Predstavljanje knjige "Teorija brojeva" akademika Andreja Dujelle

(Knjižnica HAZU, Zagreb, 21. rujna 2021.)

Govor prof. dr. sc. Luke Grubišića

Poštovani predsjedniče akademije, poštovani glavni tajniče, dame i gospodo, drage kolegice i kolege čast mi je obratiti se ovom skupu u ime PMF-Matematičkog odsjeka. Ja sam Luka Grubišić, pomoćnik sam pročelnika MO za znanost. S osobne strane, posebno mi je zadovoljstvo, za koje se zahvaljujem organizatoru akademiku Goranu Muiću, da se baš ja mogu osvrnuti na značaj koji izdavanje knjige *Teorija brojeva* akademika Andreja Dujelle ima za našu instituciju i matematiku kao struku. Ova je knjiga sukus dugogodišnjeg iskustva akademika Dujelle kao znanstvenika i predavača mnogih kolegija iz raznih aspekata teorije brojeva i njenih primjena u kriptografiji, te osnova matematike. Svima nama koji smo učenici profesora Dujelle, a to se može reći za sve kolege koji su diplomirali na PMF-MO unazad trideset godina, prvi susret s njegovim kolegijima i neposrednim pristupom matematici je u jasnom sjećanju. U mom slučaju to je bilo na kolegiju Elementarna matematika, koji je kao što svi mogu pogoditi elementaran samo u imenu. Stil predavanja profesora Dujelle poznat je po elementarnim dokazima jako teških i dubokih tvrdnji. Ovaj kolegij je, na način na kojega ga je profesor Dujella držao, dugi niz godina bio most bivšim srednjoškolcima prema području fakultetske (profesionalne) matematike. To su upravo riječi kojima je profesor Jean-Paul Allouche-a sa Sveučilišta Sorbonne u Vjesniku Europskog matematičkog društva predstavio ovu knjigu uz opasku da mu je žao što ne može ponovno početi učiti teoriju brojeva od nule, samo korištenjem ove knjige. Za kraj kao Facebook prijatelj profesora Dujelle, mogu samo posvjedočiti koliko me osobno veseli pratiti odjek koji ova knjiga, ali i ostala njegova postignuća u popularizaciji matematike, imaju i u ovom elektroničkom mediju.

Dame i gospodo, želim vam ugodan nastavak skupa. Hvala vam na pažnji!

Govor akademika Marka Tadića

Od recenzenata ćemo čuti više o ovoj izuzetnoj knjizi. Ja ću reći svoje dojmove o području koje knjiga izlaže. Jedan značajan dio tih dojmova je nastao tijekom moga dvogodišnjeg boravka u Göttingenu, gdje su djelovali velikani kao Gauss, Riemann, Kummer, Hilbert i Weyl, koje ću spomenuti u svom daljnjem govoru. Tu je također djelovao i Minkowski i Emmy Noether.

Bez moderne matematike ne bi bilo moderne znanosti, a bez teorije brojeva teško da bi bilo napredne moderne matematike kakvu danas poznajemo. Dobro je poznata slična Gaussova izjava.

Razvoj teorije brojeva je bio dugo vremena posljedica fascinacije ljudi odnosima među brojevima (koje danas nazivamo prirodnim brojevima). Rješavanje problema teorije brojeva jedva da je imalo ikakve praktične primjene. No to proučavanje problema koji nisu imali praktične primjene, rezultiralo je time da je danas teorija brojeva vrlo važna u primjenama. Komunikacije mobitelima i upotreba bankomata su neke od najjednostavnijih i najčešćih primjena. Današnji život bi bilo teško zamisliti bez tih primjena. A razvoj teorije brojeva je značajno utjecao na razvoj matematike, posebno algebre. Jedna od posljedica je i značajna algebraizacija matematike u 20-tom stoljeću.

Jedan od prvih susreta učenika s tematikom teorije brojeva su pravokutni trokuti s cjelobrojnim stranicama, tj. Pitagorejske trojke. Kao što i samo ime kaže, njih pripisujemo Pitagori, iako postoje zapisi iz Mezopotamije o njima koji prethode Pitagori znatno više od 1000 godina.

Pitagorejci su napravili mistiku od takvih trojki, i njihovog nalaženja. Kasnije su se pojavile jednostavne formule, Euklidove formule, koje generiraju takve trojke.

Interesantno je spomenuti da je ta veza, koja postoji kod Pitagore između teorije brojeva i geometrije, i danas izuzetno živa i važna (današnja geometrija se zove aritmetička algebarska geometrija i izuzetno je komplicirano i važno područje). Dijelovi ove veze se također obrađuju u knjizi akademika Dujelle.

Sada ćemo skočiti u izlaganju više od 2000 godina nakon Pitagore.

Pierre Fermat, veliki francuski matematičar koji je zarađivao za život kao sudac, čitajući Diofantovu aritmetiku se pitao da li kao što imamo sumu dva kvadrata koja je opet kvadrat, možemo imati takve slučajeve za kubove, bikvadrate i općenito više potencije. Jako je poznat njegov komentar na margini Diofantove knjige da toga ne može biti, ali da je dokaz prevelik da bi ga napisao na margini. Ta se Fermatova tvrdnja naziva Fermatov posljednji teorem.

No prošlo je više od tri i pol stoljeća nakon Fermatove tvrdnje, bez da se došlo do potpunog dokaza, i pri tome su se na tome iskušala gotova sva od najvećih imena teorije brojeva (i ne samo teorije brojeva, npr. Cauchy). Ime koje se tu posebno ističe, a koje se ne sreće tijekom fakultetskog obrazovanja, je Kummer.

Bez obzira što se u ta tri i pol stoljeća nije našao dokaz Fermatove tvrdnje, rad na ovome je rezultirao nevjerojatnim razvojem moderne matematike, posebno moderne algebre koja je do tada bila relativno mala disciplina, i algebarske geometrije. Dvadeseto stoljeće svjedoči velikoj algebraizaciji matematike (geometrija postaje algebarska geometrija, a topologija koja proučava geometrijska svojstva, najjače se razvija kao algebarska topologija, da spomenemo samo neke primjere, a mnogo je drugih kao funkcionalna analiza koja nastavlja ideje iz klasične analize).

Andrew Willes je 1990-ih godina prošloga stoljeća našao konačno potpuni dokaz Fermatove tvrdnje. Njegov dokaz uključuje neke od najsofisticiranijih i najkompliciranijih dijelova suvremene matematike. Čini se da je u trenutku kompletiranja njegovoga dokaza, bilo u svijetu svega nekoliko ljudi koji su mogli potpuno razumijeti sve dijelove koje uključuje njegov dokaz.

Općenito, kada bi se u matematici pojavila nova matematička teorija, vrlo često bi se probala primjeniti na probleme teorije brojeva.

Navesti ću jedan važan takav primjer. Veliki matematičar Riemann je sredinom 19-og stoljeća radio na izgradnji kompleksne analize. Primjenio ju je na ono što se po njemu zove Riemannova zeta funkcija. Iz članka koji je napisao o tome dolazi Riemannova slutnja, vjerojatno najslavniji nerješeni problem današnje matematike, koji je direktno povezan sa asimptotskim rasporedom prostih brojeva. Interesantno je spomenuti da je ovo jedini članak koji je Riemann napisao iz teorije brojeva.

Također, interesantno je spomenuti da se Carl Friedrich Gauss, jedan od najvećih matematičara i od kojega se smatra da počinje moderna teorija brojeva, nije bavio dokazom Fermatove tvrdnje. S druge strane, njega je vrlo impresioniralo ono što zovemo Gaussovim zakonom kvadratnog reciprociteta, nečega naizgled vrlo jednostavnoga. Smatrao ga je toliko važnim da mu je našao osam dokaza. Danas za ovaj reciprocitet postoji više od 240 dokaza.

Sada ću reći par riječi o mojoj vezi sa teorijom brojeva. Prije toga ću dati vrlo kratki povijesni uvod o dva područja, na spoju kojih je moj rad.

Prvo je harmonijska analiza. Klasična Fourierova harmonijska analiza, područje staro više od dva stoljeća, je određeni tip analize na komutativnim grupama, koja je bazirana na karakterima tih grupa, što su određene jednostavne funkcije na njima. Ova klasična teorija je jedno od najprimjenjivanijih područja matematike, kako u matematici, tako i van matematike. Vrlo dugo je postojala želja da se ova teorija proširi na nekomutativne grupe, no prije toga je trebalo uvesti neka nova područja matematike, kao npr. teoriju mjere i Hilbertove prostore. U drugoj polovici 20-tog stoljeća, nastavljajući na ideje Hermanna Weyla, Gelfand je formulirao koncept harmonijske analize na nekomutativnim nekompaktnim grupama, baziran na unitarnim reprezentacijama na beskonačno dimenzionalnim Hilbertovim prostorima.

Izvorište drugog područja je deveti Hilbertov problem, koji govori da se "nađe najopćenitiji teorem reciprociteta za proizvoljno polje algebarskih brojeva", tj. teorema koji bi generalizirao Gaussov zakon kvadratnog reciprociteta (koji odgovara kvadratnim poljima).

Robert Langlands je krajem 1960-ih predložio rješavanje ovoga problema baziranog na novoj nekomutativnoj harmonijskoj analizi koja je tada bila (a i još je) u fazi uspostavljanja. Preciznije na harmonijskoj analizi na određenim aritmetički definiranim nekomutativnim grupama. Predložena strategija za rješavanje problema se sada zove Langlandsov program. Početni nivo ovoga programa je teorija polja klasa i Artinov reciprocitet, koji su od prije bili poznati (i koji pripadaju "komutativnoj teoriji", i bili jedno od najvećih dosega dotadašnje teorije brojeva). Ovaj program je daleko od kompletiranja, no i ono što je do sada napravljeno je vrlo interesantno i važno. Npr., rezultati ovoga programa se koriste i u Wilesovom dokazu Fermatove tvrdnje.

Reciprociteti u ovom programu su specijalni slučajevi relacija koje se zovu funktorijalnosti, i koje su najvažniji objekti ovoga programa.

Hrvatska ima malu, ali u svijetu dobro poznatu grupu koja radi na problematici vezanoj uz Langlandsov program. Najvažniji članovi ove grupe su profesori Goran Muić, Marcela Hanzer, Neven Grbac i Ivan Matić.

Najvažniji i najspektakularniji rezultat ostvaren u zadnje dvije dekade u Langlandsovom programu je Arthurova uspostava funktorijalnosti između općih linearnih i klasičnih grupa. U ovome radu Arthur koristi klasifikaciju ireducibilnih unitarnih reprezentacija općih linearnih grupa, i opis njihovih karaktera koji sam ja napravio 1980-ih i 1990-ih godina prošloga stoljeća.

Završiti ću svoj govor kratkim komentarom o autoru ove izuzetne knjige koju danas predstavljamo. Opet ću početi sa vrlo kratkim povijesnim uvodom.

Diofant je uočio četvorke racionalnih brojeva sa svojstvom da množeći svaka dva među njima i dodajući jedan, dobijaju se potpuni kvadrati. Takve četvorke zovemo Diofatovim četvorkama. Fermat je našao Diofantovu četvorku koja se sastoji od prirodnih brojeva. Euler je našao beskonačnu familiju s tim svojstvima.

Kao što najčešće biva u teoriji brojeva, nije bilo posebnih razloga za traženje takvih skupova, osim čiste fascinacije tim svojstvima. Baker, dobitnik Fieldsove medalje 1968., dokazao je da se Fermatova četvorka ne može proširiti do takve petorke.

Od primjera koje su ovi velikani matematike uočili, i koji su ih fascinirali, akademik Dujella je stvorio cjelovitu teoriju, i tu svoju teoriju povezao s teorijom eliptičkih krivulja, teorijom koja je bila ključna u Wilesovom dokazu Fermatove tvrdnje. U području koje je akademik Dujella stvorio danas rade matematičari najjačih nacija. Knjiga akademika Dujelle završava s dijelom o Diofantovim m-torkama i eliptičkim krivuljama.

Nameće se paralela s Pitagorejcima koje je fasciniralo nalaženje Pitagorejskih trojki, a s kojih su Euklidove formule skinule mistiku. Tako je rad akademika Dujelle skinuo puno mistike s Diofantovih n-torki.

Knjiga akademika Dujelle počinje od samih početaka teorije brojeva, a kao što vidimo, stiže do samih rubova današnjih istraživanja, i do područja koje je stvorio akademik Dujella.

Moram priznati da mi je žao što nisam imao ovakvu knjigu kada sam stvarao bazu svog matematičkog obrazovanja.

Govor prof. dr. sc. Ivice Gusića

Obično se smatra da moderna teorija brojeva počinje knjigom *Disquisitiones Arithmeticae* iz 1798. njemačkog matematičara C. F. Gaussa, od kojega potječu izjave da je matematika kraljica znanosti, a teorija brojeva kraljica matematike. Da dočaramo novost koju je Gauss uveo, pogledajmo broj $2+\sqrt{3}$, koji je zbroj običnog cijelog broja 2 i iracionalnog broja $\sqrt{3}$. To očito nije običan cijeli broj već iracionalan, ali se pokazuje da on ima autohtoni matematički život analogan matematičkom životu običnog cijelog broja. Taj bi se broj mogao nazvati cijelim brojem drugoga reda. Slično postoje i cijeli brojevi trećeg, četvrtog ili bilo kojeg drugog reda, dok se obični cijeli brojevi mogu interpretirati kao cijeli brojevi prvog reda. Gauss je u svojoj knjizi u potpunosti opisao cijele brojeve drugog reda i neke brojeve partikularnih redova te demonstrirao kakvu oni imaju ulogu u teoriji brojeva.

Sredinom 19. stoljeća, njemački matematičari Dirichlet (za koga je zabilježeno kako je na svim putovanjima uvijek sa sobom nosio *Disquisitiones Arithmeticae*) i Dedekind uspjeli su proširiti neke važne aspekte Gaussovih rezultata na cijele brojeve bilo kojega reda. To je publicirao Dedekind 1863. u zborniku u kojemu je objavio Dirichletove lekcije o toj temi. Godinu dana prije tog važnog matematičkog događaja, u Königsbergu se rodio njemački matematičar David Hilbert, koji je do kraja stoljeća općepriznat vodećim svjetskim matematičarom. Hilbert je od Njemačkog matematičkog društva dobio narudžbu da napravi izvješće o dotadašnjem razvoju teorije brojeva. Tako je 1897. došlo do publikacije Hilbertove knjige *Zahlbericht* koja je nekoliko sljedećih desetljeća bila glavni udžbenik za učenje teorije brojeva.

Sljedeću važnu stepenicu čekalo se 70 godina, kada je André Weil, francuski matematičar židovskog podrijetla, publicirao *Basic Number Theory*, rad koji je izazvao revoluciju u pristupu teoriji brojeva. Weil je u svom pristupu uključio važna matematička područja razvijena u 20. stoljeću: topologiju, invarijantnu mjeru i invarijantnu integraciju. Uveo je pojam adela, koji je do današnjih dana ostao jedan od najvažnijih pojmova teorije brojeva. U izlaganju su središnje mjesto dobila lokalno kompaktna polja koja je klasificirao. U teoriji brojeva, naročito su važna takozvana lokalna i globalna polja. Da približimo te pojmove, spomenimo da su racionalni brojevi primjer globalnog polja, a polje realnih brojeva jedno je od lokalnih polja pridruženih tom globalnom. Iako je Weilova knjiga odigrala veliku ulogu među specijalistima, ona, zbog teškog stila, nije pogodna za prvo susretanje s teorijom brojeva.

Gdje je tu *Teorija brojeva* Andreja Dujelle? To je monografija koja će gotovo sigurno ostati jedna od posljednjih knjiga te vrste s tako opsežnim sadržajem, u kojoj su sve tvrdnje vrlo precizno i potanko dokazane. Djelo je već prevedeno na engleski jezik i sigurno će na njega često upućivati mentori kad njihovi studenti budu pitali za neki pojam ili teorem iz teorije brojeva. Može se očekivati da će po toj knjizi Hrvatska biti prepoznatljiva u matematičkom svijetu slično kao što je u nogometnom po bijelo - crvenim kockicama. Nakon Dujelline knjige hrvatska se matematika našla i u problemima, istina slatkim, jer je time teorija brojeva na neki način preskočila uobičajeno mjesto. Iako je, prema Gaussu, teorija brojeva kraljica matematike, ona ne zauzima u njoj tako veliki prostor kao neke druge matematičke discipline, npr. matematička analiza, ili njena specifična poddisciplina poznata kao kalkulus, matematika nastala na temelju radova Newtona i Leibnitza iz 17. stoljeća. Kalkulus nije samo nezaobilazna sastavnica studija matematike, već i fizike i ostalih prirodnih znanosti, tehnike i tehnologije, kao i svih područja znanosti u kojima se matematika primjenjuje, npr. u studiju ekonomije. Druga važna matematička disciplina, algebra, u samoj je biti matematike, što se može ilustrirati i proširenim shvaćanjem u razvijenim matematičkim kulturama da je matematika upravo algebarski dio matematike. To upućuje na potrebu za monografijom iz algebre na hrvatskom jeziku, a takve nemamo. Istina, odavno postoji Algebra u dva toma Đure Kurepe. Kurepa je bio čovjek široke kulture i široke matematičke kulture, kakvih je sada sve manje. U njegovim Algebrama ima razne matematike, pa i algebre. U svakom slučaju te su knjige neprikladne za suvremeno upoznavanje s algebrom. HAZU ima kapacitet za provođenje projekta pisanja monografije o algebri na hrvatskom jeziku. Pojava takve knjige odigrala bi na hrvatskoj matematičkoj sceni ulogu poput one koju je odigrala ova izvrsna Dujellina monografija.

Govor prof. dr. sc. Filipa Najmana

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 su se 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 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 parelelu 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 znantno 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 sadržaja 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 doktorskom 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 doktorskog studija, te sam za seminar za polaganje predmeta dobio temu "Torzija eliptičkih krivulja nad $\mathbb{Q}(i)$" 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 sveučilišnom 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 određenih 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 iznenađujuće, 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!