

Poštovane kolegice i kolege,

Dobar dan, drago mi je vidjeti ovako puno poznatih i dragih lica na ovoj promociji i to ovdje na ovom lijepom i važnom mjestu. Meni je osobno izuzetno drago, a i velika čast, govoriti na promociji ove sjajne, te vrlo važne knjige i njezinog engleskog prijevoda koju je napisao moj dragi i cijenjeni mentor akademik Andrej Dujella.

Tema ove knjige je matematička grana Teorija brojeva, po kojoj knjiga nosi i ime. Teorija brojeva je jedna od najstarijih i najproučavanijih grana matematike, koju je još Gauss nazvao „kraljicom matematike“, te iz koje su proizašli mnogi poznati matematički problemi i rezultati, kao što je na primjer posljednji Fermatov teorem, jedan od najpoznatijih matematičkih rezultata, za koji vjerujem da su i mnogi nematematičari među vama čuli.

Preteča ove knjige, koja se zove „Teorija brojeva“ je web skripta „Uvod u Teoriju brojeva“, pa evo reći ću par riječi o toj skripti prije nego što krenem pričati o knjizi. Važnost te skripte za teoriju brojeva, na Matematičkom odsjeku na PMFu, a i šire u cijeloj Hrvatskoj je teško preuveličati. Skripta već desetljećima služi kao nastavni materijal za kolegije „Teorija brojeva“, koji se trenutno izvodi na 2. godini preddiplomskog studija i „Elementarna teorija brojeva“ koji se izvodi na trećoj godini preddiplomskog studija na nastavničkom smjeru. Osim što pokriva gradivo predavanja, ima velik broj zadataka, te se po njoj drže i vježbe. Osim na PMFu u Zagrebu, koristi se kao glavna literatura i u Splitu, Osijeku i Rijeci. Generacije studenata, a među kojima sam i ja, upoznali s teorijom brojeva upravo kroz tu skriptu.

Ja sam osobno imao priliku skriptu upoznati iz različitih perspektiva. Prvo sam je kao student koristio dok sam se spremao za kolokvije i usmeni ispit iz Teorije brojeva. Kasnije sam kao doktorski student kao referencu i podsjetnik na razne defincije i rezultate, zatim kao asistent kao materijal po kojem sam držao vježbe i sada kao nastavnik kao materijal po kojem držim predavanja iz spomenutog kolegija Teorija brojeva.

Danas sam pričao i pričat ću vrlo pozitivno o ovoj knjizi, kako i priliči na promociji knjige. Međutim kako djela govore više o riječi, možda veću težinu o tome što sam kao student mislio o skripti i predmetu Teorija brojeva ima činjenica da sam odabrao teoriju brojeva za područje i akademika Dujellu za mentora i za diplomski i za doktorat.

Knjiga Teorija brojeva znatno proširuje spomenutu skriptu i u dubinu i širinu. To se lako vidi i letimičnim pogledom na brojeve: skripta ima 93 stranice, dok knjiga ima 612. Knjiga motivira čitatelja da uđe dublje u ovu granu matematike po kojoj je nazvana i područja povezana s njom, te pokriva sadržaj i može se koristiti i za druge matematičke predmete.

Sada ću reći par riječi o sadržaju knjige; povući ću u paralelu sa skriptom, pošto je knjiga nastala po njoj, te je matematičarima u publici možda i poznatija. Skripta ima 8 poglavlja: Djeljivost, Kongruencije, Kvadratni osatci, Kvadratne forme, aritmetičke funkcije, Diofantske aproksimacije, Diofantske jednadžbe i kvadratna polja, te je to materijal koji se obrađuje na predmetima Teorija brojeva i Elementarna teorija brojeva.

U knjizi je dodan uvod, koji je podsjetnik na osnovne matematičke pojmove i metode, kao što su Peanovi aksiomi i princip matematičke indukcije. Prvih 6 poglavlja iz skripte se pojavljuju i u knjizi u opširnijem i detaljnijem obliku. Poglavlje Diofantske jednadžbe znatno je prošireno,

te podijeljeno na 2 dijela: Diofantske jednadžbe 1 i 2, koji zajedno imaju oko 100 stranica. Ova 2 poglavlja imaju veliki presjek s kolegijem „Diofantske jednadžbe“, koji se 2006/2007 održavao kao napredni kolegij na doktorskom studiju ovdje, te koji je prvi predmet koji sam ja bio upisao na tom doktorskom studiju. Novo je poglavlje „Polinomi“ koje uvodi važne rezultate i činjenice, posebno one koje su ključne za sljedeća 2 poglavlja: Algebarski brojevi i Aproksimacija algebarskih brojeva. Sadržaj poglavlja „Kvadratna polja“ je znatno proširen, te je poglavlje preimenovano u „Algebarski brojevi“ i kao takvo prirodno čitatelja uvodi u matematiku koja se na PMFu pokiva na kolegijima Algebarska teorija brojeva 1 i 2 na zadnjoj godini studija „Teorijska matematika“. Poglavlja „Aproksimacija algebarskih brojeva“, „Diofantske aproksimacije“, te poglavlje „Primjena diofantskih aproksimacija u kriptografiji“ pokriva većinu saržaja još jednog naprednog kolegija na doktorskom studiju, „Diofantske aproksimacije i primjene“, koji se održavao 2011/2012. Konačno, zadnja 2 poglavlja „Eliptičke krivulje“ i „Diofantski problemi i eliptičke krivulje“ bave se eliptičkim krivuljama i njihovim primjenama, te pokrivaju dio gradiva kolegija „Eliptičke krivulji u kriptografiji“, izbornog kolegija na diplomskom studiju, te naprednog kolegija na doktroskom studiju „Algoritmi za eliptičke krivulje“ koji se održavao 2008/2009.

Posebno bih spomenuo važnost ovog kolegija za mene osobno, kojeg sam slušao na 3. godini dokorskog studija, te sam za seminar za polaganje predmeta dobio temu „Torzija eliptičkih krivulja nad  $Q(i)$ “ gdje sam trebao vidjeti što se zna o toj tematici, te pokušati eventualno dobiti neke nove rezultate. Ispalo je da je to otvoren problem, i štoviše da su najjednostavniji novi rezultati „dohvatljivi“, čak i jednom doktorskom studentu. S druge strane, pokazalo se da je to Pandorina kutija, te da se tu prirodno javljaju sve dublji i dublji te teži i teži problemi, pa se uglavnom tim i srodnim područjima teorije brojeva bavim i danas. Zbog tog seminara sam profesoru Dujelli zahvalan i danas.

Ovo sam ispričao jer knjiga „Teorija brojeva“ ima upravo ovo svojstvo – da kao muholovka uhvati čitatelja iskazima i dokazima nekih od najvažnijih i najljepših matematičkih rezultata dokazanim kroz stoljeća, kao što su Euklidov teorem o prostim brojevima, Lagrangeov teorem četiri kvadrata ili Mordell-Weilov teorem. Zatim čitatelja ne pušta i tjera ga da ulazi dublje u taj labirint mnogobrojnim zadacima, otvorenim problemima i slutnjama, kao što su to čuveni milenijski problemi Riemannova slutnja i Birch-Swinnerton-Dyerova slutnja. A s detaljnom bibliografijom od 442 reference, čitatelj koji želi znati više ima zaista gdje dalje otići.

Još jedna definirajuća karakteristika ove knjige je njezina pristupačnost, što i priliči jednom svučilišnom udžbeniku. Dokazi su napravljeni na najjednostavniji mogući način, izbjegavajući kompliciranu „matematičku mašineriju“ gdje god je to moguće. Vrlo je samodostatna, te se od čitatelja vrlo rijetko zahtijeva da poseže za nekom drugom literaturom. Ne očekuje se neko predznanje, a kada se negdje i očekuju neke ulazne informacije, sve je pažljivo referencirano. Međutim, njezina opširnost i potpunost u obrađivanju određenosti tema čini je korisnom i za referencu u znanstvenom radu. Nebrojeno sam puta trebao naći jednadžbe za eliptičke krivulje sa zadanom torzijom ili iskoristiti neke formule prelaska iz jednog modela krivulje u drugi, te bih uvijek tada posezao za formulama koje se mogu naći u skriptama akademika Dujelle, a sada se sve nalaze na jednom mjestu i u ovoj knjizi.

Dotaknute su mnoge teme koje su i od znanstvenog interesa, a među njima se posebno ističu teme u kojima je autor dao ključne znanstvene doprinose: Diofantove  $m$ -torke i konstrukcija eliptičkih krivulje velikog ranga. U tim područjima je akademik Dujella vodeći svjetski stručnjak, te je stekao veliku međunarodnu prepoznatost.

Knjiga je ove godine prevedena na Engleski jezik. To je svakako vrlo pozitivno i za širu matematičku zajednicu. Impresivno je, ali meni osobno ne pretjerano iznenažujuće, da se knjiga već koristi kao nastavni materijal za kolegij Teorija brojeva u SAD-u. Nemam nikakve sumnje da to nije zadnja institucija u kojoj će se teorija brojeva učiti po ovoj sjajnoj knjizi. Hvala vam svima još jednom na dolasku i na pažnji!