Predstavljanje knjige *Teorija brojeva* akademika Andreja Dujelle

Dragi gosti,

dobrodošli na predstavljanje knjige *Teorija brojeva* akademika Andreja Dujelle. Sve vas srdačno pozdravljam. Ova je knjiga sveučilišni udžbenik, ali ona nadilazi taj uski okvir. Njena pojava nije samo važan matematički, već i prvorazredni kulturni događaj. Do sada na hrvatskom jeziku nije bilo knjige koja bi bila sustavan i sveobuhvatan uvod u ovo važno matematičko područje. S *Teorijom brojeva* Andreja Dujelle korak smo bliže velikim kulturnim narodima.

Oko matematike ima puno nesporazuma. Često je doživljavaju kao računanje (za mnoge dobar matematičar je onaj tko dobro računa). Gotovo na silu je svrstavaju u prirodoslovlje, a ona je po mnogočemu bliža umjetnosti nego kemiji, biologiji pa i fizici. I među matematičarima je prijepor o tome što jest, a što nije matematika. To se očituje i u podjeli na čistu i na primijenjenu matematiku. Primijenjena matematika bila bi ona koja se primjenjuje na rješavanje realnih problema. Za neke primijenjena matematika i nije matematika. Platon je razlikovao aritmetiku (teoriju brojeva) od logistike (umijeća računanja), koju je cijenio, ali je nije priznavao izvornom matematikom. Ipak i oni najekstremniji, koji drže da ništa osjetilno nije predmet matematike, u nju uvijek svrstavaju algebru i teoriju brojeva. *Teorija brojeva* akademika Dujelle izvrstan je uvod u algebarsku teoriju brojeva, a i u gotovo sve važne teme teorije brojeva.

Teorija brojeva je centralna matematička disciplina, važna kako u čistoj matematici tako i u primjenama. Njena povijest počinje s poviješću matematike. Uobičajena je podjela teorije brojeva na *Elementarnu teoriju brojeva*, *Algebarsku teoriju brojeva*, *Analitičku teoriju brojeva*, *Diofantsku geometriju*, *Algoritamsku teoriju brojeva* i *Vjerojatnosnu teoriju brojeva*. Knjiga sustavno pokriva sve važne teme elementarne teorije brojeva i izvrstan je uvod u diofantsku geometriju te u algebarsku i analitičku teoriju brojeva. Kroz tekst se provlače teme i napomene koje se tiču algoritamske teorije brojeva. Primjeni teorije brojeva u kriptografiji posvećeno je cijelo deveto poglavlje (koje je i izvrstan uvod u kriptografiju i sigurnu izmjenu informacija) i dio petnaestoga poglavlja.

Elementarna teorija brojeva osnova je teorije brojeva. Ona se izvorno odnosi na prirodne brojeve 1,2,3,4,..., brojeve kojima brojimo (koji su time od praktične važnosti). Prirodni brojevi postaju dio matematike kad započinje proučavanje njihovih svojstava s obzirom na djeljivost. Temeljni objekti postaju prosti brojevi koji se ne mogu predočiti kao umnožak dvaju prirodnih brojeva različitih od 1. Svaki je prirodni broj umnožak prostih brojeva i taj je rastav jednoznačan (do na poredak faktora). To je osnovni teorem aritmetike. Već u Euklidovim Elementima ima argument kojim se dokazuje da prostih brojeva ima beskonačno mnogo. Vremenom se pokazalo da je prirodnije razmatrati sve cijele brojeve (a ne samo

pozitivne) i da se u teoriju brojeva trebaju uključiti svi racionalni brojevi. U ovoj knjizi elementarna teorija brojeva zasnovana je u prvih pet poglavlja i u većim dijelovima šestog, osmog i desetog poglavlja, a jezik i metode elementarne teorije brojeva protežu se kroz cijeli tekst.

Idealno bi bilo da se problem formuliran jezikom elementarne teorije brojeva i riješi tim jezikom. Izgleda da je taj ideal nedostiživ. Na primjer, formulaciju Fermatova teorema koji tvrdi da nema prirodnih brojeva x,y,z i n>2 za koje vrijedi

$$x^n+y^n=z^n$$

razumiju učenici srednjih škola, a za dokaz je bilo potrebno razviti nekoliko sofisticiranih neelementarnih matematičkih teorija. Već u slučaju n=3 trebalo je izaći iz okvira cijelih brojeva i proširiti ih s kompleksnim trećim korijenom *w* iz 1. Drugim riječima, razmatranje je trebalo provesti u prstenu cijelih brojeva kvadratnog proširenja **Q**(*w*) polja racionalnih brojeva **Q**. Općenito, postoje mnoga slična proširenja bilo kojeg stupnja i svako ima prsten cijelih brojeva koji je analogan običnom prstenu **Z** cijelih brojeva. Proučavanje tih novih aritmetičkih struktura ne može se provesti elementarnim metodama već treba uključiti algebru. Na primjer, više nije dovoljno razmatranje prostih brojeva jer rastav na proste brojeve u ovim popoćenjima cijelih brojeva nije jednoznačan. Jednoznačan je rastav ideala na umnožak prostih ideala i time smo duboko u algebri. To je algebarska teorija brojeva. Jedanaesto i dvanaesto poglavlje ove knjige izvrstan je uvod u algebarsku teoriju brojeva, a pripadni se jezik provlači i razvija kroz preostala četiri poglavlja.

U rješavanje problema elementarne teorije brojeva treba uključiti i geometriju, napose algebarsku geometriju. Tako je za dokaz Fermatova torema bila presudna njegova reformulacija u jeziku eliptičkih krivulja. Mnogi teoriju eliptičkih krivulja smatraju najljepšom matematičkom teorijom. Petnaesto poglavlje izvrstan je uvod u aritmetičke aspekte te teorije. Kod rješenja Fermatova teorema glavnu ulogu imaju L-funkcije eliptičkih krivulja nad poljem racionalnih brojeva. To su svojevrsna poopćenja Riemannove zeta funkcije koja je jedan od temeljnih pojmova analitičke teorije brojeva. Ta problematika zastupljena je u sedmom poglavlju. Diofantskim aproksimacijama i primjenama posvećeno je osmo, deveto i trinaesto poglavlje.

Teorija brojeva Andreja Dujelle na visokoj je kako stručnoj tako i metodičkoj razini. Izlaganje obično započinje motivirajućim napomenama ili povijesnim natuknicama. Ima dosta riješenih primjera i neriješenih zadataka za vježbu. Pri kraju se često navode i komentiraju posljednja otkrića i rezultati. Za matematiku su od presudne važnosti definicije, teoremi i dokazi. Knjiga se odlikuje vrlo jasnim i preciznim definicijama i formulacijama teorema te strogim dokazima. Dokazi su potanko izvedeni osim ako se argumenti ponavljaju, kada su, u pravilu, samo skicirani. Teoremi u kojima se navode posljednji rezultati u znanstvenoj literaturi i kojima dokazi izlaze izvan okvira knjige, daju se bez dokaza.

Priložena je vrlo opsežna literatura u kojoj je i nekoliko udžbenika iz teorije brojeva. Kroz tekst se provlače mnogobrojna citiranja te literature, a ona su vrlo jasno istaknuta i često popraćena napomenama i kritičkim osvrtima. Autor u predgovoru ističe dva poznata udžbenika iz teorije brojeva na kojima je temeljio osnovno izlaganje. Velik dio izlaganja u mnogočemu je izvoran, naročito onaj koji se odnosi na sadržaje koji se tiču autorova znanstvenog rada i rada njegovih suradnika u Hrvatskoj i svijetu.

I na kraju, ovo je vrlo vrijedna i korisna knjiga. Preporučam da je nabavite i koristite se njome. Čestitam akademiku Dujelli na lijepom daru hrvatskoj znanstvenoj zajednici, a Školskoj knjizi na uspješno obavljenom poslu.