Poštovane kolegice i kolege,

Srdačno Vas pozdravljam.

Dobro došli na predstavljanje knjige Teorija brojeva.

Zahvaljujem profesoru Josipu Faričiću prorektoru Sveučilišta u Zadru, kolegicama Ljiljani Zekanović Korona i Maji Cindrić te kolegi Mati Kosoru vrlo lijepim uvodnim riječima. Zahvaljujem kolegici Ljiljani Koritnik i kolegi Šimi Šuljiću na ljubaznom pozivu i inicijativi za ovo predstavljanje i predavanje.

Dozvolite mi da i ja kažem nekoliko riječi o knjizi, a potom će uslijediti predavanje pod naslovom Teorija brojeva i kriptografija.

Započeo bih sa zahvalama kolegama koji su zaslužni da izdavanje knjige i za njen konačan sadržaj i izgled.

Zahvaljujem recenzentima knjige, kolegama Ivici Gusiću, Matiji Kazalickom i Filipu Najmanu na vrlo korisnim primjedbama i sugestijama na prethodnu verziju rukopisa knjige. Zahvaljujući njihovim recenzijama, knjiga je dobila status sveučilišnog udžbenika Sveučilišta u Zagrebu, a također i financijsku potporu Ministarstva znanosti i obrazovanja. Posebna zahvala kolegi Tomislavu Pejkoviću, koji je pomno pročitao cijeli rukopis knjige te me upozorio na mnoge manje ili veće pogreške i nepreciznosti, te sugerirao brojna poboljšanja teksta. Hvala i ostalim kolegicama i kolegama koji su mi slali svoje komentare i sugestije na pojedina poglavlja ili na cijeli rukopis prethodne verzije knjige.

Hvala izdavaču knjige, uglednoj izdavačkoj kući Školska knjiga. Suradnju na knjizi sam započeo s prethodnim urednikom kolegom Gojkom Krivokapićem, a suradnja je uspješno nastavljena s urednicom knjige kolegicom Tanjom Djaković. Lektorica knjige je bila Silvija Legin, dok je naslovnicu opremio Marijan Zafron.

Hvala svima Vama što ste došli na ovo predstavljanje, te ga uveličali svojom prisutnošću. Hvala Vam što ste prepoznali koliko me veseli ova knjiga i sve vezano uz nju.

Ova je knjiga nastala na osnovi mojih nastavnih materijala 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, te sličnih kolegija koji se predaju na Sveučilištima u Osijeku, Rijeci i Splitu. Knjiga se koristiti kao literatura i u kolegiju Diofantovi skupovi kojeg ove godine na doktorskom studiju predaju kolege Alan Filipin i Zrinka Franušić. Pored toga, knjiga 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.

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.

Knjiga ima 16 poglavlja. Prvi dio knjige, preciznije poglavlja Djeljivost, Kongruencije, Kvadratni ostatci, Kvadratne forme, Aritmetičke funkcije, Diofantske aproksimacije i Diofantske jednadžbe I obuhvaćaju sadržaj kolegija Teorija brojeva i Elementarna teorija brojeva, a ujedno su i poglavlja (uz dodatak uvodnog poglavlja) koja se preporučaju čitatelju zainteresiranom za sadržaj koji se obično naziva elementarna teorija brojeva. Poglavlje Algebarski brojevi se može shvatiti kao kratki uvod u algebarsku teoriju brojeva, a poglavlje Distribucija prostih brojeva 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. Knjiga sadrži i jedno poglavlje o polinomima koje između ostalog služi i kao priprema za poglavlje o algebarskim brojevima. Eliptičkim krivuljama su posvećena zadnja dva poglavlja u knjizi, ali to naravno ne obuhvaća sve što bi se o toj temi moglo reći. To je tema na kojoj mnogi članovi hrvatske grupe iz teorije brojeva vrlo aktivno rade, a kolege Filip Najman i Matija Kazalicki spadaju među vodeće mlade svjetske stručnjake u tom području, te bi sustavan pregled njihovih najvažnijih rezultata zahtijevao još nekoliko dodatnih poglavlja.

U predgovoru knjige su precizno navedeni brojevi potpoglavlja u kojima se obrađuju teme koje su u knjigu uključene zbog autorovih afiniteta, a neće se uobičajeno naći u knjigama i udžbenicima iz teorije brojeva. 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 sam, zajedno sa svojim hrvatskim i međunarodnim suradnicima, znanstveno radio u zadnjih 25 godina.

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. Moj prvi ozbiljniji susret s teorijom brojeva došao je upravo preko matematičkih natjecanja, pa i ovom prilikom zahvaljujem svom srednjoškolskom profesoru Petru Vranjkoviću uz čiju sam se pomoć, kao učenik srednje škole Juraj Baraković, pripremao za ta natjecanja. Danas postoje brojne mogućnosti da zainteresirani učenici dođu do prikladnih materijala za pripreme za natjecanja, no tada je to ovisilo isključivo o entuzijazmu i trudu nastavnika. Tako je za moje tadašnje (pa i sadašnje) uspjehe bilo ključno veliko zalaganje profesora Vranjkovića. Hvala i svim ostalim mojim učiteljima i profesorima, od prvog učitelja Slobodana Maroje u osnovnoj školi u Novigradu, razrednice i nastavnice matematike Janje Martinović u osnovnoj školi na Stanovima, do mentora magistarskog i doktorskog rada Zvonka Čerina, Dragutina Svrtana i Dimitrija Ugrin-Šparca. 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.

Nadam se da će knjiga biti čitana, te da će čitatelji u njoj naći ponešto zanimljivo i korisno. Bit će mi posebno drago ako nekom od mlađih čitatelja knjiga bude poticaj za ozbiljnije proučavanje teorije brojeva i njenih primjena. Bit ću zahvalan svima koji ukažu na nedostatke ili moguće pogrješke u knjizi. Korekcije i dodatni komentari na knjigu bit će dostupni na mojoj internetskoj stranici. Ta stranica za sada sadrži uglavnom samo ažurirane bibliografske podatke o člancima koji su u međuvremenu objavljeni ili prihvaćeni za objavljivanje u časopisima.

Kao što piše na kraju predgovora knjige, knjiga je najvećim dijelom nastala 2018. i 2019. godine u Novigradu i Zagrebu. Iako u Novigradu, mjestu mog djetinjstva, ne provodim onoliko vremena koliko bih želio, dosta mojih znanstvenih i stručnih radova pa i velik dio ove knjige, nastali su upravo u Novigradu. Čini mi se da u Novome dangubim manje nego na drugim mjestima.

Još jednom hvala svima što ste došli na ovo predstavljanje i hvala Vam na pozornosti.

Za temu mog današnjeg predavanja, u dogovoru s kolegama, izabrao sam predavanje pod naslovom Teorija brojeva i kriptografija. Slično predavanje sam održao prije četiri godine u okviru serije predavanja na Sveučilištu u Zadru koje je bio organizirao kolega Marinko Jablan, pa se ispričavam onima koji su i tada bili nazočni. Temu sam izabrao zato što se provlači kroz skoro cijeli sadržaj knjige te povezuje neka naizgled ne jako povezana poglavlja i teme. Zbog primjena u kriptografiji, kroz cijelu knjigu je, osim na precizne iskaze i dokaze tvrdnji, naglasak dan i na algoritamsku stranu problema, dakle na pitanje kako stvarno efikasno izračunati ono za što nam teorija samo kaže da postoji.