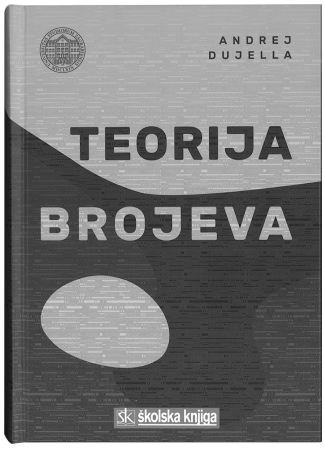
NOVE KNJIGE

Andrej Dujella, ***Teorija brojeva***, Školska knjiga, Zagreb, 2019., 612 str.



U izdanju Školske knjige izašla je *Teorija brojeva* akademika Andreja Dujelle. Ova je knjiga sveučilišni udžbenik, ali će biti vrlo korisna i za srednju školu, naročito za natjecatelje iz matematike. Do sada na hrvatskom jeziku nije bilo tako sustavna i sveobuhvatna uvoda u ovo važno matematičko područje.

Teorija brojeva je središnja 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*. Ova 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 svojevrstan uvod u kriptografiju i sigurnu izmjenu informacija. Kriptografija je zastupljena i u dijelu 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 2, 3, 5, 7, 11, 13, 17,.... Oni 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. Većina ovog materijala može biti od velike koristi za učenike srednjih škola i njihove profesore.

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. Slučaj $n = 4$ riješio je Fermat elementarnim metodama. Već u prvom dokazu za $n = 3$ trebalo je izaći iz okvira cijelih brojeva i proširiti ih s kompleksnim trećim korijenom w iz 1. Drugim riječima, razmatranje se provodilo u prstenu cijelih brojeva kvadratnog proširenja $\mathbb{Q}(w)$ polja racionalnih brojeva

$\mathbb{Q}$. Općenito, postoje mnoga slična proširenja bilo kojeg stupnja i svako ima prsten cijelih brojeva koji je analogan običnom prstenu $\mathbb{Z}$ 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 poopćenjima cijelih brojeva nije jednoznačan. Jednoznačan je rastav ideala na umnožak prostih ideala i time se ulazi u algebru, odnosno u algebarsku teoriju 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.

Pokazalo se da se u rješavanje problema elementarne teorije brojeva treba uključiti i geometrija, napose algebarska geometrija. Tako je za dokaz Fermatova teorema bila presudna njegova reformulacija u jeziku eliptičkih krivulja. Promatra se eliptička krivulja

$$y^2 = x(x - a^p)(x + b^p),$$

uz pretpostavku da za prosti neparni broj $p > 3$ i prirodne brojeve a, b, c vrijedi $a^p + b^p = c^p$, pa se pokazuje da takva eliptička krivulja ne postoji. 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, jednog od temeljnih pojmova analitičke teorije brojeva, koja je zastupljena 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 u svijetu.

Ovo je vrlo vrijedna i korisna knjiga. Od nje će imati koristi mnogi koji se profesionalno bave matematikom, studenti matematike i srednjoškolski učenici i profesori. Čestitam akademiku Dujelli na lijepom daru hrvatskoj znanstvenoj zajednici, a Školskoj knjizi na uspješno obavljenom poslu.

Ivica Gusić