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