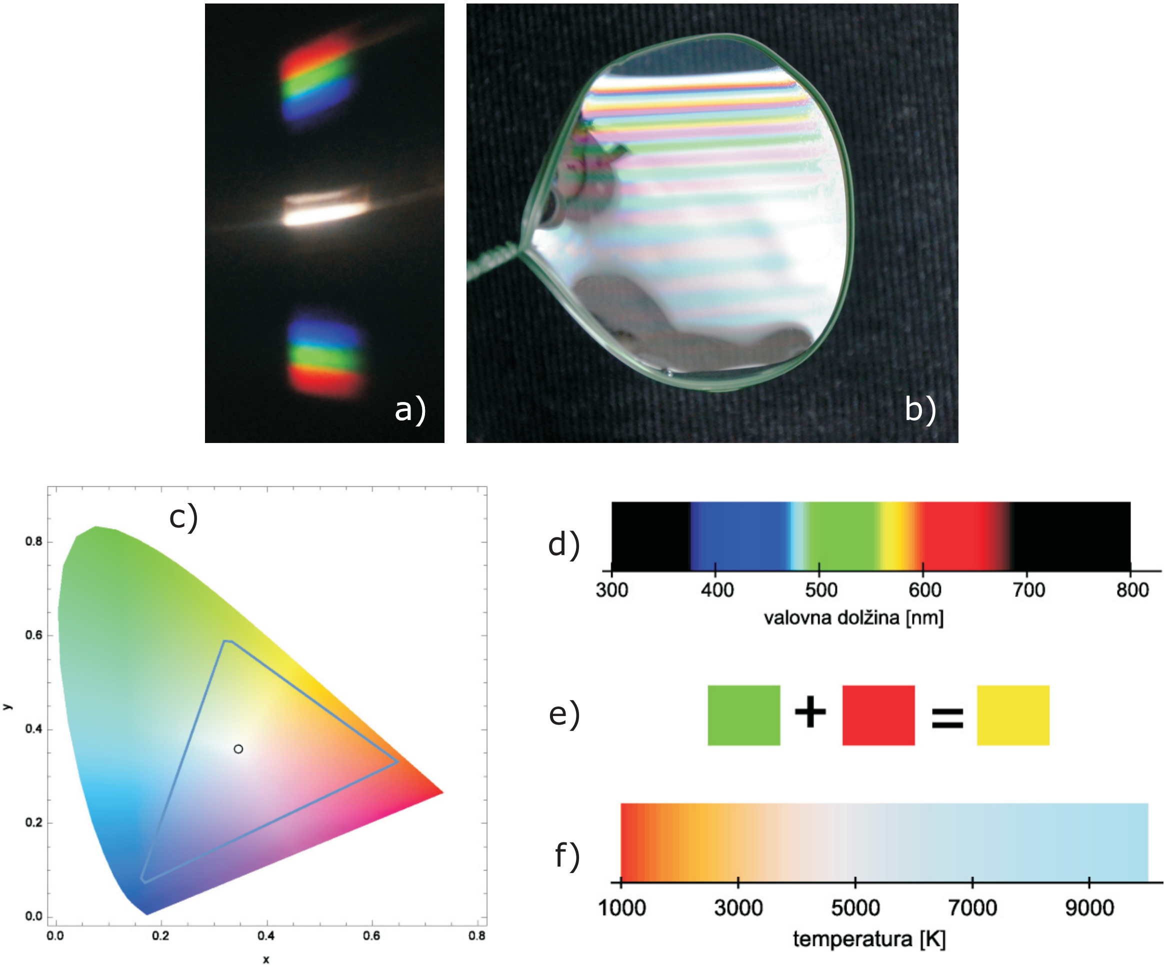
IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE

ISSN 0473-7466

2015
Letnik 62
2

OBZORNIK ZA MATEMATIKO IN FIZIKO



OBZORNIK MAT. FIZ. • LJUBLJANA • LETNIK 62 • ŠT. 2 • STR 41-80 • MAREC 2015

OBZORNIK ZA MATEMATIKO IN FIZIKO

Glasilo Društva matematikov, fizikov in astronomov Slovenije
Ljubljana, MAREC 2015, letnik 62, številka 2, strani 41–80

Naslov uredništva: DMFA–založništvo, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana **Telefon:** (01) 4766 553, 4232 460 **Telefaks:** (01) 4232 460, 2517 281 **Elektronska pošta:** zaloznistvo@dmfa.si **Internet:** http://www.obzornik.si/ **Transakcijski račun:** 03100–1000018787 **Mednarodna nakazila:** SKB banka d.d., Ajdovščina 4, 1513 Ljubljana **SWIFT (BIC):** SKBASI2X **IBAN:** SI56 0310 0100 0018 787

Jezikovno pregledal Janez Juvan.
Računalniško stavila in oblikovala Tadeja Šekoranja.
Natisnila tiskarna COLLEGIUM GRAPHICUM v nakladi 1250 izvodov.

Člani društva prejemajo Obzornik brezplačno. Celoletna članarina znaša 24 EUR, za druge družinske člane in študente pa 12 EUR. Naročnina za ustanove je 35 EUR, za tujino 40 EUR. Posamezna številka za člane stane 3,19 EUR, stare številke 1,99 EUR.

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).

Revija izhaja praviloma vsak drugi mesec. Sofinancira jo Javna agencija za raziskovalno dejavnost Republike Slovenije iz sredstev državnega proračuna iz naslova razpisa za sofinanciranje domačih znanstvenih periodičnih publikacij.

 Poštnina plačana pri pošti 1102 Ljubljana

NAVODILA SODELAVCEM OBZORNIKA ZA ODDAJO PRISPEVKOV

Revija Obzornik za matematiko in fiziko objavlja izvirne znanstvene in strokovne članke iz matematike, fizike in astronomije, včasih tudi kak prevod. Poleg člankov objavlja prikaze novih knjig s teh področij, poročila o dejavnosti Društva matematikov, fizikov in astronomov Slovenije ter vesti o drugih pomembnih dogodkih v okviru omenjenih znanstvenih ved. Prispevki naj bodo zanimivi in razumljivi širšemu krogu bralcev, diplomantov iz omenjenih strok.

Članek naj vsebuje naslov, ime avtorja (oz. avtorjev), sedež institucije, kjer avtor(ji) dela(jo), izvleček v slovenskem jeziku, naslov in izvleček v angleškem jeziku, klasifikacijo (MSC oziroma PACS) in citirano literaturo. Slike in tabele, ki naj bodo oštevilčene, morajo imeti dovolj izčrpen opis, da jih lahko večinoma razumemo tudi ločeno od besedila. Avtorji člankov, ki želijo objaviti slike iz drugih virov, si morajo za to sami priskrbeti dovoljenje (copyright). Prispevki so lahko oddani v računalniški datoteki PDF ali pa natisnjeni enostransko na belem papirju formata A4. Zaželena velikost črk je 12 pt, razmik med vrsticami pa vsaj 18 pt.

Prispevke pošljite odgovornemu uredniku ali uredniku za matematiko oziroma fiziko na zgoraj napisani naslov uredništva. Vsak članek se praviloma pošlje dvema anonimnima recenzentoma, ki morata predvsem natančno oceniti, kako je obravnavana tema predstavljena, manj pomembna pa je originalnost (in pri matematičnih člankih splošnost) rezultatov. Če je prispevek sprejet v objavo, potem urednik prosi avtorja še za izvorne računalniške datoteke. Le-te naj bodo praviloma napisane v eni od standardnih različic urejevalnikov TEX oziroma LATEX, kar bo olajšalo uredniški postopek.

Avtor se z oddajo članka strinja tudi z njegovo kasnejšo objavo v elektronski obliki na internetu.

VRNITEV ARNOLDOVE MAČKE

MITJA LAKNER[1], PETER PETEK[2], MARJETA ŠKAPIN RUGELJ[1]

[1]Fakulteta za gradbeništvo in geodezijo, Univerza v Ljubljani
[2]Pedagoška fakulteta, Univerza v Ljubljani

Math. Subj. Class. (2010): 37D45, 94A60

Hiperbolična matrika določa preslikavo na torusu, vendar jo lahko opazujemo tudi na $N \times N$ rastru, kot je to napravil V. I. Arnold [2]. Opazoval je sliko mačke, ki se je po določenem številu iteracij vrnila. Zanima nas povezava med gostoto rastra in periodo vrnitve. To lastnost lahko uporabimo tudi za šifriranje in prikrivanje informacij.

RECURRENCE OF ARNOLD'S CAT

A hyperbolic matrix yields a mapping on the torus. However we can, as V. I. Arnold [2] did, consider the picture of the cat on $N \times N$ raster. After a certain number of iterations the cat returns. We are interested in the dependence of the period of return on the density of the raster net. The property of return can be used for coding and covering up information.

Uvod

V klasični mehaniki nastopajo posebni sistemi diferencialnih enačb – hamiltonski sistemi. Pojavljajo se npr. pri nebesni mehaniki ali pri dvojnem nihalu. Standardna obravnava [1] nas pripelje do prostorov v obliki večdimenzionalnih torusov. Lokalne rešitve sistema opišemo z matriko, ki ohranja ploščino. Matrika v eno smer razteguje, v drugo stiska in je *hiperbolična*, kar pomeni, da nima lastnih vrednosti dolžine ena. V nekem smislu ta hiperboličnost zagotavlja dobro mešanje slike. Ruski matematik V. I. Arnold je obravnaval take sisteme, posebej na dvodimenzionalnem torusu. Opazoval je zanimive lastnosti, kaj se zgodi na neki ekvidistantni mreži – rastru – na torusu. Točk na mreži je končno mnogo, matrika jih zgolj premeša, permutira med sabo. Po končnem številu korakov vsaka permutacija spet pripelje stvari v prvotno stanje.

Arnold, ki je imel rad slikovite prispodobe, je vzel sliko mačke, jo rastriral in iteriral preslikavo na torusu [2]. In mačka se je spet pojavila po določenem končnem številu korakov. Seveda je perioda odvisna od gostote rastra in to precej misteriozno.

Vsaj teoretično se da uporabiti to metodo za prikrivanje podatkov, steganografijo. Pri tem ni treba slediti prvotni Arnoldovi matriki, vsaka iz splošne linearne grupe nad celimi števili je dobra. In kot je navada že v kriptografiji, kjer si želijo velikih praštevil, si tukaj želimo dolgo periodo.

Sicer pa je, če jo opazujemo na celem torusu in ne le na rastrski mreži, preslikava *kaotična*. A o tem v prihodnjem članku.

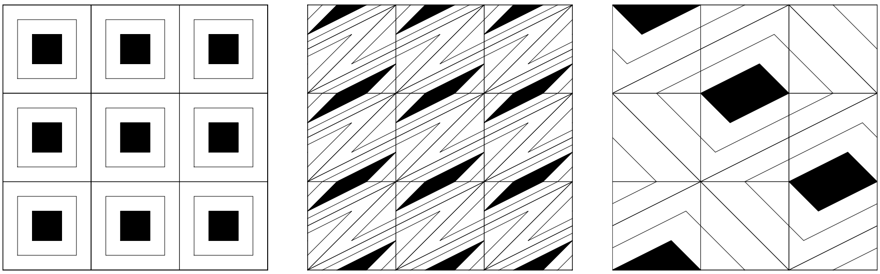
Hiperbolični avtomorfizmi torusa

Torus dobimo, če enotski kvadrat zlepimo po dveh vzporednih stranicah in isto naredimo še z nastalima krožnicama. To je vsebina naslednje definicije:

Definicija 1. Če v ravnini $\mathbb{R}^2$ identificiramo vse točke, katerih koordinate se razlikujejo za celo število, dobimo torus T.

Identifikacija definira ekvivalenčno relacijo na $\mathbb{R}^2$, kjer je $(x_1, y_1) \sim (x_2, y_2)$ natanko tedaj, ko sta $x_2 - x_1$ in $y_2 - y_1$ celi števili. Ta ekvivalenčna relacija določa projekcijo $\pi : \mathbb{R}^2 \to T$, $\pi(x, y) = [x, y]$.

Poglejmo si, kaj dobimo, če tlakovano celoštevilsko ravninsko mrežo preslikamo s celoštevilsko matriko dimenzije 2×2. Na sliki 1 na sredini vidimo, da pri množenju z matriko z determinanto 1 dobimo tlakovanje mreže s skladnimi »ploščicami«. Če pa ima matrika determinanto 2, so »ploščice« tlakovanja različne. Iz slike intuitivno sklepamo, da se je smiselno omejiti na matrike z determinanto ± 1.



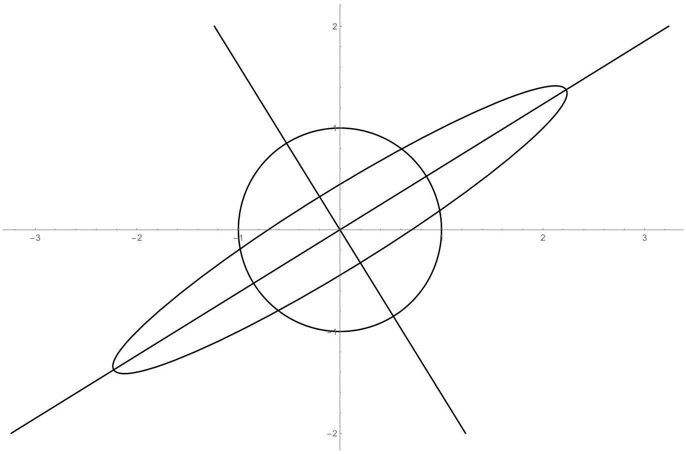
Slika 1. Tlakovanje ravninske mreže (na levi) in sliki mreže, če uporabimo matriki z determinanto 1 (na sredi) oz. 2 (na desni).

Definicija 2. Naj bo $A = (a_{ij})$ matrika dimenzije 2×2 z lastnostmi

(a) A je hiperbolična (lastni vrednosti ne ležita na enotski krožnici v kompleksni ravnini);

(b) $a_{ij} \in \mathbb{Z}$, $1 \leq i, j \leq 2$;

(c) $\det A = \pm 1$.



Slika 2. Slika krožnice pri množenju z matriko A.

Matrika A inducira tako preslikavo $L_A\colon T \to T$, da je $L_A \circ \pi = \pi \circ A$. To preslikavo imenujemo **hiperbolični avtomorfizem torusa**:

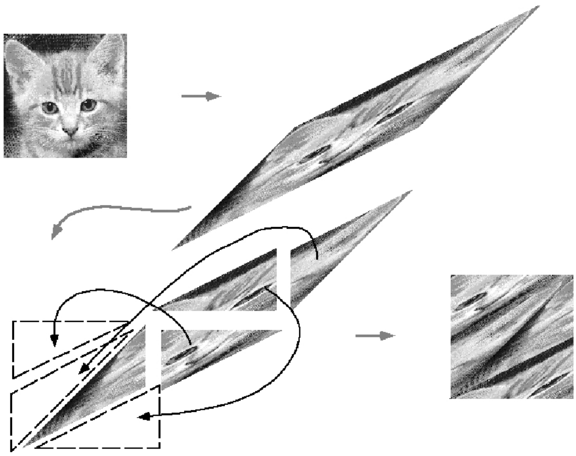
$$L_A([x, y]) \equiv A \begin{bmatrix} x \\ y \end{bmatrix} \pmod 1.$$

Opomba 1. Ker je $\det A = \pm 1$, je A^{-1} tudi hiperbolična in elementi matrike so cela števila. Torej A^{-1} tudi inducira hiperbolični avtomorfizem torusa $(L_A)^{-1}$.

Primer. Preslikavo L_A torusa, inducirano z matriko $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, imenujemo preslikava Arnoldove mačke C_A [2]. Lastni vrednosti matrike A sta $\lambda_1 = \frac{3+\sqrt{5}}{2}$ in $\lambda_2 = \frac{3-\sqrt{5}}{2}$. Na sliki 2 vidimo, kam se pri množenju z matriko A preslika krožnica s središčem v izhodišču. Ker je $\det A = 1$, je C_A hiperbolični avtomorfizem torusa. Poglejmo, kam A preslika enotski kvadrat. Ker je

$$A \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \; A \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \; A \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix},$$

se enotski kvadrat preslika v paralelogram enake ploščine (glej sliko 3). Na sliki 4 vidimo, kako se slika mačke, ki jo predstavimo s 124×124 točkami, razmaže po paralelogramu in po 15 iteracijah ponovno pojavi.



Slika 3. Avtomorfizem.

Izhodišče je edina negibna točka preslikave C_A. Bralec se lahko z uporabo popolne indukcije prepriča, da za potenco matrike A velja

$$A^n = \begin{bmatrix} F_{2n+1} & F_{2n} \\ F_{2n} & F_{2n-1} \end{bmatrix},$$

kjer je (F_n) Fibonaccijevo zaporedje s $F_0 = 0$, $F_1 = 1$ in $F_{n+1} = F_{n-1} + F_n$.

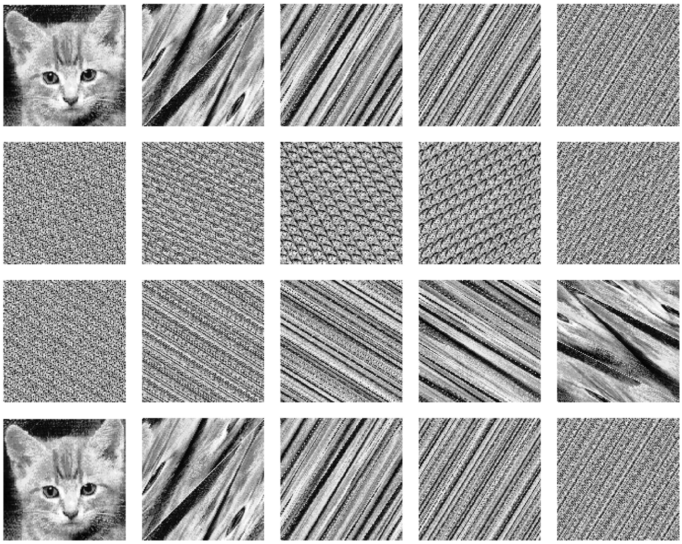
Resnično sliko predstavimo z $N \times N$ slikovnimi točkami, enakomerno razporejenimi v kvadratno mrežo. Naj bo $\Pi(N)$ najmanjše tako število, da je $A^k \equiv I \pmod N$. Potem se po $\Pi(N)$ iteracijah preslikave C_A vrne prvotna slika. Najbolj znan raster je $N = 124$, ko je $\Pi(124) = 15$ (slika 4).

Diskretna preslikava Arnoldove mačke

Diskretna preslikava Arnoldove mačke je podana s predpisom

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \equiv A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N, \tag{1}$$

kjer je $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, in deluje na kvadratni mreži z $N \times N$ točkami, katerih koordinate so cela števila $0, 1, \ldots, N-1$. Naj točke pomenijo slikovne točke slike mačke. Vsaka iteracija točke pomeša med sabo. To vidimo takole: preslikava $(x, y) \mapsto (\frac{x}{N}, \frac{y}{N})$ preslika kvadrat $[0, N)^2$ bijektivno na $[0, 1)^2$. Ker π preslika kvadrat $[0, 1)^2$ bijektivno na torus T, kjer je L_A bijekcija, je diskretna preslikava Arnoldove mačke res permutacija.



Slika 4. Iteracija avtomorfizma.

Vprašanje pa je, koliko iteracij je treba, da zopet dobimo prvotno sliko. V matričnem zapisu to pomeni, da iščemo tako število $P = P(N)$, da bo $A^P \equiv I \pmod N$ (glej sliko 4). Število $P(N)$ imenujemo perioda, s $\Pi(N)$ pa označimo minimalno periodo, ko se slika ponovi. V primeru na sliki 4 je $\Pi(124) = 15$. Izkaže se, da minimalna perioda ni naraščajoča funkcija N ([6, 3, 4]). Slika 5 prikazuje minimalno periodo do vključno $N = 5000$.

Ker velja

$$A^n = \begin{bmatrix} F_{2n+1} & F_{2n} \\ F_{2n} & F_{2n-1} \end{bmatrix}, \tag{2}$$

kjer je (F_n) Fibonaccijevo zaporedje za $F_0 = 0$, $F_1 = 1$, sta perioda in minimalna perioda preslikave (1) odvisni od deljivosti Fibonaccijevih števil. Iz enačbe (2) sledi, da je število T perioda $P(N)$ preslikave (1), če in samo če velja

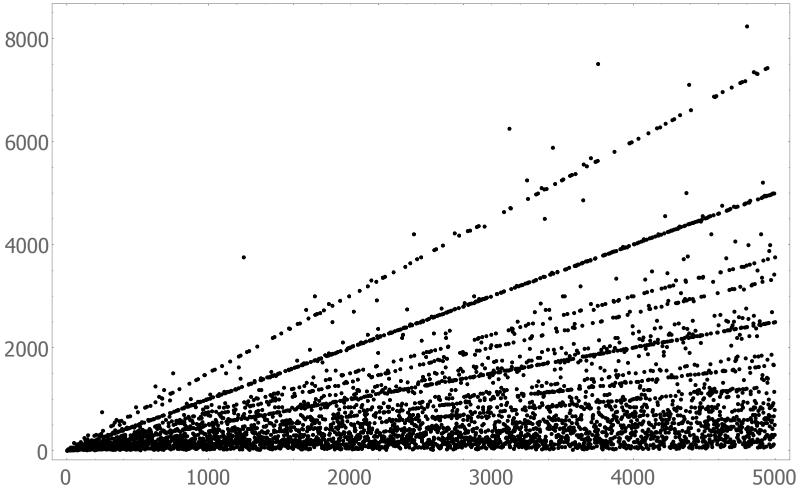
$$F_{2T-1} \equiv 1 \pmod N \ \text{ in } \ F_{2T} \equiv 0 \pmod N. \tag{3}$$

Pokažimo zelo grobo oceno za minimalno periodo.

Izrek 1. *Za poljubno sliko velikosti $N \times N$, kjer je $N \geq 3$, velja $\Pi(N) \leq \frac{N^2}{2}$.*

Za dokaz izreka potrebujemo tri kratke leme. Naj bo Φ_n najmanjši nenegativni ostanek F_n pri deljenju z N:

$$F_n \equiv \Phi_n \pmod N.$$



Slika 5. Minimalna perioda $\Pi(N)$. Na sliki opazimo premice, opisane v izrekih 6 in 7.

Primer. (a) Za $N = 2$ je zaporedje Φ_n periodično z minimalno periodo 3,

$$(0, 1, 1, 0, 1, 1, \ldots).$$

(b) Za $N = 7$ je zaporedje Φ_n periodično z minimalno periodo 16, $(0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, \ldots)$.

(c) Za $N = 11$ je zaporedje Φ_n periodično z minimalno periodo 10,

$$(0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, \ldots).$$

Lema 2. *Prvi par, ki se ponovi v zaporedju parov $\langle \Phi_1, \Phi_2 \rangle, \langle \Phi_2, \Phi_3 \rangle, \ldots, \langle \Phi_n, \Phi_{n+1} \rangle, \ldots$, je par $\langle 1, 1 \rangle$.*

Dokaz. Ker je največ N^2 različnih parov, poljubna množica $N^2 + 1$ parov vsebuje vsaj dva enaka para. Pa recimo, da je prvi par, ki se ponovi, enak $\langle \Phi_k, \Phi_{k+1} \rangle$, kjer je $k > 1$. Poiščimo torej v zaporedju tak par $\langle \Phi_r, \Phi_{r+1} \rangle$, kjer je $r > k$, da velja $\Phi_k = \Phi_r$ in $\Phi_{k+1} = \Phi_{r+1}$. Iz definicije Fibonaccijevih števil sledi

$$\Phi_{r-1} = \Phi_{r+1} - \Phi_r$$

in

$$\Phi_{k-1} = \Phi_{k+1} - \Phi_k,$$

torej

$$\Phi_{r-1} = \Phi_{k-1}.$$

To pa pomeni, da je
$$\langle \Phi_{r-1}, \Phi_r \rangle = \langle \Phi_{k-1}, \Phi_k \rangle.$$
Toda $\langle \Phi_{k-1}, \Phi_k \rangle$ se v zaporedju pojavi pred $\langle \Phi_k, \Phi_{k+1} \rangle$. To pa je v nasprotju z našo predpostavko, da je $k > 1$. Torej je $k = 1$. ∎

Lema 3. *Za poljubno pozitivno celo število N obstaja med prvimi N^2 Fibonaccijevimi števili vsaj eno, ki je deljivo z N.*

Dokaz. Iz leme 2 sledi, da je $\langle 1, 1 \rangle$ prvi par v zaporedju, ki se ponovi. Torej je $\langle \Phi_t, \Phi_{t+1} \rangle = \langle 1, 1 \rangle$ za neko celo število t, $1 < t \leq N^2 + 1$. Potem je
$$F_t \equiv 1 \pmod{N}$$
in
$$F_{t+1} \equiv 1 \pmod{N}.$$
Toda
$$F_{t-1} = F_{t+1} - F_t$$
in zato je
$$F_{t-1} \equiv 0 \pmod{N}.$$
Naj bo $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Potem je $A = B^2$ in $B^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$. ∎

Lema 4. *Naj bo $N > 2$. Če velja $F_n \equiv 0 \pmod{N}$ in $F_{n+1} \equiv 1 \pmod{N}$, potem je število n sodo.*

Dokaz. Lema je ekvivalentna trditvi, da za $N > 2$ iz $B^n \equiv I \pmod{N}$ sledi, da je n sodo število. Ker je $\det B = -1$, je $\det B^n = (\det B)^n = (-1)^n \equiv 1 \pmod{N}$. Torej je n sodo število. ∎

Dokaz izreka 1. Iz leme 2 in leme 3 sledi, da se vzorec $0, 1, 1$ v zaporedju
$$\Phi_0, \Phi_1, \Phi_2, \ldots, \Phi_n, \Phi_{n+1}, \ldots$$
prvič ponovi za $\Phi_{t-1}, \Phi_t, \Phi_{t+1}$, kjer je $0 < t - 1 \leq N^2$. Iz leme 4 sledi, da je $t - 1$ sodo število. Iz definicije minimalne periode pa dobimo, da velja $2\Pi(N) \leq 2\Pi(N) = t - 1$, kar dokazuje izrek. ∎

Za preslikavo (1) iz pogoja (3) in leme 4 sledi naslednja trditev:

Trditev 5. *Naj bo $N > 2$. Potem velja:*

(a) *T je perioda preslikave (1), če in samo če je $2T$ perioda zaporedja (Φ_n).*

(b) *T je minimalna perioda preslikave (1), če in samo če je $2T$ minimalna perioda zaporedja (Φ_n).*

Dyson in Falk [6] sta dokazala, da veljajo bistveno bolj stroge meje kot v izreku 1.

Izrek 6. **(a)** $\Pi(N) = 3N$, *če in samo če je* $N = 2 \times 5^k$, *kjer je* $k = 1, 2, \ldots$

(b) $\Pi(N) = 2N$, *če in samo če je* $N = 5^k$ *ali* $N = 6 \times 5^k$, *kjer je* $k = 0, 1, 2, \ldots$

(c) $\Pi(N) \leq \frac{12N}{7}$ *za vse preostale* N.

Primer. $\Pi(10) = 30$, $\Pi(5) = 10$, $\Pi(6) = 12$, $\Pi(30) = 60$, $\Pi(2) = 3$, $\Pi(3) = 4$.

Lastnosti, ki jih je Wall v članku [11] dokazal za periode zaporedij (Φ_n), sta Bao in Yang [3] z uporabo trditve 5 združila v naslednje izreke:

Izrek 7. *Naj bo N praštevilo, večje od 5. Potem za preslikavo (1) velja:*

(a) *Če je N oblike $10m \pm 3$, potem je $N + 1$ neka perioda preslikave (1).*

(b) *Če je N oblike $10m \pm 1$, potem je $\frac{N-1}{2}$ neka perioda preslikave (1).*

Primer. Minimalna perioda pa je lahko še bistveno manjša:
$\Pi(29) = 7$, $\Pi(47) = 16$, $\Pi(521) = 13$, $\Pi(9349) = 19$.

Izrek 8. *Če ima N praštevilsko faktorizacijo $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, potem je $\Pi(N)$ najmanjši skupni večkratnik števil $\Pi(p_1^{\alpha_1}), \ldots, \Pi(p_k^{\alpha_k})$.*

Se pravi, da moramo določiti $\Pi(N)$ le še za potence praštevil $N = p^M$. Pri tem je $p = 2$ poseben primer.

Izrek 9. *Če je $p = 2$, potem je $\Pi(2) = \Pi(4) = 3$. Za $M \geq 2$ pa je* $\Pi(2^M) = 3 \times 2^{M-2}$.

Primer. $\Pi(8) = 6$, $\Pi(16) = 12$, $\Pi(32) = 24$.

Za praštevila, večja od 2, računi kažejo, da je $\Pi(p^2) > \Pi(p)$. Velja pa

Slika 6. Skrivno sporočilo in njegov deseti iterat s preslikavo Arnoldove mačke.

Izrek 10. *Naj za praštevilo p velja $\Pi(p^2) \neq \Pi(p)$. Potem za $N = p^M$ velja $\Pi(N) = p^{M-1}\Pi(p)$. Če je k največje tako celo število, da velja $\Pi(p^k) = \Pi(p)$, potem je $\Pi(N) = p^{M-k}\Pi(p)$ za $M > k$.*

Primer. $\Pi(3) = 4$, $\Pi(9) = 12$, $\Pi(27) = 36$, $\Pi(7) = 8$, $\Pi(49) = 56$, $\Pi(343) = 392$.

Posplošena diskretna preslikava Arnoldove mačke

Če v enačbi (1) vzamemo matriko

$$A = \begin{bmatrix} 1+ab & a \\ b & 1 \end{bmatrix},$$

kjer sta a in b naravni števili, dobimo avtomorfizem torusa, saj sta lastni vrednosti različni realni števili, katerih produkt je enak 1. Tako dobljeno preslikavo imenujemo posplošena diskretna preslikava Arnoldove mačke. Posplošena preslikava se uporablja v kriptografiji in steganografiji.

Cilj kriptografíje (grško kryptós – skrit in gráphein – pisati) je narediti podatke neberljive, medtem ko je cilj kriptoanalize razkrivanje šifriranih podatkov [7]. Osnovno sporočilo po navadi imenujemo čistopis (cleartext, plaintext), zašifrirano pa šifropis ali tajnopis (kriptogram, ciphertext). Sporočilo po nekem algoritmu spremenimo v kriptirano sporočilo. Določene vrednosti parametrov, ki jih uporabimo v algoritmu, imenujemo ključ. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila. V stari Grčiji so Špartanci sporočilo zakodirali tako, da so na valj navili ozek trak in sporočilo napisali pravokotno na smer traku. Naslovniku so potem poslali odvit trak in če je želel sporočilo prebrati, je moral trak naviti na valj z enakim premerom. Ključ tega postopka je bil torej premer valja. Julij Cezar je sporočila svojim vojskovodjem zakodiral tako, da je vsako črko zamenjal s črko, ki je bila po abecedi nekaj mest za njo. Matematično tak način kodiranja lahko opišemo kot $f(a) \equiv (a+k) \pmod{n}$, kjer je n število črk v abecedi, k pa ključ. Takih sporočil ni težko dešifrirati, če uporabimo statistično analizo črk, značilnih za določen jezik. Iz daljšega besedila ugotovimo frekvenco določenih črk v jeziku in s primerjavo frekvenc črk v kodiranem besedilu lahko relativno hitro ugotovimo, katera črka pomeni določeno črko, in tako razšifriramo sporočilo. Skozi zgodovino so z uporabo matematike razvili različne postopke šifriranja. Pri moderni kriptografiji je algoritem kodiranja velikokrat znan, torej je poudarek kriptoanalize na odkrivanju ključa. Na Fakulteti za računalništvo v Ljubljani prof. dr. Aleksandar Jurišić vodi Laboratorij za kriptografijo in računalniško varnost in na strani `http://lkrv.fri.uni-lj.si/` je kar nekaj literature s tega področja.

Cilj steganografije (grško steganos – prikrit in gráphein – pisati) je prikrivanje obstoja podatkov [10]. Stari Kitajci so npr. sporočilo napisali na ozek svilen trak, ga tesno zvili, potopili v vosek in tako dobili voščene kroglice, ki jih je nato pogoltnil sel. Med najbolj znanimi metodami steganografije je zapis sporočila s črnilom, ki je pri normalni sobni temperaturi nevidno. Ko list papirja segrejemo, pa se sporočilo obarva rjavo. Kot črnilo lahko uporabimo na primer limonin sok, kis ali mleko.

Ena od možnosti uporabe posplošene preslikave Arnoldove mačke v steganografiji je, da vzamemo sliko, ki ji dodamo skrivno sporočilo, ki ga pred tem transformiramo z eno ali več različnimi preslikavami [8], [9].

Spremenjeno sliko nato pošljemo tistemu, ki mu želimo sporočiti skrivno sporočilo. Z ustreznim ključem lahko naslovnik loči sliko od šifriranega sporočila. Pri tem je pomembno, da s prostim očesom ne ločimo originalne slike od slike z dodanim sporočilom, tako da slika ni sumljiva.

Ker je ranljivost algoritmov večja, če je perioda preslikave kratka, je zelo pomembno poznavanje periode v odvisnosti od parametrov a, b in N [4,5].

Primer. Na sliki 6 je skrivno sporočilo »OMF« in njegov deseti iterat.

Na sliki 7 je na levi originalna slika muce, na desni pa je slika muce z dodanim skrivnim sporočilom. Na vseh slikah je raster enak 124, zato je minimalna perioda $\Pi(124) = 15$. Če ima naslovnik, ki mu je sporočilo namenjeno, originalno sliko muce, lahko dobi šifrirano skrivno sporočilo. Če pozna še ključ, ki je v našem primeru zaporedna številka iterata, lahko dobi originalno skrivno sporočilo. Ker smo sliki dodali deseti iterat sporočila s preslikavo Arnoldove mačke, izračunamo peti iterat šifriranega sporočila.

Slika 7. Muca brez in s skrivnim sporočilom.

Nekaj nalog

1. Vzemimo za A osnovno Arnoldovo matriko in raster $N = 50$.

   (a) Koliko je $\Pi(50)$?

   (b) Kaj pa, če se vprašamo po minimalni potenci p, da je

   $$A^p + I \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{N},$$

   seveda če tak p sploh obstaja?

2. Naj bo A posplošena Arnoldova matrika $A = \begin{bmatrix} 7 & 3 \\ 2 & 1 \end{bmatrix}$ in raster $N = 26$. Koliko je $\Pi(26)$? Kaj pa, če je raster $N = 124$?

3. Ali najdete še kakšno hiperbolično matriko, ki ni oblike $A = \begin{bmatrix} 1+ab & a \\ b & 1 \end{bmatrix}$?

4. Katera celoštevilska matrika dimenzije 2×2 ustreza enačbi $A^3 \equiv I \pmod{5}$?

Rešitve:

1. (a) $\Pi(50) = 150$.
   (b) 75.
2. $\Pi(26) = 14$, $\Pi(124) = 14$.
3. Primera takih matrik: $\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$ in $\begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$.
4. Primera takih matrik: $\begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}$ in $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$.

LITERATURA

[1] V. I. Arnold, *Mathematical Methods of Classical Mechanics*, Springer, 1989.

[2] V. I. Arnold in A. Avez, *Ergodic problems in Classical Mechanics*, Benjamin, New York, 1968.

[3] J. Bao in Q. Yang, *Period of the discrete Arnold cat map and general cat map*, Nonlinear Dynam. **70** (2012), 1365–1375.

[4] F. Chen, K. Wong, X. Liao in T. Xiang, *Period distribution of generalized discrete Arnold cat map for $N = p^e$*, IEEE T. Inform. Theory **58** (2012), 445–452.

[5] F. Chen, X. Liao, K. Wong, T. Xiang, Q. Han in Y. Li, *Period distribution of some linear maps*, Commun. Nonlinear Sci. Numer. Simulat. **17** (2012), 3848–3856.

[6] F. Dyson in H. Falk, *Period of a Discrete Cat Mapping*, Amer. Math. Monthly **99** (1992), 603–614.

[7] *Kriptografija*, dostopno na: `http://www.egradiva.net/moduli/upravljanje\_ik/14\_kriptiranje/01\_datoteka.html`, ogled 3. 6. 2015.

[8] M. Mishra, A. R. Routray in S. Kumar, *High Security Image Steganography with Modified Arnold's Cat Map*, Int. J. Comput. Appl. **37** (2012), 16–20.

[9] S. Rawat in B. Raman, *A chaotic system based fragile watermarking scheme for image temper detection*, Int. J. Electron. Commun. **65** (2011), 840–847.

[10] *Steganografija*, dostopno na: `http://www.monitor.si/clanek/skrivanje-podatkov-steganografija/123365/?xURL=301`, ogled 3. 6. 2015.

[11] D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly **67** (1960), 525–532.

BARVNI VID

ALEŠ MOHORIČ

Fakulteta za matematiko in fiziko, Univerza v Ljubljani
Institut Jožef Stefan

PACS: 42.66.Ne

V članku so predstavljeni človeški barvni vid, osnove barvnih sistemov in način, kako prikažemo barvo določenega svetlobnega spektra z dostopno programsko opremo.

COLOR VISION

The article describes human color vision, basics of color systems and a way of representing color of a light with a given spectrum by readily available software.

Kadar pri pouku obravnavamo mavrico ali interferenco na uklonski mrežici, brez zadrege opišemo mavrične barve. Pri opisu interferenčnih barv milnične opne ali plasti olja na luži pa imamo že težave. To je zato, ker barve v prvem primeru opišemo z enobarvno svetlobo in vsaki barvi pripišemo svetlobo določene valovne dolžine. V drugem primeru nastanejo barve s sestavljanjem enobarvnih svetlob različnih spektralnih gostot in enostavnega odgovora niti ne moremo dati. Za določeno smer opazovanja enostavno povemo le, katera enobarvna sestavina je v tej smeri najbolj ojačana in katera najbolj oslabljena. To velja za primere, ko nastane opazovani pojav zaradi bele svetlobe. Težav z opisom nimamo, ko pojav povzroči enobarvna svetloba. Tedaj vidimo le bolj ali manj svetle točke iste barve. Slika na naslovnici kaže a) mavrične barve, ki nastanejo z interferenco svetlobe iz žarnice na uklonski mrežici, in b) milnično opno, na kateri nastanejo barve zaradi odboja in interference sončne svetlobe na tanki plasti.

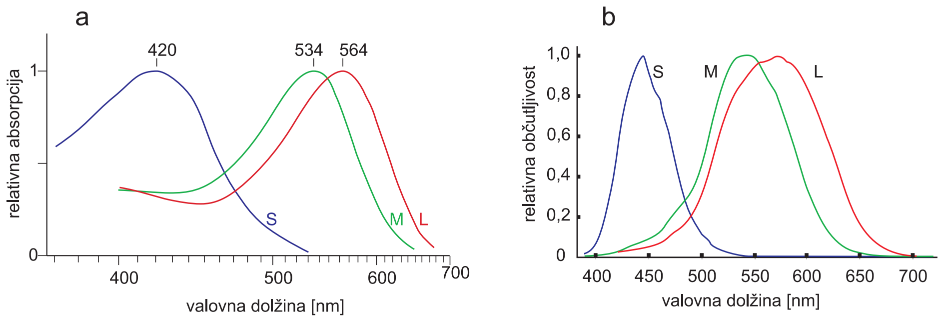
V fiziki svetlobo, ki je sestavljena iz množice enobarvnih sestavin, opišemo s spektrom. Spekter je porazdelitev gostote energijskega toka svetlobe po valovni dolžini. Svetlobni tok merimo s fotometri. Fotometri so umerjeni fotodetektorji in jih je več vrst. Nekateri temeljijo na merjenju temperature senzorja, ki ga greje vpadni svetlobni tok. Taki so bolometri: termouporniki, počrnjeni termočleni in termistorji. Ti detektorji so občutljivi za vse valovne dolžine enako. Občutljivost fotometrov, ki temeljijo na fotoefektu (fotocelice in fotopomnoževalke), polprevodniških fotometrov (fotodiode, sončne celice, CCD) ter kemičnih detektorjev (fotografski film) je odvisna od valovne dolžine svetlobe. Spektralne lastnosti svetlobe merimo tako, da svetlobo razklonimo s prizmo ali uklonsko mrežico. Iz šopa razklonjene svetlobe z zaslonko izberemo tanek curek enobarvne svetlobe in njen tok izmerimo s fotometrom. Spekter enobarvne ali monokromatične svetlobe ima pri ustrezni valovni dolžini en ozek vrh, ki ga imenujemo tudi črta, drugje pa je enak nič. Spekter sončne svetlobe ali svetlobe žarnice je zvezen in ga približno opišemo s Planckovim spektrom sevanja črnega telesa. Spekter svetlobe atomov plina, ki se relaksirajo iz vzbujenih stanj, je črtast. V splošnem je spekter svetlobe mešanica zveznega in črtastega spektra. Taka svetloba v očeh (pravzaprav v možganih) ustvari občutek, ki mu pripišemo svetlost in barvo. Svetlost je povezana z gostoto energijskega toka svetlobe, ki vpada na očesno zenico. Kakšna pa je barva, ki ustreza določenemu spektru? Odgovor dobimo, če si podrobneje ogledamo, kako deluje barvni vid pri ljudeh.

Oko

Svetlobo zaznavamo z očmi. Roženica in leča preslikata osvetljen predmet ali svetilko na mrežnico. V mrežnici sta dve vrsti svetlobnih čutnic: paličnice in čepnice. V normalnem očesu je preko 100 milijonov paličnic in več kot 6 milijonov čepnic. V točki na mrežnici, ki leži blizu optične osi očesne leče, je gostota (število na ploskovno enoto) čepnic največja. To področje mrežnice imenujemo rumena pega. Osrednji del rumene pege ima polmer 1,25 mm in gostota čepnic tam doseže 150 000 mm^{-2}. Drugod po mrežnici prevladujejo paličnice. Njihova gostota je približno homogena in tudi enaka 150 000 mm^{-2}. Na mrežnici razločimo še slepo pego. V njej vidni živec vstopa v mrežnico in na tem delu mrežnica nima čutnic. Tega dela vidnega polja oko ne zazna. Pri vidu nas to ne moti, saj oči stalno premikamo in možgani poskrbijo za primerno interpretacijo slike.

V razmerah šibke svetlobe so v mrežnici aktivne paličnice. Tak vid imenujemo skotopični vid. Skotopični vid je črno-bel; s paličnicami samo zaznavamo svetlobo, barv pa ne. Ponoči smo barvno slepi. Gostota paličnic je v rumeni pegi zanemarljivo majhna, zunaj pa je večja in približno konstantna. To je razlog, zakaj vidimo ponoči šibke zvezde bolje zunaj osi zornega polja. V razmerah močne svetlobe so v mrežnici aktivne čepnice. Tak vid je fotopični vid. V normalnem očesu so tri vrste čepnic, barvno slepi pa jih imajo manj.

Občutljivost čepnic je odvisna od valovne dolžine svetlobe in se razlikuje med vrstami čepnic. Spektralno občutljivost posameznih čepnic določajo na vzorcu ljudi. Pri enem od načinov merjenja merijo absorpcijo svetlobe v čepnicah. To metodo imenujemo mikrospektrofotometrija. Rezultati teh meritev so opisani v [1] in jih kaže slika 1a. Pri teh meritvah ne izmerijo absorpcijskih lastnosti zrkla pred mrežnico, lahko pa to dodatno upoštevajo s primernimi popravki. Drug način merjenja spektralne občutljivosti čepnic je psihofizičen. V tem primeru merijo tako, da dve vrsti čepnic opazovalca desenzibilizirajo z dovolj močnim in dolgotrajnim osvetljevanjem s svetlobo primerne valovne dolžine. Valovna dolžina mora biti taka, da nasiti čutnice, katerih občutljivosti ne merimo, merjene čutnice pa je ne zaznavajo. Po desenzibilizaciji se meri občutljivost na enobarvno svetlobo z opazovanjem utripajoče svetlobe. Te meritve primerjajo z meritvami spektralne občutljivosti pri barvno slepih dikromatih (protanopi – brez čepnic L, devteranoji – brez čepnic M in zelo redki tritanopi – brez čepnic S). Spektralne občutljivosti treh vrst čutnic, ki so rezultati meritev v [5], kaže slika 1b.



Slika 1. a) Relativna spektralna občutljivost čepnic, merjena z mikrospektrofotometrijo, pri kateri merijo absorpcijo svetlobe v čutnicah, in b) relativna spektralna občutljivost čepnic, določena s psihofizičnimi meritvami. Na obeh grafih prepoznamo tri različne vrste čepnic. Čepnice bolj občutljive za kratkovalovno svetlobo imenujemo S, čepnice občutljive na srednjevalovno svetlobo M in čepnice občutljive na dolgovalovno svetlobo L.

Meritve pokažejo, da so čepnice treh različnih vrst. Čepnice vrste L (iz ang. Long wavelength) so najbolj občutljive na svetlobo dolgih valovnih dolžin. Čepnice vrste M (iz ang. Middle wavelength) so najbolj občutljive na svetlobo srednjih valovnih dolžin. Intervala valovnih dolžin, za katere so občutljive čepnice L in M, sta dokaj podobna. Tretji tip čepnic je S (iz ang. Short wavelength). Te čepnice so najbolj občutljive za najkrajše valovne dolžine vidne svetlobe. Nekdaj so čepnice imenovali rdeča, zelena in modra, vendar to imenovanje ni ustrezno. Vsako od teh barv zazna več vrst čepnic, ne le ena. Tudi največje občutljivosti čutnic ne ustrezajo tem barvam, temveč po vrsti rumenozeleni, zeleni in vijolični.

Razlike v barvnih vtisih različnih spektrov nastanejo zato, ker so razmerja živčnih signalov posameznih čepnic drugačna. Enako razmerje signalov lahko dosežemo z različnimi svetlobnimi spektri. Npr. mešanica rdeče in zelene enobarvne svetlobe ustvari v možganih enak vtis kot rumena enobarvna svetloba.

Barvni sistemi

Tribarvni vid je preslikava iz Hilbertovega prostora spektralnih gostot v trirazsežni realni prostor (signali treh različnih čepnic). Barvni vtis vsake svetlobe lahko reproduciramo s primerno kombinacijo svetlob treh osnovnih barv. Te tri osnovne barve so baza trirazsežnega barvnega prostora. V tem prostoru vsaka barva, ki jo razloči oko, ustreza točki znotraj konveksnega lika. Lik je konveksen zato, ker ima kombinacija svetlob poljubnih dveh barv tudi neko vidno barvo. Za osnovne barve lahko vzamemo katerekoli tri različne barve, s katerimi lahko vzbudimo vse tri vrste čepnic. Pri izbiri osnovnih barv upoštevamo možnost realizacije in spektralne občutljivosti čepnic. Svetlobe morajo imeti take valovne dolžine, da jih enostavno reproduciramo s svetili ali barvili. Poleg tega barve svetlob ne smejo biti preveč podobne, da nimamo težav z ločevanjem podobnih barv in premajhnim barvnim obsegom. Barvni obsegi (gamut) različnih barvnih sistemov niso enaki. Z nekaterimi sistemi ne moremo opisati vseh barv, ki jih lahko zazna oko.

Praktičnih barvnih sistemov je več vrst. Najbolj naravni je kar sistem SML, ki temelji na občutljivosti čepnic. Uporabna in znana sta še sistem RGB, ki ga uporabljamo za aditivno mešanje barv pri barvnih prikazovalnikih, in sistem CMYK, ki ga uporabljamo pri barvnem tisku. Oznaka RGB sledi iz začetnic angleških izrazov za osnovne barve: Red (rdeča), Green (zelena) in Blue (modra). CMYK je akronim za sinja (Cyan), škrlatna (Magenta) in rumena (ang. Yellow), ki so osnovne barve pri subtraktivnem mešanju barv. Ker mešanica vseh treh ne ustvari črne ampak sivorjavo, pri tisku uporabljamo dodatno črno barvilo (ang. Key ali blacK). Pomanjkljivost sistemov RGB in CMYK je, da je njun barvni obseg manjši od obsega očesa. Prehod med barvnimi sistemi je enostaven – vrednosti v enem sistemu preslikamo v vrednosti drugega sistema z matriko 3×3.

Opišimo poskus, s katerim določijo sistem RGB. V referencah [4, 6] so osnovne barve naredili s tremi svetilkami z enobarvnimi svetlobami valovnih dolžin 436 nm (modra), 546 nm (zelena) in 700 nm (rdeča). Te svetilke so svetile v primerjalno polovico vidnega polja. To polje so opazovali udeleženci poskusa, ki so prilagajali jakosti svetilk, dokler se ni barva mešanice njihovih svetlob v primerjalnem polju ujemala z barvo, ki jo je na drugi, testni polovici vidnega polja ustvarjala enobarvna svetilka. Poskus so ponovili pri vrsti različnih enobarvnih svetlob. Zorna velikost testnega polja je bila 2°, zato da v zaznavi sodelujejo le čutnice z rumene pege. Na opisani način so katerikoli valovni dolžini enobarvne svetlobe v testnem polju pripisali tri vrednosti – jakosti, s katero v primerjalno polje svetijo svetilke osnovnih barv, ki razpenjajo barvni prostor RGB. Ustrezno normirane vrednosti teh jakosti so funkcije barvnega ujemanja $r(\lambda)$, $g(\lambda)$, $b(\lambda)$. Grafe funkcij barvnega ujemanja sistema RGB kaže slika 2a. Funkcije so normirane tako, da so ploščine pod vsemi krivuljami enake. Vrednosti treh funkcij pri neki valovni dolžini povedo, v kakšnem razmerju moramo zmešati svetlobe svetilk osnovnih barv, da ustvarimo barvni vtis enobarvne svetlobe s to valovno dolžino: $j(\lambda) \equiv r(\lambda)j_r + g(\lambda)j_g + b(\lambda)j_b$. Moči svetilk so v fiziološkem merilu med seboj v razmerju $j_r : j_g : j_b = 1 : 4{,}6 : 0{,}060$. Vrednosti funkcij barvnega ujemanja ustrezajo moči svetilk tako, da bela svetloba nastane takrat, ko se na opazovanem polju mešajo med seboj rdeča, zelena in modra svetloba s svetlostmi v razmerju $1 : 4{,}6 : 0{,}060$. Tako normiranje funkcij barvnega ujemanja je izbrano zato, ker je oko za zeleno svetlobo bolj občutljivo kot za modro ali rdečo, želimo pa, da je razpon posameznih barvnih komponent približno enak. Razmerja so določena tako, da se vsota normiranih funkcij barvnega ujemanja z ustreznimi utežmi ujema s spektralno občutljivostjo očesa $V(\lambda) = r(\lambda) + 4{,}6g(\lambda) + 0{,}060b(\lambda)$. Podroben opis normiranja funkcij barvnega ujemanja je v [3].

V intervalu okoli 500 nm so vrednosti funkcije ujemanja za rdečo svetlobo negativne, kar pomeni, da barvnega vtisa svetlobe tiste valovne dolžine ne moremo reproducirati z mešanico primarnih barv. Namesto tega moramo z rdečo svetlobo ustrezne jakosti posvetiti na testni del ploskve, kar seveda spremeni iskano barvo. Tako je, na nekoliko nenavaden način, definirano odštevanje v barvnem prostoru.

Ker so v sistemu RGB nekatere vrednosti funkcij barvnega ujemanja negativne in obstaja več različnih dogovorov, je ICE (Mednarodna zveza za razsvetljavo) sprejela enotni standardizirani barvni sistem XYZ [8]. Funkcije barvnega ujemanja tega sistema kaže slika 2b. Krivulje približno opišemo z Gaussovimi funkcijami ali njihovimi vsotami:

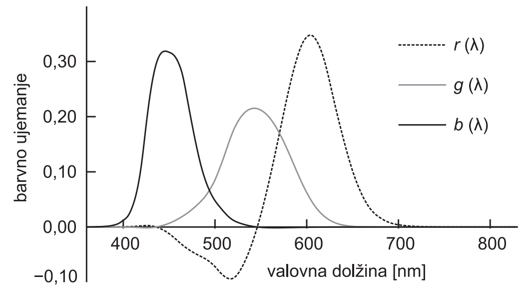
$$
\begin{aligned}
x(\lambda) &= 0{,}401 \exp\left(-\left(\frac{\lambda - 444}{28{,}1}\right)^2\right) + 1{,}13 \exp\left(-\left(\frac{\lambda - 593}{48{,}6}\right)^2\right),\\
y(\lambda) &= 1{,}01 \exp\left(-\left(\frac{\lambda - 556}{65{,}3}\right)^2\right),\\
z(\lambda) &= 2{,}06 \exp\left(-\left(\frac{\lambda - 448}{31{,}9}\right)^2\right).
\end{aligned}
$$

Valovne dolžine moramo v zgornjih izrazih vstaviti v nanometrih.

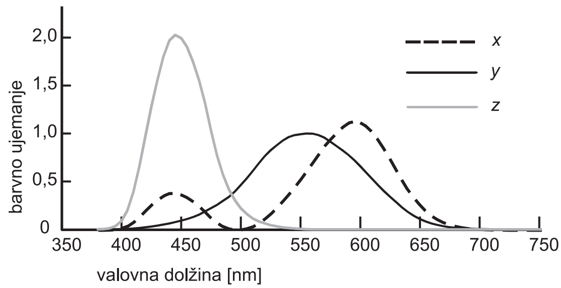
V barvnem sistemu XYZ izračunamo komponente svetlobe, ki jo opiše spekter $I(\lambda)$, z integrali:

$$X = \int_{380}^{780} I(\lambda)x(\lambda)d\lambda, \quad Y = \int_{380}^{780} I(\lambda)y(\lambda)d\lambda \quad \text{in} \quad Z = \int_{380}^{780} I(\lambda)z(\lambda)d\lambda.$$

a)



b)



Slika 2. a) Grafi treh funkcij barvnega ujemanja sistema RGB. Vrednosti funkcij pri določeni valovni dolžini so povezane z jakostmi enobarvnih svetlob primarnih barv, ki aditivno zmešane ustvarijo enak barvni vtis kot enobarvna svetloba s to valovno dolžino. Navpična skala je izbrana tako, da imajo vse krivulje enako ploščino. Negativne vrednosti rdeče v intervalu okoli 500 nm pomenijo, da barv v tem intervalu ne moremo realizirati s kombinacijo izbranih osnovnih barv. Namesto na primerjalno polje moramo z rdečo svetlobo posvetiti na testno polje. b) Grafi funkcij barvnega ujemanja barvnega sistema XYZ [8].

Ti integrali pomenijo projekcijo Hilbertovega prostora (spektra svetlobe) na trirazsežni prostor komponent X, Y in Z, ki ustrezajo določeni barvi. Z dogovorom [8] so spekter $I(\lambda)$ in funkcije barvnega ujemanja normirani tako, da ima spekter sevanja črnega telesa, segretega na 2856 K (standardno svetilo A), vrednost 100 pri valovni dolžini 560 nm in valovno dolžino v integralih izrazimo normirano na nanometer.

Funkcije barvnega ujemanja v sistemu XYZ so izbrane tako, da y približno ustreza občutljivosti čutnic M. V razmerah močne svetlobe normalno oko dojema svetlobo zelenega dela spektra svetleje kot rdečo ali modro svetlobo enake moči. Povprečna svetlobna občutljivost očesa se približno ujema s spektralno občutljivostjo čepnic M. V sistemu XYZ zato svetlost ustreza komponenti Y. Funkcija $z(\lambda)$ ustreza občutljivosti očesa za modro barvo (občutljivosti čepnic S). Funkcija $x(\lambda)$ je taka kombinacija odzivov čepnic, da nobena od funkcij barvnega ujemanja ni negativna.

Pri taki definiciji sistema pomeni komponenta Y svetlost barve, komponenti X in Z pa opišeta vse barvne odtenke pri tej svetlosti. Zato trojico X, Y in Z lahko prikažemo s trojico (x, y, Y), kjer sta deleža barvnih vrednosti definirana z $x = X/(X + Y + Z)$ in $y = Y/(X + Y + Z)$. Projekcija ploskve $X + Y + Z = 1$ na ravnino (x, y) je lik z obliko podkve. Na ukrivljenem delu oboda tega lika so spektralne barve, krajišča krakov podkve pa povezuje škrlatna daljica. Lik imenujemo barvni diagram CIE. Točke v liku določajo deleže barvnih vrednosti. Barvni diagram CIE kaže slika c na naslovnici.

Barve, kot jih zazna oko, lahko merimo s kolorimetri. V kolorimetru merimo svetlobo, ki na detektor vpada skozi različne barvne filtre. Če so spektralne prepustnosti filtrov poznane, iz izmerjenih signalov lahko izračunamo komponente barve v barvnem sistemu. Kolorimetre uporabljajo za preverjanje barv barvnih zaslonov in v barvnem tisku.

Zgledi

Opišimo nekaj zgledov, v katerih opazujemo znane spektre svetlobe, ki jim želimo določiti barvo. Prvi zgled je na uklonski mrežici uklonjena svetloba curka bele svetlobe (slika a na naslovnici). Bela svetloba se po prehodu ukloni tako, da je pod nekim kotom glede na smer prvotnega curka svetloba enobarvna. Spekter enobarvne svetlobe je črta (porazdelitev delta) pri določeni valovni dolžini. Komponente barvnega prostora za enobarvno svetlobo z relativno gostoto svetlobnega toka 1 so kar enake vrednostim funkcij barvnega ujemanja $X = x(\lambda)$, $Y = y(\lambda)$ in $Z = z(\lambda)$. Slika d na naslovnici kaže trak mavričnih barv, ki je sestavljen iz ožjih trakov, katerih barve po vrsti od leve proti desni ustrezajo enobarvnim svetlobam vedno večje valovne dolžine. Za risanje uporabimo program, ki zna interpretirati barve v prostoru XYZ. Za prikaz na zaslonu te barve potem pretvorimo v prostor RBG, za tisk pa v prostor CMYK. Primeren program je npr. Mathematica, s katerim sliko izrišemo z ukazom:

```
sp=Table[{XYZColor[x[l],y[l],z[l]],
Rectangle[{l,0},{l+1,100}]},{l,300,800,1}];
Graphics[Flatten[sp,1]]
```

Enostavno lahko pojasnimo tudi, kako lahko svetlobi z različnima spektroma ustvarita v možganih enak barvni vtis. Npr. enobarvna rumena svetloba z valovno dolžino 573 nm in normirano jakostjo ena ima komponente barvnega prostora enake $X = 0{,}95$, $Y = 0{,}94$ in $Z = 0$. Komponenti X in Y sta približno enaki, komponenta Z pa je enaka 0. Enobarvna zelena svetloba z valovno dolžino 549 nm in normirano jakostjo 1 ima komponente $(0{,}50, 1{,}0, 0)$, rdeča svetloba z valovno dolžino 665 nm in normirano jakostjo 1 pa $(0{,}13, 0{,}062, 0)$. Če zmešamo zeleno svetlobo z normirano jakostjo 0,9 in rdečo z normirano jakostjo 4, dobimo v očesu enak vtis kot z rumeno svetlobo: $(0{,}95, 0{,}94, 0) = 0{,}9(0{,}50, 1{,}0, 0) + 4(0{,}13, 0{,}062, 0)$. Tako mešanje barv demonstrira slika e na naslovnici. V splošnem velja, da linearna kombinacija katerihkoli barv, ki jih predstavimo v prostoru XYZ, ustvari neko barvo, ki jo lahko predstavimo v tem prostoru.

Opišimo barvo segretega črnega telesa. Spekter segretega črnega telesa opiše Planckov zakon:

$$I_{ct}(\lambda, T) \propto \frac{1}{\lambda^5\left(\exp\left(\frac{hc}{\lambda kT}\right) - 1\right)}.$$

Tu so h Planckova konstanta, c svetlobna hitrost, k Boltzmannova konstanta in T absolutna temperatura. Normiranje spektra je opisano v razdelku Barvni sistemi.

Rezultat predstavimo tako, da zaporedno narišemo trakove v barvah, ki ustrezajo vedno višji temperaturi (slika f na naslovnici). Telesa s sobno temperaturo sevajo večino svetlobe v infrardečem delu spektra in jih z očmi ne opazimo (opisujemo črno telo). Pri temperaturi okoli 1000 K telo žari v rdeči barvi. Ko temperatura telesa narašča, se barva preko oranžne in rumene spremeni v belo, ki ustreza telesu, segretemu na 6000 K. To je temperatura površja Sonca in njegovo svetlobo oko zazna kot belo. Še bolj segreta telesa imajo modrikast barvni ton.

Opišimo še barve tanke milnične plasti, od katere se odbija bela svetloba. Človeško oko je prilagojeno na sončno svetlobo in kot belo – barvo brez tona – zazna sončno svetlobo, to je svetloba črnega telesa, segretega na 6000 K. Žarnice so segrete na nižjo temperaturo (pod 3000 K) in njihovo svetlobo vidimo kot nenasičeno rumeno, vendar še vedno približno belo. Vprašanje, kakšen je barvni vtis svetila, zelo zanima industrijo svetil. V našem zgledu bomo kot belo svetlobo vzeli svetlobo s konstantnim spektrom. Spekter svetlobe, odbite pod pravim kotom, lahko opišemo z izrazom:

$$I_m(\lambda, d) \propto \cos^2\left(\frac{n2\pi d}{\lambda} + \frac{\pi}{2}\right).$$

Tu je n lomni kvocient snovi v tanki plasti in d je debelina plasti. Slika g na zadnji strani kaže barvo plasti v odvisnosti od debeline plasti od 0 nm do 1500 nm. To sliko lahko primerjamo s sliko b na naslovnici vendar moramo upoštevati, da se debelina milnične plasti zaradi teže spreminja z višino (na dnu je večja kot na vrhu), vendar ne sorazmerno.

Sklep

Modeli barvnih prostorov ne ponujajo popolnega opisa barvnega vida. Barvo opišejo le s tremi parametri in ne upoštevajo percepcije – prilagajanja čutnic na svetlobo, razlike signalov sosednjih čutnic, vpliva obrobja vidnega polja, vpliva paličnic idr. Popolnejši in matematično bolj zahtevni so modeli barvnega zaznavanja, v katerih barvo opišemo z njenim tonom, svetlostjo, sijajem, nasičenostjo, polnostjo in kromo [2]. Opis teh modelov presega okvir tega članka.

LITERATURA

[1] J. Bowmaker in H. Dartnall, *Visual pigments of rods and cones in a human retina*, J. Physiol. 298: 501–511 (1980).

[2] D. Javoršek, *Od CIE kolorimetrije do modelov barvnega zaznavanja*, Tekstilec **55** (2012), 3, 176–183.

[3] V. C. Smith in J. Pokorny, *The Science of Color*, Elsevier, 2003.

[4] W. Stiles in J. Burch, *N. P. L. Colour-matching Investigation: Final Report*, Optica Acta *6* (1959), 1, 1–26.

[5] A. Stockman, D. MacLeod in N. Johnson, *Spectral sensitivities of the human cones*, J. Opt. Soc. of America A **10** (1993), 2491–2521.

[6] W. D. Wright, *A re-determination of the trichromatic coefficients of the spectral colours*, Transactions of the Optical Society **30** (1928), 4, 141–164.

[7] G. Wyszecki in W. Stiles, *Colour Science*, London: J. Wiley (1967).

[8] `http://www.cie.co.at/index.php/LEFTMENUE/index.php?i_ca_id=298`, ogled: 3. 6. 2015.

Na naslovnici: a) Barvni vzorec, ki nastane na zaslonu po uklonu svetlobe žarnice na uklonski mrežici. Na določeni razdalji navzgor ali navzdol od belega traku na sredini slike so ozki, vodoravni trakovi različnih barv. Vsaki barvi lahko pripišemo enobarvno svetlobo z določeno valovno dolžino. b) Odsev sončne svetlobe na milnični opni. Opazimo barve, ki jim ne moremo pripisati enobarvne svetlobe, npr. sinja ali škrlatna. c) Barvni diagram CIE. V diagram sta vrisana še barvni podprostor, ki ga razpenja sistem RGB, in točka beline. Po loku so nanizane spektralne barve, krajišči loka povezuje škrlatna daljica. d) Navpični trakovi mavričnih barv enobarvne svetlobe, valovna dolžina narašča od leve (300 nm) proti desni (800 nm). e) Z aditivnim mešanjem zelene in rdeče enobarvne svetlobe ustvarimo v možganih enak barvni vtis kot z enobarvno rumeno svetlobo. f) Barva segretega črnega telesa kot funkcija temperature. Temperatura telesa narašča z leve proti desni od 1000 K do 10 000 K. Telo z nizko temperaturo žari rdeče, zelo vroča telesa pa so modrikasta. Telo s temperaturo 6000 K (temperatura površja Sonca) je videti belo.

Na zadnji strani: g) Barve milnične opne po pravokotnem vpadu bele svetlobe s konstantnim spektrom v odvisnosti od debeline plasti. Barve niso mavrične in jih ne moremo opisati le s svetlobo ene valovne dolžine, temveč s spektrom. Čim debelejša je plast, manj nasičene so barve. Videti so, kot da bi bile zmešane z belo. To sliko lahko primerjamo s sliko b, vendar moramo upoštevati, da debelina milnične plasti na sliki b ne narašča sorazmerno z oddaljenostjo od vrha zanke.

MOTIVACIJA ZA ŠTUDIJ FIZIKE

ALEŠ MOHORIČ

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Ste se kdaj vprašali, kaj vas je zmamilo v fiziko? Kakorkoli se kot posamezniki razlikujemo, v mnogočem smo si podobni. Tako so podobne tudi vzpodbude in želje, ki nas zapeljejo v študij. Nekatere so bolj pomembne, nekatere manj. Med seboj se razlikujemo po teži, ki jo pripisujemo določenemu razlogu, v večjem številu pa vendarle opazimo vzorec. Ta vzorec smo na skupini enainšestdesetih letošnjih brucev fizike ugotavljali z vprašalnikom. Vprašalnik je sestavljen iz dvajsetih izjav, s katerimi študenti izrazijo strinjanje na petstopenjski lestvici, vprašanj odprtega tipa ter nekaterih vprašanj za ugotavljanje statistike. Vprašalnik je nastal na podlagi sprejemnega intervjuja na Imperial College of London, ki ga že dolga leta vodi Gareth Jones. Vprašalnik je za širšo rabo priredila prva delovna skupina svetovne fizikalne mreže projekta Hope [1]. Vprašalnik so izpolnjevali še v enaintridesetih evropskih državah.

Študentom je bilo zastavljeno vprašanje: kaj vas je motiviralo za študij fizike? Sledila je vrsta izjav z lestvico od 1 (sploh ni pomembno, ne drži) do 5 (zelo je pomembno, popolnoma drži), in študenti so izjavi podelili število točk, ki najbolj ustreza njihovemu prepričanju. Sledi seznam izjav, poleg izjav je zapisano povprečno število točk pri tej izjavi in standardni odklon, kot smo jih dobili za naše študente. Izjave so urejene po vrsti glede na povprečno število točk, številka pred izjavo kaže njeno mesto v nizu.

8.	Želja, da bi razumel/a svet okoli sebe	$4{,}7 \pm 0{,}5$
13.	Želja po razumevanju, kako reči delujejo	$4{,}5 \pm 0{,}7$
16.	Želja po zanimivi službi	$4{,}4 \pm 0{,}8$
1.	Želja, da bi zares dobro razumel/a vesolje	$4{,}3 \pm 0{,}9$
14.	Želja po učenju višje fizike (npr. kvantne mehanike)	$4{,}2 \pm 0{,}9$
17.	Želja postati fizik – znanstvenik	$4{,}1 \pm 1{,}0$
19.	Fizika je predmet, ki mi leži bolje kot drugi predmeti	$3{,}7 \pm 1{,}2$
15.	Želja po tem, da bi znal/a na fizikalnih temeljih sestaviti ali/in uporabiti napravo, npr. teleskop	$3{,}6 \pm 1{,}1$
2.	Želja, da bi si povečal/a možnosti zaposlitve	$3{,}5 \pm 1{,}0$
12.	Internet, spletne strani s fizikalno tematiko, filmi na YouTube-u, ...	$3{,}4 \pm 0{,}9$

6.	Prebiranje knjig in revij	3,3 ± 1,2
5.	Dokumentarne oddaje s fizikalnimi vsebinami na TV	3,2 ± 1,1
4.	Učitelj fizike	3,1 ± 1,3
10.	Obiski znanstvenih laboratorijev (na fakulteti), CERN-u, ...	2,9 ± 1,3
9.	Obiski muzejev in specializiranih razstav	2,6 ± 1,0
20.	Starši in družina	2,5 ± 1,2
11.	Obiski znanstvenikov ali študentov s fakultete na naši šoli	2,1 ± 1,1
7.	Raziskovalec v družini	2,0 ± 1,3
3.	Spodbuda sošolcev/prijateljev	1,9 ± 1,1
18.	Želja postati učitelj fizike	1,9 ± 1,0

Sledijo odprta in statistična vprašanja s povzetki odgovorov.

21. Prosimo, napiši še druge razloge, ki so pomembno vplivali na tvoje zanimanje za študij fizike.

    Navajam najpogosteje omenjene razloge. Fizika: je zanimiva, je zahtevna, je izziv, je najpomembnejša, je matematična, je logična, razširi pogled na svet, je prestižna, zanjo se ni treba učiti na pamet, omogoča dobro zaposlitev, je na višjem nivoju kot drugi inženirski programi.

    Zanima me: vesolje, teoretična fizika, reševanje matematičnih problemov.

    Vpliv: učiteljev, staršev, tekmovanj, projektov, televizijskih osebnosti.

22. Pri kateri starosti te je fizika začela zelo zanimati?

    Izprašane bruce je fizika začela zelo zanimati pri povprečni starosti 13 let.

23. Pri kateri starosti si se odločil/a za študij fizike?

    Izprašani bruci so se za študij fizike odločili pri povprečni starosti 17 let.

24. Kateri drugi predmeti so še prišli v ožji izbor za študij?

    matematika 18, strojništvo 11, računalništvo 10, kemija 7, elektrotehnika 5, medicina 3, ekonomija 3, jeziki 2, biokemija 2, biologija 2, geografija 2, filozofija 2, arhitektura 2, gozdarstvo, fotografija, elektronika, glasba, zgodovina, šport, veterina, diplomacija, psihologija

25. Katera posebej pomembna okoliščina ali razlog te je navdihnila za študij fizike?

    dobri učitelji 4, knjiga 2, starši 2, naključje, korist, ugled, televizija, zaposlitvene možnosti, zvedavost, posebna teorija relativnosti, astrofizika, vesolje, skepticizem, krofi, fizika: je zanimiva, me veseli, je raznolika

26. Si fant ali dekle?

    Dve tretjini (42) je fantov in tretjina (19) deklet.

27. Si obiskoval/a fantovsko, dekliško ali mešano šolo?

    Mešano (vprašanje za Slovenijo ni smiselno, je pa za tujino, anketa je mednarodna).

28. Katero srednjo šolo si končal/a (gimnazijo, tehnično gimnazijo, ...)?

    Večina (57) gimnazija, drugi tehnična gimnazija.

29. Na katerem programu študiraš?

    90 % (54) fizika ter po 5 % (3) astrofizika in (4) meteorologija.

Iz podanih odgovorov si vsak lahko sam ustvari sliko o motivacijah naših študentov. Na hitro lahko strnem, da so med najpomembnejšimi motivacijami za študij želja po razumevanju sveta okoli nas, delovanju reči in razumevanju vesolja ter želja po zanimivi službi. Najmanj pomemben se zdi vpliv prijateljev in sošolcev in večina brucev ne razmišlja o učiteljski karieri. Zadnja izjava drži sicer le v povprečju. Med posameznimi odgovori je nekaj takih, katerim je učiteljski poklic pomemben. Kot kaže, tudi obiski znanstvenikov in študentov s fakultete na šolah niso zelo pomembna motivacija. Iz odgovorov na odprta vprašanja sledi, da študentje dojemajo fiziko kot zahteven, vendar zanimiv študij. Rezultati pri izjavah 20, 7 in 3 kažejo, da od domačih vzpodbude in zgleda v povprečju ni prav veliko, vendar pa relativno velik odklon in odgovori na vprašanje 25 kažejo, da pri delu vzorca vseeno močno vplivajo. To velja tudi za učitelje fizike v srednji šoli, ki so še pred knjigami, televizijo in internetom najpomembnejši motivatorji. Odgovori na vprašanje 25 so na videz v nasprotju z izjavo 4, a se je treba zavedati, da je število točk le povprečje. Iz vprašanj odprtega tipa je jasno, da učitelji na nekatere dijake močno vplivajo. Poleg fizike in narave same so ravno učitelji najboljša reklama za študij.

Nobenega presenečenja ni, katerim programom je fizika konkurirala, ko so se odločali za študij. Največ jih je v naravoslovju in tehniki. Prva je matematika, nato strojništvo, računalništvo ter kemija, kar ni presenečenje.

Med študenti dokaj krepko prevladujejo fantje, vendar ne več tako kot včasih. Večina brucev prihaja z gimnazij. Za fiziko se v povprečju začnejo zanimati pri starosti trinajst let, s sedemnajstimi pa se odločijo za študij.

Rezultati v celoti niso presenetljivi, lahko pa koristijo snovalcem študijskega programa z idejami, kaj pričakujejo od študijskega programa tisti dijaki, ki se odločijo za vpis na fiziko, in pomagajo pri strategiji privabljanja novih študentov. Kot kaže, je najpomembnejši faktor, na katerega imamo vpliv, skrb za dobre učitelje fizike v osnovnih in srednjih šolah.

LITERATURA

[1] www.hopenetwork.eu, ogled: 25. 5. 2015.

VESTI

OSEMDESET LET PROFESORJA ANTONA SUHADOLCA

Sredi aprila je dopolnil osemdeset let prof. dr. Anton Suhadolc, ki je bil v drugi polovici 20. stoletja in je še danes eden najbolj znanih in cenjenih profesorjev Oddelka za matematiko Univerze v Ljubljani. Okrogli jubilej je priložnost, da opozorimo na njegov prispevek k razvoju študija in raziskovanja matematike na Slovenskem.

Rodil se je 19. aprila 1935 v Ljubljani. Po maturi na bežigrajski gimnaziji je študiral matematiko na ljubljanski univerzi, diplomiral konec leta 1957, bil nato leto dni zaposlen na Institutu Jožef Stefan, leto dni služil vojaški rok, marca 1960 pa je postal asistent na tedanji Naravoslovni fakulteti, kasnejši Fakulteti za naravoslovje in tehnologijo (FNT).

Kot Humboldtov štipendist se je dve leti strokovno izpopolnjeval v Heidelbergu. Tam je začel pripravljati doktorat, ki ga je pod mentorstvom profesorja Ivana Vidava končal v Ljubljani in z disertacijo *Posplošitev Fourier-Laplaceove transformacije* promoviral februarja 1965. Po doktoratu je bil vse do upokojitve leta 1998 zaposlen na FNT (zadnja tri leta na novo nastali Fakulteti za matematiko in fiziko), najprej kot docent, nato izredni profesor in od leta 1981 kot redni profesor za matematiko. V tem času je bil dvakrat gostujoči profesor v ZDA, eno leto (1969/70) na University of Wisconsin v Madisonu in eno leto (1977/78) na University of Florida v Tallahasseeju. Trikrat je bil za krajši čas tudi na študijskem dopustu v Hagenu v Nemčiji.

Področje znanstvenega zanimanja in delovanja profesorja Suhadolca je bila matematična analiza, zlasti v povezavi z matematično fiziko. Poleg dvajsetih internih poročil o raziskovalnem delu na Inštitutu za matematiko, fiziko in mehaniko (IMFM), ki jih je bilo treba v šestdesetih, sedemdesetih in osemdesetih letih 20. stoletja izdelati vsako leto, je objavil dvanajst tehtnih znanstvenih člankov. Njihova vsebina sega od integralskih operatorjev te ali one vrste, Fourierove in Laplaceove transformacije, do linearizirane Boltzmannove enačbe v transportni teoriji nevtronov in do problemov pretakanja nestisljivih tekočin skozi porozni material. Za znanstveno raziskovalno delo s področja transportne teorije je leta 1974 skupaj s profesorjem Sergejem Pahorjem prejel prestižno Kidričevo nagrado, predhodnico današnje Zoisove nagrade za znanstveno delo. Recenziral je številne znanstvene članke in knjige ter o njih poročal v tujih referativnih revijah (samo v Mathematical Reviews oziroma kasnejšem MathSciNet okrog dvestokrat) in v domačem Obzorniku (skoraj štiridesetkrat). V Obzorniku in Preseku je objavil številne strokovne članke in krajše prispevke, skupaj skoraj šestdeset. Ob deseti obletnici izhajanja Preseka je prejel priznanje DMFA Slovenije. Napisal je tudi šest univerzitetnih dodiplomskih učbenikov, dva podiplomska in več krajših samostojnih strokovnih publikacij ter matematičnih prispevkov v različnih zbornikih. Prevajal je iz angleščine v slovenščino in iz ruščine v angleščino. Udeležil se je različnih kongresov v okviru bivše države in več mednarodnih konferenc. Kot gost je imel predavanja na univerzah v Mariboru, Zagrebu, Trstu, Madisonu in v Hagenu. Rad je predaval dijakom pa tudi učiteljem na strokovnih srečanjih v okviru Društva matematikov, fizikov in astronomov Slovenije (DMFA).

Profesorski ugled in splošno priljubljenost med slovenskimi matematiki pa si je zagotovo pridobil s svojimi rednimi predavanji. Generacijam študentov matematike je bil odličen vodnik na poti odkrivanja skrivnosti posameznih matematičnih disciplin: linearne algebre, numerične in funkcionalne analize, aproksimativnih metod, teorije mere, diferencialnih enačb (analiza

III in IV), enkrat tudi teorije analitičnih funkcij, pogosto pa različnih specialnih tečajev in seminarjev. Občasno je predaval matematiko tudi drugim naravoslovcem, tehnikom, računalnikarjem in slušateljem pedagoške fakultete v Ljubljani. Na podiplomskem študiju je učil na domači fakulteti (seminar, linearni topološki prostori, funkcionalna analiza, variacijske metode za mehanike), na fakulteti za elektrotehniko in na montanistiki. Svojo pedagoško poslanstvo je nekaj časa uresničeval tudi še po upokojitvi.

Njegova predavanja so se odlikovala po jasnosti in nazornosti, čeprav je bila predpisana snov večinoma med matematično najbolj zahtevnimi. Govoril je mirno in zbrano; nikoli ni povzdignil glasu, a kljub temu je bila njegova razlaga živahna in privlačna. Na izpitih je bil do študentov izjemno prijazen in korekten. Med njimi je bil na glasu kot dober in zaželen mentor. V tej vlogi se je izkazal pri šestinšestdesetih diplomah in šestih magisterijih. V resnici pa je njegovo mentorsko delo presegalo te okvire. S svojo široko matematično razgledanostjo in sposobnostjo poslušati in vživeti se v (matematične) probleme drugih je bil primeren sogovornik svojim kolegom, tako matematikom kot fizikom, o različnih strokovnih vprašanjih. Tudi do drugih sodelavcev je bil odprt in vedno vsaj z nasvetom pripravljen priskočiti na pomoč. Pomagal je npr. pri organiziranju matematične knjižnice, kasneje pri naročanju in klasifikaciji knjig, pri pripravi razstave o Vegovih logaritmih ob slovenskem matematičnem kongresu leta 1994, pri organizaciji Vegovih dnevov leta 2004 itd. Za svoje predano pedagoško delo je profesor Suhadolc upravičeno prejel pomembno priznanje domače alme mater. Leta 2002 je postal zaslužni profesor Univerze v Ljubljani.

V svoji univerzitetni karieri je moral prevzeti tudi ustrezen delež administrativnih in vodstvenih dolžnosti na Oddelku za matematiko. Dva ločena mandata je bil predstojnik oddelka, še prej namestnik predstojnika. V zgodovino se je zapisal kot prvi dekan nove Fakultete za matematiko in fiziko. To zahtevno in nehvaležno funkcijo je opravljal v kritičnih letih 1995–1997, ko je bilo treba na novo vzpostaviti celoten dekanat in vse njegove službe. Nazadnje je v letih 2006–2009 opravljal pomembno državno funkcijo na znanstvenem področju kot član Odbora za Zoisove nagrade in priznanja Republike Slovenije.

Ob koncu šestdesetih let je vodil Oddelek za matematiko na IMFM in bil v začetku devetdesetih let predsednik inštitutskega sveta. Tako rekoč vso svojo kariero je bil aktiven pri DMFA. Bil je dolgoletni član upravnega odbora društva, štiri leta njegov podpredsednik in dve leti predsednik, po upokojitvi pa član častnega razsodišča. Več kot dvajset let je bil član uredništva in kasneje svetovalec društvenega glasila Obzornik, od tega devet let urednik za matematiko. Eno leto je bil tudi predsednik Komisije za tisk. Društvo se mu je za dolgoletno nesebično delo leta 2001 zahvalilo z izvolitvijo za častnega člana.

Doslej smo govorili o profesorju Suhadolcu kot matematiku v različnih vlogah: znanstvenika in univerzitetnega profesorja, promotorja znanosti in urednika strokovne revije. Poročilo pa bi bilo nepopolno, če ne bi omenili tudi njegovih drugih zanimanj in aktivnosti, ki so le rahlo povezane z matematiko ali pa povsem zunaj matematičnega področja.

Že pred upokojitvijo ga je zanimala zgodovina matematike. Ob različnih priložnostih je predaval o znamenitih matematikih iz naše preteklosti, o Vegi, Močniku, Hočevarju, večkrat o Plemlju, pa o Zupančiču, Kušarju, o nekaterih tujih znanih matematikih, o začetkih pouka fizike na ljubljanski univerzi, o nastanku logaritmov, o starih učbenikih itd. O vsem tem je pisal v Obzorniku, pa tudi v Kroniki in drugje. Pretipkal, uredil in v samozaložbi je izdal dnevnik svojega očeta (znanega arhitekta) iz partizanskih dni. Njegovo zadnje veliko delo pa je raziskava o pozabljenem in po krivici zamolčanem predvojnem slovenskem matematiku, Plemljevem kolegu in njegovem nasledniku na rektorskem stolu Univerze v Ljubljani. O njem je napisal več poročil in člankov, krona pa je objava knjige *Življenje in delo profesorja Riharda Zupančiča*, ki jo je leta 2011 izdala domača založba DMFA – založništvo. V zadnjem času se profesor Suhadolc rad udeležuje različnih predavanj v okviru Društva univerzitetnih profesorjev in Seminarja za zgodovino matematike in matematičnih znanosti pri DMFA.

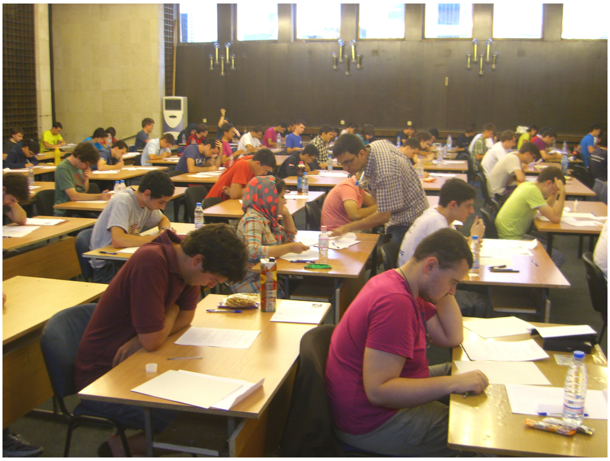
Med kolegi na fakulteti slovi tudi njegovo intenzivno ukvarjanje z rastlinami in s cvetjem. O njih si je z leti nabral ogromno praktičnega in teoretičnega znanja. S svojih številnih potovanj v tujino je prinašal eksotične rastline, jih gojil doma in občasno »razstavil« na hodnikih fakultete, da smo jih lahko občudovali tudi drugi in hkrati poslušali profesorjevo razlago. O nekaterih posebnih rastlinah je pisal v revijah Proteus in Moj mali svet. Poleg tega je profesor Suhadolc eden najboljših slovenskih poznavalcev lesa; domačega, ki ga je zbiral po vseh krajih, in tudi tujega. O tem je leta 2012 izdal knjigo *Les naših dreves in grmovnic*. Različne vrste lesa je uporabil za razne praktične predmete, celo domači parket. Posebnost so manjše in večje krogle, ki jih je dal izdelati in jih v zadnjih desetih letih prikazal na številnih razstavah po Sloveniji.

Kaj naj rečemo ob koncu tega poročila, ki seveda ne more celovito prikazati niti bogate ustvarjalnosti profesorja Suhadolca niti njegovih pedagoških zaslug in strokovnih prizadevanj, kaj šele vse širine njegovega duha? Omenili smo že nagrado za znanstveno delo ter univerzitetna in društvena priznanja. Za svoje druge uspehe in ravnanja najbrž ni dobil ničesar, razen notranjega zadovoljstva. To pa ne pomeni, da si ne zaslužijo pozornosti in da jih njegovi nekdanji učenci in kolegi ne znamo ceniti. Ob življenjskem jubileju pa mu predvsem želimo, da ostane še naprej čil in vitalen, mlad po duhu, trden v svoji intelektualno pošteni in pokončni drži ter veder v svojem odnosu do soljudi.

Še na mnoga zdrava leta, spoštovani gospod profesor!

Milan Hladnik

ENAINDVAJSETO MEDNARODNO TEKMOVANJE ŠTUDENTOV MATEMATIKE



Slika 1. Študenti med reševanjem nalog.

V Blagoevgradu v Bolgariji je od 29. julija do 4. avgusta 2014 potekalo že 21. tekmovanje študentov matematike. Iz Slovenije sta se ga udeležili dve ekipi. Fakulteto za matematiko in fiziko Univerze v Ljubljani so zastopali Vesna Iršič in Veno Mramor iz drugega letnika, Simon Bergant iz tretjega letnika ter Matej Aleksandrov in Matej Petković iz prvega letnika druge stopnje študija, Famnit Univerze na Primorskem pa študenti Marko Rajković in Marko Palangetić iz prvega letnika ter Anastasiya Tanana iz drugega letnika. Vodji ekip sva bila Gregor Šega in István Estélyi.

V dvodnevnem reševanju desetih nalog se je pomerilo 324 študentov, razvrščenih v 73 ekip. Običajno ekipo sestavljajo študenti ene univerze, včasih pa je kakšna od ekip sestavljena iz študentov različnih univerz (letos je bila taka zmagovalna ekipa, ki se je imenovala Narodna ekipa Izraela). Poleg ekip se tekmovanja vedno udeleži še nekaj posameznikov, saj se na tekmovanje lahko prijavi vsak študent matematike.

Slika 2. Ekipa Fakultete za matematiko in fiziko na podelitvi.

Naši ekipi sta bili tudi tokrat zelo uspešni. Anastasiya Tanana je osvojila prvo nagrado, Simon Bergant je prvo nagrado zgrešil za eno točko in tako osvojil drugo nagrado, ki so si jo prislužili tudi Matej Aleksandrov, Veno Mramor in Matej Petković. Marko Palangetić in Marko Rajković sta osvojila tretjo nagrado, Vesna Iršič pa pohvalo. Ekipno smo dosegli triindvajseto (ekipa Fakultete za matematiko in fiziko) ter štiriintrideseto mesto (ekipa Famnit).

Posnetek podelitve, na kateri vsak študent na odru prevzame svojo nagrado, čestitke predsednika tekmovalne komisije in zaslužen aplavz, je dosegljiv tudi na YouTubu. Ker je študentov kar veliko, prireditev traja skoraj toliko kot kakšna otvoritev olimpijskih iger. Temu primerno je potem tudi število ogledov – verjetno vsak le pogleda svoj del.

Kot običajno velja nekaj vrstic nameniti tudi družabnemu življenju. Skozi leta se je pravzaprav marsikaj spremenilo. Na začetku je bilo tekmovalcev manj kot sto, zato je bilo druženje precej lažje, ni pa bilo tako raznoliko. Sedaj je študentov prek tristo, tako da se mnogi v enem tednu niti ne srečajo. Vseeno je veliko športnih iger (tokrat vreme ni nagajalo), družabnih iger ter nočnih zabav v študentskem naselju, kjer so nastanjeni tekmovalci. Je pa bilo tokrat močno opazno čakanje na rezultate: komisija po vsakem tekmovalnem dnevu ocenjuje izdelke pozno v noč, rezultati pa se sproti objavljajo na spletni strani organizatorja. Tako so nekateri (predvsem boljši) tekmovalci sedeli pred svojimi elektronskimi pripomočki in osveževali domačo stran tekmovanja.

Kot običajno so temperamentni Španci poskrbeli za glasno zabavo pozno v noč, njeno središče je bila bikova glava, narejena iz izdolbene lubenice.

Slika 3. Obe slovenski ekipi po podelitvi.

S končnimi rezultati so bili tekmovalci večinoma zadovoljni, ne pa vsi. Na primer, tekmovalka, ki je dosegla šesto mesto, je bila tako razočarana, da se podelitve nagrad sploh ni udeležila.

Oglejmo si še tri naloge s tekmovanja ter njihove rešitve. Prva naj bi bila zelo lahka, druga srednje težavnosti in tretja malo težja.

Naloga 1. Določite vse pare (a, b) realnih števil, za katere obstaja enolično določena simetrična 2×2 matrika s sledjo enako a in determinanto enako b.

Optimisti pravijo, da za vsak problem obstaja veliko pravilnih rešitev, napačna rešitev pa je le ena. Pesimisti nasprotno trdijo, da je prava rešitev le ena, napačnih rešitev pa je mnogo. Matematiki pa vemo, da obstaja mnogo pravilnih rešitev, pa tudi mnogo napačnih.

Oglejmo si nekaj pravilnih rešitev. Najprej podajmo analitično rešitev algebraičnega problema:

Rešitev 1. Označimo matriko $M = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$. Veljati mora $x + z = a$, $xz - y^2 = b$. Iz prve enačbe dobimo $z = a - x$, vstavimo v drugo enačbo, da dobimo $ax - x^2 - y^2 = b$. Dodamo člen $-\frac{a^2}{4}$, da dobimo popolni kvadrat, in lahko pišemo

$$\left(x - \frac{a}{2}\right)^2 + y^2 = \frac{a^2}{4} - b\,.$$

Dobili smo enačbo krožnice. Ker moramo imeti le eno rešitev, mora biti radij krožnice enak 0. Tako je pogoj $a^2 = 4b$ in pri tem pogoju imamo eno

Slika 4. Vodja tekmovanja John E. Jayne v družbi španskih tekmovalcev.

rešitev, $x = \frac{a}{2}$, $y = 0$ in $z = \frac{a}{2}$. Matrika je tako enaka $M = \begin{bmatrix} a/2 & 0 \\ 0 & a/2 \end{bmatrix}$.

Lotimo se naloge bolj algebraično:

Rešitev 2. Označimo matriko $M = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$. Ker imata matrika M in matrika $\begin{bmatrix} z & -y \\ -y & x \end{bmatrix}$ isto determinanto ter isto sled, mora biti $x = z$ in $y = 0$, sicer bi imeli dve različni matriki z zahtevanima lastnostma. Tako je matrika $M = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$ in ima sled enako $2x$ in determinanto x^2. Sledi, da je $a = 2x$ in $b = x^2 = a^2/4$. Pogoj $a^2 = 4b$ je tako potreben za enolično rešitev. Preverimo, da je tudi zadosten. Za splošno matriko M kot zgoraj mora veljati $x + z = a$ in $xz - y^2 = a^2/4 = (x+z)^2/4$ oziroma $-y^2 = (x+z)^2/4 - xz = (x-z)^2/4$. Ta enačba ima le eno rešitev, $y = 0$ in $x = z = a/2$.

Ker gre le za matrike, poskusimo še bolj algebraično:

Rešitev 3. Simetrično matriko lahko diagonaliziramo, torej je $M = SDS^{-1}$. Matrika D ima enako sled kot M ter prav tako enako determinanto, ker pa je določena enolično, mora biti $M = D = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$. Vendar pa morata biti lastni vrednosti enaki, saj je za $S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ produkt $SDS^{-1} = \begin{bmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{bmatrix}$

Slika 5. Slovenski ekipi na slavnostni večerji.

(še enkrat uporabimo enoličnost). Tako je $2\lambda_1 = a$ in $\lambda_1^2 = b$, od koder spet sledi $a^2 = 4b$.

A tudi tokrat moramo preveriti enoličnost: za lastni vrednosti rešujemo enačbi $\lambda_1 + \lambda_2 = a$, $\lambda_1\lambda_2 = a^2/4$. Izračunamo

$$(\lambda_1 - \lambda_2)^2 = (\lambda_1 + \lambda_2)^2 - 4\lambda_1\lambda_2 = a^2 - a^2 = 0\,,$$

od koder sledi $\lambda_1 = \lambda_2 = \lambda$. Tako je (za poljubno matriko S) iskana matrika M enaka

$$M = S \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} S^{-1} = S\lambda I S^{-1} = \lambda I$$

in je torej določena enolično.

Težja je naloga z višjimi odvodi:

Naloga 2. Za funkcijo $f(x) = \frac{\sin x}{x}$ dokažite, da za $x > 0$ in naravno število n velja $|f^{(n)}(x)| < \frac{1}{n+1}$.

Običajno študenti pokažejo veliko iznajdljivosti, tako da skoraj vedno kdo preseneti z lepo rešitvijo. Tokrat le ni bilo čisto tako, najkrajša rešitev je prišla iz komisije.

Rešitev. Uporabimo enakosti $\int_0^1 \cos(xy)\mathrm{d}y = \frac{\sin x}{x}$ in $\frac{\partial^n}{\partial x^n}\cos(xy) = y^n \cos^{(n)}(xy)$. Ker lahko odvode funkcije cos izrazimo kot $\cos^{(n)} x = \cos(x + \frac{n\pi}{2})$, je

$$\left|f^{(n)}(x)\right| = \left|\int_0^1 \frac{\partial^n}{\partial x^n}\cos(xy)\mathrm{d}y\right| < \int_0^1 y^n \mathrm{d}y = \frac{1}{n+1}\,.$$

Naloga 3. Naj bo $n > 6$ popolno število (torej enako vsoti vseh svojih deliteljev – brez n). Faktoriziramo število n kot

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

kjer so $p_1 < p_2 < \ldots < p_k$ praštevila in e_i naravna števila. Dokažite, da je e_1 sodo število.

Rešitev. Za število $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ je vsota vseh deliteljev enaka $\prod_{i=1}^{k}(1+p_i + p_i^2 + \ldots + p_i^{e_i})$. Ker je n popolno, velja

$$\prod_{i=1}^{k}(1 + p_i + p_i^2 + \ldots + p_i^{e_i}) = 2n = 2p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\,.$$

Predpostavimo, da je e_1 liho število. Potem vidimo, da prvi faktor produkta na levi lahko razstavimo, tako da izpostavimo $1 + p_1$. To pomeni, da $p_1 + 1$ deli $2n$, od koder sledi (ker je $p_1 + 1 > 2$), da neko izmed praštevil $p_2, p_3, \ldots, p_k$ deli $p_1 + 1$. To pa je možno le, če je $p_1 = 2$ in $p_2 = 3$. Torej je število n deljivo s 6, kar pomeni, da so $n/2$, $n/3$, $n/6$ in 1 (nekateri) delitelji števila n. Njihova vsota je enaka $n/2 + n/3 + n/6 + 1 = n + 1$, kar pomeni, da n ni popolno število.

Opomba 1. Lahko bi tudi uporabili dejstvo, da je vsako popolno število oblike $2^{p-1}(2^p - 1)$, kjer sta p in $2^p - 1$ praštevili.

Za konec predlagam, da se poskusite v reševanju še enega zanimivega vprašanja:

Naloga 4. Naj bo n pozitivno celo število. Dokažite, da obstajajo pozitivna realna števila $a_0, a_1, \ldots, a_n$, tako da ima za vsak izbor predznakov $\pm$ polinom oblike

$$\pm a_n x^n \pm a_{n-1}x^{n-1} \pm \ldots \pm a_1 x \pm a_0$$

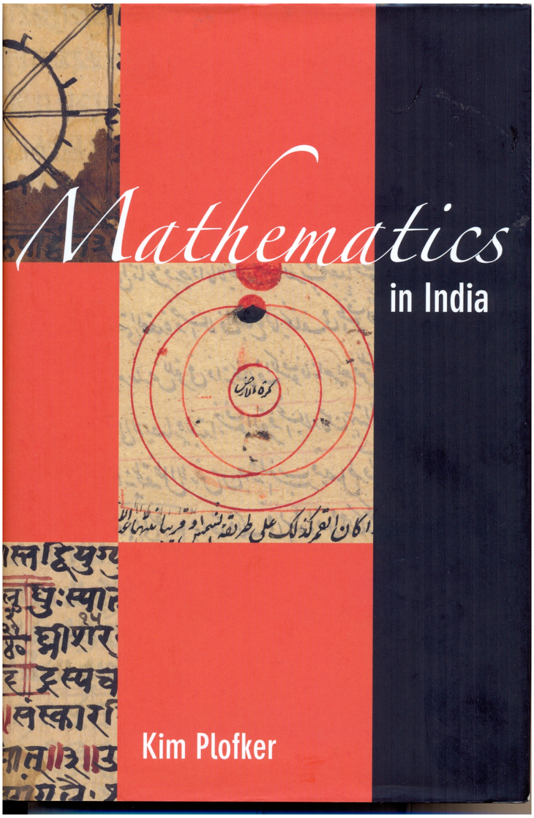
n različnih ničel.

Kogar zanima rešitev te naloge ali pa bi se rad poskusil v reševanju še kakšne naloge s tekmovanja, si jih lahko ogleda na uradni strani `www.imc-math.org.uk`.

Gregor Šega

NOVE KNJIGE

Kim Plofker, Mathematics in India, Princeton University Press, 2009, 368 strani.



Po navadi se takrat, ko omenjamo indijsko matematiko, najprej spomnimo na tako imenovane arabske številke, ki pa so svoj čas prišle iz Indije. V praksi običajno uporabljamo ravno arabske številke, redko rimske ali kakšne druge. Rimske imajo pravilno ime, saj so se pred dva tisoč leti razširile hkrati s širjenjem rimske države in so jih v Evropi še dolgo uporabljali v vsakdanjem življenju. Pravijo, da so arabski trgovci bili med prvimi, ki so spoznali indijske številke, odkrili njihovo praktičnost v zapisu in računanju z njimi ter jih postopoma s širjenjem islama posredovali vse do Alžirije, Maroka in Pirenejskega polotoka, kjer so jih prevzeli Evropejci. Zato bi upravičeno morali govoriti o indijskih, morda vsaj o indijsko-arabskih ali arabsko-indijskih številkah. Grafična podoba števk se je s krajem in časom sicer spreminjala, bistvena pa je možnost mestnega zapisa števil samo z desetimi znaki, vključno z ničlo, o kateri se da posebej razpravljati.

To pa še zdaleč ni vsa indijska matematika, o čemer nas prepriča avtorica knjige Kim Plofker, ki je na podlagi obsežnih raziskav sanskrtskih virov lahko zasledovala razvoj matematike na indijski podcelini od antike pa vse do zgodnjega novega veka. V knjigi ga skuša avtorica na podlagi dejstev, ki so splošno znana, na primer indijski izvor arabskih številk, postaviti v širši kulturni okvir. Pokaže, da sta indijska in islamska matematika ter astronomija vplivali druga na drugo. Indijska matematika ni kar tako neko neprekinjeno zaporedje odkritij, ampak je živahna, pisana, z drugimi indijskimi oblikami učenja povezana dejavnost.

Knjiga je razdeljena na devet poglavij in dva dodatka. Ne uporablja nobene indijske pisave. Besede ali krajša sanskrtska besedila prečrkuje po shemi IAST (kratica za International Alphabet of Sanskrit Transliteration, uporablja se že več kot sto let), ki natančno ohranja vse podrobnosti sanskrta, ki se originalno piše v pisavi devanagari. IAST uporablja črke angleške abecede, katerim po potrebi dodaja spodaj ali zgoraj določena znamenja. Po priporočilih Slovenskega pravopisa za prečrkovanje indijskih jezikov izgubimo razlike med nekaterimi sanskrtskimi soglasniki, pa še paziti je treba na to, kdaj je beseda zapisana po shemi IAST, kdaj po našem ali kakem drugem pravopisu.

Knjiga na začetku pove najnujnejše o zgodovini Južne Azije in sanskrtski literaturi. Seveda se ne more izogniti Vedam, obsežni zbirki indijskih spisov, ki so osnova indijske filozofije in verstev. V Vedah najdemo precej matematike in astronomije, na primer pitagorejske trojice, približke za kvadratne korene, število π, pretvorbe pravokotnikov v ploščinsko enake kvadrate, menjavanje letnih časov. Geometrijska pravila v Vedah so posvečena konstrukciji oltarjev. Pogosto je omenjen izraz *Šulba-sutra* – *Śulba-sūtra* (druga oblika je zapisana po shemi IAST), kar dobesedno pomeni pravilo za delo z merilno vrvico. Pisali so v verzih. Tako Indijci kot Mezopotamci so razdelili krožnico na 360 enakih delov, stopinje. To kaže na zgodnjo povezavo med obema kulturama. Za polmer krožnice so jemali različno število enot. Operirali so s krožnimi loki, ne pa s koti.

V obdobju približno od propada Aleksandrovega imperija naprej so se indijski matematiki in astronomi veliko ukvarjali s števili, števniki in trigonometrijo ter odkrivali tudi druga področja, na primer kombinatoriko. V trigonometriji so že poznali funkciji sinus in kosinus, ki sta bili vezani na krožnico s konkretnim polmerom. Drugače od Grkov, ki so krožnemu loku priredili tetivo, so Indijci polovici krožnega loka priredili polovico tetive, kar še danes delamo pri vpeljavi funkcije sinus z enotsko krožnico. V resnici je latinska beseda *sinus* v kasnejšem obdobju nastala kot napačen prevod sanskrtske besede za poltetivo. Poznali so že nekaj enakosti za funkcijo sinus in sestavili so zanjo tablice od loka $3°45'$ do loka $90°$ s korakom $3°45'$.

V času, ki sovpada s propadom Zahodnorimskega cesarstva, ob zori našega srednjega veka, se je kljub številnim osvajalcem Indije začelo klasično obdobje indijske matematike in astronomije. V tem obdobju so v Indiji prevladovale *siddhante*. To so v glavnem astronomske razprave, pisane v verzih. Beseda *siddhanta* je težko prevedljiva. Lahko bi bila to doktrina, tradicija, princip, pravilo, teorija, dogma, aksiom, učenje, končni sklep, rešitev ali razprava. Indijci so uporabljali geocentrični svetovni sistem. Številna preračunavanja so samo še utrdila indijski desetiški sistem mestnih vrednosti. Računali so z ulomki in negativnimi števili. Zanimivo pri tem je, da desetiških ulomkov v tabelah sinusov niso uporabljali, ampak star babilonski šestdesetiški sistem. Izumili so aproksimativno formulo za izračune sinusov, ki bi jo dandanes zapisali v obliki:

$$\sin(\pi x) \approx \frac{16x(1-x)}{5-4x(1-x)}, \quad 0 \le x \le 1.$$

Sami se lahko prepričamo o njeni natančnosti. V astronomiji so seveda napovedovali tudi Sončeve in Lunine mrke, konjunkcije planetov, sestavljali koledar in drugo. V geometriji so bili včasih precej nenatančni in marsikatera formula za ploščino in prostornino je bila le približna.

Iz klasičnega obdobja verjetno izvira tudi *Bakhšalijski rokopis*, ki so ga odkrili proti koncu 19. stoletja. Vsebuje postopke računanja z ulomki, zelo dober postopek za korenjenje in naloge, ki vodijo do linearnih enačb. Morda so razne naloge bile zapisane zato, da bi zraslo zanimanje za matematiko in astronomijo, katerima pripada primerno mesto v družbi. V 12. stoletju je nastala *Lilavati*, zbirka matematičnih razprav in nalog iz aritmetike, algebre in geometrije.

Proti koncu našega srednjega veka je v Kerali na jugozahodu Indije nastala *Keralska šola*, v kateri so se ukvarjali tudi z neskončnimi vrstami. Poznali so že vrste za sinus, kosinus in arkus tangens. Izračunali so število π na 11 decimalk natančno.

Vsa indijska matematična in astronomska znanja so počasi prek islamskega sveta prodirala na Zahod. Okorne rimske in grške številke so zamenjale indijske, Ptolemajeve tetive, ki ustrezajo krožnim lokom, so zamenjale indijske poltetive, predhodnice današnjih sinusov. V zadnjem poglavju Plofkerjeva poudari pomen indijske matematike in astronomijo za samo Indijo in za ves preostali svet.

V prvem dodatku avtorica opiše osnove sanskrta in strukturo sanskrtskega verza, ki so ga uporabljali za pisanje matematičnih in astronomskih besedil. Navedenih je nekaj primerov, kakšna je indijska matematika v verzih. Dodan je tudi kratek slovarček nekaterih besed, ki se uporabljajo v starih sanskrtskih matematičnih in astronomskih besedilih. Primeri: *gaṇita* – računanje, matematika; *jīvā* – sinus; *śūnya* – ničla.

V drugem dodatku so zbrani kratki življenjepisi pomembnih indijskih matematikov iz predhodnih poglavij. Namenoma v opisu knjige ni doslej naveden niti eden. Sodobni Indijci so na svoje stare matematike seveda zelo ponosni. Zato je čas, da omenimo tri. V Indiji so namreč ustanovili Indijski vesoljski raziskovalni program ISRO – *Bhāratīya aṃtarikṣa anusaṃdhāna saṃgaṭhana*. Svoj prvi umetni satelit so lansirali v tirnico okrog Zemlje 19. aprila leta 1975 s pomočjo Sovjetske zveze. Imenoval se je *Aryabhata*, po znanem indijskem matematiku in astronomu. Sledila sta še umetna satelita *Bhaskara I*, *Bhaskara II*, poimenovana prav tako po indijskih matematikih in astronomih.

Knjiga se konča z obseženim seznamom virov, v katerih se lahko seznanimo z raziskavami drugih avtorjev o problematiki indijske matematike. S tem delo izpolnjuje pomembno vrzel, kajti matematično zgodovinopisje je bilo doslej v glavnem oblikovano v obdobju razsvetljenstva, in to pretežno na podlagi grške matematične tradicije. Čisto na koncu je priloženo še zgledno urejeno stvarno kazalo.

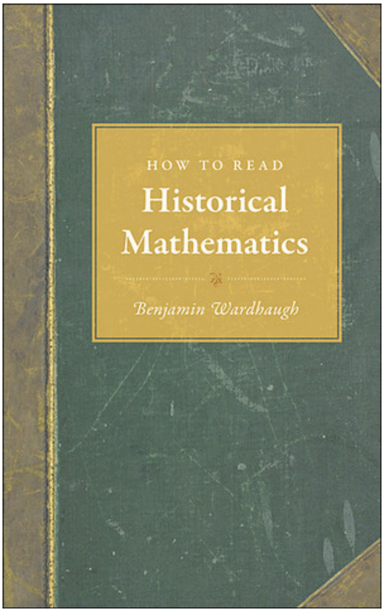
Raziskovalci indijske zgodovine matematike si niso popolnoma enotni o času, kraju in avtorstvu kakšne nove zamisli, besedila ali predmeta, zato pogosto prihaja med nepoznavalci do napačnih strokovnih sklepov. Kljub temu knjiga zagotavlja bogato in kompleksno razumevanje indijske matematične tradicije.

Avtorica je opravila izjemno delo s predstavitvijo indijske matematike. Kdorkoli, četudi ne ravno zgodovinar, ki se poglobi v problematiko pri branju lepo in dobro napisane knjige, bo našel preprosto matematično razlago, se nekaj naučil o kulturi, v kateri so nastale, in na koncu bolje razumel indijsko civilizacijo z njeno matematiko vred.

Kim Leslie Plofker, rojena 25. novembra 1964, je ameriška zgodovinarka matematike, še prav posebej indijske. Doktorirala je leta 1995 na Brown University, in sicer iz aproksimacije sinusne funkcije v srednjeveških astronomskih sanskrtskih besedilih. Delala je na MIT, bila gostujoča profesorica v Utrechtu in sodelavka na Mednarodnem inštitutu za azijske študije v Leidenu. Sedaj je gostujoča profesorica na Union Collegeu v Schenectadyju v državi New York. Leta 2010 je imela plenarno predavanje na Mednarodnem kongresu matematikov v Hyderabadu, leta 2011 pa je prejela Brouwerjevo medaljo, ki jo podeljuje Nizozemsko kraljevo matematično društvo.

Marko Razpet

Benjamin Wardhaugh, How to read Historical Mathematics, Princeton University Pres, Princeton in Oxford, 2010, 116 strani.



Drobna knjižica z dragoceno vsebino je odličen vodnik k razumevanju matematičnih zakladov preteklosti, zakopanih v starih knjigah, člankih ali celo rokopisih, dnevnikih in pismih. Bralcu ob primerih podrobne analize odlomkov originalnih besedil (npr. iz Newtonove knjige »Principia« ali iz Galoisovega predsmrtnega pisma) predstavi osnovne veščine razbiranja pomena starih matematičnih tekstov. V veliko pomoč bo prav vsakomur, ki želi globlje pronikniti v katerikoli matematični tekst iz preteklosti, lahko pa je tudi izvrstno dopolnilno gradivo za kakršenkoli študijski predmet s področja zgodovine matematike (pa tudi matematike same, saj so nekatere veščine razbiranja smisla iz teksta, predstavljene v tej knjigi, splošno uporabne, npr. tudi pri prebiranju novejših člankov).

Kdor je že imel v rokah kakršnokoli matematično knjigo, staro sto ali več let, se je zagotovo vprašal: *»Kaj ... pa je to?«*. Uporabljeni izrazi se nam zdijo nenavadni, matematična notacija je skrivnostna in jo le s težavo razvozlamo, namesto algebraičnih izrazov prebiramo dolgovezne besedne opise formul in enačb (včasih celo v verzih!), o kakršnikoli »matematični strogosti« besedila ni ne duha ne sluha. Tekst je morda v latinščini ali v stari nemščini, zapisani v gotici, ali celo v kakšnem nam povsem neznanem jeziku in pisavi. Če imamo v rokah le fragment starega pisnega vira, morda ne poznamo niti imena, kaj šele »profila« avtorja (spola, starosti, izobraženosti, profesionalnega statusa, itd.), pa tudi ne časa ne kraja nastanka besedila. Tako tavamo v popolni temi, nazadnje pa razočarani odložimo knjigo in se posvetimo kakšnemu »bolj smiselnemu« početju, npr. posodabljanju svojega profila na Research Gate (o katerem se bo kakšen raziskovalec »primitivnih računalniških kultur staroselcev« čez 500 let spraševal: *»Kaj ... pa je to?«*).

Knjižica *How to Read Historical Mathematics* nas uči *umetnosti zastavljanja vprašanj*, ki nam pomagajo k razumevanju starih matematičnih tekstov (podobno kot nas znana knjižica George Polya *How to Solve It* uči reševanja matematičnih problemov). Osnovnim vprašanjem: *Kaj besedilo pove? Kako je napisano? Komu je bil tekst namenjen? Kdo je bil lastnik knjige? Katere stare tekste brati in zakaj?* moramo pridružiti svoja lastna vprašanja, prilagojena vsakokrat drugačnemu predmetu raziskave. Ogromno informacij o avtorju, kraju in času nastanka, itd. lahko s pomočjo »lateralnega razmišljanja« in pravega »detektivskega« raziskovanja dobimo iz fizičnega nosilca besedila (knjige, pisma, dnevnika, članka). Če npr. sicer nam neznani avtor teksta omenja druge matematike kot svoje sodobnike, lahko že iz teh podatkov precej natančno določimo čas, v katerem je živel. Če imamo srečo, lahko slej ko prej iz dovoljšnega števila takšnih drobnih koščkov informacije dostikrat doženemo celo avtorjevo identiteto, podobno kot lahko natančno identificiramo npr. naravno število $n \leq a$, če poznamo a in dovolj ostankov $n \pmod{m_i}$ pri deljenju n z različnimi naravnimi števili m_i. Delo zgodovinarja matematike temelji na različnih veščinah, ki mu pomagajo iz *teksta* uganiti marsikatero informacijo o *kontekstu* njegovega nastanka. Veščina raziskovanja virov, ki je v tej knjigi zelo dobro razložena, pride prav tudi vsakemu študentu, ki hoče svoje razumevanje razširiti in poglobiti onstran predpisanega »učbeniškega« znanja s poznavanjem druge relevantne literature.

Enako pomemben in dobro razložen je problem prevajanja starega teksta v sodobni jezik in notacijo. Pri tem moramo biti zelo pozorni, da avtorjevo misel prenesemo čim zvesteje v jezik današnjega časa. Tako Newtonovih spremenljivih »količin« ne smemo avtomatično imeti za realna števila ali funkcije (saj npr. pojem realnega števila v Newtonovem času ni bil tako izčiščen kot danes!); pogosto je Newton s tem izrazom označeval neke geometrijske količine (dolžine daljic ali njihova razmerja). To se zdi povsem skregano z zahtevo, znano vsakemu matematiku, da mora imeti vsak matematični pojem svoj natančno določen pomen. Branje starih matematičnih tekstov nam jasno pokaže, kako se je pomen posameznih matematičnih izrazov skozi zgodovino spreminjal. Brez natančnejšega poznavanja širšega konteksta, v katerem je delo nastalo, ga ne moremo ustrezno raztolmačiti in prevesti. To pa nikakor ni mehaničen postopek, zato je tudi dobro prevajanje starih tekstov ne samo prava znanost, ampak tudi umetnost. Treba je pretehtati in sprejeti odločitve, kot so npr.: *Ali narisati slike na novo ali uporabiti faksimile originalnih slik? Modernizirati notacijo ali ne? Označiti neberljiva mesta ali ne ohranjati nobene informacije o tem?* Zavedati se moramo, da bo vsaka poenostavitev, ki jo bomo vnesli v tekst, v »naslednji generaciji« morda pripeljala do še večjega osiromašenja prvotnega sporočila.

Ukvarjanje z zgodovino matematike nam omogoča bolje razumeti ne samo, kako so se razvile določene matematične ideje in koncepti (npr. pojem funkcije), ampak kako so razmišljali in živeli matematiki v preteklosti. Pri tem so nam v največjo pomoč *primarni viri* (neposredni viri informacij, nastali v obdobju, ki ga preučujemo). *Sekundarni viri*, nastali kasneje na osnovi primarnih virov, ki jih praviloma navajajo med referencami, so že »en korak odmaknjeni« od dogodkov, ki jih opisujejo. *Terciarni viri*, nastali na podlagi sekundarnih virov, so »dva koraka odmaknjeni« od dogodkov, ki jih opisujejo. Pri preučevanju določenega avtorja ali teksta iz preteklosti si je dobro pomagati z vsemi temi različnimi vrstami virov.

Marsikatera oseba, ki jo matematiki sicer poznamo le po imenu, nam postane veliko bližja, če preberemo vsaj droben del njenega originalnega dela, četudi le v prevodu (kot npr. v knjižici objavljeno pismo Sophie Germain, ki ga je 1804 pisala Gaussu in podpisala s psevdonimom Le Blanc). Dobro je vedeti, da za mnoge velike matematike na spletu najdemo skenirana njihova originalna dela ali rokopise. Tudi mnoge univerze in knjižnice po svetu načrtno arhivirajo v elektronski obliki izvirnike starih tekstov. Preučevanje stare matematike je danes veliko lažje tudi zaradi novih in novih tekstov, objavljenih v elektronski obliki, ki jih zato ni treba več iskati po knjižnicah v tiskani ali rokopisni obliki. Zgodovina matematike, ki jo vsaka naslednja generacija skuša premisliti in napisati na novo, bo tudi zaradi vse lažjega dostopa do najrazličnejših virov postajala vse bolj in bolj zanimiva, privlačna in poučna. Na marsikaterih univerzah jo zato že vključujejo v svoje študijske programe.

Čeprav matematiki radi verjamemo, da je matematika ena sama, da so njeni izreki večne in nespremenljive resnice, bivajoče v svetu idej, kjer samo čakajo, da jih odkrijemo, nas že ena sama taka izkušnja, kot je npr. branje te drobne knjižice ali branje kakšnega starega matematičnega teksta (kaj šele boljše poznavanje zgodovine matematike!) kmalu prepriča, da je ta »Platonov postulat« o neodvisnosti matematike od človekovega uma daleč od resnice. Takrat se nam naenkrat odpre popolnoma nov svet. V njem definicije matematičnih pojmov niso enkrat za vselej določene, v njem jasno vidimo, da matematiko delamo *ljudje*, da jo ne le odkrivamo, ampak tudi ustvarjamo, in to ne le z razumom in logiko, temveč tudi z občutji in domišljijo! O matematiki nič več ne razmišljamo le iz ozkega zornega kota sedanjosti, marveč s hvaležnostjo sprejemamo (ne samo v svoj razum, ampak tudi v svoje srce) življenja in prispevke matematikov najrazličnejših časov in kultur.

Kdor je prebral ta prispevek do konca in je pričakoval bolj »klasičen« opis knjige, se je morda nekajkrat vprašal: *»Kaj . . . pa je to?«* – Še en nazoren dokaz Gödlovega spoznanja, da matematične misli ni mogoče ukalupiti v nobeno našo vnaprejšnjo predstavo o njej!

Knjižica *How to read historical mathematics?* (ki se ji, kakor hitro sem jo zagledal v knjigarni, nisem mogel upreti – po svoji zunanji in notranji likovni opremi posrečeno spominja na knjige iz antikvariata!), vsebuje še mnoge druge zaklade, ki jih v tem kratkem pregledu ni bilo mogoče niti omeniti, do katerih pa ne obstaja nobena druga kraljevska pot kot lasten poglobljen študij in potrpežljivo urjenje v različnih veščinah branja, razumevanja, raziskovanja, prevajanja in interpretacije, ki niso le mehanično priučljive, ampak zahtevajo tudi ustvarjalen pristop.

Jurij Kovič

OBZORNIK ZA MATEMATIKO IN FIZIKO
LJUBLJANA, MAREC 2015
Letnik 62, številka 2

ISSN 0473-7466, UDK 51 + 52 + 53

VSEBINA

CONTENTS

Na naslovnici in spodaj: Slika k članku na strani 53.