

Andrej Dujella, od osnovne škole do akademika

Željko Hanjš



Andrej Dujella

U srednjoj školi u Zadru Andrej Dujella je, kao učenik, pisao članke za Matematičko fizički list i išao na matematička natjecanja, da bi 1984. godine sudjelovao na Međunarodnoj matematičkoj olimpijadi u Čehoslovačkoj na kojoj je osvojio brončanu medalju. Po završetku studija matematike zaposlen je kao pripravnik-postdiplomand na Matematičkom odsjeku Prirodoslovno matematičkog fakulteta Sveučilišta u Zagrebu. Od 1993. je asistent, od 1997. docent, od 2000. izvanredni profesor, od 2004. redoviti profesor, a od 2009. redoviti profesor u trajnom zvanju. Bavi se teorijom brojeva, posebno diofantskim jednadžbama i eliptičkim krivuljama. Bio je dugogodišnji član Državnog povjerenstva za matematička natjecanja te urednik Hrvatskog matematičkog elektronskog časopisa math.e i znanstvenog časopisa Glasnik matematički. Predaje kolegije na preddiplomskom, diplomskom i poslijediplomskom studiju. Od 2012. g. redoviti je član Hrvatske akademije znanosti i umjetnosti. Vrlo rado se odazvao razgovoru o svom znanstvenom i privatnom životu.

Molimo Vas da navedete zanimljive detalje iz vaše osnovne i srednje škole. Vrlo rano ste se zainteresirali za matematiku, a išli i na matematička natjecanja.



Andrej Dujella u Novigradu

Rođen sam u Puli. Najranije djetinjstvo proveo sam u Žminju u Istri. Nakon povratka obitelji u rodni kraj mojih roditelja, prvih sedam razreda osnovne škole pohađao sam u Novigradu Dalmatinskom. Najprije u staroj školi u prostoru stare župne crkve, a od trećeg razreda u novoizgrađenoj školi. Prvi učitelj mi je bio Slobodan Maroja kojemu sam zahvalan što je prepoznao i razvijao moju sklonost za matematiku. Naravno, i moji su roditelji uložili puno truda oko mog školovanja. Imao sam jako dobre prijatelje i školske obaveze smo često kombinirali s igrom. Osnovna škola Novigrad, osnovana 1830. godine, jedna je od najstarijih škola u Dalmaciji. Odlikovala se glazbenim sekcijama (i sam sam sudjelovao u harmonikaškom orkestru i zboru). U njoj je kao učitelj radio i moj djed Ljubo Vukasović.

U osmom razredu obitelj mi se preselila u Zadar, te sam taj razred pohađao u Osnovnoj školi Stanovi (tada se zvala "Bratstvo i jedinstvo"). Trebalo mi je nešto vremena da se snađem u novoj sredini. Ipak, te sam se godine, uz pomoć razrednice i nastavnice matematike Janje Martinović, kvalificirao na republičko natjecanje iz matematike, i od tog vremena matematička natjecanja su postala vrlo važan dio mog školovanja i života.

Srednju školu pohađao sam u Zadru u tadašnjem Centru za odgoj i usmjereno obrazovanje "Juraj Baraković" (to je bio tadašnji naziv za ono što je godinama prije, a tako i danas, bila gimnazija). Prva dva razreda sve su srednje škole imale isti općeobrazovni program, a u trećem se biralo usmjerenje. Ja sam izabrao smjer matematičar-informatičar koji je imao veliku satnicu iz matematike, informatike i fizike. Srećom za mene, svaki od tih brojnih matematičkih, informatičkih i fizičkih predmeta nosio je posebnu ocjenu, pa su mi te dobre ocjene u konačnom prosjeku kompenzirale one nešto lošije iz većine ostalih predmeta (moj prosjek ocjena u osnovnoj i srednjoj školi, a i kasnije na fakultetu je uglavnom bio oko 4.5). Tada sam se još ozbiljnije i sustavnije spremao za natjecanja iz matematike, uz punu podršku profesora Petra Vranjkovića, koji je pripremao izabrane zadatke za vježbu za sve razine 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) matematičke uspjehe bilo ključno veliko zalaganje profesora Vranjkovića.

U trećem razredu osvojio sam 1. mjesto na republičkom natjecanju iz matematike, a u četvrtom, nakon 3. mjesta u Hrvatskoj, osvojio sam 2. mjesto na državnom natjecanju i kvalificirao se na međunarodnu matematičku olimpijadu. Na olimpijadi koja se te 1984. godine održala u Pragu osvojio sam brončanu medalju. Sudjelovanje na matematičkoj olimpijadi definitivno me je opredijelilo za studij matematike.

Učiteljima i profesorima često nije bilo lako sa mnom, ali svi su imali razumijevanja za moje nestašluke te govor na novigradskom dijalektu, i zaista sam im na tome vrlo zahvalan.

Studirali ste matematiku na PMF-u u Zagrebu. Koje Vas je područje u matematici najviše zaokupilo tokom studija? Vjerojatno je za to postojao veliki interes još iz srednje škole.

Još od srednjoškolskih natjecanja iz matematike, najviše me je zaokupljala i inspirirala teorija brojeva. To je područje matematike koje je uvijek bilo vrlo zastupljeno u zadacima na svim razinama matematičkih natjecanja. Tijekom studija matematike (bio sam tzv. inženjerski smjer, a na zadnje dvije godine studija izabrao sam smjer matematička informatika i statistika) nisam imao prilike slušati kolegije iz teorije brojeva, ali sam stekao solidno znanje iz različitih područja matematike te imao prilike slušati predavanja uglednih hrvatskih matematičara. Interes za teoriju brojeva produbljivao sam kroz literaturu koju sam nabavljao u tadašnjoj knjižari strane (uglavnom ruske, koje je jedina i bila pristupačna studentskom džepu) literature u Gundulićevoj ulici. Na zadnjoj godini studija dobio sam financijski izdašnu stipendiju Sveučilišta u Zagrebu. To je bila vrlo sretna okolnost jer mi je između ostaloga omogućila nabavljanje knjige predavanja s 2. konferencije o Fibonaccijevim brojevima održane u Grčkoj, gdje sam se prvi put susreo s jednim Diofantovim problemom kojim sam se kasnije bavio veći dio svoje znanstvene karijere. Na prvim godinama studija nisam bio baš ozbiljan student. U Zagreb sam došao nakon 14-mjesečnog služenja vojnog roka u Surdulici (na tadašnjoj jugoslavensko-bugarskoj granici), pa sam se nakon dolaska u Zagreb više družio s prijateljima (pjevanje, kartanje, i sl.) nego pohađao predavanja. Na trećoj godini studija sam se uozbiljio i počeo s ozbiljnim radom, i nisam se još zaustavio.

Kako je tekao Vaš poslijediplomski studij?



Nakon promocije doktorata: otac Josip, sestra Nataša, Andrej Dujella sa kćerkom Martom, supruga Valentina, majka Zaga

studiju matematike) i dobio prvu kćerku Martu 1994. godine. Kao pripadnik 112. brigade Hrvatske vojske u kolovozu 1995. godine sam sudjelovao u vojnoj operaciji Oluja. Godine 1996. obranio sam doktorsku disertaciju pod naslovom *Generalizirani Diofant–Davenportov problem*. Mentori disertacije su mi bili profesori Dragutin Svrtan i Dimitrije Ugrin–Šparac.

Posvetili ste se teoriji brojeva. Gdje ste se sve usavršavali u tom području? Molimo vas da navedete barem nekoliko mjesta gdje ste boravili kao i neke matematičare s kojima ste posebno surađivali.

Kao što sam već spomenuo, moj interes za teoriju brojeva počinje u srednjoj školi i usko je povezan s mojim sudjelovanjem na matematičkim natjecanjima. Moja doktorska disertacija bila je iz tog područja i sadržavala je rezultate koji su publicirani u međunarodnim časopisima. Pa ipak, mogao bih reći da je moje bavljenje teorijom brojeva bilo na pomalo amaterskoj osnovi, sve dok u srpnju 1996. godine nisam na 7. konferenciji o Fibonaccijevim brojevima, koja je održana u Grazu, upoznao profesora Attilu Pethőa sa Sveučilišta u Debrecinu u Mađarskoj. Bili smo prva dva predavača na konferenciji (on kao pozvani predavač, a ja naravno kao “obični”) i odmah smo shvatili da imamo puno zajedničkih matematičkih interesa. Mogu reći da je profesor Pethő moj pravi znanstveni mentor, koji je svojim savjetima od tog trenutka usmjeravao moju znanstvenu karijeru. Postali smo suradnici i prijatelji te objavili nekoliko zajedničkih znanstvenih radova od kojih je vjerojatno najvažniji onaj iz 1998. objavljen u *Quarterly Journal of Mathematics, Oxford*, koji je do danas citiran preko 170 puta (prema Google Scholaru). Debrecin sam prvi puta posjetio u prosincu 1996., a u studenom i prosincu 1998. bio sam tamo na znanstvenom usavršavanju kao stipendist mađarske vlade. I nakon toga sam redovito svake godine dolazio u Debrecin, gdje sam osim profesora Pethőa stekao i brojne druge suradnike (imam zajedničke radove sa 7 znanstvenika sa sveučilišta u Debrecinu), a prošle godine sam doživio i meni sasvim neočekivanu veliku počast – dodijeljen mi je počasni doktorat Sveučilišta u Debrecinu.

Na zadnjoj godini dodiplomskog studija slušao sam predavanja iz meni zanimljivog kolegija *Konveksni skupovi* kod profesora Zvonka Cerina. Budući da nisam uspio dogovoriti temu diplomskog rada iz teorije brojeva, izabrao sam temu iz konveksnih skupova, te diplomirao pod mentorstvom profesora Cerina 1990. godine. Iste godine upisao sam poslijediplomski studij matematike. Pohađao sam Seminar za topologiju, te slušao nekoliko kolegija iz topologije i jedan iz Konkretne matematike koji je donekle imao doticaja s teorijom brojeva (na koju nisam prestao misliti). Magistrirao sam 1993. godine pod mentorstvom profesora Cerina s temom *Invarijante topoloških konveksnosti*. Te iste godine objavljen mi je prvi znanstveni rad (o prije spomenutom Diofantovom problemu) u prestižnom časopisu specijaliziranom za teoriju brojeva *Acta Arithmetica*, i to mi je omogućilo da se posvetim znanstvenom radu iz teorije brojeva i pokušam napisati doktorsku disertaciju iz tog područja. U međuvremenu sam se 1993. oženio (suprugu Valentinu sam upoznao na



Hrvatska grupa iz teorije brojeva na konferenciji u Debrecinu 2015. g.

Zbog obiteljskih obaveza (sin Dominik rodio se 1999., a mlađa kćerka Jelena 2001.) izbjegavao sam duža izbijanja od kuće. Tako su moji znanstveni boravci u inozemstvu, kao predavača na doktorskom studiju ili gostujućeg znanstvenika, uglavnom bili na oko mjesec dana. Držao sam predavanja na doktorskim studijima na sveučilištima u Grazu (2001.), Debrecinu (2007.) i Bilbau (2011.), a od mjesta na kojima sam boravio kao gostujući znanstvenik izdvajam Strasbourg, Zürich (ETH), Moreliu (UNAM) i Mumbai (TIFR).

Molim Vas da opišete ukratko svoj znanstveni rad. U čemu su vaši najznačajniji doprinosi teoriji brojeva?

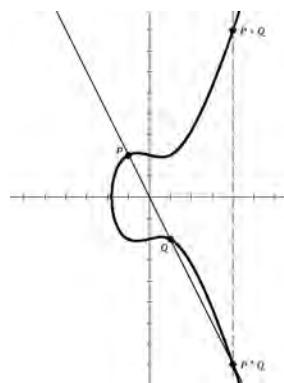
Glavno područje mog znanstvenog rada je teorija brojeva, posebno diofantske jednadžbe i eliptičke krivulje. Moj glavni znanstveni doprinos vezan je uz teoriju Diofantovih m -torki. Diofantova m -torka je skup od m prirodnih brojeva sa svojstvom da produkt svaka dva među njima uvećan za 1 daje kvadrat nekog prirodnog broja. Ako su elementi takvog skupa racionalni brojevi različiti od nule, onda ga zovemo racionalna Diofantova m -torka. Prvi je takve skupove proučavao starogrčki matematičar Diofant Aleksandrijski, koji je živio u 3. stoljeću, a po kojem su i diofantske jednadžbe i Diofantove m -torke dobile ime. On je pronašao prvu racionalnu četvorku s traženim svojstvom: $\{1/16, 33/16, 17/4, 105/16\}$. Prvu takvu cjelobrojnu četvorku pronašao je francuski matematičar i pravnik Pierre de Fermat (17. st.). To je skup $\{1, 3, 8, 120\}$. Zaista,

$$\begin{aligned} 1 \cdot 3 + 1 &= 2^2, & 1 \cdot 8 + 1 &= 3^2, & 1 \cdot 120 + 1 &= 11^2, \\ 3 \cdot 8 + 1 &= 5^2, & 3 \cdot 120 + 1 &= 19^2, & 8 \cdot 120 + 1 &= 31^2. \end{aligned}$$

Jedan od najpoznatijih rezultata u ovom području je dokaz da se Fermatova četvorka $\{1, 3, 8, 120\}$ ne može proširiti do cjelobrojne Diofantove petorke. To su dokazali 1969. godine dobitnik Fieldsove medalje Alan Baker i Harold Davenport. Taj je rezultat motivirao slutnju da ne postoji cjelobrojna Diofantova petorka. U prije spomenutom zajedničkom radu s Attilom Pethőom 1998. godine dokazali smo da se već par $\{1, 3\}$ ne može proširiti do Diofantove petorke. U radu objavljenom 2004. godine u prestižnom časopisu *Journal für die Reine und Angewandte Mathematik* dokazao sam da ne postoji Diofantova šestorka te da Diofantovih petorki ima najviše konačno mnogo. Ta dva članka su moji najcitiraniji članci i mnogo je autora kasnije radilo na poboljšanjima u smjeru dokaza nepostojanja cjelobrojnih petorki, a također i jedinstvenosti proširenja trojke do četvorke. U listopadu 2016. matematičari Bo He, Alain Togbé i Volker Ziegler najavili su dokaz nepostojanja Diofantove petorke i njihov dokaz se još provjerava.

Fermatovu četvorku $\{1, 3, 8, 120\}$ je do racionalne Diofantove petorke, i to s brojem $777\,480/2879^2$, nadopunio Leonhard Euler, švicarski matematičar, fizičar i astronom (18. st.). Pitanje postojanja racionalne šestorke ostalo je otvoreno sve do kraja 20. stoljeća kad je 1999. godine britanski fizičar Phil Gibbs (osvajatelj srebrnih medalja na matematičkim olimpijadama 1977. i 1978.) pronašao prvi primjer racionalne Diofantove šestorke. Dosta sam se bavio problemima vezanim uz Diofantove m -torke, a također i drugi članovi brojne hrvatske grupe iz teorije brojeva. Tako smo prošle godine u zajedničkom radu objavljenom u časopisu *International Mathematics Research Notices* čiji su koautori kolege Matija Kazalicki i Miljen Mikić iz Zagreba, Márton Szikszai iz Debrecina i ja, dokazali da postoji beskonačno mnogo racionalnih Diofantovih šestorki. Pitanje postojanja racionalnih sedmorki i dalje je otvoreno. O zanimljivosti problema vezanih uz Diofantove m -torke svjedoči popis od trenutno 335 naslova na popisu literature koji se može naći na mojoj web stranici <http://web.math.pmf.unizg.hr/~duje/dtuples.html> (od toga 270 naslova nakon 2000. godine), a možda i članak koji sam u kolovozu 2016. uspio objaviti u rubrici "What is. . ." časopisa *Notices of the American Mathematical Society* (najčitanijeg matematičkog časopisa na svijetu).

Također se bavim konstrukcijom eliptičkih krivulja velikog ranga. Na moguću vezu Diofantovih m -torki i eliptičkih krivulja upozorio me je profesor Attila Pethő. Kao i svi ostali njegovi savjeti, i ovaj se pokazao izvrstan. Dakle, eliptičke krivulje su krivulje 3. stupnja koje zadovoljavaju dodatni uvjet nesingularnosti. Zašto bi takve krivulje mogle biti zanimljive (zanimljivije od ostalih)? Razlog je taj da se na njima na vrlo prirodan način može definirati operacija zbrajanja točaka, koja onda ima ona svojstva koja smo naučili da ih ima obično zbrajanje brojeva. Ovo zbrajanje točaka definira se tako da se kroz dvije točke koje želimo zbrojiti povuče pravac. Budući da je promatrana krivulja 3. stupnja, ovaj siječe krivulju u točno još jednoj točki, i ova je (uz malu modifikaciju) traženi zbroj polazne dvije točke. Malu poteškoću imamo kada želimo zbrojiti točku samu sa sobom. Tada umjesto sekante povlačimo tangentu (pravac koji dira krivulju) u toj točki, pa nam zato treba dodatni uvjet postojanja tangente, tj. nesingularnost krivulje. Eliptičke krivulje se mogu promatrati nad bilo kojim skupom u kojem formula za jednadžbu pravca kroz dvije točke ima smisla. Posebno su važni slučajevi skupa racionalnih brojeva $\mathbb{Q}$ (time se bavi dio matematike koji se naziva aritmetička geometrija) i konačnih polja $\mathbb{F}_q$ (važnih za primjene u kriptografiji, faktorizaciji, dokazivanju prostosti).



Zbrajanje točaka na eliptičkoj krivulji

Diofantove m -torke se pojave u kontekstu eliptičkih krivulja kad želimo proširiti trojku $\{a, b, c\}$ do (cjelobrojne ili racionalne) četvorke. Tada imamo tri uvjeta: $ax + 1$, $bx + 1$ i $cx + 1$ su kvadrati. Ako pomnožimo ta tri uvjeta, dobivamo jednadžbu eliptičke krivulje $y^2 = (ax + 1)(bx + 1)(cx + 1)$. Svojstva Diofantovih m -torki su mi omogućila pronalaženje eliptičkih krivulja nad poljem racionalnih brojeva sa zanimljivim, prethodno nepoznatim, strukturama, tj. brojem generatora (rangom) i strukturom skupa točaka konačnog reda (torzijom). Zadnjih 15-tak godina održavam web stranicu

<http://web.math.pmf.unizg.hr/~duje/tors/tors.html>

s podacima o krivuljama rekordnog ranga za sve moguće torzijske grupe (ona osim mojih uključuje rezultate i drugih matematičara, i vrlo je popularna među onima koji se bave tim pitanjima).

S kojim matematičarima, u Hrvatskoj i inozemstvu, posebno uspješno surađujete?

Od hrvatskih matematičara najprije bih izdvojio suradnju s kolegom Ivicom Gusićem. Objavili smo 5 zajedničkih znanstvenih radova, a od 2001. godine zajednički vodimo vrlo aktivni Seminar za teoriju brojeva i algebru. Spomenuo bih da je hrvatska grupa iz teorije brojeva u studenom 2014. organizirala znanstveni skup *Workshop on Number Theory and Algebra* povodom 60. rođendana kolege Gusića. Na skupu je predavanja održalo 27 matematičara iz Hrvatske, Austrije, Francuske, Južnoafričke Republike, Mađarske i Španjolske.



*Sudionici konferencije povodom 60. rođendana Ivica Gusića;
u prvom redu u sredini stoje Ivica Gusić i Attila Pethő*

Zatim, tu je naravno suradnja s kolegama kojima sam bio (su)mentor doktorske disertacije (kronološkim redom, od 2001. do 2014.): Borka Jadrijević, Zrinka Franušić, Alan Filipin, Bernadin Ibrahimpašić, Filip Najman, Ana Jurasic, Mirela Jukić Bokun, Petra Tadić, Vinko Petričević, Tomislav Pejčević (zajedničko mentorstvo s Yannom Bugeaudom sa Sveučilišta u Strasbourgu), Ivan Soldo, Miljen Mikić (zajedničko mentorstvo s Filipom Najmanom) i Sanda Bujačić, a zajedničke radove imam i s kolegama Lukom Lasićem te Matijom Kazalickim, s kojim u zadnje vrijeme dosta surađujem na problemima vezanim uz Diofantove m -torke u skupu racionalnih brojeva i konačnim poljima.

Od matematičara iz inozemstva, već sam istaknuo veliki značaj za moju karijeru suradnje s Attilom Pethőm i ostalim članovima grupe za teoriju brojeva iz Debrecina (Kálmán Győry, Lajos Hajdu, Attila Bérczes, Ákos Pintér, Szabolcs Tengely, Márton Szikszai).

Odličnu suradnju uspostavio sam i s grupom za teoriju brojeva iz Graza koju vodi profesor Robert Tichy. Često sam bio u znanstvenim posjetima Grazu, a najviše sam surađivao s kolegom Clemensom Fuchsom (imamo 8 zajedničkih radova). Suradnju smo započeli još dok je on bio doktorski student, a ja predavač na doktorskom studiju u Grazu, a nastavili smo surađivati i nakon što je on iz Graza otišao najprije u Zürich te potom u Salzburg. Godine 2005. smo riješili jedan problem koji je postavio Euler. Naime, Euler je pronašao četiri racionalna broja $5/2$, $9/56$, $65/224$, $9/224$ sa svojstvom da produkt bilo koja dva broja među njima, uvećan za sumu ta dva broja, daje potpun kvadrat, te je postavio pitanje postoje li četiri prirodna broja s istim svojstvom. Mi smo uspjeli dokazali da takva četiri prirodna broja ne postoje, te smo o tome objavili članak u časopisu *Journal of the London Mathematical Society*.

Svakako trebam istaknuti i suradnju s kolegom Yannom Bugeaudom iz Strasbourga. Imamo 5 zajedničkih radova, a zajedno smo vodili i doktorat kolege Tomislava Pejkovića, što je bio zajednički doktorat (cotutelle) Sveučilišta u Strasbourgu i Zagrebu. Zahvaljujući suradnji na tom doktoratu, ušao sam u jedno novo područje matematike, a to je problem separacije korijena polinoma; pitamo se koliko bliska mogu biti dva različita korijena polinoma s cjelobrojnim koeficijentima, ako tu udaljenost usporedimo s visinom (maksimumom apsolutnih vrijednosti koeficijenata) polinoma. Konstruirali smo familije reducibilnih i ireducibilnih polinoma s najboljim poznatim separacijskim svojstvima, a zajednički rad s kolegama Tomislavom Pejkovićem i Brunom Salvyjem iz Lyona u kojem proučamo udaljenost apsolutnih vrijednosti korijena polinoma nedavno nam je prihvaćen za objavljivanje u časopisu *American Mathematical Monthly*.

Od 2009. godine uspostavio sam vrlo plodnu suradnju s kolegama iz Bilbaa (Universidad del Pais Vasco) Juan Carlosom Peralom i Julianom Aguirreom. Ta suradnja rezultirala je s ukupno 9 zajedničkih radova iz područja eliptičkih krivulja i njihovih primjena na neke aritmetičke i geometrijske probleme. Dio tih radova odnosi se i na konstrukciju eliptičkih krivulja velikog ranga koje su inducirane Diofantovih trojkama.

Još bih spomenuo i plodnu dugogodišnju suradnju s izvrsnim matematičarem i svjetskim putnikom Florianom Lucom. On je sada na Wits University u Johannesburgu, a najveći dio naše suradnje je realiziran u periodu dok je bio na Universidad Nacional Autónoma de Mexico u Morelii u Meksiku (bolje rečeno, tamo je bio zaposlen i jednom sam ga posjetio, ali smo se susretali i intenzivno surađivali na konferencijama širom svijeta). Objavili smo 7 zajedničkih radova iz različitih tema iz područja diofantskih jednadžbi.

Zajedno s Marcelom Maretićem napisali ste knjigu Kriptografija koja se koristi kao udžbenik za taj kolegij. Koje ste još knjige napisali, znanstvene i stručno popularne?

Godine 1999. uveo sam novi kolegij *Kriptografija* na studiju matematike. Dugo godina je taj kolegij bio izborni (ali su ga upisivali skoro svi studenti, bilo je i do 150 studenata godišnje), da bi kod zadnje reforme studija postao obavezni na diplomskom studiju Računarstva i matematike. Vrlo brzo nakon početka držanja predavanja napisao sam skriptu i postavio je na svoju web stranicu. Kasnije sam u suradnji s kolegom Marcelom Maretićem, koji je držao vježbe iz tog kolegija, proširio skriptu te smo objavili knjigu u izdanju izdavačke kuće Element.

Moj angažman u kriptografiji je za sada više u smjeru popularizacije, nego ozbiljnog znanstvenog rada. Održao sam brojna predavanja o vezi teorije brojeva i kriptografije za učenike, nastavnike i širu publiku na ljetnim školama, festivalima znanosti, aktivima nastavnika, danima otvorenih vrata i sličnim prigodama. Od ukupnog broja od 180 mentorstava diplomskih radova koliko sam ih do sada imao, priličan broj se odnosi na teme iz kriptografije. Što se tiče mog znanstvenog doprinosa u kriptografiji, objavio sam nekoliko radova u zbornicima srednjoeuropskih kriptografskih konferencija. Jedan dio rezultata odnosi se na primjene diofantskih aproksimacija u kriptanalizi RSA kriptosustava (jedan od tih članaka je bio dosta zapažen među kriptografima te ima 64 citata u Google Scholaru, a citiran je i u nekoliko monografija), a drugi na zajednički rad s kolegom Filipom Najmanom na primjenama eliptičkih krivulja s velikom torzijskom grupom u faktorizaciji velikih prirodnih brojeva.

Petnaest godina sam sudjelovao u radu Državnog povjerenstva na matematička natjecanja. U okviru te aktivnosti priredio sam 1996. godine zajedno s kolegicom Meom Bombardelli i kolegom Sinišom Slijepčevićem knjižicu *Matematička natjecanja učenika srednjih škola (izbor zadataka)*. Nadalje, 2000. godine sam objavio knjižicu *Fibonaccijevi brojevi* u izdanju Hrvatskog matematičkog društva.

Na svojoj web stranici postavio sam i skripte iz većeg broja kolegija: *Teorija brojeva* (preddiplomski studij matematike), *Eliptičke krivulje u kriptografiji* (diplomski studij

Računarska i matematike te Teorijske matematike), *Diskretna matematika* (diplomski studij na FER-u), *Teorija brojeva u kriptografiji*, *Diofantske jednačbe*, *Algoritmi za eliptičke krivulje*, *Diofantske aproksimacije* (doktorski studij matematike na PMF-MO). Nadam se da ću jednom naći dovoljno vremena pa na osnovu tih materijala napisati jednu ili dvije knjige iz teorije brojeva.



*Pedeset godišta Glasnika matematičkog
(Josip Tambača i Andrej Dujella)*

Josip Tambača). Bilo je to za mene vrlo lijepo iskustvo. Izvrsno sam surađivao s članovima uredništva, a posebno korisne savjete sam dobivao od prvog glavnog urednika časopisa, nedavno preminulog akademika Sibe Mardešića. Tijekom posljednjeg Hrvatskog matematičkog kongresa *Glasnik matematički* je proslavio 50. godišnjicu izlazenja kratkim izlaganjima dosadašnjih urednika te izložbom svih do sada objavljenih brojeva časopisa.

Ubrzo nakon izbora za redovitog člana Akademije, izabran sam za glavnog urednika časopisa *Rađ HAZU, Matematičke znanosti* kojeg izdaje Hrvatska akademija znanosti i umjetnosti. Članovi uredništva tog časopisa su matematičari redoviti članovi Akademije: Žarko Dadić, Josip Pečarić i Marko Tadić te članovi suradnici: Ibrahim Aganović, Mirko Primc, Vladimir Volenec i Zoran Vondraček.

Od 2003. do 2006. godine bio sam prvi glavni urednik *Hrvatskog matematičkog elektronskog časopisa math.e* (web adresa časopisa je <http://e.math.hr/>). Bilo je to vrlo zanimljivo iskustvo. S jedne strane suradnja s potencijalnim autorima na temama zanimljivima za objavu upravo u takvom tada relativnom novom mediju, a s druge strane rad na rješavanju tehničkih problema vezanih uz prikaz matematičkih tekstova na webu, za što u to vrijeme nije bilo nikakvog standarda.

U srednjoj školi ste rješavali zadatke iz Matematičko fizičkog lista, a bili ste i sudionik Ljetnih škola mladih matematičara u Preku na otoku Ugljanu. Koliko Vam je to pomoglo tokom studija? Što je bilo presudno u vašem usmjerenju na matematiku?

Časopis *Matematičko-fizički list* sam tijekom srednjoškolskog školovanja redovito primao, čitao članke i rješavao zadatke. Pri kraju školovanja u njemu sam objavio i svoj prvi stručni rad. U četvrtom razredu dobio sam Priznanje "Stjepan Škreblin", kao najuspješniji rješavač zadataka u toj školskoj godini. Mogu reći da je i *Matematičko-fizički list* doprinio mojoj odluci za studij matematike. Odluka se definitivno potvrdila nakon uspjeha na Međunarodnoj matematičkoj olimpijadi.

Sudjelovao sam na Ljetnoj školi mladih matematičara kao učenik trećeg razreda srednje škole. Bio je to za mene vrlo zanimljiv susret sa zahtjevnijim matematičkim temama, koji mi je dao naslutiti što me čeka na studiju matematike. Kasnije sam i sam bio predavač na Ljetnom kampu mladih matematičara, a često sam sudjelovao kao predavač na

Bili ste u uredništvu nekih časopisa iz matematike, a još danas ste urednik svjetski poznatog časopisa Glasnik matematički.

Upravo mi istiće mandat glavnog urednika *Glasnika matematičkog* i na dužnost stupa profesor Dražen Adamović kao novi glavni urednik. Ostajem u uredništvu kao član zadužen za članke iz teorije brojeva. U proteklih 15 godina bio sam u najužem uredništvu tog časopisa, najprije 10 godina kao izvršni urednik (glavni urednik je bio profesor Hrvoje Šikić), a potom 5 godina kao glavni urednik (izvršni urednici su bili profesori Dražen Adamović i

priprema hrvatskih natjecatelja na matematičkim olimpijadama. Mnoge od mladih matematičara koje sam tako upoznao, uskoro sam ponovo susreo kao studente matematike. Mogu reći da je jedno od najvećih zadovoljstava i privilegija u mom poslu sveučilišnog nastavnika to da imam priliku predavati mladim ljudima koji su među najpametnijim Hrvatima u svojoj generaciji.

Vaša najstarija kćer student je četvrte godine studija matematike, a mlađa je upisala Matematičku gimnaziju u Zagrebu. Hoće li se i Vaš sin opredijeliti za matematiku?

Marta je studentica na diplomskom studiju Teorijska matematika (vjerojatno nije izabrala studij Računarstva da ne mora slušati moja predavanja iz Kriptografije). Vrlo je uspješna na studiju. Prošle godine je dobila Rektorovu nagradu. Nisam je nagovarao prilikom izbora studija, pa neću nagovarati ni Dominika ni Jelenu. Neće mi biti krivo ako i netko od njih izabere matematiku ili nešto blisko tome. Za Dominika se u osnovnoj školi činilo da je daleko od matematike (bio je dosta uspješan u vaterpolu u mlađim kategorijama), ali u srednjoj školi (XIII. gimnazija u Zagrebu) je i njemu profesorica matematike probudila interes za matematiku. A Jelena sudjeluje na ljetnim i zimskim školama matematike, na priprema koje organizira udruga Mladi nadareni matematičari "Marin Getaldić", a prošle godine je osvojila 3. nagradu na državnom natjecanju iz matematike.

Biste li mogli uputiti poruku učenicima srednjih škola koji bi se više željeli posvetiti matematici?

Želio bih ohrabriti učenike koji imaju sklonosti ka matematici da razvijaju svoj talent i da više vremena posvete rješavanju zahtjevnijih zadataka i izučavanju matematičkih sadržaja koji nisu nužno dio redovitog školskog gradiva. Teško je predvidjeti što sve čeka današnje učenike, ali mnoga zanimanja za koja se očekuje da će biti atraktivna u skoroj budućnosti zahtijevaju dobro poznavanje matematike. Natjecanja iz matematike (a i iz ostalih područja) dobar su način za testiranje svojih sposobnosti u usporedbi s ostalim talentiranim vršnjacima. Jedna od prednosti matematike u odnosu na neke druge grane znanosti je s jedne strane njezina univerzalnost, a s druge relativna nezahtjevnost što se tiče financijskih i tehničkih preduvjeta. Iako možda nije najbolja usporedba, možda se na neki način matematika može usporediti s nogometom: ni za treniranje nogometa nisu nužni idealni uvjeti, a talentirani nogometaši i iz malih sredina imaju mogućnosti probiti se u najbolje klubove na svijetu. Slično je s matematikom: u mnogim granama matematike vrhunski rezultati ne zahtijevaju skupu opremu, već talent i puno rada (dobro dođe i sreća, kao što se vidi iz mog primjera), a stvarno važni rezultati znanstvenika iz manjih znanstvenih centara bit će prepoznati i publicirani u vrhunskim svjetskim časopisima puno lakše nego u područjima znanosti koja nisu tako univerzalno orijentirana kao matematika.