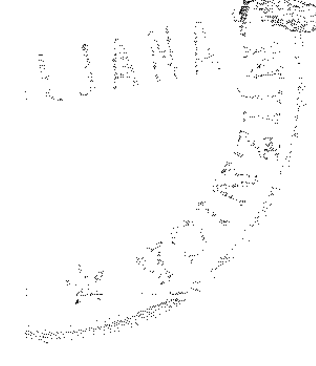


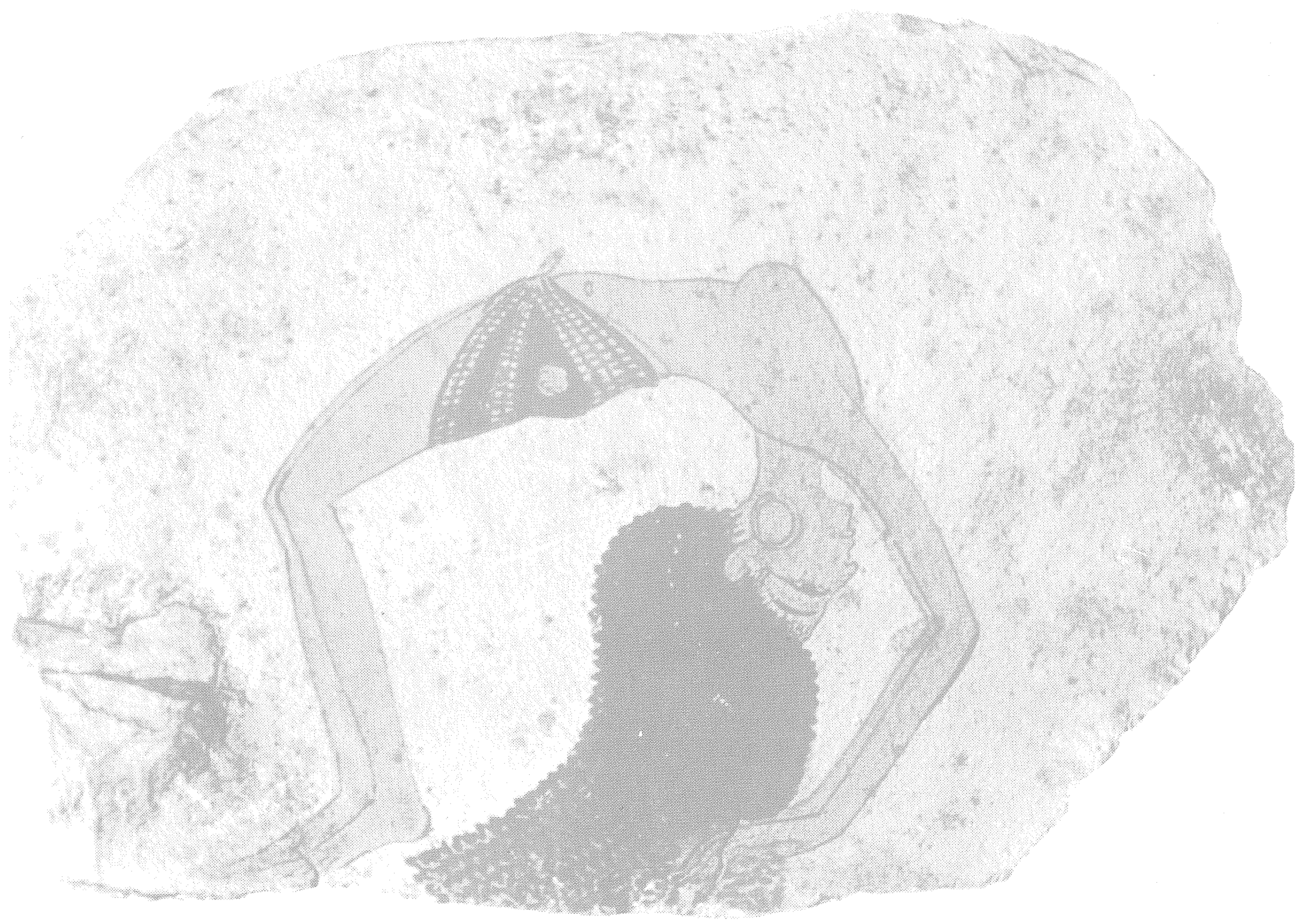
TRIALNA EKONOMSKA
IŽNICA Ljubljana

R 147/p6-4



1996
Letnik 43
4

OBZORNIK ZA MATEMATIKO IN FIZIKO



OBZORNIK ZA MATEMATIKO IN FIZIKO

LJUBLJANA, JULIJ 1996

letnik 43, številka 4, strani 97–128

Glasilo Društva matematikov, fizikov in astronomov Slovenije, 1001 Ljubljana, Jadranska c. 19, p.p. 2964, telefonska št. (061) 17-66-553, žiro račun 50106-678-47233, devizna nakazila SKB banka d.d. Ljubljana, val-27621-42961/9, Ajdovščina 4, Ljubljana.

Uredniški odbor: Bojan Magajna (glavni urednik), Boris Lavrič (urednik za matematiko in odgovorni urednik), Martin Čopič (urednik za fiziko), Boštjan Jaklič (tehnični urednik).

Jezikovno pregledal Janez Juvan, računalniško oblikoval Martin Zemljč.

Člani društva prejema Obzornik brezplačno. Celoletna članarina 2.300 SIT. Naročnina v knjigarnah in za ustanove 4.600 SIT, za študente 1.150 SIT, za tujino 50 DEM. Posamezna številka za člane 440 SIT, stare številke 320 SIT.

Tisk: Tiskarna KURIR. Naklada 1500 izvodov.

Revijo sofinancirata Ministrstvo za znanost in tehnologijo ter Ministrstvo za šolstvo in šport.

Po mnenju MZT št. 415-52/92 z dne 5.2.1992 šteje revija med proizvode iz 13. točke tarifne št. 3 zakona o prometnem davku, za katere se plačuje 5% davek od prometa proizvodov.

DMFA je včlanjeno v Evropsko matematično društvo (EMS), v Mednarodno matematično unijo (IMU), v Evropsko fizikalno društvo (EPS) in v Mednarodno združenje za čisto in uporabno fiziko (IUPAP). DMFA ima pogodbo o recipročnosti z Ameriškim matematičnim društvom (AMS).

© 1996 DMFA Slovenije – 1292

Poštnina plačana na pošti 1102 Ljubljana

VSEBINA — CONTENTS

Članki – Articles

Str.–Page

Singularna števila matrik — Singular values of matrices (Aleksij Turnšek) 97–104

Stičišča in razhajanja v poučevanju osnovnošolske in srednješolske matematike
— Points of connection and separation in teaching primary and secondary
school mathematics (Milena Strnad) 105–115

Kriptosistem RSA leta 1873? — RSA cryptosystem in year 1873? (Janez
Žerovnik) 116–118

Vesti — News

Razpis za priznanja učiteljem (Ivana Mulec) 118

Pismo ministru za znanost in tehnologijo 119 Seznam
diplomantov prve, druge in tretje stopnje ter doktorandov iz matematike
in fizike v letu 1995 (Martina Koman) 120–125

Razpis DMFA Slovenije za posebne pohvale šolam (UO DMFA Slovenije) 127

Strokovno srečanje in 48. občni zbor društva (Egon Zakrajšek) IV

Nove knjige — New books (Janez Strnad, Matija Cencelj, Niko Prijatelj,
Miran Černe, Janez Strnad) 104, 125–127, 128, 128–III, III

Na ovitku: Ostrakon z akrobatsko plesalko, 1300 pr.n.št. (k članku iz fizike).

SINGULARNA ŠTEVILA MATRIK

ALEKSEJ TURNŠEK

Math. Subj. Class. (1991) 15A18

V članku povemo dve ekvivalentni definiciji singularnih števil za kompleksne matrike in dokažemo nekaj neenakosti za lastne vrednosti in singularna števila.

SINGULAR VALUES OF MATRICES

In this note we give two equivalent definitions of singular values of complex matrices and prove some inequalities on singular values and eigenvalues.

Algebro kompleksnih $n \times n$ matrik označimo z M_n . Vsaka matrika iz M_n naj deluje kot linearen operator na prostoru $\mathbb{C}^n$. V $\mathbb{C}^n$ imejmo skalarni produkt $\langle x, y \rangle = \sum_{k=1}^n x_k \overline{y_k}$ in normo, dobljeno iz skalarne produkta. Torej je norma vektorja x iz $\mathbb{C}^n$ enaka $\|x\| = \langle x, x \rangle^{\frac{1}{2}}$. Za matriko A pa definirajmo „operatorsko“ normo z $\|A\| = \sup\{\|Ax\|; x \in \mathbb{C}^n, \|x\| \leq 1\}$. Za tako definirano normo velja $\|A\|^2 = \|A^*A\|$ in $\|A^*\| = \|A\|$, kjer smo z A^* označili adjungirano matriko. Torej za $A = (a_{ij})$ je $A^* = (\overline{a_{ji}})$. Za matriko A iz M_n pravimo, da je *pozitivna*, če obstaja taka matrika B iz M_n , da velja $A = B^*B$. Ekvivalentna je zahteva $\langle Ax, x \rangle \geq 0$ za vsak $x \in \mathbb{C}^n$. Nadalje vemo, da za vsako pozitivno matriko A obstaja pozitivna matrika kvadratni koren $A^{\frac{1}{2}}$.

Vsako kompleksno število z lahko zapišemo v polarni obliki $z = e^{i\varphi}|z|$. Ali imamo tudi za matriko $A \in M_n$ podoben zapis $A = U|A|$ in kaj bi vzeli za U in $|A|$? Za $|A|$ vzemimo pozitivni koren iz matrike A^*A , torej $|A| = (A^*A)^{\frac{1}{2}}$. Analogija k številom $e^{i\varphi}$ pa so unitarne matrike, torej take, da velja $UU^* = U^*U = I$.

Sedaj pa pokažimo:

Trditev 1 (Polarna dekompozicija). Če je A iz M_n in $|A| = (A^*A)^{\frac{1}{2}}$, obstaja taka unitarna matrika U , da je $A = U|A|$.

Dokaz. Za vsak $x \in \mathbb{C}^n$ je

$$\|Ax\|^2 = \langle Ax, Ax \rangle = \langle A^*Ax, x \rangle = \langle |A|^2x, x \rangle = \langle |A|x, |A|x \rangle = \||A|x\|^2. \quad (1)$$

Za $y = |A|x$ definirajmo $Uy = Ax$. Preslikava U je linearna in dobro definirana, kajti iz $y = 0$ sledi po vrsti $|A|x = 0$, $Ax = 0$ in $Uy = 0$. Operator U je s tem definiran za vsak y iz zaloge vrednosti $\text{Im}(|A|)$ operatorja $|A|$, in sicer slika v zalogo vrednosti $\text{Im}(A)$ operatorja A . Zaradi $\|Ax\| = \||A|x\|$ je jedro preslikave A enako jedru preslikave $|A|$. To pomeni, da je dimenzija $\text{Im}(|A|)$ enaka dimenziji $\text{Im}(A)$. Iz enakosti $\|Ax\| = \||A|x\|$ pa sledi tudi injektivnost preslikave U . Ker preslikava U slika med dvema enako razsežnima prostoroma, je tudi bijektivna. Seveda imata tudi ortogonalna

komplementa $\text{Im}(|A|)^\perp$ in $\text{Im}(A)^\perp$ enako dimenzijo. Denimo, da je ta dimenzija enaka k , in izberimo ortonormirani bazi $\{e_1, \dots, e_k\}$ v $\text{Im}(|A|)^\perp$ in $\{f_1, \dots, f_k\}$ v $\text{Im}(A)^\perp$. Za vsak $1 \leq i \leq k$ definirajmo $Ue_i = f_i$. Sedaj je operator U definiran povsod in zadošča pogoju $A = U|A|$. Dokaz, da je res unitaren, pa prepuščamo bralcu. ■

Sedaj pa postavimo tole definicijo:

Definicija 2. Lastne vrednosti matrike $|A|$ imenujemo singularna števila matrike A . Označimo jih z $\mu_k(A)$ in uredimo po velikosti $\mu_1(A) \geq \dots \geq \mu_n(A) \geq 0$.

Ker je matrika $|A|$ pozitivna, je diagonalizabilna z unitarno matriko V . Torej lahko zapišemo $V^*|A|V = \text{diag}(\mu_1(A), \dots, \mu_n(A))$, kjer smo z $\text{diag}(\mu_1(A), \dots, \mu_n(A))$ označili diagonalno matriko s števili $\mu_k(A)$ po diagonali. Iz polarne dekompozicije $A = U|A|$ pa sledi

$$A = V_1 \text{diag}(\mu_1(A), \dots, \mu_n(A)) V_2,$$

kjer sta $V_1 = UV$ in $V_2 = V^*$ unitarni matriki. Zgornjemu zapisu pravimo SVD razcep (singular value decomposition) in je pomemben v numerični matematiki.

Poleg singularnih števil lahko matriki A priredimo končno zaporedje nenegativnih realnih števil takole:

$$a_k(A) = \inf\{\|A - B\|; \text{rang}(B) < k\}, \quad 1 \leq k \leq n.$$

Definicija 3. Števila $a_k(A)$ imenujemo aproksimativna števila matrike A .

Pokažimo, da se singularna in aproksimativna števila ujemajo.

Izrek 4. Za matriko A iz M_n velja $a_k(A) = \mu_k(A)$ za vsak $1 \leq k \leq n$.

Dokaz. Ker je $|A|$ pozitivna matrika, lahko izberemo lastne vektorje $e_1, \dots, e_n$ tako, da bodo ortonormirana baza v $\mathbb{C}^n$. Za vsak $x \in \mathbb{C}^n$ potem velja

$$x = \sum_{j=1}^n \langle x, e_j \rangle e_j \quad \text{in} \quad |A|x = \sum_{j=1}^n \mu_j(A) \langle x, e_j \rangle e_j.$$

Za matriko A upoštevamo polarni razcep in dobimo

$$Ax = U|A|x = \sum_{j=1}^n \mu_j(A) \langle x, e_j \rangle Ue_j. \quad (2)$$

Tudi vektorji Ue_j so ortonormirani, saj unitarna matrika ohranja dolžino in ortogonalnost. Za izbrani $k \geq 2$ definirajmo operator A_{k-1} z

$$A_{k-1}x = \sum_{j=1}^{k-1} \mu_j(A) \langle x, e_j \rangle Ue_j.$$

znamka za

12 SIT

KT DMFA Slovenije

Jadranska 19

1001 Ljubljana

p.p. 2964



znamka za

12 SIT

Hotel JAMA

Jamska cesta 28

6230 Postojna

Naročilnica

Ime in priimek

Naslov

Pošta

Nepreklicno naročam naslednje knjige:

.....

.....

.....

.....

Podpis:



PRIJAVA

Prijavljam se na strokovno srečanje in 48. občni zbor DMFA Slovenije, ki bo v Postojni 11. in 12. oktobra 1996, v hotelu Jama, Jamska 28, tel. (067) 24-172. Prijavo pošljite do 7. oktobra.

Ime in priimek (tiskano)

Točen naslov

Želim poslušati predavanja iz fizike, uporabne matematike, pedagoške matematike (ustrezno obkrožite).

Rezervirajte mi

v enoposteljni sobi	penzion (7190 SIT)	polpenzion (6420 SIT)
---------------------	--------------------	-----------------------

v dvoposteljni sobi	penzion (6170 SIT)	polpenzion (5230 SIT)
---------------------	--------------------	-----------------------

Pridem dne, prvi obrok: zajtrk - kosilo - večerja.

Odidem dne, zadnji obrok: zajtrk - kosilo - večerja.

(ustrezno obkrožite)

ANI

seznam publikacij, ki jih je izdala Komisija za tisk pri DMFA lavedene cene veljajo za člane društva, študente in dijake. Za e so cene 25% višje. Vključujejo 5% prometni davek in jih do ne bomo spreminjali. Knjige lahko naročite s priloženo ali pa vsak dan od 10. do 14. ure po telefonu (061) 123-24-60. ni Komisije za tisk lahko kupite tudi nekatere knjige iz tega in fizikalnega področja, ki so jih izdale DZS, CZ, MK in

Hvala in lep pozdrav
Andreja Šafarič

(1996/97) - letna naročnina 1500
- skupinska naročila (letna) 1200

KNJIŽNICA

JOSIP PLEMELJ - OB 100 - LETNICI ROJSTVA 360
ASTRONOMSKA OPAZOVANJA 360
ZAČETKI SODOBNE FIZIKE 360
RELATIVNOST ZA ZAČETNIKE 360
KAJ JE TEORIJA RELATIVNOSTI 360
UKROČENA MATEMATIKA 360
PRESEKOVA ZVEZDNA KARTA (s kat.) 360
ZAČETKI KVANTNE FIZIKE 360
ENAJSTA ŠOLA IZ FIZIKE 360
TEKMUJMO ZA VEGOVA PRIZNANJA-5. in 6. RAZR. 720
TEKMUJMO ZA VEGOVA PRIZNANJA-7.RAZR. 720
OH, TA MATEMATIKA 540
NAJNUJNEJŠE O GRAFIH 360
JOŽEF STEFAN - OB 150 - LETNICI ROJSTVA 360
JOSIP PLEMELJ - OB 20 - LETNICI SMRTI 360
DO NEWTONOVIH ZAKONOV 360
NALOGE S TEKMOVANJ IZ FIZIKE V OŠ - 1.del 540
KARTI SEV. IN JUŽ. NEBA (s kat.) 1600
MATKAI 700
FIZIKALNE NALOGE IZ VSAKDANJEGA ŽIVLJENJA 540
TEKMUJMO ZA VEGOVA PRIZNANJA 880

NA DISKETAH

POSNETE DISKETE em TEX 5 1/4 HD (1.2M) (AT) 340
POSNETE DISKETE em TEX 3 1/2 HD (1.44M)(AT) 480
POSNETA DISKETA PICTeX CAD 2640

UČBENIKI IN PRIROČNIKI

ŠTALEC I. ZBIRKA VAJ-1.RAZ. 720
ŠTALEC I. ZBIRKA VAJ-2.RAZ. 720
ŠTALEC I. ZBIRKA VAJ-3.RAZ. 800
ŠTALEC I. ZBIRKA VAJ-4.RAZ. 720
URŠIČ S. MATEMATIČNE TABELE IN FORMULE 480
PUCELJ I. GEOMETRIJA - 2.DEL 440
AVSEC F. ASTRONOMIJA 960
ZMAZEK V. MATEMATIKA. PRIPRAVA NA MATURO 1200
ŽELJKO M. ALTUS, CITIUS, FORTIUS 1060
THE ROLE OF EXPERIMENT IN PHYS. EDUCATION 1320
STATISTIČNI TERMINOLOŠKI SLOVAR 1060
KOŠMELJ B. ŠTEVILSKE KRIŽANKE 540
MARNELL G.R. MERI PLATNO, TRAK NA VATLE 360
STRNAD J. NAŠE NEBO 1996 700
RANZINGER NAVODILA ZA emTeX 3.0 340
NAVODILA ZA PICTeX CAD 200
LOKAR M. dBASE III PLUS 440
KLAVŽAR S. MALI PRIROČNIK OPERAC. SISTEMA MS DOS 540
RAZPET M. SEDI IN PIŠI Z LaTeX-om! 540
LOKAR M. ZAČETI Z dBASE IV 540
LOKAR M. dBASE IV - UKAZI IN FUNKCIJE 540
LOKAR M. DERIVE 540
KLAVŽAR S. WINDOWS 3.1 PODKREPLJEN Z DOS 6.0 760
LOKAR M. TURBO PASCAL 7.0 620

KNJIŽNICA SIGMA

VIDAV I. REŠENI IN NEREŠENI PROBLEMI MATEMATIKE 760
VADNAL A. ELEMENTARNI UVOD V VERJETNOSTNI RAČUN 760
BOHTE Z. NUMERIČNO REŠEVANJE ENAČB 760
PRIJATELJ N. MATEMATIČNE STRUKTURE I. 1280
JAMNIK R. ELEMENTI TEORIJE INFORMACIJE 760
VIDAV I. ŠTEVILA IN MATEMATIČNE TEORIJE 760
VADNAL A. FUNKCIJE I. 760
JAMNIK R. TEORIJA IGER 760
PRIJATELJ N. MATEMATIČNE STRUKTURE III. 760
BATAGELJ V. REŠENE NAL.IZ MAT.Z REP.TEKM.-1.DEL(1950-1966) 760
BATAGELJ V. REŠENE NAL.IZ MAT.Z REP.TEKM.-2.DEL(1967-1975) 760
STRUIK D.J. KRATKA ZGODOVINA MATEMATIKE 760
VADNAL A. OSNOVE DIFERENČNEGA RAČUNA 760
WEINBERG S. PRVE TRI MINUTE 760
PRIJATELJ N. OSNOVE MATEMATIČNE LOGIKE-1.DEL 960
GRASSELLI J. DIOFANTSKE ENAČBE 760
POLYA G. KAKO REŠUJEMO MATEMATIČNE PROBLEME 760
MOHAR B. PROGRAMSKI JEZIK PASCAL 760
ŠEVARLIČ B. KRATKA ZGODOVINA ASTRONOMIJE - 2.DEL 760
LAVRIČ B. REŠENE NAL.IZ MAT.Z REP.TEKM.-3.DEL(1976-1987) 760
BATAGELJ V. ENAJSTA ŠOLA RAČUNALNIŠTVA 760
STRNAD J. MALA KVANTNA FIZIKA 760
SADOVSKI MATEMATIKA IN ŠPORT 760
VIRČENKO N.A. MATEMATIKA V AFORIZMIH, CITATIH IN IZREKIH 760
STRNAD J. VOZIME, AVTO, V DALJAVE 760
FELDA D. REŠENE NAL. IZ MAT. S ŠOL.IN IZB.TEKM.(1975-91) 760

GRASSELLI J.	DIOFANTSKI PRIBLIŽKI	760
HAWKING S.	BERILO H KRATKI ZGODOVINI ČASA S. HAWKINGA	1200
DEVLIN K.	NOVA ZLATA DOBA MATEMATIKE	2000
HAWKING S.	ČRNE LUKNJE IN OTROŠKA VESOLJA	1760
HAWKING S.	KRATKA ZGODOVINA ČASA	2000
ŠPÖRER Z.	MATEMATIČNI LEKSIKON ZA NEMATEMATIKE	1440
BOHTE Z.	UVOD V NUMERIČNO RAČUNANJE	1280
OMLADIČ M.	MATEMATIKA IN DENAR	1280
HLADNIK M.	MODERNA KVADRATURA KROGA	1280
ŽELJKO M.	REŠENE NALOGE IZ MAT. IZ DRŽ. IN IZB. TEKMOVANJ	1280

IZBRANA POGlavJA IZ MATEMATIKE IN RAČUNALNIŠTVA

DOBOVIŠEK M.	REŠENE NALOGE IZ ANALIZE I.	800
SUHADOLC A.	SEBI ADJUNGIRANI OPERATORJI V HILB. PROST.	240
SUHADOLC A.	LINEARNI TOPOLOŠKI PROSTORI-1.DEL	480
WIRTH N.	RAČUNALNIŠKO PROGRAMIRANJE-1.DEL	1200
HLADNIK M.	NALOGE IN PRIMERI IZ FUNKCIONALNE ANALIZE	480
	IN TEORIJE MERE	
DOBOVIŠEK M.	NALOGE IZ ALGEBRE I.	960
KOZAK J.	NALOGE IZ RAČUNALNIŠTVA	640
KRAMAR E.	REŠENE NALOGE IZ LINEARNE ALGEBRE	800
BATAGELJ V.	DS1, LOGIKA IN MNOŽICE, NALOGE	800
HLADNIK M.	POVABILO V HARMONIČNO ANALIZO	640
BATAGELJ V.	DS2, ALGEBRA IN TEORIJA GRAFOV, NALOGE	800
JUVAN M.	121 NALOG IZ PASCALA	640
SUHADOLC A.	ROBNI PROBLEMI ZA LIN. DIF. ENAČBE II. REDA	400
VRABEC J.	TRI TEME IZ TEORIJE VRST	240
SUHADOLC A.	POTENCIALNA TEORIJA	960
PAVEŠIČ P.	REŠENE NALOGE IZ TOPOLOGIJE	960
DOBOVIŠEK M.	REŠENE NALOGE IZ ANALIZE II	960
SUHADOLC A.	NAVADNE DIFERENCIALNE ENAČBE	1200

ZBIRKA IZBRANIH POGlavJI IZ FIZIKE

GROS M.	SEMINAR FIZIKA IN MEDICINA	160
	NALOGE IZ FIZIKE	720
AHLIN F.	IZPITNA VPRAŠANJA IZ FIZIKE	480
AHLIN F.	FIZIKALNI PRAKTIKUM I.	640
PAHOR J.	ELEKTRONSKI PRAKTIKUM ZA FIZIKE	480
GOLLI B.	KVARKOVSKI MODEL HADRONOV	480
STRNAD J.	NA POT K SCHWARZSCHILDU	360
LIKAR A.	OSNOVE FIZIKALNIH MERJENJ IN MERIL. SIST.	1200
LIKAR A.	NALOGE IZ FIZ. MERJENJ IN MERIL. SISTEMOV	1200
STRNAD J.	IZPITNA VPRAŠANJA IZ FIZIKE II	160
STRNAD J.	HOMOGENO GRAVITACIJSKO POLJE	480
ROSINA M.	VIŠJA KVANTNA MEHANIKA	1200

FIZIKA - MATEMATIKA

STRNAD J.	FIZIKA - 1.DEL	2400
STRNAD J.	FIZIKA - 2.DEL	2160
STRNAD J.	FIZIKA - 3.DEL	2400
STRNAD J.	FIZIKA - 4.DEL	2160
KUŠČER I.	TOPLOTA	1200
PAHOR S.	UVOD V ANALITIČNO MEHANIKO	960
KUŠČER-KODRE	MATEMATIKA V FIZIKI IN TEHNIKI	2400

MATEMATIKA - FIZIKA

JAMNIK R.	VERJETNOSTNI RAČUN	
VIDAV I.	ALGEBRA	
VIDAV I.	VIŠJA MATEMATIKA I.	
BOHTE Z.	NUMERIČNE METODE	
PRIJATELJ N.	UVOD V MATEMATIČNO ANALIZO - 1. del	
VIDAV I.	AFINA IN PROJEKTIVNA GEOMETRIJA	
JAMNIK R.	MATEMATIKA	
GRASSELLI J.	ALGEBRAIČNA ŠTEVILA	
SUHADOLC A.	INTEGRALSKE TRANSFORMACIJE	
	INTEGRALSKE ENAČBE	
KRIŽANIČ F.	NAVADNE IN PARCIALNE DIFERENCIALNE ENAČBE	
VIDAV I.	VARIACIJSKI RAČUN	
GRASSELLI J.	LINEARNA ALGEBRA	
VADNAL A.	LINEARNO PROGRAMIRANJE	
JAMNIK R.	TRIG. VRSTE, STIELTJESOV INTEGRAL,	
	LEBESGUOV INTEGRAL	
KRUŠIČ B.	DVOJNI IN MNOGOTERNI INTEGRAL	
VIDAV I.	DIFERENCIALNA GEOMETRIJA V PROSTORU	
VENCELJ M.	VEKTORSKA ANALIZA	
JAMNIK R.	VERJETNOSTNI RAČUN IN STATISTIKA	
VRABEC J.	METRIČNI PROSTORI	
VIDAV I.	ELIPTIČNE KRIVULJE IN ELIPTIČNE FUNKCIJE	
PRIJATELJ N.	OSNOVE MATEMATIČNE LOGIKE - 2. DEL	
BOHTE Z.	NUMERIČNO REŠEVANJE NELINEARNIH ENAČB	
PRIJATELJ N.	OSNOVE MATEMATIČNE LOGIKE - 3. DEL	
BOHTE Z.	NUMERIČNO REŠEVANJE SISTEMOV LIN. ENAČB	

PODIPLOMSKI SEMINAR IZ MATEMATIKE (IMFM)

BOHTE Z.	SEMINAR ZA NUMERIČNO IN RAČUNALNIŠKO MAT.	
REPOVŠ D.	SEMINAR ZA RAČUNALNIŠKO MATEMATIKO 600	
	5 CONFERENCE ON APPLIED MATHEMATICS	
	PROCEEDINGS OF THE GRAD. WORK. IN MATH...	
	ZBORNIK REF. "DELAVNICE O VAR. (EL.) POD."	
VIDAV I.	BANACHOVE ALGEBRE	
VIDAV I.	UVOD V TEORIJU C* - ALGEBER	
VRABEC J.	BORDISM, HOMOLOGY, AND STIEFEL-WHIT. NUM.	
SUHADOLC A.	NEKOREKTNI PROBLEMI	
SUHADOLC A.	LINEARNI TOPOLOŠKI PROSTORI - 2.DEL	
VIDAV I.	DIFERENCIALNA GEOMETRIJA	
MAGAJUNA B.	VLOŽITVE MATRIČNIH ALGEBER	
RAZPET M.	UMBRALNI RAČUN	
LAVRIČ B.	DELNO UREJENE GRUPE IN DEL. UR. KOLOBARJI	
LAVRIČ B.	DELNO UREJENI VEKTORSKI PROSTORI	
PAVEŠIČ P.	THE HOPF INVARIANT ONE PROBLEM	
	VEGA. VERSION 0.2 (knjiga + disketa)	

MATEMATIČNI ROKOPISI

BATAGELJ V.	UVOD V RAČUNALNIŠTVO-NALOGE	
OMLADIČ M.	KONČNORAZSEŽNI VEKTORSKI PROSTORI	
KLAVŽAR S.	IZBR. POG. IZ RAČ.-2.DEL, DISKRETNA OPTIMI.	

Gotovo ima rang manjši od k in

$$\|(A - A_{k-1})x\|^2 = \sum_{j=k}^n \mu_j(A)^2 |\langle x, e_j \rangle|^2 \leq \mu_k(A)^2 \sum_{j=1}^n |\langle x, e_j \rangle|^2 = \mu_k(A)^2 \|x\|^2.$$

Potem pa je $a_k(A) \leq \|A - A_{k-1}\| \leq \mu_k(A)$. Ostane še primer $k = 1$. Iz definicije aproksimativnih števil sledi, da je $a_1(A) = \|A\|$. Iz $|A|x = \sum_{j=1}^n \mu_j(A) \langle x, e_j \rangle e_j$ pa sledi

$$\||A|x\|^2 = \sum_{j=1}^n \mu_j(A)^2 |\langle x, e_j \rangle|^2 \leq \mu_1(A)^2 \sum_{j=1}^n |\langle x, e_j \rangle|^2 = \mu_1(A)^2 \|x\|^2.$$

Torej je $\||A|\| \leq \mu_1(A)$. Po drugi strani pa je $|A|e_1 = \mu_1(A)e_1$, iz česar lahko zaključimo, da je $\mu_1(A) = \||A|\|$. Iz enačbe (1) v dokazu prejšnje trditve pa sledi, da je $\||A|\| = \|A\|$, in enakost za primer $k = 1$ je dokazana.

Za primer $k \geq 2$ dokažimo še obratno neenakost. Vzemimo neničelna vektorja – stolpca u in v iz $\mathbb{C}^n$. Tedaj je uv^* matrika reda $n \times n$ ranga 1, ki vektor x preslika v $\langle x, v \rangle u$. Vzemimo poljubno matriko B in naj bo $\text{rang}(B) < k$. Potem lahko zapišemo

$$B = \sum_{j=1}^m u_j v_j^*, \quad m < k,$$

kjer so u_j in v_j vektorji iz $\mathbb{C}^n$. Homogeni sistem enačb

$$\sum_{i=1}^k \langle e_i, v_j \rangle \alpha_i = 0, \quad j = 1, \dots, m$$

ima netrivialno rešitev $(\alpha_i)_{i=1}^k$, saj je število enačb manjše od števila neznank. Nadalje lahko privzamemo, da je $\sum_{i=1}^k |\alpha_i|^2 = 1$. Definirajmo vektor

$$x_0 = \sum_{i=1}^k \alpha_i e_i.$$

Potem je $\|x_0\| = 1$ in

$$Bx_0 = \sum_{j=1}^m \langle x_0, v_j \rangle u_j = \sum_{j=1}^m \left(\sum_{i=1}^k \alpha_i \langle e_i, v_j \rangle \right) u_j = 0.$$

Iz enačbe (2) sledi

$$Ax_0 = \sum_{j=1}^n \mu_j(A) \langle x_0, e_j \rangle U e_j = \sum_{j=1}^k \mu_j(A) \alpha_j U e_j.$$

Torej je

$$\|A - B\| \geq \|(A - B)x_0\| = \|Ax_0\| = \left(\sum_{j=1}^k \mu_j(A)^2 |\alpha_j|^2\right)^{\frac{1}{2}} \geq \mu_k(A)$$

in seveda je tudi $a_k(A) \geq \mu_k(A)$. ■

Aproksimativna števila nam povedo, kako dobro lahko dano matriko A aproksimiramo v operatorski normi z matrikami predpisanega ranga. Če damo omejitev $\text{rang}(B) < k$, potem po prejšnjem izreku vemo, da je

$$\|A - B\| \geq \mu_k(A).$$

Denimo, da poznamo spektra matrik A in B . Potem v splošnem ne moremo nič povedati o spektru produkta AB in spektru vsote $A + B$. Tudi singularna števila so definirana s spektrom. Toda ker so enaka aproksimativnim številom, velja:

Izrek 5. *Za aproksimativna (singularna) števila veljajo naslednje lastnosti:*

- (1) $a_j(A) = a_j(A^*)$
- (2) $a_j(BAC) \leq \|B\|a_j(A)\|C\|$
- (3) $a_{j+i-1}(A + B) \leq a_j(A) + a_i(B)$
- (4) $a_{j+i-1}(AB) \leq a_j(A)a_i(B)$
- (5) $|a_j(A) - a_j(B)| \leq \|A - B\|$

Dokaz. Ker je $\text{rang}(X) = \text{rang}(X^*)$ in $\|A - X\| = \|A^* - X^*\|$, sledi točka (1). Točko (2) dobimo iz

$$\begin{aligned} \inf\{\|BAC - X\|; \text{rang}(X) < j\} &\leq \\ &\leq \inf\{\|BAC - BYC\|; \text{rang}(Y) < j\} \leq \|B\|a_j(A)\|C\|. \end{aligned}$$

Lotimo se dokazovanju točke (3). Vzemimo poljuben $\varepsilon > 0$ in poiščimo operatorja X in Y z $\|A - X\| < a_j(A) + \varepsilon$, $\text{rang}(X) < j$ in $\|B - Y\| < a_i(B) + \varepsilon$, $\text{rang}(Y) < i$. Potem je $\text{rang}(X + Y) < j + i - 1$ in

$$\|A + B - (X + Y)\| \leq \|A - X\| + \|B - Y\| < a_j(A) + a_i(B) + 2\varepsilon.$$

Ker je lahko ε poljubno majhen, je $a_{j+i-1}(A + B) \leq a_j(A) + a_i(B)$.

Točko (4) dokažemo podobno. Spet vzamemo poljuben $\varepsilon > 0$ in poiščemo operator Y , da velja $\|B - Y\| < (1 + \varepsilon)a_i(B)$, $\text{rang}(Y) < i$, ter operator X z $\|AB - AY - X\| < (1 + \varepsilon)a_j(AB - AY)$, $\text{rang}(X) < j$. Potem je $\text{rang}(AY + X) < j + i - 1$ in

$$\begin{aligned} \|AB - AY - X\| &< (1 + \varepsilon)a_j(AB - AY) \leq \\ &\leq (1 + \varepsilon)a_j(A)\|B - Y\| < (1 + \varepsilon)^2 a_j(A)a_i(B). \end{aligned}$$

Tako dobimo $a_{j+i-1}(AB) \leq a_j(A)a_i(B)$.

Točka (5) sledi z uporabo točke (3) iz

$$a_j(A) = a_{1+j-1}(A - B + B) \leq a_1(A - B) + a_j(B) = \|A - B\| + a_j(B). \quad \blacksquare$$

Opomnimo, da v drugi točki izreka matriki B in C nista nujno kvadratni. Le produkt BAC naj bo kvadratna matrika. Poglejmo si zgled.

Zgled. Vzemimo matriko A iz M_n . Nadalje naj bo e_i vektor-stolpec iz $\mathbb{C}^n$, ki ima na i -tem mestu 1, povsod drugod pa ničle. Z $e_i^\top$ pa označimo vrstico te oblike. Naj bo

$$B = \begin{bmatrix} e_1^\top \\ \vdots \\ e_k^\top \end{bmatrix} \quad \text{in} \quad C = [e_1 \dots e_k].$$

Potem je matrika BAC enaka levi zgornji $k \times k$ podmatriki matrike A . Po drugi točki prejšnjega izreka je $a_j(BAC) \leq \|B\|a_j(A)\|C\| = a_j(A)$ za $1 \leq j \leq k$. S primerno izbiro matrik B in C lahko dobimo katerokoli $k \times k$ podmatriko in vse imajo istoležna singularna števila manjša od istoležnih singularnih števil matrike A .

Sedaj vzemimo $n \times n$ matriko A in njene lastne vrednosti označimo z $\lambda_j(A)$. Uredimo jih po velikosti njihovih absolutnih vrednosti $|\lambda_1(A)| \geq \dots \geq |\lambda_n(A)|$ in upoštevajmo tudi algebraično kratnost. Tedaj velja:

Izrek 6. *Naj bo A iz M_n . Potem za vsak $1 \leq k \leq n$ velja*

$$\prod_{j=1}^k |\lambda_j(A)| \leq \prod_{j=1}^k \mu_j(A).$$

Dokaz. Pri izbiri baze v prostoru $\mathbb{C}^n$ imamo proste roke. Zato lahko predpostavimo, da je matrika A že v Jordanovi formi in da so lastne vrednosti po diagonali urejene po velikosti absolutnih vrednosti. Izberimo k med 1 in n in vzemimo matriki B in C kot v prejšnjem zgledu. Iz polarne dekompozicije $BAC = U|BAC|$ sledi $|\det(BAC)| = |\det(U)| \det(|BAC|) = \det(|BAC|)$. Upoštevajmo, da je determinanta enaka produktu lastnih vrednosti, pa dobimo

$$\begin{aligned} \prod_{j=1}^k |\lambda_j(A)| &= |\det(BAC)| = \det(|BAC|) = \prod_{j=1}^k \lambda_j(|BAC|) = \\ &= \prod_{j=1}^k \mu_j(BAC) \leq \prod_{j=1}^k \mu_j(A). \end{aligned} \quad \blacksquare$$

Vzemimo sedaj n -terico realnih števil $a = (a_1, \dots, a_n)$. Postavimo

$$a_1^+ = \max |a_i|, \quad a_2^+ = \max_{i \neq j} (|a_i| + |a_j|) - a_1^+$$

$$a_3^+ = \max_{i \neq j, j \neq k, k \neq i} (|a_i| + |a_j| + |a_k|) - a_1^+ - a_2^+ \dots \quad \text{in } a^+ = (a_1^+, \dots, a_n^+).$$

Torej smo s tem števila $|a_i|$ uredili po velikosti od največjega k najmanjšemu.

Trditev 7. Naj bosta a in b n -terici realnih števil, za kateri velja $a_1 \geq \dots \geq a_n \geq 0$, $b_1 \geq \dots \geq b_n \geq 0$ in $\sum_{j=1}^k b_j \leq \sum_{j=1}^k a_j$ za vse $1 \leq k \leq n$. Potem obstajajo take n -terice $a^{(1)}, \dots, a^{(m)}$, da velja $(a^{(s)})^+ = a$, $1 \leq s \leq m$ in

$$b = \sum_{s=1}^m \lambda_s a^{(s)}, \quad 0 \leq \lambda_s \leq 1, \quad \sum_{s=1}^m \lambda_s = 1.$$

Dokaz. Naj bo $K \subset \mathbb{R}^n$ konveksna ogrinjača vseh takih n -teric c , za katere je $c^+ = a$. Torej je K množica končnih vsot oblike $\sum \lambda_s c^{(s)}$, $0 \leq \lambda_s \leq 1$, $(c^{(s)})^+ = a$, in $\sum \lambda_s = 1$. Radi bi pokazali, da točka b leži v množici K . Če b ne leži v K , potem obstaja hiperravnina $M = \{x \in \mathbb{R}^n; f(x) = \alpha\}$, f linearen funkcional, ki separira K in b . Torej je $f(c) < \alpha$ za vsak $c \in K$ in $f(b) > \alpha$ [2, stran 329]. Linearen funkcional f lahko zapišemo v obliki $f(x) = \sum_{j=1}^n u_j x_j$. Naj bo $\beta = \max_{c \in K} f(c)$. Označimo $f^+(x) = \sum_{j=1}^n u_j^+ x_j$. Potem je

$$\begin{aligned} |f(b)| &= \left| \sum_{j=1}^n u_j b_j \right| \leq \sum_{j=1}^n |u_j| b_j = \\ &= b_n \sum_{j=1}^n |u_j| + (b_{n-1} - b_n) \sum_{j=1}^{n-1} |u_j| + \dots + (b_1 - b_2) |u_1| \leq \\ &\leq b_n \sum_{j=1}^n u_j^+ + (b_{n-1} - b_n) \sum_{j=1}^{n-1} u_j^+ + \dots + (b_1 - b_2) u_1^+ = f^+(b). \end{aligned}$$

Nadalje je

$$f^+(b) = \sum_{j=1}^n u_j^+ b_j = u_n^+ \sum_{j=1}^n b_j + (u_{n-1}^+ - u_n^+) \sum_{j=1}^{n-1} b_j + \dots + (u_1^+ - u_2^+) b_1 \leq f^+(a),$$

zaradi predpostavke $\sum_{j=1}^k b_j \leq \sum_{j=1}^k a_j$. Toda v množici K gotovo obstaja tak c , da velja $f(c) = f^+(a)$. Potem pa je $f(b) \leq f^+(b) \leq f^+(a) = f(c) \leq \beta < \alpha$. Prišli smo do protislovja. Torej točka b res leži v množici K . ■

Posledica 8. Naj bo $a_1 \geq \dots \geq a_n \geq 0$, $b_1 \geq \dots \geq b_n \geq 0$ in $\prod_{j=1}^k b_j \leq \prod_{j=1}^k a_j$ za vsak $1 \leq k \leq n$. Potem je za vsak $p > 0$ in vsak $1 \leq k \leq n$

$$\sum_{j=1}^k b_j^p \leq \sum_{j=1}^k a_j^p.$$

Dokaz. Brez izgube za splošnost lahko predpostavimo, da so vsi a_j in b_j različni od 0. Toda potem lahko za dovolj velik M dosežemo, da so vsi Ma_j in Mb_j večji od 1. Namesto a_j in b_j povsod pišemo Ma_j in Mb_j in nič se ne spremeni. Torej lahko predpostavimo, da so a_j in b_j večji od 1. Tedaj n -terici $(\ln(a_1), \dots, \ln(a_n))$ in $(\ln(b_1), \dots, \ln(b_n))$ ustrezata pogojem prejšnje trditve. Torej lahko najdemo n -terice $a^{(s)} = (a_1^{(s)}, \dots, a_n^{(s)})$, $(a^{(s)})^+ = (\ln(a_1), \dots, \ln(a_n))$, $1 \leq s \leq m$, da za vsak $1 \leq j \leq n$ velja

$$\ln(b_j) = \sum_{s=1}^m \lambda_s a_j^{(s)}, \quad 0 \leq \lambda_s \leq 1 \quad \text{in} \quad \sum_{s=1}^m \lambda_s = 1.$$

Potem je

$$\begin{aligned} \sum_{j=1}^k b_j^p &= \sum_{j=1}^k e^{p \ln(b_j)} = \sum_{j=1}^k e^{p(\sum_{s=1}^m \lambda_s a_j^{(s)})} \leq \sum_{j=1}^k \sum_{s=1}^m \lambda_s e^{p a_j^{(s)}} = \\ &= \sum_{s=1}^m \lambda_s \sum_{j=1}^k e^{p a_j^{(s)}} \leq \sum_{s=1}^m \lambda_s \sum_{j=1}^k e^{p \ln(a_j)} = \sum_{j=1}^k e^{p \ln(a_j)} = \\ &= \sum_{j=1}^k a_j^p, \end{aligned}$$

kjer smo pri računanju upoštevali konveksnost in naraščanje funkcije $x \rightarrow e^{px}$. ■

Posledica 9. Za matriko A iz M_n , $p > 0$, $1 \leq k \leq n$, velja

$$\sum_{j=1}^k |\lambda_j(A)|^p \leq \sum_{j=1}^k \mu_j(A)^p.$$

Posebej pogledimo primer $p = 2$ in izračunajmo vrednost izraza $\sum_{j=1}^n \mu_j(A)^2$. Naj bo $A = (a_{ij})$ iz M_n matrika, ki pripada operatorju A glede na neko ortonormirano bazo $e_1, \dots, e_n$ prostora $\mathbb{C}^n$. Vsoti vseh diagonalnih elementov matrike A pravimo sled in jo označimo s $sl(A)$. Torej $sl(A) = \sum_{j=1}^n \langle Ae_j, e_j \rangle$. Iz znane formule $sl(AB) = sl(BA)$ in Jordanove forme $J = S^{-1}AS$, sledi

$$sl(A) = sl(SS^{-1}A) = sl(S^{-1}AS) = sl(J) = \sum_{j=1}^n \lambda_j(A).$$

Števila $\mu_j(A)^2$ so lastne vrednosti matrike A^*A . Torej je

$$\begin{aligned}\sum_{j=1}^n \mu_j(A)^2 &= \text{sl}(A^*A) = \sum_{j=1}^n \langle A^*Ae_j, e_j \rangle = \sum_{j=1}^n \|Ae_j\|^2 = \\ &= \sum_{j=1}^n \sum_{i=1}^n |\langle Ae_j, e_i \rangle|^2 = \sum_{i,j=1}^n |a_{ij}|^2.\end{aligned}$$

Zgornji račun nam pove še nekaj. Ker je izraz $\sum_{j=1}^n \mu_j(A)^2$ neodvisen od izbire baze, je tudi izraz $\sum_{i,j=1}^n |\langle Ae_j, e_i \rangle|^2$ neodvisen od izbire ortonormirane baze $e_1, \dots, e_n$ prostora $\mathbb{C}^n$. Po prejšnji posledici pa dobimo neenakost

$$\sum_{j=1}^n |\lambda_j(A)|^2 \leq \sum_{i,j=1}^n |a_{ij}|^2.$$

Na koncu še povejmo, da lahko singularna števila na enak način definiramo za kompaktne operatorje na separabilnem Hilbertovem prostoru. Vse neenakosti iz tega članka veljajo tudi v tem splošnejšem primeru in so dokazane v knjigi [1]. Aproksimativna števila pa lahko definiramo tudi za operatorje na Banachovih prostorih in izrek 5 velja tudi v tem primeru.

LITERATURA

- [1] H. König, *Eigenvalue distribution of compact operators*, Operator theory: Advances and applications, Vol. 16.
- [2] S. Kurepa, *Funkcionalna analiza*, Školska knjiga, Zagreb 1981.

NOVE KNJIGE

DIRAC P. A. M., General Theory of Relativity, Princeton University Press, Princeton, NJ. 1996, Princeton Landmarks in Mathematics and Physics, 72 str.

Princetonska univerzitetna založba je ponovno ponatisnila knjižico o splošni teoriji relativnosti. Prvič je izšla pred dvajsetimi leti po predavanjih P. A. M. Diraca za zadnje letnike dodiplomskega študija na univerzi zvezne države Floride. Kot v kvantni mehaniki, v kateri je dosegel svoje glavne uspehe, si je tudi tu prizadeval, da bi podal enačbe v kolikor mogoče pregledni in zgoščeni obliki. Knjiga vsebuje vse, kar potrebuje fizik za začetek, tako da mu ni treba iskati pomoči v drugih knjigah. Imeti mora le osnovno znanje iz posebne teorije relativnosti in biti pripravljen, da se spoprime z matematiko ukrivljenega četvernega prostora. V razmeroma drobnih knjigi ni odveč nobena beseda ali enačba. Nobeno od 35 poglavij ni daljše od treh strani, veliko pa jih je še krajših. Broširana knjiga bo prišla prav vsem matematikom in fizikom, ki se bodo želeli po čim krajši poti poučiti o splošni teoriji relativnosti.

Janez Strnad

STIČIŠČA IN RAZHAJANJA V POUČEVANJU OSNOVNOŠOLSKE IN SREDNJEŠOLSKE MATEMATIKE¹

MILENA STRNAD

Math. Subj. Class. 00A35

Primerjava poučevanja matematike na osnovni in srednji stopnji lahko razkrije nekaj mogočih vzrokov za to, da je matematika resen problem za marsikaterega učenca. Prispevek razpravlja o bolj ali manj znanih vprašanjih v poučevanju matematike ob predvideni prenovi šolskega sistema. Postavlja tudi številna vprašanja, na katera bi bilo dobro odgovoriti, če hočemo ta pouk izboljšati. Tisti, ki bodo sodelovali pri prenavljanju, naj bi upoštevali izkušnje in pomisleke učiteljev, da bo matematika v šoli postala prijaznejša.

POINTS OF CONNECTION AND SEPARATION IN TEACHING PRIMARY AND SECONDARY SCHOOL MATHEMATICS

Comparison of the teaching of mathematics at primary and secondary level may disclose some possible grounds why mathematics represents a serious problem for many a pupil. In the contribution more or less known questions are discussed with respect to the anticipated reform of the educational system. Questions appear that should be answered if the teaching should be improved. Those who will take part in reforming should consider the experience and hesitation of teachers in order that mathematics in school will get more friendly.

Uvod

Poučevanje matematike na osnovni in srednji stopnji je zahtevno delo. Različni prijemi, ki jih včasih radi uporabljamo pri poučevanju, na primer podajanje snovi v obliki zgodbic, popestritvi predavanj z zgodovinskim ozadjem in podobno, lahko v začetku prispevajo k prijetnejšemu ozračju. A navsezadnje je matematika predmet, ki vedno zahteva od učenca trdo delo. Učenec je tisti, ki mora na koncu marsikaj razumeti in se marsičesa tudi naučiti. Ni kraljevske poti v matematiko.

Dobro se je tudi že od vsega začetka zavedati, da poučevanje matematike ni znanost. Prej spominja na umetnost, s katero ustaljeno, znano posredujemo mlajšim rodovom. Poučevanje je proces, ki celo znotraj enega šolskega sistema ni enoličen. Kot tak presega stroga navodila o tem, kako učiti. Še več, poučevanje ni niti linearno – kolikor vložiš, toliko dobiš – temveč navadno poteka nezvezno in nosi v sebi tudi zametke kaotičnosti, saj se neprestano spreminja in uspešnost poučevanja ni napovedljiva. Celo podajanje iste snovi pri istem učitelju poteka vedno malo drugače in končno privede do različnih rezultatov.

Pogoj za dobro poučevanje matematike je predvsem učiteljevo široko in na nekaterih mestih tudi globoko poznavanje stroke. To mu omogoča iskanje novih metodičnih prijemov pri obravnavi posameznega dela snovi.

¹ Po predavanju na sprotnem izobraževanju srednješolskih učiteljev matematike

H kvaliteti poučevanja v veliki meri prispevajo osebnostne značilnosti učitelja in zato golo posnemanje učnih metod ni priporočljivo. To ne pomeni, da ni koristno poznati različnih metod dela, o njih razmišljati in iskati novih rešitev. Veliko prispeva tudi učiteljeva predanost stroki.

V javnosti preveč odmevajo predvsem očitki o nizki ravni znanja naše osnovnošolske in srednješolske matematike. Ob tem se premalo pove, s kakšnim merilom, kako, kdo in zakaj je to meril.

Nedvomno pa drži, da je matematika velik problem, če že ne travma za marsikaterega učenca.

Do tega spoznanja so me privedle izkušnje pri delu z učbeniki matematike od razredne do univerzitetne stopnje in z njimi povezana srečanja s številnimi domačimi in tujimi pisci, recenzenti, tujimi založniki ter domačimi in tujimi univerzitetnimi učitelji, pogovori z nekaj sto osnovnošolskimi učitelji na številnih seminarjih ter prirejanje in pisanje osnovnošolskih gradiv in učbenikov.

Takoj se porodita vprašanji: Zakaj je tako? Kako je to mogoče? Poskusimo odgovoriti takole:

Matematika je poleg materinščine osrednji šolski predmet, ki spremlja učenca skozi vse njegovo šolanje od prvega dne, ko vstopi v malo šolo. Zaradi možnega kvantitativnega načina merjenja pridobljenega znanja učencev matematika veliko bolj kot drugi predmeti vpliva na *rangiranje* učencev. Pri tem se prezre, da učenčev uspeh pri matematiki ni samo kazalec njegovih zmožnosti in bistrosti, ampak poleg njegove pridnosti in prizadevnosti vpliva nanj še veliko drugih dejavnikov.

Četudi rangiranje učencev prek matematike ni pravično, obstaja. Tako matematika opredeli učenca že na razredni stopnji. Še bolj ga zaznamuje na predmetni stopnji. V tem času tudi v učencu dozori njegovo lastno spoznanje, ali je sposoben za matematiko ali ne. Ker na to odločitev vpliva veliko zunanjih dejavnikov – od uspeha v šoli do učenčevega osebnega odnosa do učitelja matematike in tudi njegovo domače okolje – je ta odločitev lahko usodna. Ob tem učenca čaka še zaključno preverjanje znanja, ki bistveno vpliva na njegovo nadaljnjo poklicno pot in posredno tudi na njegov odnos do matematike.

Končno učenec s svojo predstavo o uspehu in prikritimi dvomi in strahovi o lastnem neuspehu vstopi v srednjo šolo. Velikokrat se prav zaradi matematike ne more vpisati na izbrano smer. Njegova odločitev je pogosto povezana tudi s predvidenim obsegom matematike, ki ga čaka v naslednjih štirih letih, kar spet lahko izzove nove bojazni, morda celo odpor do matematike.

Tudi v srednji šoli se pojavi kot osrednji predmet matematika, za nekatere še večji strah in trepet, za manj številne izziv in veselje. Po nekaj tednih pride učenec pogosto še do spoznanja, da je srednješolska matematika

čisto drugačna od tiste, s katero se je ubadal pretekla štiri leta. Učitelj pri obravnavi iste snovi uporablja drugačna imena. Več in drugače razlaga. V eni uri obravnava bistveno več snovi. Pri razlagi se sklicuje na nekatere pojme. Nič več ni navdušen samo nad lepimi risbicami ali dobro mehansko rešenimi nalogami. Od učenca pričakuje razumevanje snovi. Samoumevno se mu zdi, da bo učenec segal tudi po učbeniku in ne bo uporabljal samo zbirke vaj.

Toda učbenik je pisan drugače, zbirke nalog so manj slikovite, manj povedo vnaprej. V pisnih preverjanjih znanj se pogosto znajdejo zahtevne naloge. Učitelj sprašuje ustno, tudi teorijo. Kmalu začne opozarjati še na maturo ali zaključni izpit.

Učenec razume, da do določenih sprememb pride zato, ker je zdaj srednješolec, in se začuda hitro prilagodi. Težje pa dojame, zakaj obstajajo številna terminološka razhajanja in zakaj se je moral na nižji stopnji ubadati z marsikatero zahtevno snovjo, o kateri si je morda prav zato ustvaril napačno predstavo. Recimo: zakaj je moral število 0,56 dosledno imenovati *desetiški ulomek*, *zapisan z decimalno številko*? Zakaj mu je učitelj postregel s teorijo množic takoj na začetku petega razreda? Zakaj ga je učitelj mučil s premim in obratnim sorazmerjem tako, da mu ga je razlagal funkcijsko in pri tem zamolčal pojem funkcije ter prezrl sklepni račun? Zakaj je spregovoril o razmerju za sorazmerjem? Zakaj mu ni olajšal dela vsaj pri reševanju enačb? Zakaj je dal tolikšen poudarek stereometriji? Zakaj mu ni dovolil uporabljati žepnega računalnika niti pri računanju zapletenih računov, iskanju korenov? Zakaj je na koncu šolskega leta samo načel zanimive nove teme in jih v naslednjem šolskem letu kar poskušal nadaljevati, ko so bile vmes počitnice?

Učenec namreč ne ve in tudi ne more razumeti, da sta se morala njegov osnovnošolski in srednješolski učitelj ravnati po učnem načrtu, da morda nista imela na voljo več potrjenih učbenikov in da sta se morala držati obstoječe terminologije. Učenec ne ve, da pri tem učitelja nista nič kriva, da na teh področjih niso vse stvari urejene. Svoje težave pri matematiki hitro pripiše kar matematiki in morda celo učiteljevi nesposobnosti.

Da pa se da obstoječe stanje že z majhnimi premiki znotraj predpisane osnovnošolske snovi popraviti, je pokazalo delo skupine, ki ji je ob podpori nekaterih svetovalcev za matematiko uspelo v novih učbenikih *Presečišča* realizirati nekaj namigov številnih učiteljev. Tako je v njih iz petega razreda izločena algebra. Iz začetka petega razreda je izločena teorija množic, ki je ponujena v snopiču z napotki, v kolikšni meri in kako naj se obravnava skozi vsa leta. Osnove logike so vpeljane zgolj na implicitni ravni. Funkcijski postopek pri obravnavi premega in obratnega sorazmerja je nadomeščen s sklepnim računom. Eksplicitna vpeljava neodvisne in odvisne spremenljivke se pojavi šele na koncu sedmega razreda, ko kvadratno mrežo nadomesti

kartezični koordinatni sistem. Ob tem se je pokazalo, da bi se še z manjšimi premiki snovi znotraj učnega načrta in njegovo delno krčitevijo lahko naredilo matematiko dostopnejšo marsikateremu učencu.

Prvi korak k prijaznejši matematiki skozi vse šolanje je že v tem, da se čimbolj celovito seznanimo z obstoječim stanjem pri poučevanju matematike. Pri tem si lahko pomagamo z ugotovitvami srednješolskih učiteljev o znanju matematike, ki ga prinesejo v srednjo šolo učenci, in jih najdemo v knjižici Zavoda za šolstvo [2].

Poskusimo v ta namen analizirati bolj ali manj znana stičišča in razhajanja med osnovnošolsko in srednješolsko matematiko. Predstavljen vrstni red, še manj pa obseg predstavitve, ne pomenita njihove prioritete.

Stičišča

1. Pomanjkanje ustrezno izobraženih učiteljev.
2. Neustrezno vrednotenje učiteljevega dela.
3. Preveč zagreti in preveč boječi učitelji.
4. Opredeljenost z učnim načrtom.
5. Prevelika zaverovanost matematikov v stroko.
6. Tuji vplivi.

Pomanjkanje ustrezno izobraženih učiteljev.

Poučevanje matematike naj bi bilo prilagojeno učenčevi dojemljivosti pri določeni starosti. Zato naj bi se razlikovalo ne le po snovi, temveč tudi po oblikah in načinih sporočanja. Skladno s tem tudi obstajajo tri različne smeri študija za poučevanje na razredni, predmetni in srednji stopnji. Njihovi programi so naravnani tako, da učitelje usposabljaajo glede vsebine in načinov poučevanja za izbrano stopnjo.

V našem šolstvu že nekaj časa lahko opazujemo, da osnovnošolski učitelji prosto prehajajo na srednjo šolo. Tako ravnanje utegne biti za matematiko na daljši rok usodno. Nevarnost ni le v pomanjkljivi strokovni usposobljenosti, temveč predvsem v tem, da se s to selitvijo ustvarja praznina pri poučevanju osnovnošolske matematike. Prav njo pa bi morali poučevati zares dobri in dobro metodično usposobljeni učitelji.

Vprašanje: Zakaj so taki avtomatični prehodi sploh mogoči?

Neustrezno vrednotenje učiteljevega dela.

Del odgovora na zgornje vprašanje lahko poiščemo v splošno razširjenem javnem mnenju o potrebnih kvalitetah učitelja matematike:

Matematiko v osnovni šoli zna poučevati skoraj vsak, ki je končal srednjo šolo, da o končanem letniku kakšne visoke tehniške šole ali absolventu katerekoli tehniške višje ali visoke šole ne govorimo.

Matematiko v srednji šoli, zlasti po tehniških šolah, in še bolj po tri-letnih in dvoletnih šolah, zna poučevati že vsakdo, ki je opravil maturo, kaj šele inženir končanega dveletnega tehniškega študija, da o diplomiranem inženirju tehniških smeri in diplomantu ustrezne dvopredmetne smeri pedagoške fakultete ne govorimo.

Vse to priča o nepoznavanju stroke, predvsem pa zapostavljanju in nepoznavanju različnih metodično-didaktičnih postopkov, ki so značilni za posamezno stopnjo poučevanja.

Kaj lahko naredimo proti takemu mnenju matematiki sami? Zagotovo matematiki navzven premalo poudarjamo, da se od učitelja matematike bolj kot od učiteljev drugih predmetov pričakuje zlasti na razredni in predmetni stopnji, da obvlada poleg ustreznega obsega matematike tudi veliko dodatnih znanj. Poučevanje matematike namreč zaradi njenih specifičnih lastnosti vodi do številnih učnih ciljev znotraj in zunaj matematike. Zato je način poučevanja matematike treba izbrati še posebej odgovorno, saj pedagoška neozaveščenost lahko celo usodno zaznamuje učenčevo nadaljnjo pot. Preveč govorimo samo o neprimerno ovrednotenem delu učitelja na sploh. Z opozarjanjem na posledico verjetno ne bo odpravljen vzrok.

Vprašanje: Ali je za učitelja zares sposoben vsak, ne glede na to, kolikšni so bili njegovi poprejšnji šolski uspehi, sposobnost izražanja, prilagodljivost...? Ali ne bi bila potrebna selekcija že na začetku izobraževanja? Zanimivo je ob tem pomisliti na pogoje, ki jih neusmiljeno postavljajo druge smeri študija, na primer medicina, arhitektura, gradbeništvo..., šport, da o umetniških akademijah ne govorimo. Kaj storiti, da ravnatelji sploh ne bi mogli zaposlovati ljudi po opisanem javnem mnenju?

Preveč zagreti in preveč boječi učitelji.

Učitelji smo skoraj brez izjem in ne glede na stopnjo, posebno v prvih letih poučevanja, preveč zahtevni do učencev. Zaradi navdušenja nad stroko bi najraje učencem posredovali preveč svojega znanja. Zaradi bojazni, da naši učenci ne bodo uspešni v nadaljnjem šolanju, predvsem pa na zunanjih preizkušnjah vseh vrst, od njih zahtevamo več in več. Posledica je še dodatno širjenje že tako preobsežnega učnega načrta.

V osnovni šoli so tako nekatere teme, namenjene izključno delu pri dodatnem pouku za najboljše učence, prišle v učbenike, torej v redni pouk. Teh tem se učitelji oklepajo, češ da ta znanja zahteva od njihovih učencev srednja šola. Ne da se jih izvreči.

Prav tako se na marsikateri srednji šoli učenci poglobljajo v razne teme in urijske spretnosti, čeprav naj bi v to snov učenci dobili samo prvi vpogled. Odgovor, zakaj je tako, je podoben kot v osnovni šoli. Številni srednješolski učitelji so prepričani, da menda višje in visoke šole pričakujejo obvladovanje teh spretnosti.

Po drugi strani pa smo učitelji tudi preveč boječi. Le redki si upajo vsaj delno zaiti s strogo predpisane poti učnega načrta, četudi jim to nakazujejo izkušnje in osebno strokovno prepričanje. Glede na to, da je učiteljevo delo že od nekdaj pod uradno kontrolo in v zadnjem času tudi širše javnosti, je tako vedenje povsem razumljivo.

Vprašanje: *Kaj lahko naredimo, da na učitelja ne bo delovalo toliko notranjih in zunanjih pritiskov?*

Opredeljenost z učnim načrtom.

(1) Učni načrt je najpomembnejši šolski dokument, ki obvladuje in usmerja poučevanje matematike.

Izrazito vpliva na delo piscev učbenikov.

Potrjeni učbeniki ne smejo odstopati od učnega načrta; možna je samo pre-razporeditev učne snovi znotraj letnika. Tudi za manjše vsebinske odstopke je bilo doslej potrebno pridobiti soglasje Zavoda za šolstvo.

Močno usmerja delo učitelja.

Učiteljevo delo v razredu omejujejo poleg učnega načrta še znani dodatni pogoji: upoštevati mora šolski koledar, se podrediti razpisanim datumom raznih matematičnih tekmovanj, ki so vezana na obseg predelane učne snovi. Zaradi uporabe matematike pri drugih predmetih mora učitelj upoštevati, kaj mora najprej naučiti. Primerneje za učenca je, da se učitelj pri razlagi drži razporeditve snovi v učbeniku.

Vpliva na delo sestavljavcev tekmovalnih nalog, preglednih eksternih testov, zaključnih izpitov in mature.

(2) V prvem približku celoten učni načrt obsega:

V osnovni šoli velik del snovi prvega letnika štiriletne srednje šole.

V srednji šoli v grobem vso snov prvega letnika manj zahtevne višje ali celo visoke tehniške šole. Pristop k snovi na vseh treh stopnjah naj bi bil matematično neoporečen, le izvajanje naj bi bilo prilagojeno različni razvojni stopnji učencev. Ta naj bi prešla vse faze, od opazovanja, risanja, primerjanja, posploševanja, sklepanja do dokazovanja.

(3) Za oba učna načrta velja:

Večina matematikov, ki ni neposredno vključena v izobraževalni proces izbranega učnega načrta, z njim ni zadovoljna.

Med uporabniki posameznega učnega načrta pa so mnenja o primernosti v njem zajete vsebine različna. Tako visokošolski učitelji menijo, da je predpisana vsebina za srednjo šolo preobsežna. Večina srednješolskih učiteljev meni, da ni tako. Ni malo učiteljev, ki bi še marsikaj dodali. To še ne pomeni, da so z učnim načrtom v celoti zadovoljni.

Podobno sliko dobimo, če pogledamo v osnovno šolo. Večina srednješolskih učiteljev meni, da je osnovnošolski učni načrt preobsežen. Osnovnošolski učitelji pa se s tem ne strinjajo. To spet ne pomeni, da so zadovoljni z učnim načrtom, kakršen je.

Vprašanja: *Kdo, kdaj in kako lahko vpliva na vsebino učnega načrta?*

Ali je mogoče vplivati na izbor ljudi, ki naj bi sodelovali v pripravah za sestavljanje učnega načrta?

Prevelika zaverovanost matematikov v stroko.

Matematiki imamo svojo stroko radi, veseli nas njena splošna uporabnost, hkrati pa nas ljubezen do stroke velikokrat tudi zavede. Marsikdaj nas to pripravi do tega, da ne vidimo ali pa nočemo videti, da ima matematika poleg dobrih vplivov lahko tudi slabe in celo pogubne posledice za učenca.

Za matematiko zahtevamo na vseh stopnjah in v vseh šolah nesporno prioriteto nasproti preostalim predmetom. Težko se damo prepričati, da so v predpisani snovi tudi teme, ki so za marsikaterega učenca na tej stopnji prezahtevne.

Matematiki se ne želimo odreči tudi v tistih skrajšanih programih, ki predvidevajo le malo ur. Ob načrtovanju le-teh se je verjetno pozabilo, da obseg predpisane snovi še zdaleč ni edino merilo za potrebno število ur, ki spremlja njihovo izvedbo.

Vprašanja: *Zakaj ni vpisovanje učencev v posamezne programe tako izpeljano, da učenec, ki je v določen program sprejet, tega tudi more ne pa mora narediti?*

Zakaj ni dopustna naravna selekcija učencev, temveč je učitelj vedno dolžan delati čudeže?

Tuji vplivi.

Z vse pogostejšim odhajanjem učiteljev na študij v tujino, s poznavanjem tuje literature, z vključevanjem posameznikov ali ustanov v razne mednarodne projekte postajajo tuji vplivi na način poučevanja matematike številni in raznolični. Za zdaj to še ne velja tudi za vsebino učnega načrta.

Poznavanje različnih možnih načinov poučevanja matematike je po eni strani dobro, ker lahko izboljša kvaliteto poučevanja. Po drugi strani pa je lahko tudi nevarno, saj se rado zgodi, da spremljajoče navdušenje posameznika ali skupine oslabi kritičnost in povzroči prehitro in ne dovolj globoko premišljeno presajanje tujih idej na domača tla. Pojavi se še nevarnost mešanja raznih zamisli. Iz različnih dežel prihajajo različni dobri metodični postopki. Pozabljamo pa, da so ti poudarki naravnani na drugačne učne načrte, prirejeni drugačnemu kulturnemu in družbenemu okolju. Velikokrat se zgodi, da tuje zamisli prav zato z domačimi niso združljive. Ob tem se je dobro zavedati, da moramo Slovenci zaradi majhnosti še toliko bolj varovati in negovati svoje zamisli, jih ohranjevati in jih razvijati.

Naj omenim dva zgleda: Velikokrat smo se matematiki že obregnili ob eno prvih mednarodnih raziskav matematičnega znanja naših osnovnošolcev in srednješolcev, ki so jo opravili pred več leti na Pedagoškem inštitutu. Ugovori, da rezultati zaradi navedenih razhajanj niso verodostojni, izvajalcev niso prepričali. V javnosti je prevladalo mnenje, da je znanje naših osnovnošolcev v primeri s tujimi izredno slabo.

Na podobne težave smo naleteli tudi izvajalci projekta *Presečišče*, katerega prvotni namen je bil prevajanje in le manjše prirejanje tujih učbenikov. Delo je pokazalo, da direktno prevajanje tujih učbenikov, če so še tako premišljeni, ni primerno. V prevod je bilo potrebno vključiti veliko domačega dela, morda celo več, kot če bi se tega dela lotili od vsega začetka povsem z domačimi možgani. Tako so iz prevodov nastale temeljite priredbe, ki so v veliki meri domača dela, obogatena s številnimi tujimi nalogami.

Vprašanje: *Ali je sploh mogoče vplivati na to, da bodo novi učni načrti zares zrastle iz domače osnove, iz katere bodo odstranjene že dolgo znane pomanjkljivosti?*

Razhajanja

1. Ustreznost vsebine obstoječih načrtov.
2. Metodično-didaktični postopek.
3. Zunanja diferenciacija pouka.
4. Neenotna terminologija.
5. Ponudba učbenikov in gradiv za učence in učitelje.

Ustreznost vsebine obstoječih načrtov.

Več nezadovoljstva je z vsebino osnovnošolskega učnega načrta kot srednješolskega.

Vzrok je verjetno v tem, da so srednješolske učne načrte prečistili z ukinitvijo usmerjenega izobraževanja in ponovno ustanovitvijo gimnazij in preostalih srednjih šol. Veliko je k temu prispeval tudi katalog znanj, ki je osnova za pripravo na eksterno maturo in zaključni izpit.

V osnovni šoli še vedno velja učni načrt iz leta 1984. Razen splošnega nezadovoljstva učiteljev uradno ni znano, *kdaž in v kateri smeri* bo stekla prenova. Prav tako niso uradno znani rezultati obsežnega anketiranja učiteljev pred nekaj leti, s katerim so zbirali njihove pripombe o učnem načrtu. Bistvene pomanjkljivosti osnovnošolskega učnega načrta pa se da posredno razbrati iz knjižice Z. Perata *Znanje matematike ob vstopu v srednje šole* [2].

Vzrok, da je učni načrt iz leta 1984 še vedno v celoti v veljavi, je morda skrit tudi v veliki boječnosti osnovnošolskih učiteljev. Ti si vse do nastanka

novih potrjenih alternativnih učbenikov za predmetno stopnjo niso upali niti metodično, kaj šele vsebinsko skreniti s poti, ki so jo oblikovali predpisani učbeniki, čeprav so jim izkušnje govorile drugače. Šele ob seminarjih, ki spremljajo nove alternativne učbenike, se stanje počasi spreminja.

Tako ravnanje učiteljev je povsem razumljivo. Veliko bolj kot njihovi srednješolski kolegi delajo pod lupo staršev in šolskih oblasti. Nanje močno vpliva zaključno preverjanje znanja matematike in dejstvo, da se matematika uporablja za selekcijo učencev pri vstopu na številne srednje šole. Pritiski so še večji, ker osnovna šola sama ne priznava *nobene selekcije učencev*. *Vprašanja: Ali bodo prenovo učnih načrtov izvajali isti ljudje, ki so sestavljali prejšnje? Ali učitelj, kljub temu da je bil z raznimi anketami že velikokrat izzvan, zares ne bo prispeval k popravkom ali prenovi učnih načrtov? Ali bo prenova učnih načrtov temeljila samo na dodajanju novih vsebin in zanemarila izločanje starih?* *Ali se bo z uvedbo mature in zaključnega izpita občutje boječnosti razpaslo tudi po srednjih šolah?*

Metodično-didaktični postopek.

Poučevanje matematike v osnovni in srednji šoli se mora razlikovati v metodah, kako se lotiti snovi. V osnovni šoli se uporablja induktivni postopek: od posameznega k splošnemu in od konkretnega k abstraktnemu. V poučevanje je vključeno veliko iger, ponazarjanj, urjenja ročnih spretnosti, veliko vaj. Malo je teoretiziranja, malo ali skoraj nič strogega matematičnega dokazovanja. Matematična strogost je podrejena razumevanju, kar pa ne pomeni, da je v osnovni šoli dovoljeno učiti matematično neresnico. Umetnost poučevanja je nedvomno skrita tudi v zamolčevanju.

V srednji šoli način, kako se lotimo snovi, prehaja od induktivnega vse bolj k deduktivnemu. Uvaja se dokazovanje in matematična strogost.

Vprašanja: Ali je učitelj primerno podkovan z različnimi metodičnimi načini, kako se lotiti posamezne snovi glede na stopnjo, kjer poučuje?

Ali ima učitelj na voljo dovolj primerne literature (učbeniki, gradiva, učila), da se lahko spoprime z vsemi problemi poučevanja?

Ali je kvaliteta poučevanja odvisna predvsem od učiteljeve zagnanosti, spretnosti, iznajdljivosti in samoizobraževanja?

Zunanja diferenciacija pouka.

Obstaja potrebna delitev srednjih šol po vsebini in zahtevnosti: gimnazije, tehniške šole, skrajšani programi. . .

Obstaja enotna državna osnova šola. Pustimo ob strani nekatere nove smeri privatnih šol, kot so waldorfska idr. Diferenciacija je zajeta samo v dodatku k učnemu načrtu v obliki dopolnilnega in dodatnega pouka. Prvi je obvezen za vse učence s slabšimi sposobnostmi; drugi je namenjen samo boljšim učencem in ni obvezen.

Ideja sama je dobra, izvedba pa ne povsod. Vzrokov je več: od pomanjkanja denarja do pomanjkanja prostorov, preobremenjenosti otrok znotraj rednega pouka in preobremenjenosti učiteljev. Ob tem ima pri dodatnem pouku osnovnošolski učitelj matematike zelo veliko svobodo izbire. S tem prevzema nase tudi veliko odgovornost, ki je povezana z dodatnim zahtevnim delom.

Vprašanja: *Ali bo nova sprememba šolstva prinesla tudi diferencirano šolo znotraj obstoječe osnovne šole?*

Kako je s programi raznih privatnih šol?

Ali so vsebine zaključnega preverjanja osnovnošolskega znanja zagotovo naravnane samo na bistvene in najpomembnejše točke iz učnega načrta?

Ali bodo osnovnošolska matematična tekmovanja pripravljena tako, da ne bodo pogojevala uporabe določenih učbenikov?

Neenotna terminologija.

Imena za iste pojme se v osnovnošolski in srednješolski matematiki večkrat razlikujejo, kar precej moti. V osnovni šoli je veliko večji poudarek na doslednem matematičnem izražanju, npr. poimenovanju, čeprav smo tam precej manj matematično strogi.

Prav tako še ni določeno, ali naj se v osnovni šoli dosledno uporabljajo samo poslovenjeni izrazi za matematične pojme. Učitelji so za tuje izraze, čeprav zdaj uporabljajo oboje. Primer: Dosledno se uporablja na primer izraz produkt, kvocient pa je skoraj prepovedan.

Vprašanje: *Kdo, kdaj in kako bo rešil terminološke probleme?*

Ponudba učbenikov in gradiv za učence in učitelje.

V zadnjem času obstaja večja ponudba učbenikov in gradiv za vse stopnje. Za učitelja je to vsekakor zaželeno, a zato je tudi izbira težja in odgovornejša.

Za srednjo šolo obstaja več kompletov potrjenih učbenikov:

1. Berila *F. Križaniča* (zahtevnejši način),
2. Komplet učbenikov *P. Legiša*, dopolnjen z učbenikoma *A. Cokana* in *A. Čibeja*: *Zaporedje* in *A. Čibeja*: *Kombinatorika. Verjetnostni račun. Statistika*.
3. Del kompleta prenovljenih učbenikov *I. Štalca*. 1.del je izšel, drugi izide v jeseni, tretji in četrti v naslednjih letih.

Za učence srednje šole obstaja več različnih gradiv. Pri DZS je izšlo na primer 11 zvezkov nalog, v samozaložbi F. Oblaka naloge za delo po Križaničevih berilih, pri Komisiji za tisk zbirke vaj Ivana Štalca. Pri drugih založbah ali samozaložbah so izšle tudi številne druge zbirke.

Za srednješolske učitelje je slabše poskrbljeno. Za zdaj obstaja en sam priročnik za učitelje, in sicer *P. Legiša*: *Priročnik za poučevanje ravninske*

geometrije. V pripravi je obsežnejši priročnik za poučevanje kombinatorike, verjetnostnega računa in statistike.

V osnovi šoli je bera učbenikov in gradiv še bogatejša. Obstaja:

1. Komplet potrjenih učbenikov od 1. do 4. razreda I. Hafnerja in drugih.
2. Komplet potrjenih učbenikov od 5. do 8. razreda F. Galiča in drugih z ustreznimi spremljajočimi potrjenimi zbirkami nalog od 1. do 8. razreda.
3. Komplet potrjenih učbenikov *Presečišče* od 5. do 8. razreda. Le prvi je prevod, drugi so že domača dela, ki vključujejo večji del tujih nalog. Vsak učbenik je didaktično podprt s priročnikom za učitelje *Vodnikom* in *Letno rapozreditvijo učne snovi* in s knjigo *Rešitve nalog*. V pripravi so tudi dodatna didaktična gradiva. Razveseljivo je, da je novi komplet učbenikov spodbudil pri učiteljih ustvarjalne ideje. Upati je, da se bo tako počasi zadostilo potrebi po tovrstni literaturi.

Poleg omenjenih gradiv – vsa, ki so izšla pri DZS, so potrjena – obstaja na trgu v zadnjem času več novih gradiv, ki izhajajo pri raznih založbah ali pa jih izdajajo učitelji celo v samozaložbi. Pred odločitvijo za posamezno knjigo se je pametno na 2. strani knjige podučiti, kdo so bili recenzenti in kje je bilo delo izdano. Obstajajo primeri, ni jih ravno malo, ko so dela, ki pri eni založbi niso bila izdana zaradi negativnih strokovnih ocen, potem izšla nepopravljena pri drugi založbi z manj zahtevnimi kriteriji. Obstajajo tudi primeri, ko se pojavijo na trgu tudi razna gradiva, ki jih podpirajo razne finančne ustanove. Znan je primer neke zavarovalnice. Zaradi obojestranskih komercialnih povezav so take knjige navadno poceni, niso pa nujno tudi strokovno kvalitetne.

Vprašanje: *Kako naj bo učitelj dovolj dobro poučen o ponudbi in kvaliteti obstoječe literature?*

LITERATURA

- [1] *Program življenja in dela osnovne šole*, 4. zvezek, naravoslovno-matematično vzgojno-izobraževalno področje, Zavod SR Slovenije za šolstvo, Ljubljana 1984.
- [2] Z. Perat, *Znanje matematike ob vstopu v srednje šole*, Zavod za šolstvo, Ljubljana 1991.
- [3] Z. Perat, *Matematika na zaključnem izpitu*, Aktivni učitelji matematike na srednjih šolah: družbeno-jezikovne dejavnosti, Naravoslovno-matematične dejavnosti, Jesenice 1991.
- [4] F. Galič in drugi, *Komplet osnovnošolskih učbenikov od 5. do 8. razreda*, DZS, Ljubljana 1995.
- [5] R. Maroska in drugi, *Komplet osnovnošolskih učbenikov od 5. do 8. razreda*, DZS, Ljubljana 1995.
- [6] M. Strnad, *Presečišče 7, Vodnik*, DZS, Ljubljana 1995.

KRIPTOSISTEM RSA LETA 1873?¹

JANEZ ŽEROVNIK

Math. Subj. Class. (1991) 01A55

Opozorimo na razdelek v knjigi W. S. Jevonsa iz leta 1873, v katerem anticipira bistveni del ideje RSA algoritma.

RSA CRYPTOSYSTEM IN YEAR 1873?

In [5] W. S. Jevons writes that direct operations are 'easy' and inverse operations are 'hard'. Among a number of examples, he gives encyphering-decyphering and multiplication-factorization. It is reasonable to conclude that he anticipated one critical feature of the RSA algorithm, but not the algorithm itself [4].

Uvod

Kriptosistem RSA se je uveljavil kot zanesljiva metoda za varno prenašanje sporočil v modelu z javno dostopnim ključem. Metoda, ki je bila sprva strogo varovana državna skrivnost, temelji na znani domnevi, da je mnogo lažje zmnožiti dve števili kot pa razstaviti dano število na faktorje. Bralcem Obzornika je kriptosistem RSA znan že dolgo, saj je bil članek [11] objavljen v istem letu kakor prva široki strokovni javnosti dostopna publikacija v svetu [8]. Nekateri številsko teoretični temelji algoritma so opisani v [7], o tajnopisih pa je pisal tudi že Presek [10]. Avtorju znano literaturo v slovenščini zaključuje zbornik [6].

V tej notici želimo opozoriti, da je gornja domneva, pa tudi njena povezava s tajnopisjem, že zelo dolgo znana, saj jo najdemo že v častitljivo stari knjigi Williama Stanleya Jevonsa, *The Principles of Science; a Treatise on Logic and Scientific Method* (prva izdaja 1873). V izdaji iz leta 1958 [5] na straneh 122–126 v poglavju o indukciji in inverznih operacijah preberemo, da so direktne operacije „lahke“, inverzne pa „težke“. Na strani 124 kot primer navaja, da je šifriranje lahko, dešifriranje pa težko. In končno, na straneh 122–123 piše, da je množenje števil lahko, iskanje faktorjev pa težko. In še dobeseden prevod vprašanja: „Ali lahko bralec pove, kateri dve števili je treba zmnožiti, da dobimo število 8 616 460 799? Mislim, da ni verjetno, da bo to kdaj kdo vedel razen mene.“

Smiselno je povzeti, da je Jevons torej poznal pomembni del ideje algoritma RSA. Če si dovolimo še malo ugibanja, lahko rečemo, da bi lahko kriptosistem RSA odkrili in uporabljali že pred dobo računalnikov. Morda so ravno hitri računalniki opozorili na šibkosti večine metod, ki so jih uporabljali prej. Ena od posledic je bila definicija modelov kriptosistema z javno dostopnim ključem.

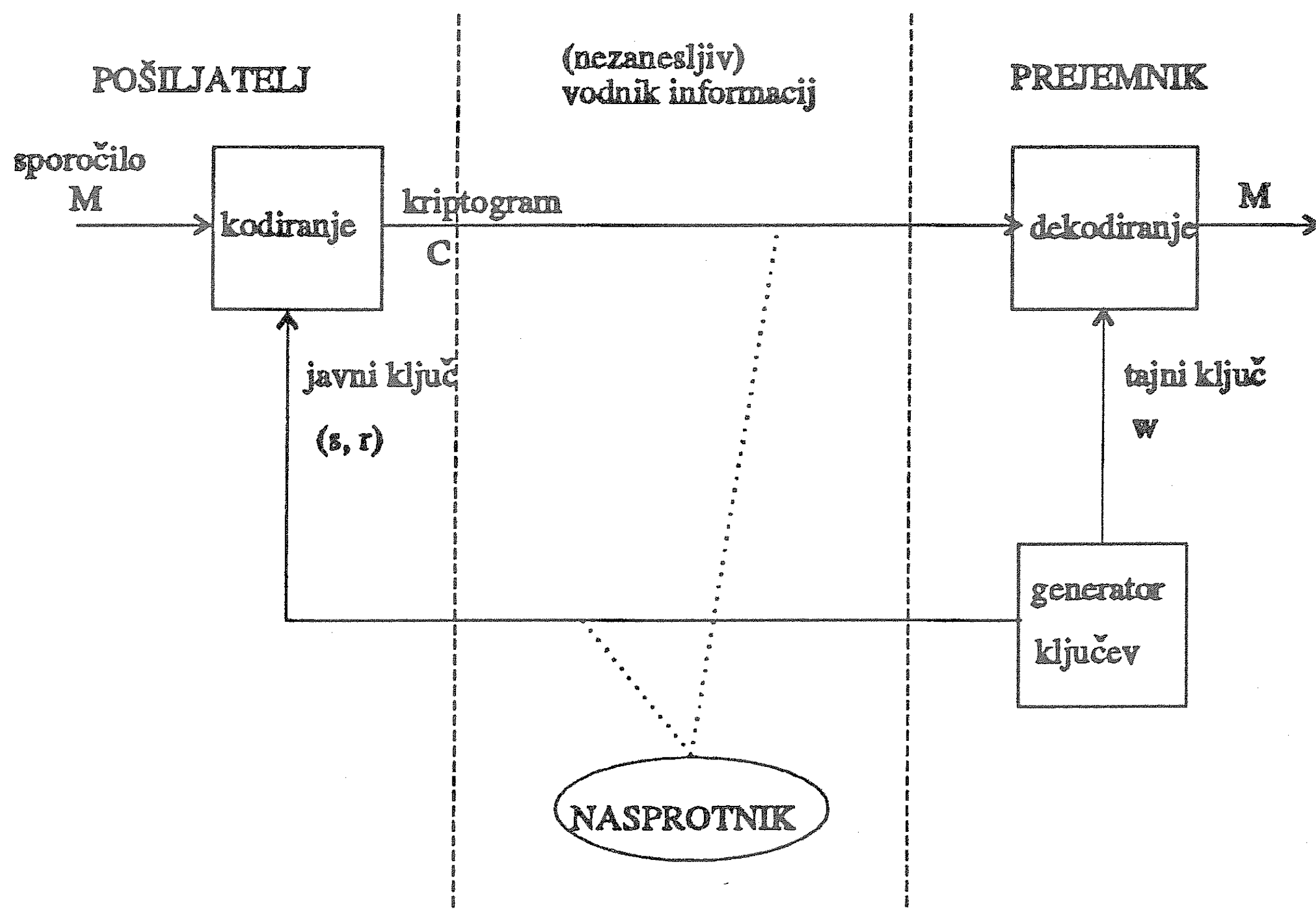
Povejmo še Golombov komentar k Jevonsovemu vprašanju o razcepu števila. Jevonsovo število $8\,616\,460\,799 = J$ je z navadnim kalkulatorjem

¹ Idejo in referenco na knjigo je avtorju posredoval profesor Solomon Golomb iz University of Southern California.

razcepil v manj kot šestih minutah. Uporabil je dejstvo, da lahko produkt dveh števil zapišemo kot razliko dveh kvadratov:

$$J = A^2 - B^2 = (A + B)(A - B).$$

Definiral je $A_0 = \lfloor \sqrt{J} \rfloor$ in $A_k = A_0 + k$ in preverjal, ali so števila $A_k^2 - J$ kvadrati. Začeni s $k = 1, 2, 3, \dots$ je uspel pri $k = 56$. Sam sem preveril račun z Mathematico, vendar nisem pogledal na uro, ali sem potreboval več ali manj kot šest minut.²



Asimetrični kriptosistem z javnim ključem. V primeru RSA je $C = M^s \pmod{r}$ in $M = C^w \pmod{r}$ za primerno izbrano število $r = pq$ in ključa s, w .

Opombe. Domneva, da je mnogo lažje zmnožiti dve števili kot pa ugotoviti, ali je dano število sestavljeno število, v jeziku teorije (časovne) zahtevnosti algoritmov povemo takole. Za množenje števil obstajajo algoritmi, ki v najslabšem primeru potrebujejo za izvajanje čas, ki je polinomska funkcija dolžine vhoda (števili p in q lahko zapišemo z $\lceil \log p \rceil + \lceil \log q \rceil$ biti). Za faktorizacijo ne poznamo polinomskega algoritma, problem faktorizacije je eden od redkih kandidatov za problem razreda $\text{MPI} = \text{NP} \setminus (\text{P} \cup \text{NPC})$ (glej [3] in [9]).

Za testiranje praštevilstosti obstajajo verjetnostno polinomski algoritmi, vendar ti ne rešijo problema faktorizacije. Pri teh algoritmih dobimo odgovor, ali je število praštevilo (v tem primeru je mogoča napaka, vendar z majhno verjetnostjo) ali ne (v tem primeru sicer ni napake, pa tudi faktorjev ne dobimo) [12].

Od zapažanja težavnosti razstavljanja števil do sheme RSA je bilo treba narediti kar znaten korak (čeprav se „ex post facto“ zdi preprost), ki so ga opravili Rivest, Shamir in Adleman in zanj poželi precejšnjo slavo. V praksi

² Mathematica 2.2 (Windows) poišče razcep $J = 89681 \times 96079$ v 7.25 sekunde (PC 486/66 MHz). (Opomba recenzenta.)

delujoči kriptosistemi RSA seveda uporabljajo še vrsto „malenkosti“, ki vsaka zase prispevajo k učinkovitosti metode. Podrobnosti daleč presegajo namen te notice, zato naj jih bralec poišče v navedeni literaturi.

LITERATURA

- [3] M. R. Garey, D. S. Johnson, *Computers and Intractability*, W. H. Freeman and Co., San Francisco 1979.
- [4] S. Golomb, pismo, 3.1.1995.
- [5] W. S. Jevons, *The Principles of Science; a Treatise on Logic and Scientific Method*, Reprint of the second edition, Dover Publications, New York 1958.
- [6] B. B. Lavrenčič, T. Pisanski (ur.), *Zbornik referatov „Delavnice o varovanju (elektronskih) podatkov“*, DMFA Slovenije, Ljubljana 1995.
- [7] B. Magajna, *Tajnopisi*, Obzornik mat. fiz. **38** (1991) 9–18.
- [8] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978) 120–126.
- [9] J. Seberry, J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice Hall, New York 1989.
- [10] M. Vencelj, *To in ono o tajnopisih*, Presek **22** (1994/95) 257–263.
- [11] J. Zupan, *Nekaj o kriptografskih metodah*, Obzornik mat. fiz. **25** (1978) 129–136.
- [12] J. Žerovnik, *Verjetnostni algoritmi*, Obzornik mat. fiz. **39** (1992) 129–139.

OBVESTILO

Društvo matematikov, fizikov in astronomov Slovenije,
Komisija za pedagoško dejavnost, objavlja

RAZPIS ZA PRIZNANJA UČITELJEM

V skladu s predlogom dopolnjenih pravil o podeljevanju priznanj učiteljem matematike, fizike, astronomije in računalništva za *delo z mladimi in za popularizacijo teh znanosti* lahko prejme priznanje član DMFAS, ki:

- s svojim delom izboljša pouk matematike, fizike, astronomije ali računalništva v osnovni, srednji ali visoki šoli;
- razširja zanimanje za svoj predmet med učenci, jih uspešno uči, vodi in usmerja njihovo delo v krožkih, tako da dosega vidne uspehe v šoli in na tekmovanjih;
- sodeluje s članki, učbeniki in drugimi učnimi in strokovnimi knjigami predvsem pri društvenih izdajah in s tem znatno prispeva k popularizaciji svojega predmeta in k izboljšanju poučevanja;
- neposredno ne dela z mladimi, njegova društvena, pedagoška, publicistična ali znanstvena dejavnost pa je tako izrazita, da vpliva na razvoj, popularizacijo in ugled teh znanosti.

Pisne predloge za priznanja, ki morajo obsegati dovolj podatkov za vsestransko presojo, sprejema do 1. oktobra 1996 Komisija za pedagoško dejavnost DMFA Slovenije, 1001 Ljubljana, Jadranska 19, p.p. 64.

Ivana Mulec

Prof. Andrej UMEK, minister za znanost in tehnologijo
Slovenska cesta 50, 1000 Ljubljana

Spoštovani gospod minister,

oglašamo se s pritožbo o zadevi, ki po našem mnenju daleč presega dogovarjanja o delitvi denarja med posameznimi vejami znanosti ali raziskovalnimi ustanovami.

Vaša odločitev, da matematiki ne priznate statusa fundamentalne znanosti in pravice do javnega raziskovalnega inštituta, ki ga imajo vsi drugi deli naravoslovno-matematičnih ved v Sloveniji, ter odrekanje ustanoviteljskih obveznosti inštitutu, ki je nacionalni inštitut za slovensko matematiko, dejansko pomeni za tretjino manjša sredsta za te vrste raziskav. S tem se bistveno spreminja delitev sredstev za raziskovalno delo, ki je bila opravljena na osnovi mednarodno recenziranih raziskav, odločitev pristojnih strokovnih svetov in upravnih organov. Jasno je, da skrčitev denarja za osnovne raziskave prej ali slej neizogibno prinese padec kvalitete v samem pedagoškem delu, posledice tega pa bo kasneje čutiti vse do osnovnih šol. To torej dolgoročno pomeni degradiranje znanja vseh Slovencev.

Zato vaše zmanjšanje sredstev za matematiko, naj bo formalno razloženo tako ali drugače, pomeni uničevanje ene od zares fundamentalnih vej znanosti. Zmanjšanje s potezo peresa, brez kvalitativne osnove, saj smo bili matematiki mednarodni selekciji in svetovnim merilom vedno kos. Ne sprašujemo se, ali ima vaša odločitev politično ali drugačno osnovo. Z nobeno od razlag se ne da strinjati. Zato je naša dolžnost, da s tem seznanimo ne le vas, ampak širšo javnost. Matematika je bila vedno gonilo znanja in razvoja. Dan-današnji brez nje ne gre, ne v osnovni, ne v srednji šoli, ne med študijem, ne v poklicu. Kaj šele v znanosti.

In še tole. Na hitro uničiti, naj bo to veja znanosti, kot je matematika, ali kaj drugega, je lahko. Zgraditi nekaj pa je dosti težje. Slovenska matematika je nastajala vse od Jurija Vege do Josipa Plemlja, ki jo je dvignil v svetovni vrh. In tam smo jo matematiki, na čelu z Ivanom Vidavom, za zdaj še obdržali.

Lep pozdrav.

Vladimir Batagelj, Matej Brešar, Andrej Brodnik, Josip Globevnik, Janko Gravner, Dragan Marušič, Bojan Mohar, Matjaž Omladič, Bojan Orel, Marko Petkovšek, Tomaž Pisanski, Dušan Repovš, Peter Šemrl, Borut Zalar, Janez Žerovnik.

Pismo so podpisali nosilci in sonosilci raziskovalnih projektov na področju matematike in teoretičnega računalništva v imenu vseh matematikov.

SEZNAM DIPLOMANTOV PRVE, DRUGE IN TRETJE STOPNJE TER DOKTORANDOV IZ MATEMATIKE IN FIZIKE V LETU 1995*

Pedagoška fakulteta, Maribor

2. stopnja

Matematika – fizika

- | | |
|---------------------|--|
| 39. Brantuša Vojko | Kontinuumi |
| 40. Denžič Martina | Odvajanje na prakolobarjih in polprakolobarjih |
| 41. Kremser Brigita | Modularne, Boolove in konceptualne mreže |
| 42. Kremzer Alenka | Kataklizmične spremenljivke |
| 43. Mord Natalija | Družine ortogonalnih polinomov |
| 44. Rajh Sonja | Matroidi |
| 45. Šuman Romana | Geometrija celoštevilске mreže |

Proizvodno-tehnična vzgoja – fizika

- | | |
|---------------------|---|
| 5. Goznik Anton | Modeliranje šolske tehnične delavnice v teoriji in praksi |
| 6. Jevtović Miodrag | Matematični model prenosa snovi skozi celično membrano z upoštevanjem difuzije v izvencelični raztopini |
| 7. Kobale Damjan | Matematični model prehoda lipidnih molekul med plastmi membrane eritocita |
| 8. Petauer Marjan | Fazni prehod omejenega tekočega kristala |
| 9. Sabolić Goran | Poskusi iz aerodinamike rakete na vodo in stisnjen zrak, praktikumska vaja kvadratni zakon upora |
| 10. Zupanc Iris | Resonanca v mehaniki, elektriki in kvantni mehaniki |

Kemija – fizika

- | | |
|-----------------|---|
| 1. Toš Nikolaja | Stanje in razvoj standardizacije s poudarkom na polimernih materialih |
|-----------------|---|

3. stopnja

Matematika – področje izobraževanja

- | | |
|--------------------|----------------------------------|
| 1. Čer-Titan Jasna | Urnik kot optimizacijski problem |
|--------------------|----------------------------------|

* Seznam diplomantov iz leta 1993 je bil objavljen v Obzorniku mat. fiz. 42 (1995) 3.

Pedagoška fakulteta - Ljubljana

2. stopnja

Fizika – tehnika

- | | |
|---------------------|---|
| 7. Šrabec Majda | Ležaji – preizkus in razlaga za nivo osnovne šole |
| 8. Senica Jožefa | Delovanje dinamike – opis in modelni preizkus za osnovno šolo |
| 9. Ogrinec Damijana | Dinamika krmiljenja mehanskega sistema z eno prostostno stopnjo |
| 10. Kožle Jelka | Poraba energije v gospodinjstvu |
| 11. Livk Karolina | Uvajanje osnov robotike k pouku tehnične vzgoje |
| 12. Červ David | Natančnost merjenja na zračni drči |

Fizika – kemija

- | | |
|-------------------|--|
| 9. Naglič Mateja | Analiza rezultatov maturitetnega izpita – splošna in anorganska kemija |
| 10. Tavčar Marija | Analiza rezultatov maturitetnega izpita – splošna in anorganska kemija |

Matematika – fizika

- | | |
|-----------------------|---|
| 44. Kranjc Sonja | Bifurkacijski diagram in Mandelbrotova množica |
| 45. Mozetič Vesna | Eulerjeva karakteristika in njena uporaba |
| 46. Stjepović Tamara | Analiza republiškega tekmovanja iz matematike v maju 1994 |
| 47. Kenda Urška | Zgodovinski pregled računanja števila |
| 48. Jankovec Alenka | Seštevanje divergentnih vrst |
| 49. Ferkolj Marinka | Feigenbaumova konstanta |
| 50. Kovač Tatjana | Preslikava Žukovskega |
| 51. Petkovšek Jerneja | Topologija ploskev |
| 52. Vidmar Danijela | Uvod v teorijo vozlov |
| 53. Furlan Gabrijela | Schröderjeva enačba |
| 54. Virant Pavel | Osnove teorije realnih analitičnih funkcij |
| 55. Ravbar Ingrid | Negibne točke zveznih preslikav |
| 56. Zupančič Jana | Projektivna geometrija |
| 57. Firm Agata | Energija in entropija |
| 58. Ferbar Domen | Statistične igre in ireverzibilnost |

Matematika - tehnika

- | | |
|-------------------|--------------------------------|
| 4. Mohorič Marija | Kooperativno učenje matematike |
| 5. Pavlovič Vesna | Razumevanje pojma ploščina |

Fakulteta za matematiko in fiziko

1. stopnja

Matematika – uporabna smer

275. Koselj Marko	278. Rebolj Blaž	281. Kocbek Kristijan
276. Sušnik Matej	279. Bohar Igor	282. Arh Maja
277. Justin Mateja	280. Lorgar Miran	

2. stopnja

Matematika – pedagoška smer

485. Cuderman Andrej	Linearna algebra v geometriji
486. Podhostnik Silvestra	Uvod v nestandardno analizo
487. Iveta Željka	Konveksne množice

Matematika – uporabna smer

484. Jamnik Anka	Računanje matričnih funkcij
485. Brus Miroslav	Polinomi prirejanja grafov in sistemi monomer in dimer
486. Kranjec Matevž	Delovanje diskretnih grup na C^* -algebrah
487. Krajnc Antonija	Reševanje inverznega kinematičnega problema robotskih manipulatorjev z Gr(bnerjevimi bazami
488. Lisac Blaž	Reševanje Toeplitzovih sistemov linearnih enačb
489. Keržič Mateja	Analiza referenčnih omrežij
490. Zabukovec Blaž	Čakalni sistemi s Poissonovim vhodnim procesom
491. Petek Simona	Youngove tabele in upodobitve simetrične grupe
492. Šilar Nina	Monotone norme na končno razsežnih vektorskih prostorih
493. Toškan Barbara	Interpolacija z geometrijsko zveznimi Bezierjevimi krivuljami
494. Budja Andreja	Matematični model ponudbe in povpraševanja
495. Molan Gregor	Risanje grafov ravnincev
496. Šmuc Damjan	Pogovorna nadgradnja knjižice Turbo Vision

Matematika – teoretična smer

43. Jamnik Borut	Matrična karakterizacija podprostorov C^* -algeber
44. Raič Martin	Lefschetzovo število in točke ujemanja para preslikav
45. Vavpetič Aleš	Nielsenova teorija negibnih točk
46. Potočnik Primož	Po točkah tranzitivni grafi, ki niso Cayleyevi

Fizika – pedagoška smer

136. Iršič Aleš	Prikaz spektra β pri šolskih poskusih
137. Rovšek Matej	Halo

Fizika – tehnična smer

- | | |
|-------------------------|---|
| 619. Dijanošič Roman | Meritev nevtronov z detektorjem jedrskih sledi CR - 39 |
| 620. Zorko Benjamin | Določanje vodika s spektrometrijo odrinjenih protonov |
| 621. Peršak Boštjan | Meritev parametrov plazme v napravi za ionsko nanašanje |
| 622. Demšar Jure | Raziskave relaksacij fotovzbujenih elektronov v visokotemperaturnih superprevodnikih |
| 623. Verbovšek Polona | Preučevanje vpliva temperature na transport v liposome vgrajenih snovi v kožo z metodami elektronske paramagnetne resonance |
| 624. Močnik Griša | Izkoristek določanja okusa mezonov B z nabojem razpadnih kaonov v spektrometru HERA - B |
| 625. Bobnar Vid | Dielektrične lastnosti antiferoelektričnega tekočega kristala |
| 626. Borštnik Anamarija | Polimerna mreža v izotropnem tekočem kristalu: paranematična ureditev |
| 627. Grabec Daša | Srpasta oblika rdečih krvnih celic |
| 628. Merkan Matjaž | Merjenje aktivnosti nehomogenih vzorcev z Ge detektorjem |
| 629. Perko Katarina | Sipanje svetlobe v aerogelu, napolnjenem z nematikom |
| 630. Cok Alenka | Model residualnega toka v plimovanju ob ravni steni |
| 631. Šprogar Miha | Študij strukurnega stekla $(\text{NH}_4\text{T})_x(\text{KI})_{1-x}$ z jedrsko magnetno resonanco ^{14}N |
| 632. Gomboc Andreja | Kako je videti padec zvezde v črno luknjo |
| 633. Komelj Matej | Izračun plimovanja v lineariziranem modelu plitve vode |
| 634. Jug Boštjan | Peltierov hladilnik |
| 635. Šlibar Matjaž | Magnetno polje in električni potencial vzbujene rastlinske celice Chare coralline |
| 636. Kirn Borut | Domenska struktura celične membrane |
| 637. Praprotnik Blaž | Konvektivni prenos toplote skozi mejno plast pare v toku tekočine |
| 638. Černe Gregor | Vodni udar v dvofaznih sistemih |
| 639. Bračko Marko | Dvofotonske reakcije s protonom, antiprotonom in dvema pionoma v končnem stanju |
| 640. Guštin Andrej | Model geostrofskega toka v Tržaškem zalivu |
| 641. Dolenc David | Merjenje koncentracije in porabe kisika v živih celicah |
| 642. Prešeren Rok | Absorpcijska rentgenska spektrometrija kovinskih par |
| 643. Kramberger Gregor | Meritev in simulacija signalov izvora ^{90}Sr v pozicijsko občutljivem silicijevem detektorju |
| 644. Prelovšek Saša | Sipanje mezona ρ na mezonu ρ |
| 645. Tement Daniel | Iskanje elektronov in pozitronov s števcem Čerenkova v spektrometru HERA-B |

646. Weibl Tomaž Študij inkomenzurabilnega faznega prehoda v Rb_2ZnCl_4 z meritvami spin mrežne relaksacije v laboratorijskem in rotirajočem sistemu
647. Gabrovšek Franci Amplitude v refleksijski seizmiki
648. Vidic Klemen Večdimenzionalni mnogokanalni analizator
649. Kuzman Drago Temperaturni senzor z optičnim vlaknom na osnovi merjenja fluorescenčnega časa
650. Vdovč Barbara Elektrooptični pojav v aerogelu, napolnjenem z nematičnim tekočim kristalom
651. Pust Marko Fazno sklenjeni krožni Nd:YAG laser
652. Kalin Jan Meritev dvofotonske razpadne širine $\Gamma(\eta' \rightarrow \gamma\gamma)$

Fizika - meteorologija

60. Hrabar Andrej Numerična simulacija nastanka in razkroja jezer hladnega zraka

3. stopnja

Matematika – izobraževalna smer

11. Žakelj Amalija Lakunarne Fourierove vrste
12. Rozman Franci Grupe avtomorfizmov linearno urejenih množic

Matematika – raziskovalna smer

68. Marinček Jože Cikli predpisanih homotopij v grafih na kompaktnih ploskvah
69. Strle Sašo Smaleova domneva

Fizika – elektrooptika

156. Rupnik Tanja Meritve dinamike gretja in inverzne zasedenosti v kristalu Er:YAG pri optičnem črpanju

Biofizika

157. Peterlin Primož Fosfolipidni mehurček v zunanjem električnem polju
158. Majhenc Janja Merjenje termičnih fluktuacij fosfolipidnih mehurčkov in določitev elastične upogibne konstante fosfolipidne membrane

Fizika trdne snovi

159. Škarabot Miha Dinamika feroelektričnega tekočega kristala v submikronskih plasteh

Fizika jedra in osnovnih delcev

160. Galičič Mirjam Opazovanje spreminjanja optičnega izseva pulzarja PSRO531+21 na kratkih časovnih skalah
161. Žontar Dejan Razvoj pozicijsko občutljivih silicijevih detektorjev za spektrometer DELPHI

Jedrska tehnika

162. Čepin Marko Optimizacija obratovalnih omejitev v jedrski elektrarni na osnovi verjetnostnih analiz
163. Šalamun Igor Digitalni sistemi kot pomoč operaterju pri vodenju jedrske elektrarne med nezgodnim obratovanjem

Meteorologija

164. Pristov Neva Začetna interpolacija za potrebe variacijske analize polja vetra

Doktorati – fizika

145. Filipčič Andrej Meritev parametrov kršitve simetrije CP pri razpadih nevtralnih kaonov v $\pi^+\pi^-\pi^0$
146. Kopač Samo Optimizacija in optodinamska analiza laserske izdelave rastra za optične dajalnike
147. Prosen Tomaž Kvantna Poincarejeva preslikava
148. Rokavec Aleš Študij gibalnih količin protonov v jedru ^{16}O z reakcijo $^{16}\text{O}(e, e'p)$
149. Zidanšek Aleksander Študij gelov z jedrsko magnetno resonanco
150. Živko Tomi Meritve tvorbe $\rho^0\rho^0, \rho^+\rho^-$ in $\omega\omega$ v dvofotonskih interakcijah s spektrometrom Argus

Martina Koman

NOVE KNJIGE

QUINN, Franck (ed.): Prospects in Topology, Proceedings of a conference in honor of William Browder, Annals of mathematics studies, 138, Princeton University Press, Princeton, New Jersey, 1995, 340 strani.

Ob šestdesetem rojstnem dnevu profesorja Williama Browderja so v Princetonu organizirali konferenco o topologiji s posebnim poudarkom na tistih področjih, ki jih je slavljenec v veliki meri soustvarjal. To so predvsem: teorija homotopije, transformacijske grupe in topologija mnogoterosti.

Prof. Browder je najbolj znan po tem, da je eden od očetov (matematične) kirurgije. Ob pomembnih raziskovalnih dosežkih pa je bil tudi predsednik American Mathematical Society, urednik prestižne revije Annals of Mathematics in imel še veliko drugih administrativnih funkcij. Poleg tega je bil izjemno uspešen pedagog. Imel je 28 doktorskih študentov, ki so tudi pomembno prispevali k razvoju matematike. Na začetku te knjige so naštetni vsi ti doktorandi in tudi njihovi doktorandi. Med slednjimi je tudi Žarko Bižaca, ki je pred leti magistriral na ljubljanski univerzi pri prof. Vrabcu.

Na tej konferenci se je zbralo veliko odličnih matematikov in predstavilo pomembne rezultate z raznih področij topologije (4-mnogoterosti, homologija, mnogoterosti imerzij, teorija indeksa, mnogoterosti z delovanjem grup,

teorija izglajevanja), pa tudi geometrije, algebre, algebraične geometrije, teorije števil in še česa. Nekateri od teh referatov, preoblikovani v članke, so zbrani v obravnavanem zborniku.

Posebej omenimo le tiste članke, o katerih je lažje kaj reči.

Homotopski razredi homotopskih ekvivalenc $X \rightarrow X$, kjer je X neki topološki prostor, sestavljajo grupo $\mathcal{E}(X)$ in homomorfizmu $G \rightarrow \mathcal{E}(X)$ pravimo homotopsko delovanje grupe G na prostor X . Vsako topološko delovanje $G \times X \rightarrow X$ inducira neko homotopsko delovanje G na X , G. Cooke pa je v članku iz leta 1978 pokazal, da ni vsako homotopsko delovanje inducirano s topološkim. Konstruiral je tudi neko teorijo ovir za tako inducirano, a ta ni niti lahka za računanje niti geometrijsko nazorna. Zato je A. H. Assadi v svojem članku v tej knjigi konstruiral algebrsko-geometrijske invariante, s pomočjo katerih lahko ugotovimo, ali je določeno homotopsko delovanje inducirano s topološkim.

S. Illman se je v svojem prispevku posvetil Hilbertovemu petemu problemu. Grupi G , ki je tudi taka realno-analitična mnogoterost, da sta množenje in invertiranje realno-analitični preslikavi, pravimo Liejeva grupa. Naj lokalno kompaktna grupa G deluje učinkovito na mnogoterost M . V tem primeru se lahko vprašamo:

1. ali je G tedaj tudi mnogoterost,
2. če je G mnogoterost, ali je tudi Liejeva grupa v primernih koordinatah,
3. če je G Liejeva grupa, ali lahko izberemo take koordinate v G in M , da so transformacijske funkcije analitične?

Prvemu vprašanju ponavadi pravimo Hilbert-Smithova domneva in menda še ni bila dokazana. Pozitivni odgovor na drugo vprašanje so dali Gleason, Montgomery in Zippin že leta 1952. V svojem članku sta Montgomery in Zippin pokazala tudi to, da je odgovor na tretje vprašanje v splošnem negativen. V pričujočem članku pa S. Illman dokaže, da je pri še nekaterih predpostavkah odgovor na tretje vprašanje vendarle pozitiven. Omenimo le en tak primer: če je G Liejeva grupa, ki deluje gladko na gladko mnogoterost M in je to delovanje tako, da je preslikava $G \times M \rightarrow M \times M$, $(g, m) \mapsto (gm, m)$ prava, obstaja taka realno-analitična struktura na M , usklajena z gladko strukturo na M , da je delovanje grupe G na M realno-analitično.

Prispevek V. Puppeja je motiviran z naslednjim vprašanjem, postavljenim leta 1978: splošno mnenje je, da naj bi imela ,naključno izbrana' mnogoterost zelo malo simetrije; ali se da to izraziti bolj precizno in konkretno, ali obstaja enostavno povezana mnogoterost, ki ne dopušča nobenega učinkovitega delovanja kake končne grupe (šibkejša verzija: ki ne dopušča nobene involucije)? Vprašanje je bilo tako zastavljeno zato, ker so takrat že bili znani primeri mnogoterosti brez netrivialnih delovanj končnih grup, a pri vseh tistih primerih je imela mnogoterost netrivialno fundamentalno

grupo. V. Puppeju je uspel pomemben korak k rešitvi omenjenega problema. Med drugim je pokazal, da obstajajo povezane gladke 6-dimenzionalne enostavno povezane spinske mnogoterosti, ki ne dopuščajo nobenega takega delovanja končne grupe, ki bi ohranjalo orientacijo.

Knjiga je zanimivo in poučno branje za raziskovalce, ki se ukvarjajo s topologijo ali z njo povezanimi področji matematike.

Matija Cencelj

OBVESTILO

Razpis DMFA Slovenije za posebne pohvale šolam

Šola, ki kandidira za pohvalo, naj izpolnjuje naslednje pogoje:

- da aktivno sodeluje z DMFA Slovenije ali njenimi podružnicami vsaj 20 let;
- da je v obdobju zadnjih 5 let organizirala vsaj eno republiško oziroma regijsko tekmovanje za srednješolce za matematiko ali fiziko oziroma sodelovala pri organizaciji republiškega in regijskega tekmovanja za osnovnošolce;
- da so v zanjih 20 letih učitelji matematike ali fizike na šoli prejeli društvena priznanja;
- da imajo vsi učitelji matematike in fizike na šoli ustrezno izobrazbo;
- da se vsa leta udeležujejo tekmovanj iz fizike in matematike ter sodelujejo na seminarjih, ki jih organizira DMFA Slovenije;
- da skrbijo za branje strokovnih revij na šoli (so redno naročeni na PRESEK, knjižice SIGMA), da izpopolnjujejo strokovno knjižnico za učitelje in učence in opozarjajo na novosti tako učitelje kot učence;
- da na šoli vsa leta redno delujeta matematični in fizikalni krožek (občasno pa tudi astronomski krožek ali krožek logike);
- da šola organizira naravoslovne dneve z vsebinami iz fizike ali astronomije;
- da učenci izdelujejo seminarske naloge s področja fizike, matematike ali astronomije;
- da šola organizira strokovne ekskurzije s področja matematike, fizike ali astronomije (tako za učitelje kot za dijake);
- da je njihovo delo odmevno tudi v regiji;
- da učitelji sodelujejo s prispevki v vsaj eni od društvenih revij ali objavljajo strokovne prispevke s področja matematike, fizike ali astronomije;
- da so v zadnjih 10 letih njihovi učitelji sodelovali na strokovnih zborih in seminarjih z lastnimi prispevki.
- da na šoli izvajajo še druge dejavnosti, ki prispevajo k popularizaciji matematike, fizike ali astronomije.

UO DMFA Slovenije

NOVE KNJIGE

ROBINSON, A., Non-standard Analysis, Revised Edition, Princeton University Press (Princeton Landmarks in Mathematics and Physics), Princeton, New Jersey 1966; 293 str.

To je že tretja izdaja znamenitega dela, ki je upravičeno izšlo v knjižni zbirki s imenom Mejniki v matematiki in fiziki. Abraham Robinson je namreč leta 1960 dokazal, da je mogoče Leibnizovo interpretacijo diferencialnega in integralnega računa kot igro neskončno majhnih in neskončno velikih količin, ki je doživela hudo kritiko strogih utemeljiteljev sodobne matematike, logično neoporečno rekonstruirati. Na videz upravičeno začudenje, da je bilo treba za rehabilitacijo Leibnizove intuitivne ideje čakati kar 300 let, brž uplahne, ko se seznanimo z Robinsonovo stvaritvijo. V matematiki se pogosto zgodi, da se je za potrditev kakšne domneve, naj bo ta intuitivno še tako prosojna, treba nasloniti na zelo abstraktne teorije. Če takih teorij še ni, jih je pač treba izumiti. In prav to se je zgodilo tudi v zvezi z Leibnizovo domnevo. Robinsonov dokaz sloni namreč vsaj na treh abstraktnih teorijah, ki so se bolj ali manj dokončno izoblikovale šele v prvi polovici 20. stoletja. Pri tem imamo v mislih predvsem matematično logiko kot teorijo o formalnih jezikih in njihovih interpretacijah, strukturalno teorijo abstraktnih algebrskih sistemov in s tem v zvezi splošno teorijo modelov, ki nam odkriva tudi nestandardne modele takih sistemov. Prav v sklopu takih raziskav je Robinson res našel nestandardni model višjega reda, ki predstavlja, na kratko povedano, tako razširitev obsega realnih števil, v katerem nastopajo tudi neskončno majhni in neskončno veliki elementi.

Knjiga, o kateri poročamo, je natančen opis tega velikega odkritja. Vendar ni samo to. Avtor je temu opisu dodal še obširen pregled vpliva in uporabe tega nestandardnega vidika v različnih področjih matematike. Naslovi posamesnih poglavij so:

Splošni uvod – Logična sredstva – Diferencialni in integralni račun – Splošna topologija – Funkcije ene realne spremenljivke – Funkcije ene kompleksne spremenljivke – Linearni prostori – Topološke in Liejeve grupe – Izbrani primeri – 0 zgodovini infinitezimalnega računa.

Čeravno je A. Robinson izvrsten pisec, je knjiga zaradi same narave snovi kar precej zahtevno branj. To velja predvsem za poglavje o logičnih sredstvih, ki se iz predikatnega računa 1. reda brž razširijo na formalne jezike višjih redov in s tem v zvezi tudi na osnovno uporabo teorije tipov.

Če se bralec zanima za to pomembno odkritje, ki bo nedvomno vplivalo tudi na prihodnjo podobo matematike, lahko dobi prve informacije v zelo berljivem članku B. Magajna, Infinitezimali, Obzornik mat. fiz. 30 (1983) 2, str. 33–41.

Niko Prijatelj

MODERN METHODS IN COMPLEX GEOMETRY, The Princeton Conference in Honor of Gunning and Kohn, Edited by T. Bloom, D. Catlin, J. P. D'Angelo, Y.-T. Siu, Princeton University Press, 1995, New Jersey, 342 str.

Več kot 150 matematikov z vsega sveta se je marca 1992 zbralo na konferenci v Princetonu, da bi počastili šestdesetletnici dveh znamenitih princetonovskih matematikov: Roberta C. Gunninga in Joshepa J. Kohna. Širše raziskovalno področje obeh slavljencev so analitične funkcije več kompleksnih spremenljivk. Delo R. C. Gunninga je blizu algebraični geometriji in je povezano z vprašanji o holomorfnih prerezih svežnjev nad kompleksnimi mnogoterostmi. Omenimo tudi znamenito knjigo „Analytic Functions of Several Complex Variables“, Prentice-Hall, Engelwood Cliffs, NJ, 1965, ki jo je napisal skupaj s H. Rossijem in predstavlja eno prvih knjig, ki se je področja analitičnih funkcij več kompleksnih spremenljivk lotila na celovit način.

J. J. Kohn je zaslovel po svoji metodi reševanja $\bar{\partial}$ -Neumannovega problema in vprašanja regularnosti njegovih rešitev. Za dano diferencialno formo α , $\bar{\partial}\alpha = 0$, na omejenem psevdokonveksnem območju Ω v $\mathbb{C}^n$ je treba poiskati tisto rešitev u Cauchy-Riemannove enačbe $\bar{\partial}u = \alpha$, ki je pravokotna na jedro operatorja $\bar{\partial}$. Ta rešitev je danes znana kot Kohnova rešitev $\bar{\partial}$ -Neumannovega problema.

Knjiga, ki je pred nami, je zbornik petnajstih člankov, katerih večina (ne pa vsi) so bili predstavljeni na konferenci v Princetonu. Njihovi avtorji (R. Bott, M. Christ, J. P. D'Angelo, P. Eyssidieux, N. Mok, C. Fefferman, J. E. Fornaess, N. Sibony, H. Grauert, R. S. Hamilton, G. M. Henkin, A. M. Nadel, L. Nirenberg, Y.-T. Siu, F. Treves in S. M. Webster) so danes med vodilnimi raziskovalci na področju analitičnih funkcij več kompleksnih spremenljivk in sorodnih matematičnih področij, zato vsakdo, ki ga analiza (ali pa tudi geometrija) zanima vsaj od daleč, ne bo mogel mimo nje.

Miran Černe

EDMONDS A. R., Angular Momentum in Quantum Mechanics, Princeton University Press, Princeton, NJ, 1996, Princeton Landmarks in Mathematics and Physics, 146 str.

Vrtilna količina je ena izmed najpomembnejših količin v mehaniki, še posebno v kvantni mehaniki. V zbirki broširanih ponatisov je princetonovska univerzitetna založba ponovno izdala tudi klasično delo A. R. Edmondsa o vrtilni količini v kvantni mehaniki. Pri tem gre za uspešnico, ki je doslej od leta 1957 izšla že v treh popravljenih izdajah in več natisih. Fizik, ki se je z vrtilno količino srečal v fiziki atomov, jeder ali delcev, je zelo verjetno knjižico že imel v roki. Vsebuje poglavja: grupnoteoretične osnove, kvantizacija vrtilne količine, sklopitev vektorjev vrtilne količine, reprezentacije končnih zasukov, sferični tenzorji in tenzorski operatorji, konstrukcija invariant iz koeficientov za sklopitev vektorjev, izračunavanje matričnih elementov pri dejanskih nalogah in dodatka. Knjiga bo prišla prav vsem, ki pri svojem delu v kvantni mehaniki računajo z vrtilno količino.

Janez Strnad

VABILO

Upravni odbor Društva matematikov, fizikov in astronomov Slovenije v sodelovanju z Zavodom RS za šolstvo vabi matematike, fizike in astronome na

STROKOVNO SREČANJE IN 48. OBČNI ZBOR DRUŠTVA
ki bo 11. in 12. oktobra 1996 v hotelu Jama v Postojni.

PROGRAM

Petek, 11.10.1996, dopoldne

Fizika

- 9.30–11.00 Bogdan Martinčič: Kamera, računalnik, šport in fizika
11.30–13.00 Brane Mušič: Optične komunikacije

Uporabna matematika

- 9.30–11.00 Mihael Perman: Verjetnost po lahkotni poti
11.30–12.15 Janez Žerovnik: Topološki indeksi v kemijski teoriji grafov
12.30–13.15 Tomaž Pisanski: Kubični grafi

Pedagoška matematika

- 9.30–11.00 Vesna in Matjaž Omladič: Matematika in denar
11.30–12.15 Dušan Pagon in Silva Kmetič: Prispevki k poučevanju matematike
12.30–13.15 Darjo Felda: Tekmovanje Kenguru

Popoldne

- 15.30–16:00 Otvoritev razstave slovenskih matematičnih učbenikov Blaža Matka ob stoletnici prvega izida
16.15–17.15 Nadja Zupan Hajna: Kras
17.30–18:30 Franci Gabrovšek: Alpski kras
19.30 Večerja in družabni večer z živo glasbo

Sobota, 12.10.1996

- 9.00 Občni zbor DMFA Slovenije
- Otvoritev in izvolitev delovnega predsedstva
 - Društvena priznanja
 - Poročila o delu društva
 - Razprava o poročilih
 - Poročilo nadzornega odbora
 - Volitve novega odbora
 - Pregled sklepov
 - Razno
- 14.00 Ogled Predjamskega gradu

Predsednik DMFA Slovenije:
Egon Zakrajšek