	Hilbertov simbol
$R[x]$	prsten polinoma nad R
$\text{cont}(f)$	sadržaj polinoma f
$\text{Res}(f, g)$	rezultanta polinoma f i g
$\text{Disc}(f)$	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
$\sigma_k(x_1, \dots, x_n)$	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}
$\langle \alpha \rangle$	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
$F(\alpha, \beta, \gamma x)$	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
$E(\mathbb{Q})_{\text{tors}}$	torzijska grupa eliptičke krivulje
$\text{rank}(E(\mathbb{Q}))$	rang eliptičke krivulje
\hat{h}	kanonska visina
$\langle P, Q \rangle$	Néron-Tateovo sparivanje
\mathbb{F}_q	konačno polje s q elemenata
$\text{rad}(f)$	radikal polinoma f
$\text{rad}(m)$	radikal prirodnog broja m

Indeks pojmova

- 2-Selmerov rang, 497
- abc*-slutnja, 560
- abc*-teorem za polinome, 557
- AKS-algoritam, 531
- algebarski broj, 355
 - stupanj, 357
- algebarski cijeli broj, 357
 - ireducibilni, 361, 381
 - prosti, 361, 381
- analitički rang, 500
- anomalne krivulje, 516
- Artin, Emil, 62
- asocirani algebarski brojevi, 380

- Baker, Alan, 394
- Baker-Davenportova redukcija, 431
- Baker-Wüstholzov teorem, 430
- Bernoulli, Jakob, 167
- Bernoullijevi brojevi, 167
- Bertrandov postulat, 156
- beskonačni produkt
 - apsolutno konvergentan, 168
 - konvergentan, 168
- binarna kvadratna forma, 106
 - pozitivno definitna, 107
 - primitivna, 110
 - reducirana, 109
- Binetova formula, 16
- binomni koeficijent, 8
- binomni teorem, 8
- Birch i Swinnerton-Dyerova (BSD) slutnja, 500

- Blichfeldtov teorem, 228
- broj klasa
 - binarne kvadratne forme, 110
 - polja brojeva, 384
- BSGS-metoda, 516

- Carmichael, Robert, 71
- Carmichaelov broj, 71
- Carmichaelov teorem, 99
- Cassinijev identitet, 14
- Chevalleyov teorem, 312
- ciklotomsko polje, 387
- Coppersmithov teorem, 259
- Čebišev, Pafnuti Lvovič, 152
- Čebiševljeve funkcije, 157
- Čebiševljevi polinomi
 - druge vrste, 345
 - prve vrste, 341

- $D(n)$ - m -torka, 445
- Davenportov teorem, 558
- Dedekindova zeta-funkcija, 386
- determinanta visina, 489
- Dicksonov polinom, 341
- Diffie-Hellmanov problem (DHP), 520
- Diofant Aleksandrijski, 440
- Diofantova m -torka, 440
- Diofantova četvorka
 - regularna, 442
- Diofantova trojka
 - regularna, 443
- Dirichlet, Peter Gustav Lejeune, 170
- Dirichletov karakter, 170

INDEKS POJMOVA

- Dirichletov produkt, 145
 Dirichletov teorem
 o diofantskim aproksimacijama, 185
 o jedinicama, 381
 o prostim brojevima u aritmetičkom nizu, 169
 o simultanim aproksimacijama, 226
 Dirichletova L -funkcija, 174
 diskretni logaritam, 519
 diskriminanta
 eliptičke krivulje, 452
 kvadratne forme, 106
 polinoma, 336
 polja algebarskih brojeva, 371
 djelitelj, 21, 326
 dobra aproksimacija, 208
 domena glavnih ideala, 385
 domena jedinstvene faktorizacije, 326
 Doudov algoritam, 476

 ECDLP, 524
 Edwards, Harold, 464
 Edwardsove krivulje, 464
 Eisensteinov kriterij ireducibilnosti, 339
 ekvivalentne dekompozicije, 340
 ekvivalentne kvadratne forme, 107, 120
 ekvivalentni brojevi, 210
 elementarni simetrični polinomi, 347
 ElGamalov kriptosustav, 520
 eliptička krivulja, 451
 anomalna, 525
 inducirana Diofantovom trojkom, 562
 supersingularna, 526
 eliptičke funkcije, 456
 eliptički integrali, 455
 Eratostenovo sito, 32
 Erdős, Paul, 155
 Erdős-Strausova slutnja, 134
 Euklid, 25
 Euklidov algoritam, 24

 euklidsko polje, 362
 Euler, Leonhard, 52
 Euler-Maclaurinova formula, 161
 Eulerov kriterij, 80
 Eulerov teorem, 52
 Eulerova funkcija, 52
 Eulerova konstanta, 143
 Eulerova produktna formula, 169

 faktorijel, 8
 faktorska baza, 522
 Fareyjev niz, 187
 Faulhaberova formula, 168
 Fermat, Pierre de, 36
 Fermatovi brojevi, 36
 Fibonacci, Leonardo Pisano, 10
 Fibonaccijevi brojevi, 11
 Fibonaccijevi polinomi, 345
 formalna derivacija, 332
 formula parcijalne sumacije, 161
 Frobeniusov automorfizam, 505
 Frobeniusov broj, 266
 Frobeniusov endomorfizam, 518
 Frobeniusov trag, 512
 fundamentalna jedinica, 360
 funkcija
 analitička, 166
 derivabilna, 165
 meromorfna, 166
 najveće cijelo, 130
 razlomljeni dio, 130
 strop, 130

 Galois, Évariste, 366
 Galoisovo proširenje, 366
 gama-funkcija, 167
 Gauss, Carl Friedrich, 40
 Gaussova hipergeometrijska funkcija, 396
 Gaussova lema, 85
 Gaussova lema za polinome, 329
 Gaussova suma, 509
 Gaussovi brojevi, 358
 GCD-domena, 326
 genus krivulje, 456

- glavni karakter, 171
 Goldbachova slutnja, 37
 grupa klasa ideala, 383
- Hardy, Godfrey Harold, 569
 Hardy-Ramanujanov broj, 569
 Hasse, Helmut, 500
 Hasseov teorem, 512
 Henselova lema, 58
 Hilbertov simbol, 316
 produktna formula, 317
 Holzerov teorem, 305
 homomorfizam grupa, 171
 Hurwitzov teorem, 191
- ideal, 373
 glavni, 374
 maksimalni, 375
 nerazgranati, 380
 prosti, 375
 totalno razgranati, 380
- indeks, 63
 indeks grananja, 380
 index calculus, 522
 integralna baza, 370
 integralna domena, 324
 ireducibilni element, 326
- j -invarijanta, 466
 Jacobijev simbol, 91
 Jacobijeva formula, 118
 Jacobijeve projektivne koordinate, 463
 jaka Diofantova m -torka, 442
 jedinica, 380
- kanonska visina, 484
 kanonski rastav, 31
 karakteristika, 333
 Kineski teorem o ostatcima (CRT), 49
 Koblitzove krivulje, 518
 kompaktni skup, 228
 konduktor, 470
 kongruencija, 40
 kongruentni broj, 540
 konveksni skup, 227
- korijen jedinice, 509
 primitivni, 509
 korijen polinoma, 331
 kratnost, 332
 Korseltov kriterij, 71
 kriptografija, 243
 kriptosustav, 243
 Kroneckerov algoritam, 338
 Kroneckerov simbol, 92
 Kummer, Ernst Eduard, 373
 kvadratna forma, 119
 pozitivno definitna, 120
 kvadratna iracionalnost, 215
 reducirana, 217
 kvadratni neostatak, 79
 kvadratni ostatak, 79
 kvadratni zakon reciprociteta, 87
 kvadratno polje, 357
 imaginarno, 359
 realno, 359
 kvadratno slobodni broj, 32
- López-Dahabove koordinate, 513
 Lagrange, Joseph-Louis, 115
 Lagrangeov teorem
 o broju rješenja kongruencije, 57
 o četiri kvadrata, 116
 o najboljim aproksimacijama, 206
 Legendre, Adrien-Marie, 80
 Legendreov simbol, 80
 Legendreov teorem
 o ternarnim jednadžbama, 300
 o verižnim razlomcima, 203
 Lenstrin algoritam za faktorizaciju (ECM), 533
 Liouvilleov broj, 390
 Liouvilleov teorem, 389
 LLL-algoritam, 236
 LLL-reducirana baza, 234
 loše aproksimabilni broj, 209
 logaritamska Weilova visina, 409
 logaritamsko-integralna funkcija, 152
 lokalno-globalni princip, 316
 Lucas, Edouard, 10
 Lucas-Lehmerov algoritam, 529

INDEKS POJMOVA

- Lucasov broj, 10
 Lucasovi nizovi, 98
 Lutz-Nagellov teorem, 473
- Mahler, Kurt, 408
 Mahlerova mjera, 409
 Mali Fermatov teorem, 53
 Markovljeva konstanta, 211
 Matijasevičeva lema, 101
 Mazurova ograda, 502
 Menezes-Vanstoneov kriptosustav, 521
 Mersenneovi brojevi, 36
 Mertensova konstanta, 163
 Mestreova polinomijalna metoda, 499
 metoda kongruencija, 444
 Midyjev teorem, 68
 Miller-Rabinov test, 74
 minimalna Weierstrassova jednadžba, 468
 minimalni polinom, 357
 cjelobrojni, 357
 Minkowski, Hermann, 227
 Möbiusova formula inverzije, 136
 Möbiusova funkcija, 134
 Mordell, Louis Joel, 471
 Mordell-Weilov teorem, 471
 Mordell-Weilova baza, 490
 Mordellova jednadžba, 543
 multiplikativna funkcija, 53
- NAF prikaz, 515
 najmanji zajednički višekratnik, 31
 najveći zajednički djelitelj, 22, 326
 Néron-Tateovo sparivanje, 488
 Newtonov aproksimant, 222
 Newtonova metoda, 222
 Newtonove formule, 351
 Noetherin prsten, 388
- norma
 algebarskog broja, 368
 ideala, 378
 normalna baza, 508
 nul-polinom, 325
 nultočka polinoma, 331
 optimalna normalna baza, 508
- Osnovni teorem aritmetike, 30
 Osnovni teorem o simetričnim polinomima, 348
- p -adska norma, 314
 p -adska valuacija, 314
 p -adski brojevi, 315
 p -adski cijeli brojevi, 315
 Pascalova formula, 8
 Pellova jednadžba, 277
 fundamentalno rješenje, 279
 pelovska jednadžba, 289
 dvoznačna klasa, 289
 klasa rješenja, 289
 Pitagorina trojka, 267
 primitivna, 267
 Pocklingtonov teorem, 528
 Pohlig-Hellmanov algoritam, 524
 polinom, 325
 ireducibilan, 337
 koeficijenti, 325
 nedekompozabilan, 340
 normiran, 325
 primitivan, 329
 reducibilan, 337
 simetričan, 347
 stupanj, 325
 totalni stupanj, 347
 polinomijalna baza, 508
 polje, 324
 algebarski zatvoreno, 334
 polje algebarskih brojeva, 367
 polje razlomaka, 338
 Pollardova ρ -metoda, 525
 Pollardova $p - 1$ metoda, 532
 potencijska integralna baza, 371
 potpun kvadrat, 32
 potpuni sustav ostataka, 42
 primitivni korijen, 60
 primitivni prosti djelitelj, 99
 princip Hassea i Minkowskog, 316
 princip matematičke indukcije, 4
 problem diskretnog logaritma (DLP), 519
 produkt ideala, 374

- prosti brojevi, 30
 blizanci, 37
 Sophie Germain, 37
 prsten, 324
 komutativni s jedinicom, 324
 prsten polinoma, 325
 pseudoprosti broj, 70
 jaki (spsp), 72
 Lucasov (lpsp), 98

 racionalna Diofantova m -torka, 440
 radikal polinoma, 557
 radikal prirodnog broja, 559
 Ramanujan, Srinivasa, 569
 rang eliptičke krivulje, 471
 red broja, 60
 reducirani sustav ostataka, 51
 redukcija
 aditivna, 468
 dobra, 467
 multiplikativna, 468
 nerascjepiva, 468
 rascjepiva, 468
 regulator eliptičke krivulje, 490
 regulator polja algebarskih brojeva, 382
 relacija paralelograma, 485
 relativno prosti brojevi, 23
 u parovima, 23
 rešetka, 233
 baza, 233
 reziduum, 166
 rezultanta polinoma, 335
 Riemann, Bernhard, 165
 Riemannova slutnja (RH), 167
 generalizirana (GRH), 175
 proširena (ERH), 175
 Riemannova zeta-funkcija, 165
 Rothov teorem, 391
 RSA, 247
 rebalansirani, 255

 sadržaj polinoma, 329
 savršeni broj, 137

 Schmidtov teorem o potprostorima, 393
 Schönemannov kriterij ireducibilnosti, 338
 SD prikaz, 515
 Segreov teorem, 192
 Selbergova formula, 165
 Shanks-Mestreova metoda, 516
 Siegelov identitet, 553
 Sierpiński, Waclaw, 267
 simetričan skup, 227
 singularitet, 166
 bitni, 166
 izoliran, 166
 pol reda n , 166
 uklonjiv, 166
 složeni brojevi, 30
 suma ideala, 375
 sume potencija, 348
 supersingularne krivulje, 516
 svojstvo jedinstvene faktorizacije, 362
 Sylvesterov teorem, 266

 Tateova normalna forma, 479
 Taylorov red, 166
 Taylorova formula, 334
 Teorem Hasse-Minkowski, 315
 Teorem Minkowskog
 o konveksnom tijelu, 230
 o linearnim formama, 230
 Teorem o dijeljenju s ostatkom, 22
 Teorem o dijeljenju s ostatkom za polinome, 327
 Teorem o prostim brojevima (PNT), 152
 ternarna kvadratna forma, 298
 Thue, Alex, 417
 Thueov teorem, 418
 Thueova jednadžba, 417
 torzijska grupa, 471
 totalno multiplikativna funkcija, 134
 trag algebarskog broja, 368
 transcendentan broj, 355
 trinomijalna baza, 508
 trokutasti brojevi, 126

INDEKS POJMOVA

- Tunnell, Jerrold, 541
- Tunnelov teorem, 541
- unimodularne matrice, 108
- Vandermondeova matrica, 410
- Veliki Fermatov teorem za polinome, 558
- verižni razlomak
 - konvergenta, 198, 201
 - parcijalni kvocijent, 198, 201
 - potpuni kvocijent, 198, 201
 - sekundarna konvergenta, 207
- verižni razlomci, 195
 - beskonačni, 200
 - čisto periodski, 215
 - konačni, 198
 - periodski, 215
 - duljina perioda, 215
- Vinogradov, Ivan Matvejevič, 82
- visina
 - algebarskog broja, 403
 - polinoma, 408
- višekratnik, 21, 326
- Von Mangoldtova funkcija, 157
- Weierstrass, Karl, 455
- Weierstrassova forma, 452
 - kratka, 452
- Weierstrassova \wp -funkcija, 455
- Weil, André, 471
- Wienerov napad, 250
- Wilsonov teorem, 55
- Wirsingov teorem, 404
- Worleyjev teorem, 204
- zakret eliptičke krivulje, 517

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

Tiskanje dovršeno u siječnju 2024.

CIP zapis je dostupan u računalnome katalogu

Nacionalne i sveučilišne knjižnice u Zagrebu pod brojem 001209657.

ISBN 978-953-0-30894-7