



PRESEK LETNIK 51 (2023/2024) ŠTEVILKA 1



PRESEK



- O DELITVAH NA ENAKOVREDNE DELE
- PEVEC KOT INŠTRUMENT
- TERAN NA ASTRONOMSKEM
TEKMOVANJU TREH DEŽEL
- KRATICE

ISSN 0351-6652



9 770351 665111

Nenavadno število 6174



→ Izberimo si poljubno štirimestno število, ki nima vseh števk enakih, na primer 2731. Iz števk začetnega števila sestavimo novi števili: pri prvem številke zapišemo v naraščajočem zaporedju, pri drugem v padajočem zaporedju. Nato izračunajmo pozitivno razliko novih števil: $7321 - 1237 = 6084$. Z dobljenim štirimestnim številom postopek ponovimo; če ima število manj kot štiri mesta, dodamo ustrezno število vodilnih ničel.

Po nekaj korakih računanja iz začetnega števila 2731 dobimo nova števila: $8640 - 0468 = 8172$, $8712 - 1278 = 7434$, $7443 - 3447 = 3996$, $9963 - 3699 = 6264$, $6642 - 2466 = 4176$ in $7641 - 1467 = 6174$. Tu se zaporedje novih števil ustavi, saj pri vsakem naslednjem koraku uporabimo iste številke in dobimo razliko $7641 - 1467 = 6174$.

To na prvi pogled morda ni nič posebnega, toda izkaže se, da se vsako štirimestno število, ki ima vsaj dve številki različni, po tem postopku v največ sedmih korakih spremeni v število 6174 (če ima začetno število vse številke enake, se v prvem koraku spremeni v število 0). Število 6174 imenujemo Kaprekarjeva konstanta, saj je njegovo nenavadno lastnost odkril indijski učitelj in ljubitelj matematike *Dattatreya Ramchandra Kaprekar* (1905–1986). Podobno lastnost ima med trimestnimi števili število 495. Čeprav ni znano, da bi imela Kaprekarjeva konstanta kakšen globlji pomen v matematiki ali fiziki, nam lahko v matematični učilnici služi kot zabaven čarovniški trik, v računalniški učilnici pa kot programerski izziv, ko iščemo podobna števila tudi med 5-ali večmestnimi števili. $\times \times \times$



Presek

list za mlade matematike, fizike, astronome in računalnikarje
letnik 51, šolsko leto 2023/2024, številka 1

Uredniški odbor: Vladimir Batagelj, Nino Bašič (računalništvo), Mojca Čepič, Mirko Dobovišek, Vilko Domajnko, Andrej Guštin (astronomija), Maja Klavžar, Damjan Kobal, Lucijana Kračun Berc (tekmovanja), Boštjan Kuzman (matematika), Peter Legiša, Andrej Likar (fizika), Matija Lokar, Aleš Mohorič (odgovorni urednik), Marko Razpet, Grega Rihtar (jezikovni pregled), Matjaž Vencelj, Matjaž Zaveršnik.

Dopisi in naročnine: Fakulteta za matematiko in fiziko, Presek, Jadranska ulica 19, 1000 Ljubljana, telefon (01) 4766 558.

Internet: www.presek.si

Elektronska pošta: zalozba@mf.uni-lj.si

Naročnina za šolsko leto 2023/2024 je za posamezne naročnike 25,00 EUR – posamezno naročilo velja do preklica, za skupinska naročila učencev šol 22,00 EUR, posamezna številka 6,00 EUR, stara številka 4,00 EUR, letna naročnina za tujino pa znaša 30 EUR.

Transakcijski račun: 01100-6030708962.

List sofinancira Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije iz sredstev državnega proračuna iz naslova razpisa za sofinanciranje domačih poljudno-znanstvenih periodičnih publikacij.

Založila Fakulteta za matematiko in fiziko

Oblikovanje Tadeja Šekoranja

Tisk Collegium Graphicum, Ljubljana

Naklada 1100 izvodov

© 2023 Društvo matematikov, fizikov in astronomov Slovenije in Fakulteta za matematiko in fiziko

ISSN 2630-4317 (Online), ISSN 0351-6652 (Tiskana izd.)

Razmnoževanje ali reproduciranje celote ali posameznih delov brez poprejšnjega dovoljenja založnika ni dovoljeno.

Poština plačana pri pošti 1102 Ljubljana.

NAVODILA SODELAVCEM PRESEKA ZA ODDAJO PRISPEVKOV

Presek objavlja poljudne in strokovne članke iz matematike, fizike, astronomije in računalništva. Poleg člankov objavlja Priказe novih knjig s teh področij in poročila z osnovnošolskih in srednješolskih tekmovanj v matematiki in fiziki. Prispevki naj bodo zanimivi in razumljivi širšemu krogu bralcev, učencem višjih razredov osnovnih šol in srednješolcem.

Članek naj vsebuje naslov, ime avtorja (oz. avtorjev) in sedež institucije, kjer avtor(ji) dela(jo). Slike in tabele, ki naj bodo oštevilčene, morajo imeti dovolj izčrpen opis, da jih lahko večinoma razumemo ločeno od besedila. Slike v elektronski obliki morajo biti visoke kakovosti (jpeg, tiff, eps ...), velikosti vsaj 8 cm pri ločljivosti 300 dpi. V primeru slabše kakovosti se slika primerno pomanjša ali ne objavi. Avtorji člankov, ki želijo objaviti slike iz drugih virov, si morajo za to sami priskrbeti dovoljenje (copyright). Zaželena velikost črk je vsaj 12 pt, razmak med vrsticami pa vsaj 18 pt.

Prispevke pošljite odgovornemu uredniku na naslov uredništva **Fakulteta za matematiko in fiziko, Presek, Jadranska 19, 1000 Ljubljana** ali na naslov elektronske pošte zalozba@mf.uni-lj.si.

Vsak članek se praviloma pošlje vsaj enemu anonimnemu recenzentu, ki oceni primernost članka za objavo. Če je prispevek sprejet v objavo in če je besedilo napisano z računalnikom, potem uredništvo prosi avtorja za izvirne 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.

Kazalo

MATEMATIČNI TRENUTEK

- 2 Nenavadno število 6174

UVODNIK

- 4 Več uspehov, manj ujm
(Aleš Mohorič)

MATEMATIKA

- 5-7 O delitvah na enakovredne dele
(Tadej Starčič)

FIZIKA

- 11-14 Pevec kot inštrument
(Andrej Likar)

ASTRONOMIJA

- 18-21 Teran na Astronomskem tekmovanju
treh dežel 2023
(Simon Bukovšek in Vid Kavčič)

RAČUNALNIŠTVO

- 22-28 Kratice – od tod do točke brez vrnitve
(Aleksandar Jurišić in Klemen Klanjšček)

RAZVEDRILO

- 15 Bilo je некоč v reviji Presek –
Na Presekovi črpalki
- 16-17 Nagradna križanka
(Marko Bokalič)
- 21 Križne vsote
- 29 Rešitev nagradne križanke Presek 50/6
(Marko Bokalič)
- 21 Križne vsote

TEKMOVANJA

- 8-10 Mednarodna matematična olimpijada 2023
na Japonskem
(Luka Horjak)
- 30-31 MaRSovski Estimathon
(Izak Jenko)

SLIKA NA NASLOVNICI: Zvezde in strele. Letošnje poletje je zaznamovalo neprizanesljivo vreme. Fotografija je bila posneta 18. julija v Braniku. Foto: Andrej Guštin

Več uspehov, manj ujm



ALEŠ MOHORIČ, ODGOVORNI UREDNIK

→ Pol stoletja izdajanja je za nami, z veseljem in polni elana gremo novim izzivom naproti. Letos Presek dobiva novega izdajatelja, svoje moči združujeta Društvo matematikov, fizikov in astronomov Slovenije in Fakulteta za matematiko in fiziko Univerze v Ljubljani. To se na vsebini seveda ne bo poznalo. Še vedno se lahko veselite matematičnih bombončkov, fizikalnih skrivnosti, zanimivosti iz astronomije in razcveta računalništva. Priloge z nalogami ne tiskamo več, jih pa najdete na spletni strani www.dmfa.si/Tekmovanja/, kjer v levem pasu izbere tekmovanje in nato arhiv nalog.

Minulo poletje je prineslo veliko uspeha in veselja slovenskim tekmovalcem na množici mednarodnih tekmovanj. Naj omenim 16. mednarodno olimpijado iz astronomije in astrofizike, ki je avgusta potekala v poljskem mestu Katowice, na kateri je Peter Andolšek postal najboljši mladi astronom na svetu, pa tudi drugi člani ekipe so bili izjemni. Slovenija je osvojila prvo zlato medaljo na 6. Mednarodni ekonomski olimpijadi. Na tekmovanju v znanju ekonomije, finančne pismenosti in reševanju poslovnega primera jo je osvojil Jakob Grmek. S 53. Mednarodne fizikalne olimpijade se vsi naši tekmovalci vračajo z medaljami. Peter Andolšek je osvojil zlato medaljo, že tretjo za Slovenijo na zadnjih sedmih olimpijadah. V Chibi na Japonskem se je zaključila 64. Mednarodna matematična olimpijada in na njej je Matija Skrt prejel bronasto medaljo.

Letos se bomo z več prispevki spomnili 150. obletnice rojstva Josipa Plemlja, pomembnega slovenskega matematika, prvega rektorja ljubljanske univerze. Predvidoma bodo decembra tudi izdani kovanci s Plemljevo podobo.

Poleg naštetih uspehov pa je za nami tudi poletje hudih ujm, poplav in nenavadnega vremena. Upam, da vas niso hudo prizadele in da ste vsi, ki ste potrebovali pomoč, to hitro dobili. Seveda ljudje ob takih nenavadnih pojavih marsikaj razmišljajo in govorijo, tudi o človeškem vplivu na vreme. V tem letniku pričakujte kakšen prispevek tudi na to temo.

Ker pa je revija namenjena vam, bralcem, nam sporočite, kaj ste z zanimanjem prebrali, o čem bi radi izvedeli kaj več. Uredniki bomo veseli vašega pisma.



SLIKA 1.

Vse slovenske medalje 16. mednarodne olimpijade iz astronomije in astrofizike 2023. Od leve: Marija Judež (pohvala), Žan Ambrožič (srebrna medalja), Peter Andolšek (zlata medalja, 1. mesto – zmagovalec olimpijade, zmagovalec v opazovalnem delu, zmagovalec v obdelavi podatkov), Miha Brvar (srebrna medalja), Žan Arsov (bronasta medalja). Foto: Andrej Guštin



O delitvah na enakovredne dele



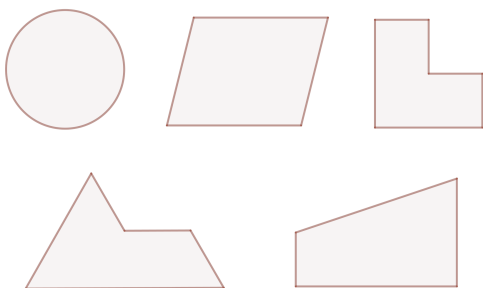
TADEJ STARČIČ

→ Vsakdo izmed vas je gotovo že kdaj naletel na kakšen problem delitve na enakovredne dele, morda zgolj v obliki kakšne miselne naloge ali kaj bolj konkretnega. V tem sestavku se bomo dotaknili nekaterih zanimivih problemov delitev, od bolj teoretičnih, pa do bolj praktičnih.

Kdaj sploh sta dva dela enakovredna? To je odvisno od tega, kaj nas zanima. Enkrat bo to pomenilo, da sta dela skladna geometrijska lika, drugič lika enakih ploščin, tretjič pa množici enakih kardinalnosti.

Začnimo z zabavnim izzivom.

Problem 1. (Delitev lika na skladne dele) Dane like z eno potezo (tj. z neprekinjeno krivuljo) razrežite na dva skladna lika:



SLIKA 1.

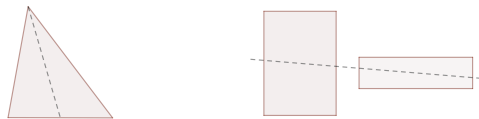
Ravninski liki.

Ali gre tudi z ravnim (tj. premočrtnim) rezom? Je to mogoče storiti na več načinov? Ali lahko katerega izmed likov razrežete na 3, 4 ali še več skladnih likov?

S prvimi tremi liki na sliki 1 zagotovo ne boste imeli večjih težav, kratko obravnavo drugih dveh pa po potrebi najdete v knjigi [1, pogl. 3]. Rešitev nameroma nismo skicirali, saj bi z njimi lahko marsikoga prikradjali za veselje pri reševanju.

Problem 2. (Delitev likov na ploščinsko enake dele) Ali lahko poljuben trikotnik z ravnim rezom razrežemo na dva ploščinsko enaka dela? Ali lahko

tudi poljuben dva pravokotnika v ravnini hkrati razrežemo na dva ploščinsko enaka dela z enim ravnim rezom? Ali velja to tudi za like bolj kompliciranih oblik?



SLIKA 2.

Razpolovitev z enim ravnim rezom.

Vemo, da težiščnica razdeli trikotnik na dva trikotnika s skladnima stranicama in višinama nanju, ter sta zato enakih ploščin. Rešitev drugega dela problema 2 je rez, ki gre skozi središči pravokotnikov, saj vsaka premica skozi središče pravokotnika le-tega razdeli celo na skladna dela; glejte sliko 2. Odgovor na tretje vprašanje pa je morda za koga malce presenetljiv.

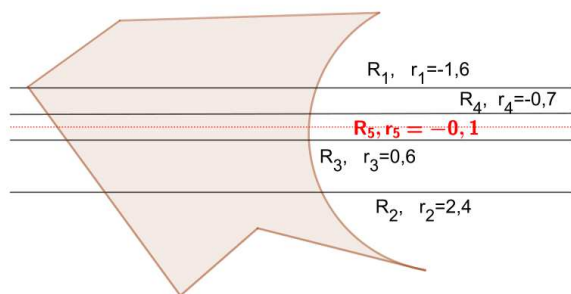
Izrek 1. (Obstoj delitve lika na ploščinsko enaka dela) Poljuben ravninski lik¹ je z ravnim rezom vedno mogoče razdeliti na dve ploščinsko enaki polovici. Obstaja več takih rezov.

Dokaz. S postopkom, ki mu rečemo bisekcija, bomo konstruirali zaporedje vodoravnih rezov R_n , ki se bo pomikalo proti iskanemu rezu. Ideja je vsak naslednji rez malo vzporedno premakniti, da se ploščini pripadajočih delov še bolj približata polovici ploščine lika. Naj rez R_n razdeli lik s ploščino p na dva dela, tisti del na zgornji polravnini naj ima ploščino p_n , ter naj bo $r_n := \frac{p}{2} - p_n$. Če je r_n blizu 0, potem je p_n blizu $\frac{p}{2}$. Izberimo najprej reza R_1 in R_2 tako, da bo $r_1 < 0 < r_2$. Nadalje denimo, da smo za neki $n \geq 2$ že izbrali take vzporedne vodoravne reze $R_1, \dots, R_n$, da je $r_1, \dots, r_n \neq 0$. Rez R_{n+1} nato izberemo na sredini med rezom R_n in njemu najbližjim

¹Ravninski lik je območje v ravnini, omejeno z enostavno sklenjeno krivuljo. Kakorkoli ga s premico razrežemo na dva dela, vedno lahko določimo ploščini posameznih delov.



→ že izbranim rezom, označimo ga z R_m ($m < n$), da je r_m nasprotnega predznaka kot r_n (slika 3). Tako bo število r_{n+1} zagotovo med r_n in r_m , razdalja med R_n in R_{n+1} pa se v primerjavi z razdaljo med R_{n-1} in R_n prepolovi. Bralec bo z nekaj osnovnega znanja o limitah znal utemeljiti, da nas to pripelje k rešitvi. Jasno je tudi, da lahko naklon rezov izberemo poljubno, zato je ustreznih rezov neskončno. ■



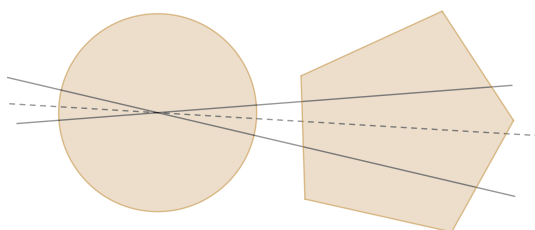
SLIKA 3.

Primer štirih korakov bisekcije lika na dva dela.

Izrek 2. (Izrek dveh palačink) Dva ravninska lika poljubnih oblik je mogoče z enim ravnim rezom enkrat razrezati na dva ploščinsko enaka dela.

Skica dokaza. Uporabimo prvi del izreka, natančneje reze, ki prvi lik razdelijo na ploščinsko enaka dela; na sliki 4 je poseben primer z rezi skozi eno točko. Rešitev da spet bisekcija.

Podrobnosti oziroma natančen dokaz najdemo med drugim v odlični knjigi [3, pogl. 22], kjer so sicer na izviren način lepo prestavljeni še številni drugi matematični problemi. ■



SLIKA 4.

Poseben primer izreka dveh palačink za en zelo simetričen lik.

Velja še splošnejši izrek o delitvi treh teles v prostoru na enake dele, t. i. **izrek o sendviču**: *Sendvič je mogoče z ravnino razrezati na dva dela, ki vsebujeta prostorninsko enako kruha, salame in sira*. Kot vprašanje ga je leta 1938 zastavil Steinhaus², s pomočjo izrekov višje matematike pa dokazal Banach³; glejte monografijo [2, pogl. 3].

Oglejmo si sedaj delitev množice s števno končno točkami.

Problem 3. (Razdelitev dveh vrst draguljev na dva enaka dela) Krona vsebuje 6 rubinovih in 4 diamantne dragulje. Ali jo lahko z ravnim rezom vedno prežemo tako, da bo vsak od dveh delov vseboval enako število rubinovih oziroma diamantnih draguljev? Kaj pa, če je draguljev več?

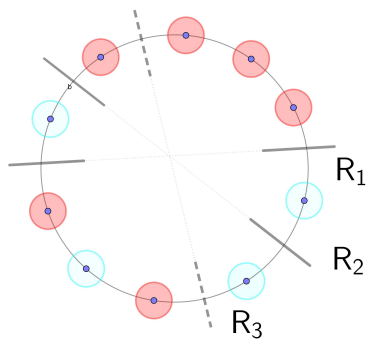
Začnimo s parom rezov R_1 , ki krono razrežeta na dve polovici s po petimi dragulji. Sedaj induktivno nadaljujemo z zaporedjem R_n takih parov rezov, da je vsak naslednji premaknjen za eno mesto v pozitivni smeri. Na sliki 5 spodaj vidimo primera rezov R_1, R_2 in R_3 .

Jasno je število rubinovih draguljev na obeh straneh enako natanko tedaj, ko je na obeh straneh enako tudi diamantnih draguljev. Za vsak rez R_n označimo število rubinovih draguljev prve polovice z r_n , število rubinovih draguljev na drugi polovici je potem $6 - r_n$, razlika med polovico 3 in r_n pa je $d_n := 3 - r_n$ (slika 5). Opazimo, da se R_6 ujema z R_1 , le vlogi polovic se zamenjata, t.j. $r_6 = 6 - r_1$, ter zato $d_6 = 3 - r_6 = r_1 - 3 = -d_1$. Po drugi strani se na posameznem koraku število rubinovih draguljev ne spremeni bodisi se poveča ali zmanjša za 1; s tem se d_n ne spremeni ali se spremeni za 1. Če je $d_1 = 0$, je R_1 že v redu, sicer pa sta začetni in končni člen zaporedja d_n različnega predznaka, ter lahko spet z bisekcijo, kot v dokazu izreka 1, pridemo do nekega vmesnega člena zaporedja, ki je enak 0. Pripadajoči rez je seveda rešitev naloge.

Bralcu bo zagotovo uspelo rešitev problema 3 prilagoditi za primer poljubnih dveh sodih števil rubi-

²Hugo Steinhaus (1887–1972) je bil poljski matematik; dejaven je bil na različnih področjih, med drugim je bil med začetniki teorije verjetnosti in teorije iger.

³Stefan Banach (1892–1945) je bil poljski matematik; začetnik moderne funkcionalne analize.



n	1	2	3	4	5	6
r_n	4	4	3	3	2	2
$6 - r_n$	2	2	3	3	4	4
d_n	-1	-1	0	0	1	1

SLIKA 5.

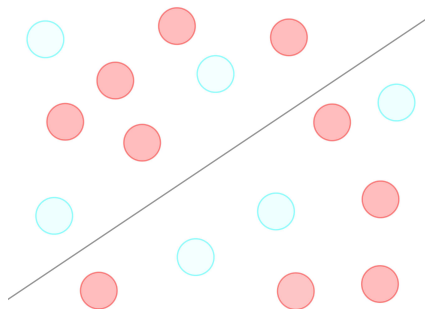
Primer krone z razrezi R_1 , R_2 in (iskanim) R_3 , ter tabela vrednosti pripadajočih zaporedij r_n in d_n .

novih in diamantnih draguljev. V duhu te rešitve bi bilo mogoče dokazati naslednji izrek.

Izrek 3. (Diskretna verzija izreka dveh palačink)

V ravnini je $2r$ rdečih in $2m$ modrih točk v splošni legi, tj. nobene tri ne ležijo na isti premici. Potem obstaja premica, ki ravnino razdeli na dve polravnini tako, da je na vsaki od polravnin r rdečih in m modrih točk (slika 6).

Z orodji višje matematike je mogoče dokazati t. i. **diskretno verzijo izreka o sendviču**: *Točke treh*



SLIKA 6.

Diskretna verzija izreka dveh palačink.

barv (sodo število točk vsake barve) v prostoru je mogoče z ravnino razdeliti na dva dela, ki vsebujeta številčno enako točk vsake od barv. Uporaba tega izreka omogoča posplošitev problema 3 na krono z dragulji treh vrst dragih kamnov, ki je v literaturi znana tudi kot **problem ogrlice**; več o tem najdete v že omenjenem viru [2, pogl. 3].

Za konec je tu nekaj kratkih geometrijskih nalog o razpolavljanju, ki jih poskusite rešiti sami.

Naloga 1. Dani dve daljici s premico hkrati razdelite na dva skladna dela. Kaj pa tri daljice?

Naloga 2. Dokažite, da vzporednica stranice danega trikotnika, ki ploščinsko razpolovi ta trikotnik, razdeli ostali dve stranici v razmerju $1 : (1 + \sqrt{2})$.

Naloga 3. Trikotnik z ravnim rezom razdelite na dva trikotnika z enakima obsegoma. Ali lahko vsak ravninski lik prerežemo na dve polovici z enakima obsegoma?

Naloga 4. Poiščite kakšno ravnino, ki dano tristrano piramido (lahko poševno) razdeli na dva prostorninsko enaka dela.

Naloga 5. Samo z uporabo šestila (brez ravnila) razdelite dano krožnico na dve polkrožnici. Nekoliko težje je dano daljico s šestilom razdeliti na dva skladna dela. Poskusite.

Morda se boste bralci kdaj srečali s kakšnim novim oziroma drugačnim problemom delitve. Tudi v tem primeru vam utegne pridobljeno znanje ter širši pogled na tematiko priti zelo prav.

Literatura

- [1] M. Gardner, *Aha! pa te imam: paradoksi za nape-njanje možganov in razvedrilo*, DZS, ZOTKS, Ljubljana, 1988.
- [2] J. Matoušek, *Using the Borsuk-Ulam theorem. Lectures on topological methods in combinatorics and geometry*, Springer-Verlag, Berlin, 2003.
- [3] J. Tanton, *Solve This: Mathematical Activities for Students and Clubs*, Mathematical Association of America, 2012.

× × ×

Mednarodna matematična olimpijada 2023 na Japonskem



LUKA HORJAK

→ Med 2. in 13. julijem je v Chibi na Japonskem potekala 64. Mednarodna matematična olimpijada. Slovensko ekipo so na tekmovanju zastopali Erik Červek Roškarič (II. gimnazija Maribor), Lenart Dolinar (Gimnazija Bežigrad), Katarina Grilj (Srednja šola Slovenska Bistrica), Kaja Rajter (II. gimnazija Maribor), Matija Skrt (Gimnazija Nova Gorica) in Hugo Trebše (Gimnazija Bežigrad). Tekmovalce sva na olimpijadi spremljala Gregor Dolinar in Luka Horjak.

Matija Skrt je ponovil svoj lanski dosežek in znova osvojil bronasto medaljo. Tokrat se z Japonskega prav vsi naši tekmovalci vračajo s pohvalo, ki jo prejmejo tisti udeleženci, ki v celoti pravilno rešijo vsaj eno izmed šestih zahtevnih nalog. Slovenija je med 112 sodelujočimi državami zasedla 64. mesto. Prvo mesto je že petič zapored osvojila Kitajska – edina država, ki si je letos prislužila 6 zlatih medalj, sledile pa so ji ZDA, Južna Koreja in na 4. mestu še Romunija, ki je bila najuspešnejša med evropskimi državami.

Na olimpijadi sta tekmovalce čakala dva tekmovalna dneva. Vsak dan so imeli 4 ure in pol časa za reševanje treh zahtevnih nalog. Te nekaj mesecev pred tekmovanjem predlagajo države, ki ne gostijo tekmovanja, organizator pa je zadolžen za sestavo komisije, ki izmed teh izberejo najprimernejše, s katerimi sestavijo ožji izbor. Letos je 52 držav skupaj predlagalo 167 nalog, izmed teh jih je v ožji izbor prišlo 30. Izmed teh nekaj dni pred samim tekmovanjem vodje ekip glasujejo za 6 problemov, ki se nato pojavijo na tekmovanju. O njihovi težavnosti priča dejstvo, da je vseh 42 možnih točk doseglo le 5 izmed 618 tekmovalcev, povprečno število točk pa je bilo 17,7. Da si bomo te izzive lažje predstavljali, si oglejmo dve nalogi s tekmovanja in njuni rešitvi. Nalogi sta predlagali Kolumbija in Nizozemska.



SLIKA 1.

Slovenska ekipa na 64. Mednarodni matematični olimpijadi

Naloga 1. Določi vsa sestavljena naravna števila $n > 1$, ki imajo naslednjo lastnost: če so $d_1, d_2, \dots, d_k$ vsi pozitivni delitelji števila n , pri čemer je $1 = d_1 < d_2 < \dots < d_k = n$, potem d_i deli $d_{i+1} + d_{i+2}$ za vsak $1 \leq i \leq k - 2$.

Rešitev 1. naloge Da razvijemo intuicijo, katera naravna števila sploh rešijo nalogo, si oglejmo nekaj posebnih primerov. Pogosta strategija je vstavljanje konkretnih vrednosti, na primer $n = 12$, lahko pa se tega lotimo splošneje. Oglejmo si najprej števila, ki imajo zelo malo deliteljev. Ker naloga sprašuje le o sestavljenih številih, začnimo s primerom $n = pq$, kjer sta p in q praštevili.

Če velja $p < q$, se lahko hitro prepričamo, da so 1, p , q in pq kar vsi delitelji števila n , poleg tega pa so še urejeni po velikosti. Tako mora veljati

$$\blacksquare \quad 1 \mid p + q \quad \text{in} \quad p \mid q + pq.$$

Prva deljivost očitno vedno velja, pri drugi pa naletimo na težavo, saj mora veljati $p \mid q$. To seveda

ne velja, saj smo predpostavili, da sta p in q različni praštevil.

Majhno število deliteljev dobimo tudi v primeru $p = q$ oziroma $n = p^2$, kjer je p praštevilo. Vsi delitelji števila n so tako kar 1, p in p^2 . Ni težko videti, da je v tem primeru pogoj z deljivostjo izpolnjen, zato kvadrati praštevil izpolnijo dan pogoj.

Na podlagi primera $n = pq$ se zdi, da imajo iskana naravna števila n največ enega praštevilskega delitelja, oziroma, da so to natanko potence praštevil. Ta sum lahko dodatno potrdimo z dejstvom, da vse potence praštevil res izpolnijo dan pogoj. Če je $n = p^\ell$, so namreč vsi delitelji kar 1, p , $p^2, \dots, p^\ell$. Pogoj je tako ekvivalenten

$$\blacksquare \quad p^i \mid p^{i+1} + p^{i+2}$$

za vse $0 \leq i \leq \ell - 2$, kar seveda drži.

Sedaj predpostavimo, da ima n vsaj dva različna praštevilska delitelja. Naj bosta p, q , kjer je $p < q$, njegova najmanjša praštevilska delitelja. Za delitelje števila n torej velja $d_1 = 1$, $d_2 = p$, za d_3 pa imamo 2 možnosti – lahko velja $d_3 = q$, ali pa $d_3 = p^2$.

Obravnavajmo najprej primer, ko je $d_3 = q$. V tem primeru mora veljati deljivost

$$\blacksquare \quad p \mid q + d_4.$$

Za primerno izbiro delitelja d_4 bi ta deljivost lahko bila izpolnjena. To nam celo zagotavlja Dirichletov izrek, ki pravi, da za vsaki tuji si naravni števili a in b obstaja neskončno mnogo praštevil oblike $ak + b$.⁴ Dovolj je namreč najti praštevilo oblike $d_4 = kp - q$, ki obstaja po Dirichletovem izreku. Izrek sicer ne zagotavlja, da bo pri tem še vedno izpolnjena urejenost deliteljev, nam pa pove, da ne bomo prišli do protislovja na elementaren način. Z najmanjšimi delitelji tako ne bomo prišli prav daleč.

Drugi ekstrem so največji delitelji števila n . Znano je, da delitelji naravnih števil nastopajo v parih – če je d delitelj števila n , je to tudi $\frac{n}{d}$. S tem predpisom se najmanjši delitelji preslikajo v največje. Največji delitelji števila n so torej n , $\frac{n}{p}$ in $\frac{n}{q}$. Sledi, da mora veljati

$$\blacksquare \quad \frac{n}{q} \mid \frac{n}{p} + n,$$

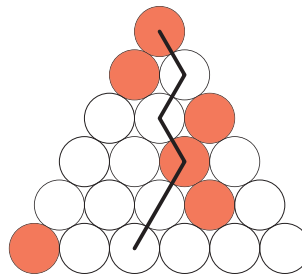
kar je ekvivalentno

$$\blacksquare \quad \frac{\frac{n}{p} + n}{\frac{n}{q}} = \frac{q}{p} + q \in \mathbb{N}.$$

To seveda ni mogoče, saj sta p in q različni praštevil.

Preostane nam še primer, ko je $d_3 = p^2$. V tem primeru so najmanjši delitelji števila n po vrsti 1, p , $p^2, \dots, p^\ell$ in q . Tudi tu lahko hitro pridemo do protislovja, in sicer z zaporednimi delitelji $p^{\ell-1}$, p^ℓ in q ali pa $\frac{n}{q}$, $\frac{n}{p^\ell}$ in $\frac{n}{p^{\ell-1}}$. Pogoj tako res izpolnijo natanko potence praštevil.

Naloga 5. Naj bo n naravno število. *Japonski trikotnik* je sestavljen iz $1 + 2 + \dots + n$ krogov, ki so razporejeni v obliki enakostraničnega trikotnika, tako da je za vsak $i = 1, 2, \dots, n$ v i -ti vrstici natanko i krogov in je v vsaki vrstici natanko en krog pobarvan rdeče. *Nindževa pot* v japonskem trikotniku je zaporedje n krogov, ki se začne v krogu v najvišji vrstici, nato pa se ponavljajoče nadaljuje iz trenutnega kroga v enega izmed krogov, ki sta neposredno pod njim, in se konča v najnižji vrstici. V odvisnosti od n poišči največji k , tako da za vsak japonski trikotnik obstaja nindževa pot, ki vsebuje vsaj k rdečih krogov.



SLIKA 2.

Primer nindževe poti za $n = 6$, ki vsebuje 2 rdeča kroga

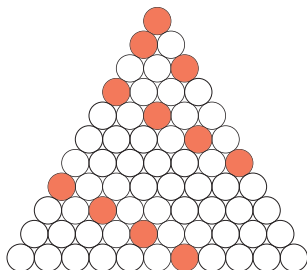
Rešitev 5. naloge Za začetek si oglejmo, kaj se zgodi za majhne vrednosti števila n . Ni težko videti, da pri $n = 1$ vedno dobimo nindževo pot dolžine 1, pri $n = 2$ pa pot dolžine 2. Podobno za $n = 3$ dobimo pot dolžine 2.

Nadaljnje konstrukcije lahko poiščemo rekurzivno. Intuitivno bi želeli v zaporednih vrsticah imeti

⁴Pri tem je število b lahko tudi negativno.



rdeče kroge čim bližje, a ne tako blizu, da bi lahko nindževa pot vsebovala oba. Tako lahko začnemo z rdečim krogom skrajno levo, v vsaki naslednji vrstici pa pozicijo rdečega trikotnika povečamo za 2. Tako dobimo nekakšne »diagonale«, ki jih vidimo na sliki 3.



SLIKA 3.

Japonski trikotnik, ki nam da mejo $k \leq \lfloor \log_2(n) \rfloor + 1$

Opazimo, da lahko nindževa pot vsebuje kvečjemu en rdeč krog z vsake diagonale. Za omejitev števila k zadošča, da preštejemo te diagonale. Ni se težko prepričati, da i -ta diagonala vsebuje 2^{i-1} rdečih krogov (lahko tudi manj, če vsebuje rdeč krog v zadnji vrstici). Če trikotnik vsebuje ℓ diagonal, mora tako veljati

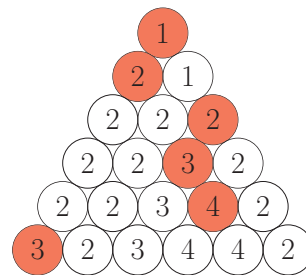
$$\blacksquare \quad n \leq 2^0 + 2^1 + \dots + 2^{\ell-1} = 2^\ell - 1.$$

Ta neenakost je prvič izpolnjena pri $\ell = \lfloor \log_2(n) \rfloor + 1$. Tako dobimo $k \leq \lfloor \log_2(n) \rfloor + 1$.

Sedaj moramo dokazati še, da vsak japonski trikotnik vsebuje nindževo pot z vsaj $\lfloor \log_2(n) \rfloor + 1$ rdečimi krogi. Začnimo tako, da v vsak krog v japonskem trikotniku zapišemo število, in sicer največje možno število rdečih krogov, ki so vsebovani v neki poti od vrha trikotnika do tega kroga. Primer takega oštevilčenja lahko vidimo na sliki 4.

Sedaj je dovolj pokazati, da v zadnji vrstici obstaja krog s številom vsaj $\lfloor \log_2(n) \rfloor + 1$. Seveda se je dovolj omejiti na števila $n = 2^m$, saj lahko vsako nindževo pot razširimo do nindževe poti v večjem trikotniku.

Oglejmo si števila v dveh zaporednih vrsticah. Da dobimo števila v novi vrstici, za vsak krog vzamemo največje število v njegovih dveh predhodnikih. Če je krog rdeč, na koncu še prištejemo 1. Denimo, da so $v_1, v_2, \dots, v_i$ števila v i -ti vrstici, v_m pa je največje izmed teh. Sledi, da so števila v vrstici $i+1$ večja ali enaka od $v_1, v_2, \dots, v_{m-1}, v_m, v_m, v_{m+1}, \dots, v_i$,



SLIKA 4.

Oštevilčenje trikotnika

pri čemer še nismo upoštevali rdečega kroga v vrstici $i+1$.

Sedaj pridemo do naslednje pomembne ideje – opazujemo lahko vsoto števil v vrstici. Večja kot bo vsota, večja morajo namreč biti števila v tej vrstici. Po zgornji opazki je vsota števil v vrstici $i+1$ večja ali enaka

$$\blacksquare \quad v_1 + v_2 + \dots + v_i + v_m + 1.$$

Sedaj zadošča dokazati, da je v vrstici $n = 2^t$ vsota večja ali enaka $t \cdot n + 1$. Po Dirichletovem principu bo namreč sledilo, da obstaja krog s številom vsaj $t+1$, kar je ravno naš cilj. To dokažimo z indukcijo. Baza je seveda izpolnjena, saj je za $t=0$ neenakost trivialno izpolnjena.

Sedaj si oglejmo $n = 2^{t+1}$. Vsota števil v vrstici $\frac{n}{2}$ je po indukcijski predpostavki večja ali enaka $t \cdot 2^t + 1$. V naslednji vrstici se vsota poveča za vsaj $v_m + 1$, kjer je v_m največji element vrstice 2^t . Po Dirichletovem principu pa velja, da je

$$\blacksquare \quad v_m \geq \frac{t \cdot 2^t + 1}{2^t} > t,$$

zato je vsota naslednje vrstice enaka vsaj

$$\blacksquare \quad t \cdot 2^t + 1 + (t+1) + 1.$$

Opazimo lahko še, da se največji element z vsako novo vrstico lahko kvečjemu poveča. Tako je vsota v zadnji vrstici enaka vsaj

$$\blacksquare \quad t \cdot 2^t + 1 + 2^t \cdot (t+1) + 2^t \cdot 1 = (t+1) \cdot 2^{t+1} + 1,$$

kar smo želeli dokazati.

xxx

Pevec kot inštrument



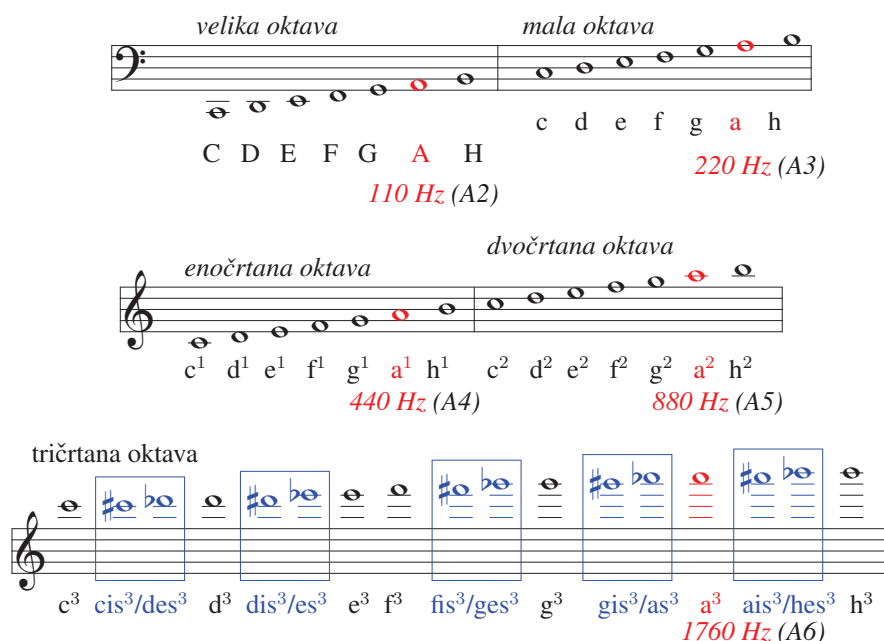
ANDREJ LIKAR

→ Glasbo izvajamo z glasbenimi inštrumenti. Način vzbujaanja zvočnih valov je pri inštrumentih zelo različen. Godala in brenkala uporabljajo napete strune, ki nihajo v zraku. Pri trobilih nihajo glasbenikove ustnice, pri pihalih pa tenki jezički. Pevci ne potrebujejo inštrumenta, inštrument so kar sami. Zvok tvorita glasilki, tenki opni v grlu pevca. Preden se zvok razširi v okolico, se od vira v instrumentih še oblikuje. Pri godalih za to skrbijo resonančne škatle, pri trobilih in pihalih cevi, pri pevcih pa ustna in nosna votlina.

Glasilke ne nihajo povsem harmonično, bolj kot ne se iz njih širijo hitro ponavljajoči se poki, ki v ustni in nosni votlini vzbudijo nihanja z dvakrat, trikrat, štirikrat ... višjimi frekvencami, kot je frekvenca teh pokov, ki ji rečemo osnovna frekvenca ali osnovni ton. Zvok pevca je zato sestavljen iz številnih to-

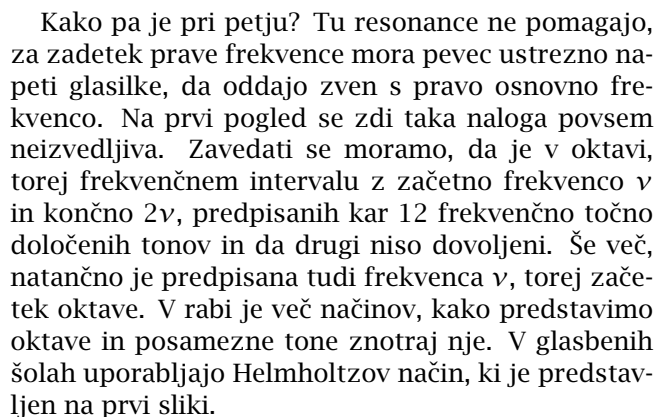
nov, je torej neke vrste zven. Tone pri višjih frekvencah od osnovne imenujmo *formante* in prav jakosti zvoka teh formantov ločijo dobre pevce od slabih. Pri vrhunskih opernih pevcih jakost zvoka v danem formantu lahko močno preglesi zvok orkestra, kar omogoča, da slišimo pevca tudi ob glasni spremljavi.

Zanimivo vprašanje je, kako glasbeniki zadevajo predpisane tone v skladbi. Pri glasbilih s tipkami je to vprašanje odveč, saj s pritiskom na tipko dobimo dan zven, na njegovo osnovno frekvenco ne moremo vplivati, pravilnost frekvence zagotavlja dobra uglasitev inštrumenta. Pri godalih mora izvajalec postaviti prst na določeno mesto na struni in pri hitrih menjavah not navadno nima možnosti kaj prida popravljati frekvence. Pri trobilih mora glasbenik kar se da natančno nastaviti napetost ustnic, da izzove ustrezen ton. Iz izkušenj z igranjem kljunaste flavte sklepam, da trobilcem in pihalcem pomagajo priti do ustreznega zvena resonance različno dolgega ocevja. Njegovo dolžino spreminjajo z odpiranjem in zapiranjem ventilov, luknjic ali pri pozavni z izvlekom cevi.



SLIKA 1.

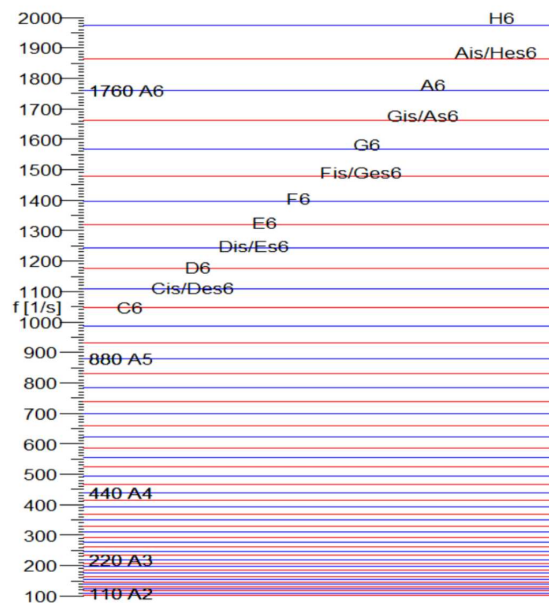
Helmholtzov način predstavitve oktav. V zadnji vrstici so v okvirjih zapisane note, ki jih na klavirju zaigramo z isto črno tipko.



Preprostejši (znanstveni) način pa podaja slika 2. Imenu tona preprosto pripišemo številko oktave, pri čemer je tista s predpisano frekvenco tona A $\nu_{A4} = 440$ Hz četrta oktava (ton A4), iz tega pa sledijo frekvence tona A drugih oktav (A3 pri 220 Hz, A5 pri 880 Hz ...). Toni oktav se začnejo z oznako Cn, potem pa sledijo toni Cis, Dn, Dis, En, Eis ... do Hn in nato spet C(n+1). Razmerje frekvenc med posameznimi zaporednimi dovoljenimi toni je vedno $2^{1/12}$, torej je frekvenca naslednjega tona 1,0594631 ... krat večja od prejšnjega. In ne pozabimo, da dobro slišimo kar 8 oktav, torej je v kromatični tonski lestvici predpisanih kar okrog 100 tonov. Na sliki 2 smo predstavili dovoljene tone v intervalu med 100 Hz in 2000 Hz z vodoravnimi črtami izmenjaje z modro in rdečo barvo. Imena tonov so v obeh načinih predstavitve oktav pač enaka.

Dovoljene frekvence so torej v glasbi natančno določene. Na njih so uglasjeni inštrumenti, jasno pa jih vidimo na klaviaturi inštrumentov s tipkami, kjer vsaki tipki pripada tak dovoljeni osnovni ton. Igranje v skupinah seveda terja pristop z dovoljenimi frekvencami, sicer bi se glasba slišala zelo razglašeno in za uho neprijetno. Nas niti ne bo zanimalo kaj več kot to, kar smo povedali. Če koga zgodovina glasbenih lestvic bolj zanima, najde na spletu pregleden Presekov članek Marije Vencelj z naslovom *Glasba in matematika. 1. in 2. del*.

Kako pevci pridejo do zvena s predpisano osnovno frekvenco? Pevci imajo pretanjen posluh in vedo, kdaj je osnovna frekvenca zvena prava. Na misel nam zato pride princip povratne zanke, ki je splošno uporaben pri vsakovrstnih merjenjih in regulacijah. Pri povratni zanki primerjamo dve količini – referenčno, torej predpisano, in opazovano (izmer-

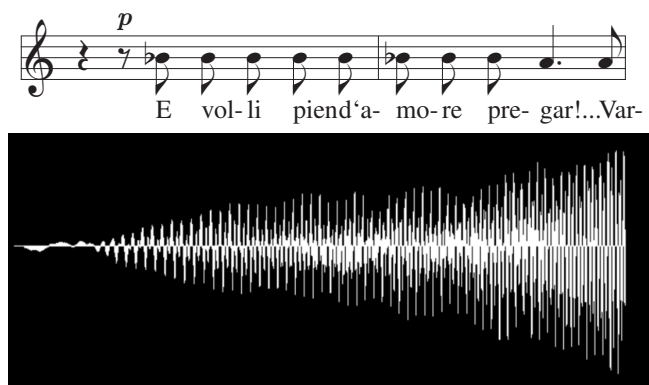


Kromatična tonska lestvica, ki jo zadnjih 300 let uporabljamo v zahodni glasbi. Oktave štejemo od tonov C, poimenovani so toni šeste oktave.

jeno), ter na osnovi njune razlike spreminjamo opazovano, da se kar se da hitro približa referenčni. To v našem primeru pomeni, da bi pevec poslušal svoj glas in ga spreminjal toliko časa, da bi se približal predpisanemu. Pa preizkusimo to možnost! V ta namen bomo natančno analizirali posneto petje kakega znanega pevca. Zame je Luciano Pavarotti daleč najboljši operni pevec, kar sem jih slišal, analizirajmo torej njegovo petje. V operi Andrea Chenier skladatelja Umberta Giordana, je Pavarotti pel skupaj z Montserrat Caballe in Leom Nuccijem ter v spremstvu orkestra angleške Nacionalne Opere. Posnetek opere imam na voljo na dveh CD ploščah, torej lahko po mili volji analiziram digitalni zapis zvočnih valov.

Na CD plošči najdemo digitalni zapis signala iz dveh mikrofонов, vzorčenega 44100-krat v sekundi. Vsak vzorec je predstavljen z dvema baytoma, torej 16 biti. V zapisu sledita baytoma za levi mikrofón bayta za desni. Podatkovne datoteke so zato zajetne, arija Andree v prvem dejanju opere, na primer, vsebuje nekaj nad 48 megabaytov. Zapisa na CD plo-

šči moramo pretvoriti v običajno .wav ali .mp3 datoteko, da prenesemo zvočni zapis v spomin računalnika. V ta namen sem uporabil na spletu dostopen program (Switch Sound File Converter), sam pa sem napisal program, ki zapis prevede v običajni ASCII zapis v .dat datoteko. Pred tem sem moral iz zajetnega .wav zapisa izrezati koščke, ki sem jih analiziral. Za to sem uporabil na spletu dosegljiv program Audacity, s katerim izrežemo, predstavljamo in lepimo dele glasbenega zapisa iz .wav datoteke. Tudi ko pevca ne spremlja orkester ali zbor, je zvočni val videti presenetljivo zapleten. Na sliki 3 je kot primer prikazan val začetka petja brez orkestrske spremljave. Vidimo, da je val postopoma vse bolj intenziven, vrhovi so vse višji, vmes pa se začnejo pojavljati tudi vrhovi višjih frekvenc. Pavarotti v tem primeru zapoje, kar je z notami zapisano takole:

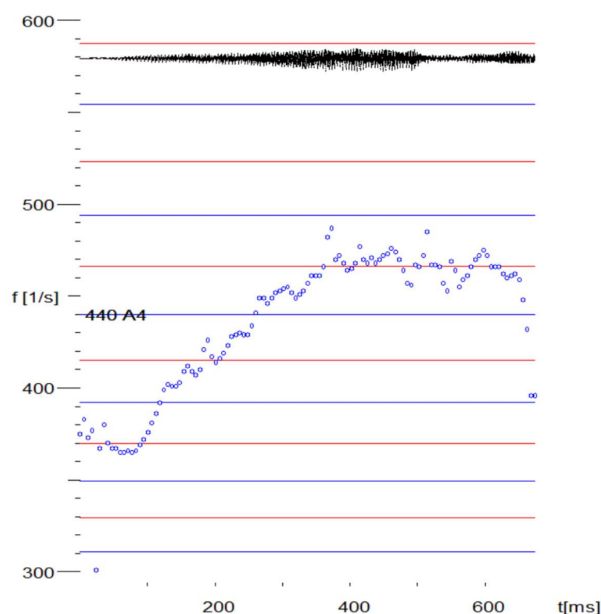


SLIKA 3.

400 ms dolg zvočni val Pavarottijevega vstopa v ariji Colpito qui m'avete ... v 1. dejanju opere, ko sam, brez spremljave orkestra ali zbora, začne peti *E volli pien d'amore pregar!* ...

Sedaj pogledimo, kako je pevec prilagajal frekvenco svojega petja. V ariji Andree *Colpito qui m'avete ov'io celo geloso* v prvem dejanju opere sem izrezal začetni del verza *E volli pien d'amore pregar!*, ko pevca ne spremlja orkester ali zbor. Ker je šele začel peti, je imel dovolj časa, da bi nadaljeval napetost svojih glasilk točno na zeleno frekvenco. A na sliki 4 vidimo, da je začel precej nižje, skoraj cela dva tona in se potem v kakšnih 300 ms približal pravi frekvenci. Prehodni čas 300 ms je prekratek, da bi poslušalec zaznal ta glissando, to je zvezno spreminjanje frekvence s časom, ko slišimo vse vmesne, torej tudi

prepovedane tone. Poleg tega pa je na začetku glas pretih, da bi ga poslušalec dobro slišal, kar vidimo v posnetem zvočnem valu na vrhu grafa. Frekvenčni potek kar dobro potrjuje, da je pevec poslušal samega sebe in postopoma prilagajal glasilke pravemu osnovnemu tonu. Analiziral sem več vstopnih točk in vselej prišel do podobnega grafa. Ko pevec že poje in zvezno preide na precej višji zven, pa njegov glissando, če smo le dovolj pozorni, dobro slišimo. V takem primeru seveda pevec mora med petjem spreminjati napetost glasilk in je relativno počasen prehod neizogiben, morda umetniško celo zaželen.



SLIKA 4.

Frekvenčni potek osnovnega tona začetka Pavarottijevega petja *E volli pien* ... Na vrhu slike je s črno barvo nakazano nihanje tlaka ob mikrofону, kot je zapisano na CD-ju. Tu vidimo, kako se glasnost zapisanega zvoka spreminja s časom.

Glede na povedano pevec potrebuje kakih 200 ms, da zadane pravi osnovni ton. Kaj pa, če tega časa preprosto nima? Spomnimo se arije Kraljice noči iz drugega dejanja Mozartove opere Čarobna piščal. Pri tej ariji, ki slovi kot ena najtežjih v vsem opernem repertoarju, mora pevka več kot desetkrat na hitro, vsakih 100 ms, zapeti in odpeti različne glasove izredno visokih frekvenc. Ker nima na voljo prav nič časa za





kakšno prilagajanje, mora v kratkem presledku med dvema glasovoma nastaviti napetost glasilk in zapeti na ves glas in kar zapoje, pač zapoje. Ker imam na voljo prenovljen posnetek (iz leta 1963) te opere na dveh CD ploščah, sem analiziral petje slovite slovaške sopranistke Lucie Popp. Del petja, ki sem ga analiziral, je v notnem zapisu označen z rdečo barvo.



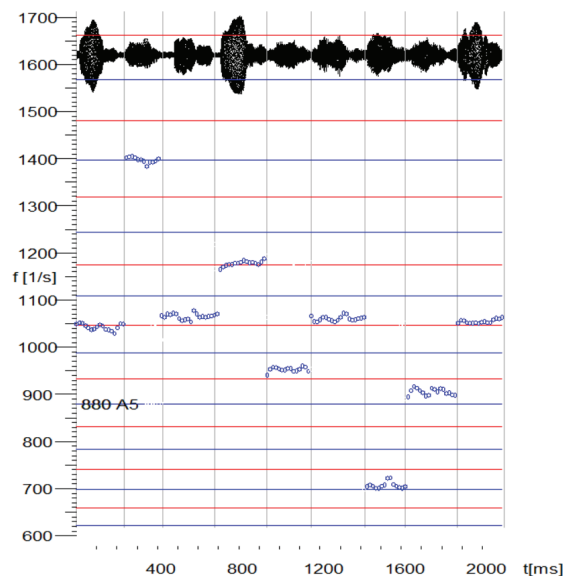
SLIKA 5.

Notni zapis dela arije Kraljice noči iz Mozartove opere Čarobna piščal. Analiziran je bil del petja, zapisan z rdečo barvo.

Na sliki 6 je prikazan potek njenega petja v delu arije, kjer poje posamezne glasove nepovezano (staccato), torej vsak glas ločen od drugih. Potek valovanja kaže dele s petjem, sledijo pa precej tišji intervali, ki so le odmevi delov s petjem. V času odmeva pevka prilagodi svoje glasilke za naslednji glas. Glasovi se hitro izmenjujejo, v dveh sekundah pevka odpoje 9 različnih glasov. Iz časovnega poteka frekvenc vidimo, da nekatere osnovne tone zadene povsem natančno, nekaterih pa ne, razlike med zapetim in napisanim so lahko tudi četrtno tona. Te napake pa pri poslušanju ne motijo, ker se toni tako hitro menjavajo in so vedno vmes povsem pravilno zapeti. Ko pa ta pevka v isti ariji zapoje dalj časa trajajočo noto, se spet po kakšnih 200 ms približa pravemu tonu z obilico vibrata.

Pri hitrem igranju violine so glasbeniki v podobnem škripcu, Za prilagajanje ni časa, če pa violinist igra solo brez orkestra, nima niti tonalne zaslombe pri njem. Izraelsko-ameriški violinist Itzhak Perlman je tako hitro skladbo, kjer mestoma zaigra kar 10 not v sekundi, predstavil na enih svojih CD plošč z Bachovimi sonatami in partitami za violino solo. Analiza pokaže, da nekateri toni pri tem niso povsem natančno zadeti, a je napaka povsod manjša kot četrtna predpisanega tona.

Za konec naj povemo, da s to analizo nismo imeli namena kakorkoli kritizirati omenjenih glasbenikov. Lahko se le čudimo, kako so z vajo in izrednim glasbenim poslušom prišli do skoraj popolnega izvajanja. Omenili smo le petje in igranje na violino, a



SLIKA 6.

Dve sekundi trajajoč odlomek iz arije Kraljice noči iz Mozartove Čarobne piščali. Nekateri osnovni toni niso povsem natančno zapeti.

ne dvomimo, da nekaj podobnega velja tudi za glasbenike na drugih instrumentih. Prav zanimivo bi bilo proučiti igranje trobilcev, morda tudi pihalcev in ugotoviti, kako oni pridejo do predpisanih osnovnih tonov. O fiziki petja, posebno o zvenu pevčevega glasu, pa bo bralec več izvedel v članku The Acoustic of the Singing Voice avtorja Johana Sundberga, objavljenega v reviji Scientific American marca leta 1977.

Ob strani smo pustili vprašanje, kako smo prišli do iskanih osnovnih tonov pri glasovih. Ker so zvočni valovi praviloma izjemno zapleteni, je metoda s preštevanjem vrhov v izbranih časovnih intervalih prepočasna in nezanesljiva. Kot rečeno, so zveni pri petju hitro zelo zapleteni in niti ne vemo, ob katerem času se pojavi kak vrh. S to metodo sem sicer začel, a kmalu uvidel, da bom moral analizo avtomatizirati. Tak avtomatski način iskanja spektrov, to je tonov v danem zvenu, ni prav zelo zahteven za nekoga, ki pozna osnove tako imenovane Fourierove analize signalov, a o tem morda kdaj drugič.

× × ×

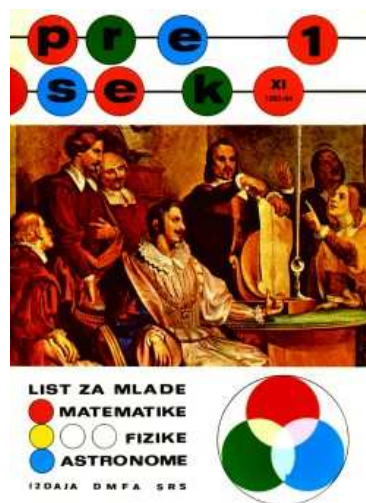
Na Presekovi črpalki

LETNIK 11, ŠTEVILKA 1, 1983/84

↓↓↓

→ Starejši bralci in bralke revije Presek se bodo gotovo spomnili, da je bila cena goriva v osemdesetih letih zaradi visoke inflacije in pomanjkanja zelo pogosta tema vsakdanjih pogovorov. Zato ni čudno, da je pred skoraj natanko 40 leti Presekova znamenita teta Amalija bralcem o tem zastavila tudi spodnjo matematično nalogo. Gotovo jo znajo rešiti vsi starejši bralci, z dodatnim pojasnilom pa jo bodo morda ugnali tudi današnji osnovnošolci (če kakšnega sploh še imamo med bralci): tedanji 1 jugoslovanski dinar je veljal 100 par (podobno kot danes 1 EUR velja 100 centov), cena litra goriva pa je bila določena do pare oziroma na dve decimalni mesti natančno. Pa izvolite poskusiti!

× × ×



NA PRESEKOVI ČRPALKI

Teta Amalija je ustavila na Presekovi črpalki, da natoči gorivo. Cene bencij na ni poznala. Dvakrat je med točenjem pogledala na števec, videla je le dinarski del cene, par pa ne, saj se je kolesce števca prehitro vrtelo. Pogledajte, kaj je videla in povejte ceno litra bencina na Presekovi črpalki!



Rešitve nam pošljite do 1. 10. 1983.

Peter Petek

A large, 3D-rendered word 'LOL' in a vibrant red color. The letters are thick and blocky, with a slight shadow underneath, giving it a three-dimensional appearance. The 'O' is a perfect circle, while the 'L's are composed of a vertical stem and a horizontal base. The entire word is centered horizontally.

NIGERIJSKA VALUTA								GRAFIČNO OBLIKOVANJE MATEVŽ BOKALIČ	VODNIK KONJ	GRAFIČNI FORMAT, OSMERKA	SPLETNA OZNAKA TURČIJE	PRODUKT VELIKEGA NAPORA V KRVİ	REKA V MÜNCHNU	PRIPADNIK NAJVEČJEGA GERMAN. NARODA	OBMORSKO MESTO NA JUGU JORDANIJE
								NIŽJI, ZAPRT SVET MED HRIBI							
								DEKORATIVNI ELEMENT							
								NIKOLA TESLA			INDIJSKI BOG LJUBEZNI				
								VELIKA UJEDA							
								OKROGLA POSODA ZA PEČENJE							
													KALCIJ		
													ANITA OGULIN		
ETIOPSKA DENARNA ENOTA	PEVKA Z ZELENOTSKIH OTOKOV (CESARIA)	TEKMOVANJE JADRNIC	OBLIKA NAKLJUČNE IZBIRE	GLAVNO MESTO GANE	ZAČETEK OBSTOJA	ZDRAVILIŠČE Z VODO TOPLEGA IZVIRA	PRES-TOLNIČA NORVESKE	OTO VRHOVNIK V NJEM JE 2. ODVOD ENAK NIČ			HIŠICA NA VRTU ELEMENT ZA PRENOS NAVORA			NAŠ VELIKI MATEMATIK (JOSIP)	OBČUTEK NEMIRA V TEŽKI SITUACIJI
				4		TOPLJIVOST							ŽENA BOGA SATURNA ŠPORTNIK V CEVLJIH S KOLESCI		
						NAŠ POKOJNI FIZIK (MILAN)							SOSEDNJI ČRKI		
						NEZAŽE-LENA RASTLINA V VRTU					RUMENO-RJAVA BARVA		NEKD. HRV. PREMIERKA (JADRANKA)		
GLAVNO MESTO MAROKA						PLENITEV DIVJADI			AMPER-SEKUNDA		RUS. REKA IN POGORJE				
VESLAČ V GUMENJAKU						LASTNIK KAVARNE			ZNAČAJ						
			MESTO POVEZAVE DELOV	GORSKA REŠEVALNA PRIPRAVA AM. FIZIK (LUIS W.)			OKAY			PRAŠIČ, SVINE					"IZJAVA" OSLA
	IZBOLJ-SANJE ŽIVLJENJSKIH RAZMER						INKOVSKI VLADAR			NAŠ RADIJEK (ANDREJ)					
	MORJE, KI OBDAJA CELINE	MESTO V SEVERNI BOLGARII RAZKOŠJE, SLJAJ						IRANSKA VALUTA STARO IRANSKO LJUDSTVO				OKSIDNA PLAST NA POVRŠINI ŽELEZA			
						FRANCOSKA PEVKA (PATRICIA) GRŠKI BOG VETROV		6							
					TIP NEKD. SRED. SOLE NEKDANJI FIATOV MALI AVTO										
			SUROVA OVCJA VOLNA				OČE								
			ROMAN DRNOVŠEK				HRVAŠKI OTOK								
UŽIVA V VZNEMIR-LJIVIH DEJAV-NOSTIH															
KONTROLA						PLOD BUKVE				ZRNATO HIDRATNO ŽIVILO					

NAGRADNI RAZPIS

→ Črke iz oštevilčenih polj vpišite skupaj z osebnimi podatki v obrazec na spletni strani www.presek.si/krizanka ter ga oddajte do 15. oktobra 2023, ko bomo izžrebali tri nagrajence, ki bodo prejeli knjižno nagrado.



Teran na Astronomskem tekmovanju treh dežel 2023



SIMON BUKOVŠEK IN VID KAVČIČ

→ Med 28. junijem in 1. julijem 2023 je v Zagrebu potekalo Astronomsko tekmovanje treh dežel, ki je pripravljala tekma astronomskih olimpijskih ekip Hrvaške, Madžarske in Slovenije pred Mednarodno olimpijado iz astronomije in astrofizike (MOAA).

Izjemen uspeh slovenske ekipe

Uspeh slovenske ekipe je bil letos izjemen. Na tekmovanju je **zmagal Peter Andolšek**, drugi je bil **Miha Brvar** in oba sta prejela **zlati medalji**. Tretji je bil **Alexander Gaydukov**, četrta pa **Marija Judež**. Oba sta prejela **srebrni medalji**. Sedmi je bil **Žan Arsov**, najmlajši član naše ekipe, ki je prejel **bron**. Ekipo sta vodila **Vid Kavčič** in **Simon Bukovšek**.

Ekipo se je na tekmovanje v Zagreb odpravila z vlakom. Nastanjeni smo bili v Domu Rdečega križa na vzpetini Sljeme nad mestom, daleč proč od pregretega asfalta in avtomobilskega renčanja. Medtem ko so po prihodu tekmovalke in tekmovalci z žičnico obiskali Zagreb ter si ogledali njegovo staro mestno jedro, so se mentorji potopili v razpravo o nalogah, ki so jih pripravili hrvaški kolegi.

Že prvi večer so se astronomke in astronomi lahko spopadli z opazovalnim delom tekmovanja, saj so bile vremenske razmere naravnost čudovite. Na opazovalnem delu, ki šteje eno četrtno skupnih točk, so morali izkazati svoje znanje orientacije po nebu ter dela z različnimi tipi teleskopov.

Po končanem opazovalnem delu so se mentorji posvetili zaključnim razpravam in prevajanju nalog. Prihodnje jutro je bilo tako vse pripravljeno za teoretični del tekmovanja, ki je trajalo tri polne ure in je zajemalo polovico vseh možnih točk. Medtem so mentorji uredili in prevedli tudi naloge iz obdelave podatkov astronomskih opazovanj, v katere so tekmovalci zagrizli popoldne. Tudi ta del tekmovanja je trajal tri polne ure, štel pa je četrtno vseh točk. Po napornem dnevu so se tekmovalci sprostili v igranju badmintona in drugih družabnih iger, mentorje pa je čakalo še popraviljanje izdelkov.

Zadnji dan so tekmovalci dobili še sklepni izziv, in sicer ekipno tekmovanje, na katerem so morali določiti merilo zagrebškega modela Osončja. Nato so organizatorji na zaključni slovesnosti v zagrebški Zvezdarnici podelili medalje, sledila pa je pogostitev z okusnimi picami. Po poslednjem prijetnem druženju s hrvaško in madžarsko astronomsko posadko smo se z vlakom odpravili proti Ljubljani, kamor smo prispeli v večernih urah.

Teran v Dobsonu

K prijateljskemu vzdušju na tekmovanju so prispevale tudi izjemno sveže in izvirne naloge. Med nalogami na teoretičnem delu je bila prav gotovo najbolj povezovalna naloga o teranu v Dobsonovem teleskopu, ki se je je domislil Andrej Guštin, dovršeno pa jo je spisal Simon Bukovšek.

Naloga sprašuje po tem, koliko terana moramo naliti v Dobsonov teleskop, da lahko z njim varno opazujemo Sonce. Pojasnimo naj, da je Dobsonov teleskop Newtonov zrcalni teleskop na alt-azimutalni montaži (slika 2).



SLIKA 1.

Astronomske divizije Slovenije, Hrvaške in Madžarske na vrhu observatorija hrvaške Zvezdarnice.

Ker opazovanje Sonca ni hec, saj lahko hitro pride do očesnih poškodb, moramo paziti, da se reševanja naloge lotimo premišljeno, hkrati pa moramo imeti v mislih tudi, da v tem primeru teran uporabljamo za znanstvene namene. V ta namen bomo najprej obnovili in oplemenitili svoje znanje o svetlobi, očesu in optiki.

Podatki in predpostavke

Interakcija svetlobe z očesom je zelo zapletena veja optike in biologije, težko je najti konsistentne pogoje za »varno opazovanje«. V namen te naloge so bili zbrani podatki iz različnih virov in zaradi varnosti namenoma nekoliko znižani. Tudi podatek o absorpcijskem koeficientu terana je zgolj spodnja ocena, saj je primerne podatke težko pridobiti.

Pogoja za »varno opazovanje« sta:

- nikjer na mrežnici ne sme gostota svetlobnega toka presegati $j_{mr} = 10 \text{ W/m}^2$,
- skupen svetlobni tok, ki pada v oko, ne sme presegati $P_{oko} = 10 \text{ mW}$,

Podatki o teleskopu:

- goriščna razdalja objektiva: $f_{ob} = 1,0 \text{ m}$,
- premer objektiva: $D_{ob} = 20 \text{ cm}$,
- goriščna razdalja okularja: $f_{ok} = 25 \text{ mm}$,
- navidezen premer vidnega polja za okular: $FoV_{nav.} = 52^\circ$,

Podatki o očesu:

- razdalja med lečo in mrežnico: $f_{oko} = 17 \text{ mm}$,
- v zelo močni svetlobi ima oko goriščno razmerje $f/8,5$,

Nekaj splošnih podatkov:

- gostota svetlobnega toka Sonca na površju Zemlje: $j_0 = 1,0 \text{ kW/m}^2$,
- navidezna velikost Sončeve ploskvice je $\varphi_\odot = 32'$,
- absorpcijski koeficient terana za sončno svetlobo je $\mu = 77,5/\text{m}$.

Predpostavili bomo, da Sonce opazujemo v zenitu. Zanimarili bomo odboj svetlobe na površini med vidnim in zrakom ter spremembo goriščne razdalje objektiva zaradi dodanega vina.

Rešitev naloge

Pri reševanju naloge moramo upoštevati dva kritična pogoja za »varno opazovanje«, in sicer kritično gostoto svetlobnega toka na mrežnici j_{mr} in skupni svetlobni tok P_{oko} . Najprej razložimo, zakaj sta oba tako pomembna.

Prvi pogoj lahko ponazorimo na primeru **laserja**. Vsem je znano svarilo »ne glej naravnost v laser«, ki pa nikakor ni nedolžno. Čeprav ima laser lahko relativno majhno moč, je gostota svetlobnega toka zelo velika in s tem nevarna za mrežnico.

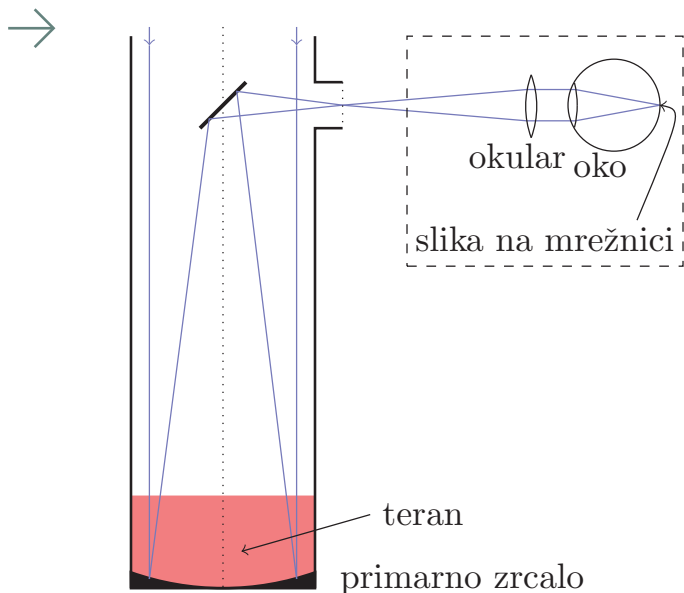
Nasprotno si za ponazoritev drugega pogoja predstavljajmo, da na sončen zimski dan hodimo po belo zasneženih hribih. V tem primeru nobena specifična točka (z izjemo Sonca) ni nevarno svetla, kljub temu pa lahko zaradi prevelike skupne moči svetlobe (še posebej UV) pride do poškodb očesa, na primer vnetja roženice. To očesno stanje imenujemo **snežna slepota**. Pred poškodbami se lahko zaščitimo z uporabo posebnih zaščitnih sončnih očal.

Pri reševanju naše naloge bomo tako morali izračunati mejno vrednost vpadle svetlobe v teleskop za oba pogoja »varnega opazovanja« in upoštevati tisto, ki je manjša.

Najprej si oglejmo pogoj za največjo gostoto svetlobnega toka na mrežnici. Vemo, da je premer Sončeve ploskvice na nebu enak $\varphi_\odot = 32'$. Povečavo p teleskopa izračunamo kot

- $p = \frac{f_{ob}}{f_{ok}} = 40.$





SLIKA 2.

Skica k nalogi.

Navidezna kotna velikost Sonca v vidnem polju okularja je tako enaka $\alpha_{\odot} = \varphi_{\odot} \cdot p = 21^{\circ}20'$. Ker je ta vrednost manjša od navidezne velikost vidnega polja ($\text{FoV}_{\text{nav.}} = 52^{\circ} > \alpha_{\odot}$), v okularju vidimo celo Sonce.

Poleg tega opazimo, da je izstopna zenica teleskopa D_{iz} večja od zenice očesa D_{oko} . Velja namreč:

$$\blacksquare D_{\text{oko}} = \frac{f_{\text{oko}}}{8,5} = 2 \text{ mm}, \quad D_{\text{iz}} = \frac{D_{\text{ob}}}{m} = 5 \text{ mm}.$$

Naj bo j_1 največja gostota svetlobnega toka, ki pride skozi teran, ki ustreza prvemu pogoju. Pri izračunu svetlobnega toka P_{oko} moramo upoštevati zgornjo ugotovitev $D_{\text{oko}} < D_{\text{iz}}$, saj se na ta račun med okularjem in očesom nekaj energije izgubi. Velja

$$\blacksquare P_{\text{oko}} = j_1 \cdot \frac{\pi D_{\text{ob}}^2}{4} \cdot \frac{D_{\text{oko}}^2}{D_{\text{iz}}^2}.$$

Tako izražena moč se razporedi po površini $S = \frac{\pi}{4} (\alpha_{\odot} \cdot f_{\text{oko}})^2$. Gostoto svetlobnega toka na mrežnici

tako izrazimo kot

$$\blacksquare j_{\text{mr}} = \frac{P_{\text{oko}}}{S} = \frac{j_1 \cdot \frac{\pi D_{\text{ob}}^2}{4} \cdot \frac{D_{\text{oko}}^2}{D_{\text{iz}}^2}}{\frac{\pi}{4} (\alpha_{\odot} f_{\text{oko}})^2} = j_1 \frac{4\pi D_{\text{ob}}^2 D_{\text{oko}}^2 p^2}{4\pi D_{\text{ob}}^2 f_{\text{oko}}^2 \varphi_{\odot}^2 p^2} = j_1 \frac{D_{\text{oko}}^2}{f_{\text{oko}}^2 \varphi_{\odot}^2}. \quad (1)$$

Opazimo, da je gostota svetlobnega toka na mrežnici popolnoma neodvisna od teleskopa, skozi katerega gledamo. Še več, za vsak netočkasti objekt je gostota svetlobnega toka na mrežnici ob gledanju skozi kateri koli teleskop manjša oziroma kvečjemu enaka, kot če bi ta objekt gledali s prostim očesom. Manjša bi bila v primeru, če bi bila izstopna zenica manjša od velikosti očesne zenice. Ta ugotovitev se zdi nekoliko neintuitivna. Hkrati pa zelo spominja na dejstvo, da z nobenim optičnim pripomočkom ne moremo segreti objekta na višjo temperaturo, kot jo ima svetlobni vir.

Zdaj iz enačbe (1) izrazimo j_1 in izračunamo njegovo numerično vrednost. Pri tem smo pozorni na to, da mora biti kót $\alpha_{\odot}$ izražen v radianih. Dobimo

$$\blacksquare j_1 = \frac{j_{\text{mr}} f_{\text{oko}}^2 \varphi_{\odot}^2}{D_{\text{oko}}^2} = 0,626 \text{ W/m}^2.$$

Posvetimo se zdaj drugemu pogoju za »varno« opazovanje, to je pogoju z maksimalnim svetlobnim tokom. Naj bo j_2 največja gostota svetlobnega toka, ki sme priti skozi teran, da je zagotovljen drugi pogoj. Podobno kot prej zapišemo

$$\blacksquare P_{\text{oko}} = j_2 \cdot \frac{\pi D_{\text{ob}}^2}{4} \cdot \frac{D_{\text{oko}}^2}{D_{\text{iz}}^2},$$

iz česar izrazimo j_2 in izračunamo njegovo numerično vrednost:

$$\blacksquare j_2 = \frac{4P_{\text{oko}} D_{\text{iz}}^2}{\pi D_{\text{ob}}^2 D_{\text{oko}}^2} = 1,99 \text{ W/m}^2.$$

Če želimo zagotoviti »varno« opazovanje, mora skozi teran prehajati največ toliko svetlobe, kot je manjša vrednost od j_1 in j_2 . Izračunali smo, da je $j_1 < j_2$, kar pomeni, da je pri opazovanju Sonca s teleskopom bolj kritična gostota svetlobnega toka na mrežnici kot pa skupen svetlobni tok. Zato za nadaljnje izračune vzamemo manjšo od teh dveh vrednosti, torej $j_1 = 0,626 \text{ W/m}^2$.

Nekaj odstavkov zgoraj smo ugotovili, da je gostota svetlobnega toka na mrežnici neodvisna od teleskopa, zdaj pa smo sklenili, da je pri opazovanju sonca kritična ravno slednja. Pozoren bralec bi se ob teh ugotovitvah vprašal, zakaj je kljub temu toliko nevarneje opazovati Sonce s teleskopom kot s prostim očesom. Odgovor najverjetneje tiči v tem, da se učinka gostote svetlobnega toka in skupnega svetlobnega toka seštevata.

Prebili smo se do zadnjega dela naloge. Zaradi absorpcije svetlobe v plasti terana z debelino x se mora gostota svetlobnega toka z j_0 zmanjšati na j_1 . Pri izračunu x uporabimo absorpcijski zakon:

$$j(x) = j_1 = j_0 e^{-\mu x},$$

iz česar izrazimo

$$x = \frac{\ln\left(\frac{j_0}{j_1}\right)}{\mu} = 9,52 \text{ cm.}$$

Ko sončna svetloba vstopi v teleskop, najprej potuje do primarnega zrcala, se tam odbije, nato pa svojo pot nadaljuje do sekundarnega zrcala in proti okularju. Pri tem po teranu napravi dvakrat isto pot. Zato višina h terana, ki ga moramo naliti v teleskop, ustreza ravno polovici optične poti x svetlobe po teranu:

$$h = \frac{x}{2} = 4,76 \text{ cm.}$$

Preostane nam izračunati le še prostornino V potrebnega terana. Dobimo

$$V = Sh = \frac{\pi D_{\text{ob}}^2}{4} h \approx 1,5 \text{ l.}$$

Zaključek

Izkaže se, da bi za astronomski eksperiment zadoštovali dve buteljki domačega kraškega terana. Seveda pa najbrž ni treba dodatno poudarjati, da praktične izvedbe tega poskusa ne svetujemo; domačega teleskopa bi bilo namreč neznansko škoda.

× × ×

Križne vsote

↓↓↓

→ Naloga reševalca je, da izpolni bele kvadratke s števkami od 1 do 9 tako, da bo vsota števk v zaporednih belih kvadratih po vrsticah in po stolpcih enaka številu, ki je zapisano v sivem kvadratu na začetku vrstice (stolpca) nad (pod) diagonalo. Pri tem morajo biti vse številke v posamezni vrstici (stolpcu) različne.

	10	12			
16			7		
10				14	
		9			7
			10		
			5		

↓↓↓

REŠITEV KRIŽNE VSOTE

4	1	5			
3	7	10			
7	9	3	6		
	14	4	5	1	10
		7	7	6	16
			12	10	

× × ×

Kratice

OD TOD DO TOČKE BREZ VRNITVE



ALEKSANDAR JURIŠIĆ IN KLEMEN KLANJŠČEK

→ V vsakdanjem življenju pogosto *krajšamo dolga imena in nazive* zaradi hitrejšega sporazumevanja. Učiteljica bo pogosto na tablo ali novinarka v članku prvič zapisala neskrajšano ime, nato bo dodala tudi *kratico* in jo kasneje uporabljala. V tem besedilu bomo predstavili matematično ozadje krajšanja, kot se uporablja pri računalniški varnosti, s poudarkom na kriptografiji (npr. če želi novinar prikriti ime neke osebe, bo praviloma uporabil začetnice imena in priimka – ne nujno pravih).

Za nas bo **krajšanje** postopek, pri katerem poljubnemu nizu znakov dodelimo neko **kratico** oz. **okrajšavo**, kratko oznako, npr. začetnice uporabljenih besed, glej **sliki 1 in 2** ter tudi nalogo 2.

Primeri krajšanja

Primer 1. (Oznake) Ko učence na začetku šolskega leta razporedimo v razrede, npr. 100 učencev v 4 razrede A–D (24+23+27+26), je pogosto posamezni učenec na kratko označen npr. »A-jevec«.

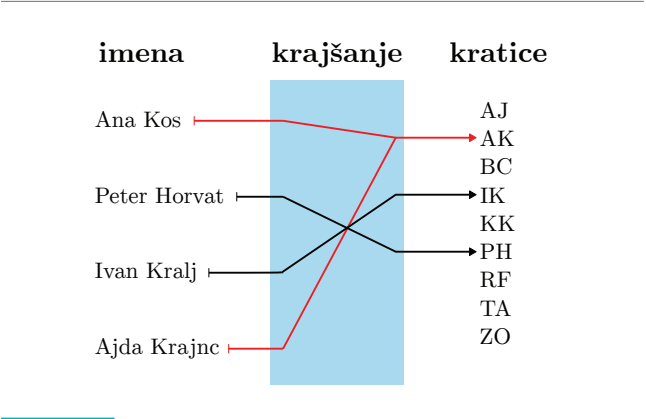
Zgornji primer omogoči kuharici, da v jedilnici hitro pokliče del učencev ali pa večje skupine razdeli na manjše in jih zato lažje razporedi za deljenje malice.

Primer 2. (Začetnice) Ko se v jedilnici štirje posedejo k eni mizi, ugotovijo, da dogovor o klicanju po začetnicah imena in priimka zanje žal ne pride v poštev, glej **sliko 2**.

V zadnjem primeru vidimo, da je treba biti pri krajšanju precej previden.



SLIKA 1. Stiskanje, zmešnjava, razpršenost, kot pri stiskanju grozdja ali jabolk, pri tem pa gredo nekatere stvari tudi med odpadke.



SLIKA 2. Trčenja pri začetnicah.

Primer 3. (Konice – gr. akronimi), in (radijske) kode. Krajšanje se pogosto uporablja za hitrejšo posredovanje informacij.

Omenili smo že novinarje, a tudi policija, vojska in interventne službe uporabljajo kratice, s katerimi lahko zelo hitro opišejo stanje na terenu. Če pa želimo ohraniti posredovane informacije še tajne, v kriptografiji pravimo, da gre za uporabo **kodnih knjig**. Čeprav tak pristop štejemo v kriptografiji za zastarelega, se je splošno uporabljal v drugi svetovni vojni (glej npr. nalogo 3) in je v nekaterih primerih še vedno aktualen (npr. ko celotne fraze nadomestimo s kraticami iz kodnih knjig).

Namesto gesel v računalniških sistemih hranimo le njihove »okrajšave«. **Zakaj?** Pri shranjevanju podatkov pogosto poleg samega podatka hranimo še njegovo »okrajšavo«. **Zakaj?**

Primer 4. (Serijske številke) Za evidentiranje naprav (knjig, ljudi ...) namesto dolgih opisov, hranimo le pripisano številko vsake naprave (npr. evidenčna, registrska, telefonska, matična, davčna, datum).

Poznamo pa tudi druge tehnično bolj zapletene primere uporabe krajšanja, kot so digitalni podpisi, denar ali zaprisege, tvorjenje naključnih števil in podobno. Ti primeri pridejo na vrsto v kakšnem nadaljevanju.

Vsaka tehnika krajšanja ima svoje prednosti in slabosti, zato po navadi ni namenjena splošni uporabi. Besedi krajšanje in kratica nista niti nujno najbolj primerni za vsako tehniko, zato omenimo še nekaj možnosti. Najbolj pogosta je **zgoščevanje** in **zgostitev** (angl. hash). Za rezultat zgoščevanja pa so tu še **prstni odtis**, **izvleček** in **povzetek**.

Zaželeni lastnosti krajšanj

Predstavljamo nekaj zaželenih lastnosti tehnike krajšanja, ki so uporabne na splošno:

1. **Določenost** — krajšanje istih izrazov vedno pripelje do iste okrajšave. Enostavna posledica te lastnosti je, da različni okrajšavi dveh (neznanih) izrazov pomenita, da morata biti izraza zagotovo različna.
2. **Učinkovitost** — postopek krajšanja je hiter in enostaven (vsaj za računalnike). Daljše izraze bomo sicer običajno krajšali dlje, npr. računanje vsote števk števila za potrebe ugotavljanja njegove deljivosti s 3.

3. **Enosmernost** — iz same okrajšave (brez dodatnih informacij) je težko najti izraz, ki smo ga krajšali. Iz okrajšave ne moremo sklepati, kako se glasi neokrajšani izraz. Posledično mora biti vsak delček okrajšave odvisen od vseh delov vhoda ali pa od nobenega (v kriptografiji tej lastnosti pravimo **zmešnjava** – angl. confusion), npr. zadnja številka vsote števk neznanega števila.
4. **Skoraj brez trčenj** — možnost, da imata dva različna izraza enako okrajšavo, je majhna. Tako je npr. pri pravih/fizičnih prstnih odtisih. Dodatna zahteva: najti dva različna izraza z isto okrajšavo je težko. Posledično mora celoten izraz vplivati na izbrano okrajšavo (v kriptografiji tej lastnosti pravimo **razpršenost** – angl. diffusion).

Lastnosti 1 in 2 držita za večino krajšanj, če pa k temu dodamo še lastnosti 3 in 4, potem smo z eno nogo že vstopili v deželo (tete) kriptografije. A preden gremo po tej poti, omenimo še nekaj zanimivih primerov.

Hranjenje velikih datotek

Najprej smo na telefonu shranjevali samo številke in še to kar v SIM-kartici. Ko pa je telefon postal še fotoaparati, predvajalnik glasbe ter celo filmov, lahko hitro zapolnimo še tako velik pomnilnik. Ker so za nas podatki pomembni (po navadi šele, kadar jih izgubimo), smo se naučili delati varnostne kopije. Če pri tem nismo pazljivi, zelo hitro porabimo ves prostor tako na telefonu kot na računalniku ali v oblaki storitvi in se pri tem ne zavedamo, da hranimo vse več kopij z isto vsebino. Pojavi se še problem različnih verzij in kaj hitro se nam lahko zgodi, da s staro verzijo »povozimo« novejšo datoteko. Pri reševanju teh problemov si pomagamo tako, da poleg datotek hranimo še njihove zgostitve, preko katerih znamo učinkovito (lastnost 2) ugotoviti:

1. zelo verjetno imamo na disku več kopij iste datoteke (lastnost 4),
2. pri prenosu datotek je/ni prišlo do napak (lastnosti 1 in 4).

Ker je hitrost prenosa pogosto omejena, je hitrost primerjanja še bolj pomembna. V nekem smislu je



→ prva zgostitev ime datoteke, naslednji sta njena velikost in datum zadnje spremembe (celo kreiranja ali dostopa), nato pa si pomagamo še s kakšnim bolj zapletenim zgoščevanjem.

Preverjanje celovitosti podatkov

Kako bi preverili, ali manjka kakšna stran iz dnevnika ali kakšno sporočilo (recimo pri nekem dopisovanju)? Običajna rešitev je, da uvedemo števce, a se nato zaplete, če želimo dodati novo stran ali kaj izbrisati. Na nivoju besedila je lahko pomemben že en sam dodani, izbrisani ali spremenjeni znak (npr. ocena v spričevalu) oz. beseda/stavek (npr. v pogodbi). Vse te probleme celovitosti podatkov rešujemo z zgostitvami. V tem primeru je zelo pomembno, da tudi najmanjša sprememba v vhodnem nizu vrne drugačno zgostitev (npr. t. i. *vsota za preverjanje* – angl. checksum). Uporablja se pri prenosu datotek (npr. z Bittorrent protokoli), upravljanju z varnostnimi kopijami, hitrem iskanju po zbirkah podatkov/dokumentih itd. Verjetno pa je najbolj pomembna uporaba pri digitalnih podpisih, saj daljša sporočila podpisujemo tako, da v resnici podpišemo njihove zgostitve.

Hranjenje (uporabniških) gesel

O geslih smo že pisali v članku Ključi (v Preseku), vendar takrat še nismo omenili postopkov zgoščevanja. Tokrat pojdimo korak dlje. Namesto da bi računalniški sistemi (ki nam omogočajo dostop do osebnega računalnika, spletne učilnice, forumov ...) shranili uporabniška gesla, hranijo le njihove zgostitve. Na ta način gesla ostanejo skrita, tudi če si napadalec pridobi dostop do sistema. Ker bodo ista gesla imela iste zgostitve (lastnost 1), je tak načni shranjevanja gesel nepopoln. Napadalec lahko vnaprej izračuna/sestavi tabelo vseh možnih parov

zgostitev gesla g_1	geslo g_1
$\vdots$	$\vdots$
zgostitev gesla g_n	geslo g_n

za zbirko pogostih gesel g , urejeno po zgostitvah. Tako zlahka razbije manj varna gesla – za vsako zgostitev v shrambi preveri, ali se nahaja v tabeli. Če

njegova zbirka vsebuje vse besede iz slovarja, v kriptografiji rečemo, da gre za **napad s slovarjem**. Omenimo še napad z *mavričnimi tabelami* (velikosti nekaj 100 GiB), s katerim lahko razbijemo skoraj vsa krajša gesla (recimo z manj kot 9 znaki – tudi posebnimi).

Kako preprečimo možnost hitre primerjave takšnih gesel prek pripadajočih zgostitev?

Ena možna rešitev je, da za vsakega uporabnika izberemo drugačen postopek zgoščevanja, ki ga tudi hranimo. V tem primeru bi bilo potrebno za ugibanje gesel sestaviti zgornjo tabelo za vsakega uporabnika posebej.

Igra kamen-škarje-list

Okoli 2000 let staro kitajsko igro po navadi igrata dva igralca takole:

- (1) vsak od igralcev si na skrivaj izbere eno izmed treh možnosti *kamen/škarje/list*,
- (2) igralca drug drugemu istočasno razkrijeta izbiro,
- (3) zmagovalca se določi po pravilu:

- *kamen* uniči *škarje*,
- *škarje* prerežejo *list*,
- *list* pokrije *kamen*,
- v vseh drugih situacijah imamo izenačenje.

Za poštenost igre je ključnega pomena istočasnost. Lahko jo zagotovimo s sodnikom.

Kaj pa če nimamo sodnika ali pa želimo igro igrati preko telefona/interneta?

Podobna vprašanja si je postavljal že leta 1982 Manuel Blum — glej nalogo 5.

Problem istočasnosti lahko rešimo z uporabo **kriptografsko varne zgoščevalne funkcije**. Takšna funkcija za poljubno zaporedje znakov x učinkovito (z računalnikom) izračuna zgostitev $z := F(x)$. Zaradi predstavitve medijev v digitalni obliki je lahko x tudi slika, video ... Veljati mora tudi, da je praktično nemogoče uganiti/izračunati dva različna izraza z enakima okrajšavama ali pa vrednost x iz zgostitve z (tudi za najzmogljivejše računalnike) ⁵.

Primer poteka igre med Ano in Bojanom (brez sodnika):

⁵Ti dve možnosti sta manjši, kot da 3-krat zapored zadene nemo sedmico na Lotu, in to s prvimi tremi kupljenimi srečkami!

(1) Ana na skrivaj izbere (dovolj dolg) naključni niz H6FUcfqtAGf3 in list, Bojan pa izbere uAD22TWTNTz2 in škarje.

(2) Ana izračuna (z računalnikom) zgostitev $z_A = F(\text{H6FUcfqtAGf3 list})$, Bojan pa izračuna $z_B = F(\text{uAD22TWTNTz2 škarje})$.

(3) Izmenjata si zgostitvi z_A in z_B .

(4) Izmenjata si naključna niza (lahko pa tudi še izbiri).

(5) Določita izid igre. (Kako?)

Hranjenje množic (na papirju oz. računalniku – beri: digitalnem mediju)

Pred več kot pol stoletja smo v šole hkrati s števili (aritmetiko) začeli uvajati še množice (glej https://en.wikipedia.org/wiki/New_Math). Zato je čisto prav, da nanje pomislimo danes, ko smo že povsem obkroženi z računalniki, še iz tega zornega kota. Tu se namreč pojavijo zanimivi problemi, ki so povezani z našim krajšanjem.

Kaj odgovorimo na vprašanje, ali je neki element v množici?

Če je množica majhna in »vidimo« vse njene elemente, potem to najbrž sploh ni težko. Če je elementov več, moramo izbrati neko drugo primerno strategijo. Kako bi na primer ugotovili, ali je neka beseda slovenska oziroma, da pripada množici vseh slovenskih besed. Kako bi na to vprašanje odgovoril striček Google, če nanj ne bi bil pripravljen? Kako naj zbere vse slovenske besede, če vseh sploh ne pozna. Za občutek omenimo še, da imajo najbolj bogati jeziki tudi do četrta milijona besed (pa pri tem ne štejemo sklonov).

Če se da elemente urediti po vrsti, potem jih radi hranimo urejene, kot je to narejeno z besedami nekega jezika v slovarjih (*leksikografska ureditev*). V tem primeru je za preverjanje prisotnosti elementa v množici potrebno le nekaj primerjav, da preverimo, ali je neka beseda v slovarju (npr. metoda bisekcije). Na srečo ni potrebno prelistati vseh strani. Zakaj?⁶

Kaj pa če elementov sploh ne znamo enostavno primerjati?

Recimo, da iščemo nekega vojaka, ki je storil nekaj slabega, pa se nam zdijo vsi vojaki na prvi pogled zelo podobni. Upajmo, da imamo na voljo vsaj kakšen prstni odtis nepridiprava, pravzaprav kar vseh vojakov. Lahko so na voljo le njihove slike, ki jih je posnela skrita kamera. Kako urediti po vrstnem redu slike? Če bi vojake slikali ob vstopu v vojsko, potem bi najbrž vsak dobil številko in k tej številki pripeto sliko. Če pa ne gre za naše vojake, potem je stvar še nekoliko bolj zapletena (sicer bi lahko šlo tudi za bakterije, viruse itd., a ne želimo zaiti na področje biologije ali medicine), saj smo rekli, da je naš zorni kot računalništvo. Predpostavimo, da primerjamo slike vojakov (a tu ne bomo reševali problemov računalniškega vida).

Ena možna rešitev je, da namesto elementov primerjamo njihove zgostitve. Za hitro iskanje in dodajanje elementov najprej izračunamo zgostitve vseh elementov ter sestavimo tabelo na naslednji način. Element spravimo v tisto vrstico tabele, ki jo določa njegova zgostitev. Vsaki zgostitvi namenimo svoj prostor (to je lahko list papirja, del pomnilnika ali vrstica v tabeli). Zgostitve igrajo vlogo kazala (npr. rokovnik z naslovi, zgostitev predstavljata prvi dve črki priimka – trki so tukaj dopustni, ampak nezaželeni).

Podobno tehniko uporablja sistem za spletno izmenjevanje datotek prek t. i. *magnetnih povezav* (angl. Magnet Link), ki so pretežno zgostitve h_{magnet} . Če poznamo neko zgostitev, lahko prek *Bittorrent protokolov*, prenesemo željeno datoteko (ali pa mapo z datotekami). Najprej poizvemo, kdo si trenutno deli pripadajočo datoteko. Podatek o tem, kateri računalniki si trenutno delijo datoteko vezano na dano magnetno povezavo, se hrani v velikem skupnem »imeniku« na spletu, kjer za »začetnico« imenika vzamemo zgostitev h_{magnet} , za »naslov« pa IP naslov in vrata (angl. port) računalnikov. Ker je imenik velik in se neprestano spreminja, noben računalnik nima celotnega imenika, le nekaj »strani«.

Ko najdemo računalnike, ki trenutno delijo željeno datoteko, najprej prejmemo od njih t. i. *torrent* datoteko. Ker so datoteke, ki jih na ta način izmenjujemo, ponavadi velike, jih prenašamo po manjših delih/koščkih. Zaradi tega prejeto torrent datoteko sestavljajo zgostitve vseh koščkov datoteke in njihove

⁶Po omenjeni metodi bisekcije bi slovar odprli na sredini in če tam ne bi našli besede, bi nadaljevali v prvi ali drugi polovici – po istem postopku vse do konca, ko bi ugotovili, ali je sploh iskana beseda v slovarju.

→ velikosti, ter ime datoteke. Skupna zgostitev vseh teh treh informacij je h_{magnet} in osnovni del magnetne povezave, glej sliko 3. Ker se zgoščevanje izvaja s kriptografsko varno zgoščevalno funkcijo H , so zgostitve datotek praktično unikatne. Prednost takega načina prenosa datotek je, da lahko datoteke prejemamo od več računalnikov hkrati (od vsakega le nekaj koščkov) in smo zato neodvisni od mrežnih problemov (npr. prekinitve, napake). Namenoma nismo podali celotne zgodbe, saj je še veliko bolj zapletena. Primer magnetne povezave: `magnet:?xt=urn:btih:e0d9af6671db5bc4fc77ab5462c50e2f3545dad9`. Število s 40-timi znaki v šestnajstiškem zapisu `e0d9a...` (20 »bajtov«) tukaj predstavlja zgostitev (SHA-1) za prenos DVD-ja (velikosti 3,59 GiB = 14741 koščkov velikosti 256 KiB, torrent datoteka je velikosti 288 KiB $\approx 14741 \times 20$ B) za namestitve operacijskega sistema Ubuntu 20.04.5 (za celoten vpogled v vsebino te torrent datoteke glej povezavo <https://gist.github.com/k1lemen/47c7d8782-c81afbb76bc7ff19d172588>).

Zaključek

Če boste rešili vsaj nekaj spodnjih nalog, boste opazili, da se zdi na prvi pogled konstrukcija kriptografskih zgoščevalnih funkcij (pre)zahtevna naloga. V resnici sploh ni lahko najti (sestaviti) takšno funkcijo. Tudi če nam jo nekdo predlaga, ne moremo biti prepričani, da se ne bo v prihodnosti izkazalo, da ena od zahtevanih lastnosti ne drži. Prve zasnove kriptografskih zgoščevalnih funkcij segajo 45 let nazaj (glej Merkle 1979 in npr. Damgård). V devetdesetih letih prejšnjega stoletja je zelo hitro naraslo število modelov zgoščevalnih funkcij, vendar so bile

pri številnih od teh predlogov ugotovljene varnostne pomanjkljivosti, npr. najbolj popularnim Rivestovim zgoščevanim funkcijam MD4 in MD5 (angl. Message Digest) se je po več 10-letni uporabi zgodilo prav to. **Odprt problem: ali kriptografske zgoščevalne funkcije sploh obstajajo?**

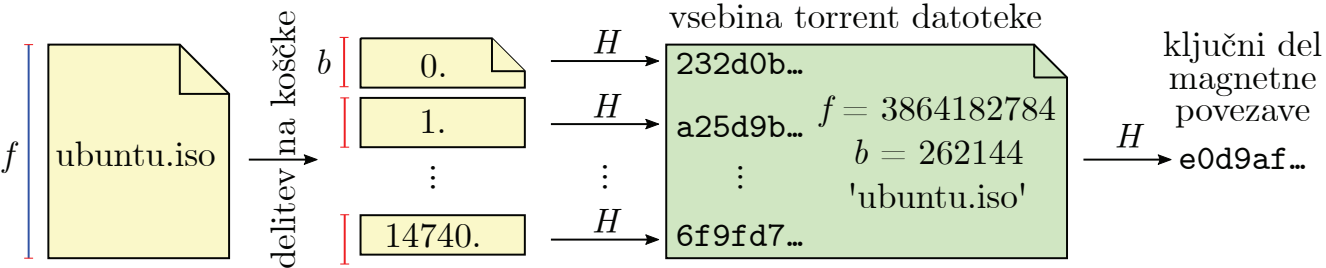
Ta čas sicer imamo kar nekaj kriptografskih zgoščevalnih funkcij, za katere se smatra (ali vsaj upa), da navedene lastnosti držijo in jih zato uporabljamo v praksi: BLAKE, RIPEMD (Bitcoin), SHA (za digitalno potrdila v osebni izkaznici oz. v splošni uporabi), Whirlpool itd. Teh funkcij nikoli ne računamo na roke (<https://md5calc.com/hash/sha1> bralec lahko poskusi preveriti njihovo delovanje oziroma se poigrati s simulacijo računanja funkcije <https://sha256algorithm.com/>). Kakšno med njimi bi si enkrat celo lahko približje ogledali. Že sedaj pa lahko omenimo:

Odprt problem: najdi zalogo vrednosti zgoščevalne funkcije MD4 ali SHA-1.

Lahko pa se vprašamo tudi, ali obstajajo kriptografsko varne zgoščevalne funkcije primerne za »ljudi«? Za zdaj kaže, da brez pomoči računalnika, vsaj za večino nas, žal ne gre.

Naloge

- 1. Možni ostanki pri deljenju celega števila s 3 so 0, 1 in 2. Krajšanje, ki nam za naravno število vrne njegov ostanek pri deljenju s 3, ima očitno prvi dve lastnosti (*določenost* in učinkovitost). Prepričaj se, da ni tako pri zadnjih dveh lastnostih (enosmernost oz. iskanje *praslike* in *problem trčenja*).



SLIKA 3.
Ustvarjanje magnetne povezave.

2. Teta kriptografija se je pogovarjala z mlajšo kolegico in izvedela, da bodo mladi bralci ob besedi krajšanje najprej pomislili na krajšanje ulomkov. Pri tem postopku običajno iz velikega imenovalca in števca izpostavimo njun največji skupni delitelj D in končamo po krajšanju z manjšim imenovalcem in števcem (če le ni $D = 1$), medtem ko vrednost ulomka ostane ista. Tudi pri našem krajšanju si želimo podobno – krajši zapis. katerim od omenjenih štirih lastnosti ustreza omenjeno krajšanje ulomkov?
3. Ameriška mornarica je zbrala 29 mož indijanskega plemena Navajo (<https://www.intelligence.gov/people/barrier-breakers-in-history/453-navajo-code-talkers>) in ustvarili kode, zasnovane na njihovem zapletenem, nenapisanem jeziku. Koda je v prvi vrsti uporabljala povezovanje besed tako, da je ključnim frazam in vojaškim taktikam dodelila besedo Navajo. Če se želite preizkusiti v odšifriranju kode v jeziku Navajo, uporabite <https://www.cia.gov/stories/story/navajo-code-talkers-and-the-unbreakable-code/> za odšifriranje naslednje kode:
TKIN-KE-YAH YIL-DOI AH-JAH YEH-HES
KLESH DIBEH-YAZZIE
WOL-LA-CHEE TSAH BE TKIN YIL-DOI
WOL-LA-CHEE
oziroma odšifrirajte spodnjo kodo, da ugotovite, v kateri bitki je koda pomagala doseči zmago ZDA:
Tkin-Gloe-Ih-A-Kha Ah-Ya-Tsinne-Tkin-Tsin-Tliti-Tse-Nill
4. (a) Kaj bi bil primeren način zgoščevanja glasbe, ki bi ljudem še vedno omogočal prepoznavanje/ločevanje? (b) Katere izmed tistih štirih lastnosti si tukaj želimo? (c) Kako bi tako prepoznavanje naredil z računalnikom (torej brez uporabe naših možganov)? Na telefonu bi lahko uporabili aplikacijo *Shazam*. (d) Ali mogoče veš, kako *YouTube* portal ve, da si uporabil avtorsko zaščiteno glasbo v svojem videu (ker jih očitno ne pregledujejo »na roke« – razen morda čisto na koncu, ko pride do kakšne tožbe)?
5. Kako varno vreči kovanec prek telefona (iz članka M. Bluma, *Coin Flipping by Telephone*, 1982)? Ana in Bojan želita vreči kovanec prek telefona. (Nasledni mesec bosta delala v različnih mestih in želita sprejeti odločitev, kdo bo dobil skupni avto.) Bojan noče povedati Ani »cifra« in slišati (na drugi strani linije), kako ona odvrne »Vržem kovanec ... Izgubil si!«. Ali bi znal predelati igro *kamen-škarje-list z uporabo zgoščevalnih funkcij* tako, da rešiš Anin in Bojanov problem?
6. Kako zaščititi idejo, da nam je kdo ne ukrade in predstavi kot svojo? Recimo, da je sošolec prišel do naše seminarske naloge, še preden smo jo oddali in se je odločil, da jo bo oddal s svojim imenom. Ali obstaja način, da prepričamo učiteljico o našem avtorstvu?
7. Katere lastnosti želimo pri zgoščevalnih funkcijah za hranjenje gesel v računalniških sistemih?
Kako bi problem primerjav gesel rešil le z eno zgoščevalno funkcijo (torej v nasprotju s predlogom v samem članku)?
8. Zakaj pri shranjevanju podatkov pogosto poleg podatka hranimo še njegovo *okrajšavo*? (Namig: kako preverimo, ali podatek ni pokvarjen, zakaj je iskanje po velikem disku lahko dolg proces, kako lahko na hitro primerjamo, kaj imamo shranjeno v oblaku in kaj lokalno na svojem domačem računalniku — ali lahko ugotoviš, kaj ti sistemi v ozadju počnejo.)
9. Poišči način krajšanja, ki ima lastnost 3, ne pa tudi lastnosti 4.
10. Poišči način krajšanja, ki ima lastnost 4, ne pa tudi lastnosti 3.
11. Zakaj lahko pri prenosu datotek prek BitTorrent protokola, sproti preverjaš ali si doslej prejel pravilne/nepokvarjene kose datotek.
12. Kako se pri igri kamen-škarje-list odkrije goljufanje? Čemu služi naključen niz, ki si ga Ana





in Bojan izbereta na začetku? Kaj gre lahko narobe, če ta niz ni naključno izbran? Zakaj Ana ne more iz vrednosti zgoščitve z_B ugotoviti Bojanove izbire? Zakaj lahko izmenjavo zgoštev z_A in z_B izvedemo z zamikom? Kako bi se dalo goljufati, če za funkcijo F lastnost 4 ne bi držala?

13. Kako so shranjena gesla za dostop do spletne učilnice na vaši šoli oz. tvojega računalnika?
14. Za kriptografske zgoščevalne funkcije skoraj vedno velja, da če se spremeni en sam bit vhoda, se mora spremeniti približno polovica bitov na izhodu. Zakaj je to pomembno? Ali bi bil problem, če bi se v izhodu spremenili skoraj vsi biti?
15. Uporabi seštevanje ali množenje števil (v $\mathbb{Z}$ ali $\mathbb{R}$) za sestavo nove zgoščevalne funkcije in jo analiziraj. Enosmernost nam zagotavlja problem iskanja seštevancev ali faktorjev. Ali je uporaben poseben primer, kadar vemo, da gre za enaka števila?
16. Ali je krajšanje, ki vrača začetnici imena, kriptografsko varna zgoščevalna funkcija? Možnost, da imata dva izmed petih učencev enake začetnice, je sicer majhna, 2,7 %, a v svetu zgoščevalnih funkcij je to ogromno. Za primer lahko naredimo tudi scenarij, da je v razredu 20 učencev. Takrat je možnost, da imata dva učenca enak izhod, že 57,1 % (z upoštevanjem, da niso vsa imena in priimki enako verjetni; če tega ne upoštevamo, zmanjšamo možnosti na 1,0 % pri 4 učencih in 26,5 % pri 20 učencih). Kako smo prišli do teh ocen?
17. Bločne šifre (najbolj slavna je danes AES) razdelijo tekst, ki ga želimo šifrirati, na bloke enake dolžine (npr. 128 bitov), nato pa šifrirajo vsak blok posebej. Če to naredimo z enim samim ključem K , se identični bloki sporočila $m = m_1 m_2 \dots m_t$ zašifrirajo v identične bloke tajnopisa:

$$c = c_1 c_2 \dots c_t, \text{ kjer je } c_i = \text{AES}_K(m_i),$$

kar je lahko problem, glej (zašifrirano) sliko 4.



SLIKA 4.

Zašifrirana slika znanega Linuxovega pingvina.

Zato včasih šifriranje nekoliko prepletemo, npr. po postopku

$$c_0 = IV, \quad c_i = \text{AES}_K(c_{i-1}) \text{ XOR } m_i, \text{ za } i \geq 1,$$

kjer je IV neka (javno) znana konstanta, bitni XOR pa v računalništvu zelo znana operacija, ki ji v slovenščini rečemo *ekskluzivni ali*. Postopek se je dolgo uporabljal za preverjanje celovitosti sporočila. Kako? Bi ga znal zapisati? Običajno zaključimo pismo s kakšno običajno frazo (Lep pozdrav) in če to napadalec ve, potem se da to izkoristiti (brez poznavanja ključa K). V bistvu lahko zadnji blok zamenja s poljubnim svojim. Bi znal pokazati, kako to stori?

18. Nad enosmernostjo se zamislimo še zunaj sveta računalnikov. Kateri pojavi iz našega običajnega življenja imajo lastnost enosmernosti?

× × ×

www.presek.si

www.fmf.uni-lj.si/sl/zalozba/

Nekaj iz ponudbe Založbe FMF

V Založbe Fakultete za matematiko in fiziko izdajamo matematično in fizikalno literaturo.
V nadaljevanju vam predstavljamo dve knjigi.

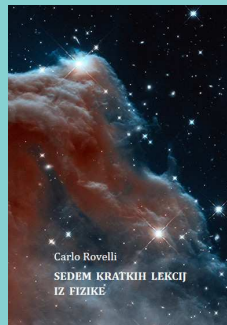


Mirko Dobovišek:

MATEMATIKA ZA FARMACEVTE

260 strani
format 16,5 × 23,5 cm
mehka vezava

18,00 EUR



Carlo Rovelli:

SEDEM KRATKIH LEKCIJ IZ FIZIKE

76 strani
format 12 × 17 cm
mehka vezava

9,50 EUR

Poleg omenjene ponujamo tudi druga matematična, fizikalna in astronomska dela. Spletna stran je še v delu, bodo pa podrobnejše predstavitve na spodnjem naslovu, kjer lahko vse publikacije tudi naročite:

<https://www.fmf.uni-lj.si/sl/zalozba/katalog/>

Dijaki in študentje imate ob naročilu pri Založbi Fakultete za matematiko in fiziko 20 % popusta, razen za najnovejše knjige! Dodatne informacije lahko dobite v knjižnici Fakultete za matematiko in fiziko po telefonu (01) 4766 558.



**REŠITEV
NAGRADNE
KRIŽANKE
PRESEK 50/6**

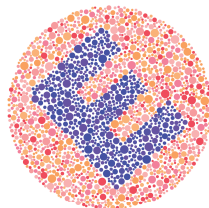
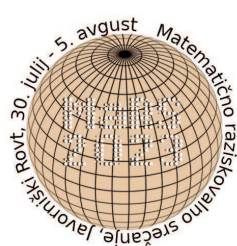
→ Pravilna rešitev nagradne križanke iz šeste številke Preseka letnika 50 je **Trigonometrija**. Med pravilnimi rešitvami smo izžrebali naslednje reševalce: Eva Šolinc iz Ljubljane, Izak Pelicon iz Šempasa in Janko Rušt iz Nove Gorice, ki bodo nagrade prejeli po pošti.



MaRSovski Estimathon



IZAK JENKO



Estimathon

→ Estimathon je razburljiva ekipna igra, ki združuje kviz s hitrim matematičnim razmišljanjem in ocenjevanjem. Ekipa ima 30 minut časa, da po svojih najboljših močeh ocenijo odgovore na 13 vprašanj iz raznoraznih področij. Ekipa, ki konča z najboljšim naborom ocen, zmaga.

Pravila igre

Igra traja 30 minut, v katerih vsaka od ekip sočasno rešuje 13 ocenjevalnih problemov, ki niso standardni in si jih organizator vsakič posebej pripravi vnaprej, lahko pa jih tudi reciklira. Vsi problemi imajo točno rešitev, ki je pozitivno realno število, vsaka od ekip pa rešitev ocenjuje in odgovor odda tako, da poda interval s pozitivnimi mejami, za katerega meni, da vsebuje točno rešitev.

Točkovanje. Pravimo, da je dani interval, ki ga odda ekipa, *dober*, če vsebuje točen odgovor. Število točk izračunamo s formulo

$$\left(10 + \sum_{\text{dobri intervali}} \left\lfloor \frac{\max}{\min} \right\rfloor \right) \cdot 2^{13 - (\text{št. dobrih intervalov})}.$$

Seštejemo torej spodnje cele dele razmerij zgornjih in spodnjih mej vseh dobrih intervalov, temu prištejemo 10 in na koncu rezultat pomnožimo s tolikšno potenco števila 2, kot je bilo praznih ali intervalov, ki niso vsebovali točnega odgovora. Za vsak prazen ali napačen odgovor se tako rezultat podvoji. Zmaga ekipa, ki na koncu zbere *najmanjše* število točk.

Oddaja odgovorov. Vsaka ekipa ima na voljo 18 listkov, na katere zapiše ime svoje ekipe, številko problema, ki ga ocenjuje, ter krajišči intervala, torej zgornjo in spodnjo mejo svoje ocene rešitve danega problema. Za dani problem lahko tako ekipa odda več listkov z odgovori, vendar pa za rezultat vedno šteje zadnji oddani listek. Listke je možno oddajati tekom celotnih 30 minut igranja. Ves čas tekmovanja je razvidna tudi tabela rezultatov, ki se sproti posodablja.

Prepovedana je uporaba računal, telefonov, interneta in drugih zunanjih pripomočkov.

Igra Estimathon je bila zasnovana leta 2013 s strani podjetja Jane Street. Več o Estimathonu lahko izvedemo na povezavi www.estimathon.com/.



SLIKA 1.

Ekipa marsovcev zavzeto ugiba in ocenjuje odgovore.

Estimathon na MaRSu

Na letošnjem MaRSu 2023 smo se v sklopu družabnega programa pomerili v ocenjevanju naslednjih 13 reči:

1. Koliko kilometrov je Mars oddaljen od Sonca v najdaljši točki svoje orbite?
2. Koliko kilometrov zračne razdalje so udeleženci v povprečju prepotovali od doma do tabora?

vprašanje	1	2	3	4	5	6	7
rešitev	249.261.000	72,2	42	12.586.269.025	70.030	$2660 \cdot 10^7$	706
vprašanje	8	9	10	11	12	13	
rešitev	5.053.908	$2,997 \cdot 10^{15}$	2.233	$45 \cdot 10^9$	17,3	250	

TABELA 1.

Podatek z dne 30. 7. 2023.

- 3. Kolikokrat se pojavi »ti« v skladbi Modrijanov »Ti, moja rožica«?
- 4. Katero je 50. Fibbonacijevo stevilo?
- 5. Koliko je svetovni rekord v pomnenu števil pi?
- 6. Koliko objav ima Borut Pahor na Instagramu?
- 7. Koliko prostih metov je zgrešil Luka Dončić v svoji NBA karieri?
- 8. Koliko znaša površina Javorniškega jezera v enotah največje ploskve čokolade Mars?
- 9. Na koliko različnih načinov lahko 27 dijakov razdelimo v trojice?
- 10. Koliko vrstic kode html je v letošnji spletni strani MaRS?
- 11. Koliko ameriških dolarjev so bili v letu 2022 prihodki »Mars, Inc.«, podjetja, ki proizvaja Mars čokolade?
- 12. Koliko kilometrov je dolga najkrajša ruska kopenska meja z eno izmed sosednjih držav?
- 13. Leta 2020 so uspeli faktorizirati največje splošno število do sedaj. Koliko števk je imelo?

Točne rešitve na vprašanja lahko najdemo v tabeli 1.

Rezultati in zaključek

Ekipe na MaRSu so se najboljše odrezale pri vprašanjih 2 in 3, prav nobena ni podala pravilne ocene za odgovor na kombinatorično vprašanje številka 9, vprašanja 13 pa se ni lotila praktično nobena ekipa. Zgodil pa se nam je tudi nepredvidljiv zaplet. Bivšemu predsedniku Borutu Pahorju so namreč na dan MaRSovskega Estimathona vdrli v Instagram račun in naglo izbrisali nezanemarljivi del objav. Pri

razglasitvi rešitev, ki so si jih organizatorji pripravili že prejšnji dan, je zato prišlo do neskladja pri problemu 6, kar so dijaki hitro opazili in vložili pritožbe. Nazadnje se je upošteval trenutni znesek objav tistega dne. Do spremembe na vrhu lestvice ekip na srečo ni prišlo, zmagala je ekipa Človeška ribica.

Posebni zahvali za organizacijo MaRSovskega Estimathona gresta Davidu Opaliču in Matiji Likarju.

xxx

Križne vsote

↓↓↓

→ Naloga reševalca je, da izpolni bele kvadratke s števki od 1 do 9 tako, da bo vsota števk v zaporednih belih kvadratih po vrsticah in po stolpcih enaka številu, ki je zapisano v sivem kvadratu na začetku vrstice (stolpca) nad (pod) diagonalo. Pri tem morajo biti vse številke v posamezni vrstici (stolpcu) različne.

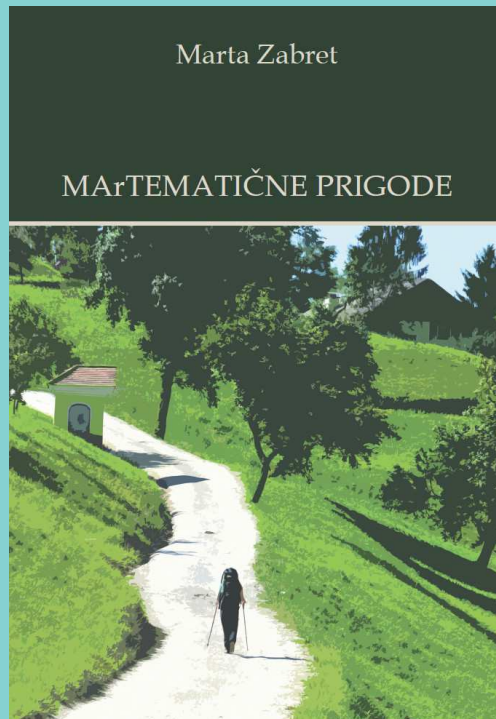
	5	17					
7						10	17
13			17		18		
	10			16			
			11				
		24					
			12				

xxx

MaRtematične prigode

Izšel je že tretji natis knjige MARTEMATIČNE PRIGODE

To je unikatna zbirka kratkih zgodb, v katerih je strnjeno veliko življenjskih izkušenj avtorice MARTE ZABRET. Izredno zanimive so zgodbe, ki izvirajo od njenih dijakinj in dijakov. Besedila so izpiljena in večinoma napisana strnjeno; včasih prav minimalistično, brez odvečnih besed. Poglavlja: Zakva bom pa jest to rabu?!; Pomoč ali potuha; Boš že videla; INTERNO, EKSTERNO, INFERNO dajejo humoren, a tudi neprizanesljiv pogled na probleme poučevanja, in to ne samo pouka matematike. Izvirne in posrečene ilustracije ter vinjete sta prispevali Ariana Godicelj in Ana Hafner.



12,50 EUR

Poleg omenjene ponujamo tudi druga matematična, fizikalna in astronomska dela. Spletna stran je še v delu, bodo pa podrobnejše predstavitve na spodnjem naslovu, kjer lahko vse publikacije tudi naročite:

www.fmf.uni-lj.si/sl/zalozba/katalog/

Dijaki in študentje imate ob naročilu starejših zbirk pri založbi Fakultete za matematiko in fiziko 20 % popusta na zgornje cene - izkoristite ga! Dodatne informacije lahko dobite v knjižnici Fakultete za matematiko in fiziko po telefonu (01) 4766 558.