



# PRESEK

- KDAJ NAS PRI PLAVANJU (NE) ZEBE?
- HITRO DO DA VINCIJEVE ŠIFRE
- NAGRADNA NALOGA
- NAGRADNA KRIŽANKA



ISSN 0351-6652



9 770351 665463

# Igranje iger

➔ Video igre so zelo zabavne, a bi bile precej manj brez matematike. Geometrija, analiza in linearna algebra pomagajo narediti znake, scene in akcijo manj dvodimenzionalno in bolj realistično. Kot je pripomnil nek izvršni direktor podjetja za izdelovanje iger, je napredovanje skozi matematiko podobno napredovanju skozi vse zapletenejše nivoje video igre. Kdo ve, morda boš do diplome pridobil dovolj spretnosti, da boš rešil svet.

Pri večini gibanja likov je vključena inverzna kinematika: Na primer, kakšni naj bodo koti stopala, golenice in stegna medtem, ko lik teče? To je pomembno področje raziskav, ki vključuje tudi trke in prepoznavanje kontaktov (kar je sicer očitno v realnem svetu, vendar zahteva eksplicitno izračunavanje v video svetu). Obstaja nešteto možnih odgovorov na take probleme, toda hitri algoritmi morajo poiskati realistične rešitve hitreje, kot lahko izgovorimo "stegenica je povezana s kolkom". ✖



**POJASNILO:** Gornji prispevek je prevod iz rubrike "The Mathematical Moments", ki jo objavlja Ameriško matematično društvo AMS na spletni strani [www.ams.org/mathmoments](http://www.ams.org/mathmoments).

## ➔ Presek

list za mlade matematike, fizike, astronome in računalnikarje letnik 34, šolsko leto 2006/2007, številka 6

**Uredniški odbor:** Vladimir Batagelj, Tanja Bečan (jezikovni pregled), Mojca Čepič, Mirko Dobovišek (glavni urednik), Vilko Domajnko, Darjo Felda (tekmovanja), Bojan Golli, Andrej Guštin (astronomija), Marjan Jerman (matematika), Martin Juvan, Maja Klavžar (odgovorna urednica), Damjan Kobal, Andrej Likar (fizika), Matija Lokar, Franci Oblak, Marijan Prosen, Marko Razpet, Andrej Taranenko (računalništvo), Marija Vencelj, Matjaž Vencelj.

**Dopisi in naročnine:** DMFA-založništvo, Presek, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana, telefon (01) 4766 553, 4232 460, telefaks (01) 4232 460, 2517 281.

**Internet:** [www.presek.si](http://www.presek.si)

**Elektronska pošta:** [presek@dmfa.si](mailto:presek@dmfa.si)

**Naročnina** za šolsko leto 2006/2007 je za posamezne naročnike 16,69 EUR (3.999,59 SIT) – posamezno naročilo velja do preklica, za skupinska naročila učencev šol 14,61 EUR (3.501,14 SIT), posamezna številka 3,76 EUR (901,05 SIT), dvojna številka 6,89 EUR (1.651,12 SIT), stara številka 2,71 EUR (649,42 SIT), letna naročnina za tujino pa znaša 25 EUR.

Transakcijski račun: 03100-1000018787.

Devizna nakazila: SKB banka d.d. Ljubljana, Ajdovščina 4, 1513 Ljubljana, SWIFT (BIC): SKBASIX, IBAN: SI56 0310 0100 0018 787.

**List sofinancirata** Javna agencija za raziskovalno dejavnost Republike Slovenije ter Ministrstvo za šolstvo in šport

**Založilo** DMFA-založništvo

**Oblikovanje, ilustracija in tehnično urejanje**  
Polona Šterk in Matjaž Čuk

**Tisk** Tiskarna Pleško, Ljubljana

**Naklada** 2100 izvodov

© 2007 Društvo matematikov, fizikov in astronomov Slovenije – 1672

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 prikaze 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, učenec 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 odgovorni urednici na naslov uredništva DMFA-založništvo, Uredništvo revije **Presek**, p. p. 2964, 1001 Ljubljana ali na naslov elektronske pošte [presek@dmfa.si](mailto:presek@dmfa.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 izvorno datoteko. 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 TRENUTKI

Igranje iger ..... 2

## ■ MATEMATIKA

Goldbachova domneva (*Irena Kosi-Ulbi*) ..... 4-7

Faktorialni številski sestav in parnost permutacij v  
leksikografski urejenosti (*Gorazd Mušič in Marko Petkovšek*) ..... 8-10

Nekaj nalog za počitnice (*Matjaž Kovše, Gašper Mekiš, Gordana  
Radič in Simon Špacapan*) ..... 10-13

Predstavitev nove knjige (*Dominik Benkovič*) ..... 31

## ■ FIZIKA

Kvantna kriptografija - Drugi del

- Varna izmenjava ključa (*Marko Žnidarič*) ..... 14-15, 18-19

Kdaj nas pri plavanju (ne) zebe? (*Mitja Rosina*) ..... 19-20

Kuhinjska poizkuševalnica - Kartezijev plavač, odgovor na  
nalogo iz prejšnje številke (*Mojca Čepič*) ..... 22-23

## ■ ASTRONOMIJA

Odkrivanje planetov s spektroskopskim merjenjem radialne  
hitrosti zvezd (*Nikolaj Štritof*) ..... 24-25

Izmerimo svetlobno onesnaženje v svojem kraju (*Andrej Guštin*) 26-27

## ■ RAČUNALNIŠTVO

Hitro do Da Vincijeve šifre (*Aleksander Vesel*) ..... 28-30

## ■ RAZVEDRILO

Nagradna križanka (*Marko Bokalič*) ..... 16-17

Rešitev nagradne križanke Presek 34/5 ..... 21

Nagradna naloga - povezana skrita računa (*Marija Vencelj*) ..... 21

## ■ TEKMOVANJA

Tekmujmo v razvedrilni matematiki ..... priloga

Naloge z državnega fizikalnega tekmovanja srednješolcev  
Slovenije v šolskem letu 2005/06 ..... priloga

Naloge z regijskega fizikalnega tekmovanja srednješolcev  
Slovenije v šolskem letu 2005/06 ..... priloga



# Goldbachova domneva

IRENA KOSI-ULBL

➔ Med množico matematičnih izjav (večino med njimi matematiki dokažejo in tako postanejo trditve ali izreki) se včasih pojavijo tudi domneve, za katere smo skoraj prepričani, da so resnične, vendar jih ni še nihče dokazal. Včasih mine več sto let, preden je katera med njimi dokazana (ali ovržena). V prispevku bomo predstavili eno izmed (zaenkrat) nedokazanih domnev s častitljivo starostjo – Goldbachovo domnevo.

## ■ Christian Goldbach

Christian Goldbach se je rodil 18. marca 1690 v Königsbergu v Prusiji (sedaj Kaliningrad, Rusija). V St. Petersburgu je postal profesor matematike in zgodovine. V 20-ih letih 18. stoletja se je zaposlil kot učitelj carja Petra II. v Moskvi. Potoval je po Evropi in se sestajal z vidnimi matematiki tistega časa (Leibniz, de Moivre, N. in D. Bernoulli). Goldbach je znan po svojem prispevku k razvoju teorije števil, zagotovo pa je najbolj odmevna njegova domneva, ki jo je zapisal v pismu Eulerju 7. junija 1742 (*Goldbachova prva domneva*):

- ▶ *Vsako liho naravno število, večje ali enako 9, lahko predstavimo kot vsoto treh lihih praštevil.*

Euler je v odgovoru Goldbachu postavil novo domnevo:

- ▶ *Vsako sodo število, večje ali enako šest, lahko predstavimo kot vsoto dveh lihih praštevil.*



Euler je izrazil svoje prepričanje, da sta domnevi resnični, vendar ju ne more dokazati. Ker prva domneva sledi iz druge (znane tudi kot *Goldbachova strožja* ali *druga domneva*), ne pa tudi obratno, je bila svetovna matematična javnost od takrat (pa vse do danes) bolj pozorna na drugo trditev.

Christian Goldbach se je za vedno poslovil 20. novembra 1764 in se v času svojega življenja skoraj zagotovo ni zavedal, da je v pismu Eulerju zastavil matematično nalogo, ki bo burila duhove še v tretjem tisočletju.

## Raziskovanje v zvezi z Goldbachovo domnevo

Najprej bomo navedli nekaj primerov, povezanih z Goldbachovo domnevo:

- Leta 1923 sta Hardy in Littlewood dokazala prvo domnevo za dovolj velika naravna števila. Pokazala sta, da obstaja tako naravno število  $n_0$ , da je vsako liho naravno število  $n > n_0$  vsota treh lihih praštevil.
- Leta 1937 je ruski matematik Vinogradov spet dokazal prvo domnevo za dovolj velika naravna števila. Po njegovih izračunih ima število  $n_0$  kar 6.846.169 števk!
- Leta 1966 je Chen Jing-Run dokazal, da lahko vsako dovolj veliko naravno število zapišemo kot vsoto praštevil in števila, ki je produkt dveh praštevil.
- Leta 1977 je Pogorzelski trdil, da je dokazal Goldbachovo domnevo, vendar njegov dokaz ni bil splošno priznan.

TABELA 1

|               |               |               |               |
|---------------|---------------|---------------|---------------|
| $6 = 3 + 3$   | $8 = 3 + 5$   | $10 = 3 + 7$  | $12 = 5 + 7$  |
| $14 = 3 + 11$ | $16 = 3 + 13$ | $18 = 5 + 13$ | $20 = 3 + 17$ |
| $22 = 3 + 19$ | $24 = 5 + 19$ | $26 = 3 + 23$ | $28 = 5 + 23$ |
| $30 = 7 + 23$ | $32 = 3 + 29$ | $34 = 3 + 31$ | $36 = 5 + 31$ |
| $38 = 7 + 31$ | $40 = 3 + 37$ | $42 = 5 + 37$ | $44 = 3 + 41$ |
| $46 = 3 + 43$ | $48 = 5 + 43$ | $50 = 3 + 47$ | $52 = 5 + 47$ |

Vrnimo se h Goldbachovi drugi domnevi. Predstavitev prvih nekaj sodih naravnih števil, večjih ali enakih 6, kot vsote dveh lihih praštevil, naredimo “na pamet” (tabela 1).

Pri večjih številih si pomagamo z žepnimi računalni, nato še z računalniki, ki pa so v zvezi z reševanjem Goldbachovega problema omejeni le na računsko preverjanje domneve.

Tabela 2 in diagram na sliki 1 sta povzeta po [3]. Tabela je nastala na osnovi zelo preproste računalniške procedure (računalniški programi, s katerimi preverjajo Goldbachovo domnevo za števila do reda velikosti  $10^{17}$ , delujejo na osnovi drugačnih postopkov, ki omogočajo hitrejše preverjanje). Vzemimo sodo število  $n$  in po vrsti praštevil  $p$  (začnemo s 3) do  $n/2$ . Razliko  $n - p$  testiramo, če je praštevilo. Če je razlika praštevilo, smo našli Goldbachovo particijo danega števila  $n$ . Prvi par, ki ga najdemo, imenujemo minimalna Goldbachova particija. Označimo z  $g(n)$  manjše od obeh praštevil v minimalni Goldbachovi particiji. V tabeli 2 so v prvem stolpcu prikazana nekatera soda naravna števila  $n$ , manjša od  $10^9$ , drugi in tretji stolpec prikazujeta minimalno Goldbachovo particijo danega števila  $n$ , skrajni desni stolpec pa kvocient  $g(n)/n$ . Iz tabele razberemo, da je zaporedje števil  $g(n)$  sicer naraščajoče, vendar vrednosti  $g(n)$  naraščajo veliko počasneje od zaporedja sodih naravnih števil  $n$ .

TABELA 2

| $n$  | $g(n)$ | $n - g(n)$ | $g(n)/n$    |
|------|--------|------------|-------------|
| 6    | 3      | 3          | 0.500000000 |
| 12   | 5      | 7          | 0.416666667 |
| 30   | 7      | 23         | 0.233333333 |
| 98   | 19     | 79         | 0.193877551 |
| 220  | 23     | 197        | 0.104545455 |
| 308  | 31     | 277        | 0.100649351 |
| 556  | 47     | 509        | 0.084532374 |
| 992  | 73     | 919        | 0.073588710 |
| 2642 | 103    | 2539       | 0.038985617 |
| 5372 | 139    | 5233       | 0.025874907 |

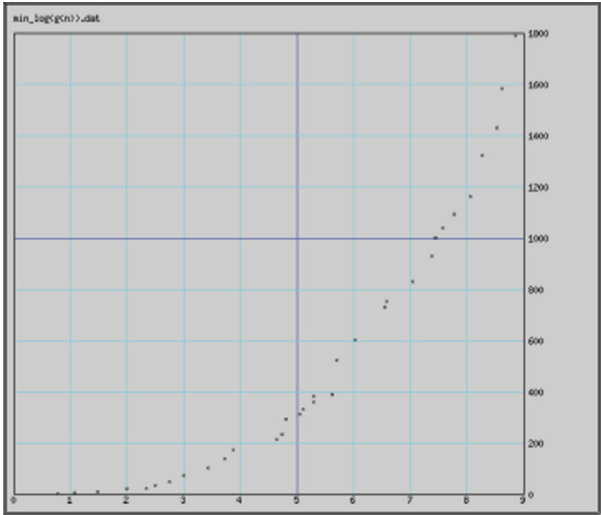




|           |      |           |             |
|-----------|------|-----------|-------------|
| 7426      | 173  | 7253      | 0.023296526 |
| 43532     | 211  | 43321     | 0.004847009 |
| 54244     | 233  | 54011     | 0.004295406 |
| 63274     | 293  | 62981     | 0.004630654 |
| 113672    | 313  | 113359    | 0.002753536 |
| 128168    | 331  | 127837    | 0.002582548 |
| 194428    | 359  | 194069    | 0.001846442 |
| 194470    | 383  | 194087    | 0.001969455 |
| 413572    | 389  | 413183    | 0.000940586 |
| 503222    | 523  | 502699    | 0.001039303 |
| 1077422   | 601  | 1076821   | 0.000557813 |
| 3526958   | 727  | 3526231   | 0.000206127 |
| 3807404   | 751  | 3806653   | 0.000197247 |
| 10759922  | 829  | 10759093  | 0.000077045 |
| 24106882  | 929  | 24105953  | 0.000038537 |
| 27789878  | 997  | 27788881  | 0.000035876 |
| 37998938  | 1039 | 37997899  | 0.000027343 |
| 60119912  | 1093 | 60118819  | 0.000018180 |
| 113632822 | 1163 | 113631659 | 0.000010235 |
| 187852862 | 1321 | 187851541 | 0.000007032 |
| 335070838 | 1427 | 335069411 | 0.000004259 |
| 419911924 | 1583 | 419910341 | 0.000003770 |
| 721013438 | 1789 | 721011649 | 0.000002481 |

Zelo nazoren je tudi grafični prikaz minimalnih Goldbachovih particij oziroma njihovih manjših sumandov. Na osi  $x$  so zaradi preprostejšega prikaza vrednosti  $\log(n)$ , na osi  $y$  pa vrednosti  $g(n)$ . Pravzaprav nam graf pripoveduje isto zgodbo kot zadnji stolpec v tabeli 2.

Na Goldbachovo domnevo lahko pogledamo tudi



Slika 1. Diagram prikazuje odvisnost manjšega praštevila  $g(n)$  v minimalni Goldbachovi particiji od  $\log(n)$ , pri čemer je  $n$  sodo naravno število.

| število $n$ | število Goldbachovih<br>particij števila $n$ |
|-------------|----------------------------------------------|
| 10          | 2                                            |
| 50          | 4                                            |
| 100         | 6                                            |
| 500         | 13                                           |
| 1000        | 28                                           |
| 5000        | 76                                           |
| 10000       | 127                                          |

TABELA 3

iz drugega zornega kota. Za dano sodo število  $n$  poiščimo število vseh različnih Goldbachovih particij, npr.:

$12 = 5 + 7$  (1 particija)  
 $24 = 5 + 19 = 7 + 17 = 11 + 13$   
(3 različne particije)  
 $48 = 5 + 43 = 7 + 41 = 11 + 37 = 17 + 31 = 19 + 29$   
(5 različnih particij)  
Tabela 3 (povzeto po [1]) prikazuje število različnih Goldbachovih particij za nekatera soda števila.

Iz tabele razberemo, da število različnih particij števila  $n$  narašča z rastočim številom  $n$  (obstajajo sicer redke izjeme). Če bomo kdaj našli sodo naravno število  $n$ , ki ne bo imelo nobene ustrezne particije, bo Goldbachova domneva ovržena. Do sedaj znani podatki kažejo ravno v nasprotno smer.

Oglejmo si še kratek zgodovinski pregled (povzeto po [2] in [4]), ki prikazuje, do katerega števila  $n$  je bila Goldbachova domneva preverjena ter kdo in kdaj jo je preveril.

| število $n$       | avtor                               |
|-------------------|-------------------------------------|
| $10^4$            | Desboves, 1885                      |
| $10^5$            | Pipping, 1938                       |
| $10^8$            | Stein in Stein, 1965                |
| $2 \cdot 10^{10}$ | Granville in drugi, 1989            |
| $4 \cdot 10^{11}$ | Sinisalo, 1993                      |
| $10^{14}$         | Deshouillers, 1998                  |
| $4 \cdot 10^{14}$ | Richstein, 1999                     |
| $2 \cdot 10^{16}$ | Oliveira e Silva, 24. marec 2003    |
| $6 \cdot 10^{16}$ | Oliveira e Silva, 3. oktober 2003   |
| $2 \cdot 10^{17}$ | Oliveira e Silva, 5. februar 2005   |
| $3 \cdot 10^{17}$ | Oliveira e Silva, 26. december 2005 |

## ■ Namesto zaključka

Kljub velikim naporom, ki so bili do danes vloženi v dokazovanje Goldbachove domneve, se matematiki iz celega sveta oklepajo rekla "Nikoli ne reci nikoli." Ob tem imamo v mislih še eno domnevo, znano pod imenom Fermatova domneva ali Fermatov zadnji iz-

rek. Okoli leta 1637 je Fermat namreč predpostavil, da za  $n > 2$  enačba  $x^n + y^n = z^n$  nima rešitev v množici celih števil, razen trivialnih rešitev, pri katerih je vsaj ena izmed neznank  $x, y, z$  enaka nič. Ta domneva je bila skrivnostna matematična uganka kar celih 350 let, dokler trditve ni dokazal nadarjeni Britanec Andrew Wiles, ki je sedaj zaposlen na Univerzi v Princetonu.

Založniška hiša Faber & Faber je za vzpodbudo pri dokazovanju Goldbachove domneve ponudila nagrado v višini 1.000.000 dolarjev za splošno priznan dokaz med 20. marcem 2000 in 20. marcem 2002. Po oceni strokovnjakov naj bi bilo na svetu okoli 20 ljudi, ki bi bili sposobni razrešiti to staro matematično uganko. Za enega največjih favoritov je veljal Alan Baker, profesor na Univerzi v Cambridgu, sicer dobitnik Fieldsove medalje. Fieldsove medalje – najprestižnejše nagrade na področju matematike – podeljujejo vsaka štiri leta najuspešnejšim matematikom, starim do 40 let. Alan Baker je ob razpisani nagradi menil, da človek nikoli ne more predvideti, kaj se bo zgodilo, vendar je mnenja, da je obdobje dveh let relativno kratek čas in da so trenutno znane matematične metode preveč preproste in neprimerne, da bi lahko naredili pomemben korak naprej pri dokazovanju Goldbachove domneve.

Kljub mikavni nagradi je ostala Goldbachova domneva še vedno nerešen problem. Oliveira e Silva, profesor na Oddelku za elektroniko in telekomunikacije Univerze v Aveiru, Portugalska, načrtuje preverjanje domneve za števila, manjša od  $10^{18}$ . Predvideva, da bo postopek preverjanja trajal več let, zato preko svetovnega spleta prosi za pomoč.

Morda pa se bo v prihodnosti vendarle pojavil skriti matematični genij in dokazal Goldbachovo domnevo. Najboljši matematiki se nikoli ne predajo, mar ne?

## ■ Literatura

- [1] <http://www.andrews.edu/~calkins/math/biograph/biogoldb.html>
- [2] <http://mathworld.wolfram.com/GoldbachConjecture.html>
- [3] <http://www.petrspec-technologies.com/Herkommer/goldbach.html>
- [4] <http://www.ieeta.pt/~tos/goldbach.html>
- [5] <http://www.maths.ex.ac.uk/~mwatkins/isoc/faber.html> ☒

# Faktorialni številski sestav in parnost permutacij v leksikografski urejenosti

GORAZD MUŠIČ in MARKO PETKOVŠEK

## ■ Permutacije

◉ Razvrstitev elementov končne množice imenujemo *permutacija*. Tako ima npr. množica {matematika, fizika, astronomija} šest permutacij, in sicer:

- (matematika, fizika, astronomija),
- (fizika, astronomija, matematika),
- (matematika, astronomija, fizika),
- (astronomija, matematika, fizika),
- (fizika, matematika, astronomija),
- (astronomija, fizika, matematika).

Koliko različnih permutacij množice z  $n$  elementi lahko sestavimo? Na prvo mesto lahko postavimo kateregakoli od  $n$  elementov, na drugo mesto kateregakoli od preostalih  $n - 1$  elementov ..., na zadnje mesto postavimo edini preostali element. Množica z  $n$  elementi ima torej  $n \times (n - 1) \times \dots \times 1$  permutacij. To število, produkt vseh naravnih števil od 1 do  $n$ , imenujemo  *$n$  faktorialno*, zapišemo pa kot  $n$  s klicajem ( $n!$ ).

| $n$  | 1 | 2 | 3 | 4  | 5   | 6   | 7    | 8     | 9      | 10      |
|------|---|---|---|----|-----|-----|------|-------|--------|---------|
| $n!$ | 1 | 2 | 6 | 24 | 120 | 720 | 5040 | 40320 | 362880 | 3628800 |

Več o permutacijah lahko izvemo v članku M. Juvana "O razvrstitvah in permutacijah", *Presek* 31 (2003-04), str. 22-27.

## ■ Faktorialni številski sestav

V desetiškem številskem sestavu uporabljamo kot mestne vrednosti potence števila 10. Zapis

■  $(c_d c_{d-1} \dots c_0)_{(10)}$

predstavlja število

■  $c_d \times 10^d + c_{d-1} \times 10^{d-1} + \dots + c_1 \times 10 + c_0$ ,

pri čemer so števke  $c_d, c_{d-1}, \dots, c_0$  iz množice  $\{0, 1, \dots, 9\}$ . V *faktorialnem številskem sestavu* pa za mestne vrednosti vzamemo števila  $n!$ . Zapis

■  $(c_d c_{d-1} \dots c_1)_{(f)}$

predstavlja število

■  $c_d \times d! + c_{d-1} \times (d - 1)! + \dots + c_2 \times 2! + c_1 \times 1!$ ,

pri čemer je  $c_i \in \{0, 1, \dots, i\}$ . Naslednja tabela prikazuje zapise prvih desetih naravnih števil v faktorialnem številskem sestavu (indeks ( $f$ ) je izpuščen).

| število           | 1 | 2  | 3  | 4  | 5  | 6   | 7   | 8   | 9   | 10  |
|-------------------|---|----|----|----|----|-----|-----|-----|-----|-----|
| faktorialni zapis | 1 | 10 | 11 | 20 | 21 | 100 | 101 | 110 | 111 | 120 |

Faktorialni zapis dobimo z zaporednim deljenjem



števila z 2, 3, 4, ... Ostanki, ki jih pri tem dobivamo, so števke  $c_1, c_2, c_3, \dots$ . Za zgled poiščimo faktorialni zapis števila 10000:

- $10000 : 2 = 5000$ , ostane 0;
- $5000 : 3 = 1666$ , ostane 2;
- $1666 : 4 = 416$ , ostane 2;
- $416 : 5 = 83$ , ostane 1;
- $83 : 6 = 13$ , ostane 5;
- $13 : 7 = 1$ , ostane 6;
- $1 : 8 = 0$ , ostane 1.

Torej je  $10000 = 1651220_{(f)}$ . Preskus:  $1 \times 7! + 6 \times 6! + 5 \times 5! + 1 \times 4! + 2 \times 3! + 2 \times 2! + 0 \times 1! = 1 \times 5040 + 6 \times 720 + 5 \times 120 + 1 \times 24 + 2 \times 6 + 2 \times 2 = 10000$ .

Faktorialni sestav ni zares uporaben za zapisovanje števil, saj v njem kot števke prej ali slej nastopijo vsa naravna števila. Ima pa nekatere zanimive lastnosti, ki so včasih koristne.

## ■ Inverzije in parnost

Naj bo  $p$  permutacija neke končne množice naravnih števil. Par števil  $(a, b)$  je *inverzija* permutacije  $p$ , če je  $a > b$ , v permutaciji  $p$  pa je  $a$  pred  $b$ . Permutacija  $p = (4, 2, 6, 5, 1, 3)$  ima npr. 9 inverzij, in sicer  $(4, 2)$ ,  $(4, 1)$ ,  $(4, 3)$ ,  $(2, 1)$ ,  $(6, 5)$ ,  $(6, 1)$ ,  $(6, 3)$ ,  $(5, 1)$ ,  $(5, 3)$ .

Pogosto je pomembna *parnost* števila inverzij v permutaciji. Permutacije s sodim številom inverzij imenujemo – kako le? – *sode permutacije*, tiste z lihim številom inverzij pa *lihe permutacije*. Permutacija  $p = (4, 2, 6, 5, 1, 3)$  je torej liha.

## ■ Leksikografska urejenost

Vse permutacije množice  $\{1, 2, \dots, n\}$  je morda najnaravneje naštet v *leksikografskem vrstnem redu*, torej podobno, kot so razvrščene besede v slovarju: najprej pridejo na vrsto permutacije, ki se začno z 1, nato tiste, ki se začno z 2, itd. Permutacije, ki se na prvem mestu ujemajo, razvrstimo po velikosti drugega elementa, tiste, ki se ujemajo na prvih dveh mestih, pa po velikosti tretjega elementa. Splošno pravilo se glasi: Če se permutaciji ujemata na prvih  $k - 1$  mestih, na  $k$ -tem pa ne, pride prej na vrsto tista z manjšim elementom na  $k$ -tem mestu. Naštejmo zdaj vseh 24 permutacij množice  $\{1, 2, 3, 4\}$  v leksikografskem vrstnem redu in jih označimo  $p_0, p_1, \dots, p_{23}$  (tabela 1).

|                       |                       |                       |                       |                       |                       |
|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| $p_0$<br>(1,2,3,4)    | $p_1$<br>(1,2,4,3)    | $p_2$<br>(1,3,2,4)    | $p_3$<br>(1,3,4,2)    | $p_4$<br>(1,4,2,3)    | $p_5$<br>(1,4,3,2)    |
| $p_6$<br>(2,1,3,4)    | $p_7$<br>(2,1,4,3)    | $p_8$<br>(2,3,1,4)    | $p_9$<br>(2,3,4,1)    | $p_{10}$<br>(2,4,1,3) | $p_{11}$<br>(2,4,3,1) |
| $p_{12}$<br>(3,1,2,4) | $p_{13}$<br>(3,1,4,2) | $p_{14}$<br>(3,2,1,4) | $p_{15}$<br>(3,2,4,1) | $p_{16}$<br>(3,4,1,2) | $p_{17}$<br>(3,4,2,1) |
| $p_{18}$<br>(4,1,2,3) | $p_{19}$<br>(4,1,3,2) | $p_{20}$<br>(4,2,1,3) | $p_{21}$<br>(4,2,3,1) | $p_{22}$<br>(4,3,1,2) | $p_{23}$<br>(4,3,2,1) |

Tabela 1. Permutacije množice  $\{1, 2, 3, 4\}$  v leksikografski urejenosti

## ■ Zaporedna številka in parnost

Vprašanje, ki nas zanima, je naslednje: *Kako bi iz zaporedne številke permutacije v leksikografskem vrstnem redu neposredno razbrali njeno parnost?* V tabelo 2 zapišimo parnosti permutacij množice

|                          |               |               |               |               |               |               |
|--------------------------|---------------|---------------|---------------|---------------|---------------|---------------|
| permutacija:<br>parnost: | $p_0$<br>S    | $p_1$<br>L    | $p_2$<br>L    | $p_3$<br>S    | $p_4$<br>S    | $p_5$<br>L    |
| permutacija:<br>parnost: | $p_6$<br>L    | $p_7$<br>S    | $p_8$<br>S    | $p_9$<br>L    | $p_{10}$<br>L | $p_{11}$<br>S |
| permutacija:<br>parnost: | $p_{12}$<br>S | $p_{13}$<br>L | $p_{14}$<br>L | $p_{15}$<br>S | $p_{16}$<br>S | $p_{17}$<br>L |
| permutacija:<br>parnost: | $p_{18}$<br>L | $p_{19}$<br>S | $p_{20}$<br>S | $p_{21}$<br>L | $p_{22}$<br>L | $p_{23}$<br>S |

Tabela 2. Parnosti permutacij množice  $\{1, 2, 3, 4\}$

$\{1, 2, 3, 4\}$  (S – soda permutacija, L – liha permutacija). Iščemo torej postopek, s katerim bi ugotovili, da je npr. permutacija  $p_{19}$  soda, ne da bi jo sploh zapisali.

Pogled na tabelo 2 nam pokaže, da se prva vrstica (S,L,L,S,S,L) ponovi v drugi vrstici v zrcalni obliki (L,S,S,L,L,S), v tretji vrstici v nespremenjeni obliki, v četrti vrstici pa spet v zrcalni obliki. Kako bi to razložili?

Če permutacijam v tabeli 1 odstranimo prvi element, dobimo v posameznih vrsticah permutacije množic  $\{2, 3, 4\}$ ,  $\{1, 3, 4\}$ ,  $\{1, 2, 4\}$  oz.  $\{1, 2, 3\}$ , vse



→ v leksikografskem vrstnem redu. Zaporedje parnosti dobljenih krajših permutacij je v vseh štirih primerih enako, namreč S,L,L,S,S,L. Če odstranjeni element (označimo ga z  $i$ ) postavimo spet nazaj na prvo mesto, nastane  $i-1$  novih inverzij, saj je  $i$  večji od števil  $1, 2, \dots, i-1$ . Parnost ostane torej enaka, če je  $i$  liho število oz. se spremeni, če je  $i$  sodo število.

Naj bo  $Z_n$  zaporedje parnosti permutacij množice  $\{1, 2, \dots, n\}$ , zapisanih v leksikografskem vrstnem redu. Zdaj vidimo, da  $Z_n$  dobimo iz  $Z_{n-1}$  takole: zaporedje  $Z_{n-1}$  ponovimo  $n$ -krat, pri tem pa pri vsaki drugi ponovitvi vse parnosti zamenjamo z nasprotnimi. Oglejmo si to za  $n = 1, 2, 3, 4$  (tabela 3, zamenjane parnosti so natisnjene krepko).

| $n$ | $Z_n$                                                     |
|-----|-----------------------------------------------------------|
| 1   | 0<br>S                                                    |
| 2   | 0 1<br>S L                                                |
| 3   | 0 1 2<br>S, L, L, S, S, L                                 |
| 4   | 0 1 2 3<br>S, L, L, S, S, L, L, S, S, L, L, S, S, L, L, S |

Tabela 3. Zaporedje parnosti permutacij množice  $\{1, 2, \dots, n\}$

Za parnost permutacije množice  $\{1, 2, 3, 4\}$  je pomembno, v kateri šesterki zaporedja  $Z_4$  se nahaja, v

katerem paru te šesterke in na katerem mestu v tem paru. Začnimo šteti z 0. Potem se npr. parnost permutacije  $p_{19}$  nahaja v šesterki št. 3, v paru št. 0, na mestu št. 1. Velja namreč  $19 = 3 \times 6 + 0 \times 2 + 1 \times 1$  oz.  $19 = 301_{(f)}$ . V tabeli 3 sledimo parnosti permutacije  $p_{19}$  s kvadratnim okvirčkom. Začetna permutacija v prvi vrstici je soda, v vsaki naslednji vrstici pa se parnost spremeni, če je kvadrater v podzaporedju z liho številko, oz. ostane, če je kvadrater v podzaporedju s sodo številko. Te številke pa so ravno številke števila 19 v faktorialnem zapisu. Na koncu je parnost soda, če se je spremenila sodo mnogokrat, oz. liha, če se je spremenila liho mnogokrat. Tako smo prišli do rešitve zastavljenega problema:

**TRDITEV 1.** Permutacija  $p_k$  je soda natanko tedaj, ko ima faktorialni zapis števila  $k$  sodo mnogo lihih števk.

Permutacija z zaporedno številko  $19 = 301_{(f)}$  je soda, tista z zaporedno številko  $10000 = 1651220_{(f)}$  pa liha.

Spomnimo se še, kako poiščemo faktorialni zapis, pa lahko zaključimo:

**TRDITEV 2.** Permutacija  $p_k$  je soda natanko tedaj, ko pri zaporednem deljenju števila  $k$  z  $2, 3, 4, \dots$  dobimo sodo mnogo lihih ostankov.

Zanimivo je, da je parnost permutacije  $p_k$  množice  $\{1, 2, \dots, n\}$  (kjer je seveda  $n! > k$ ) odvisna le od števila  $k$ , nič pa od števila  $n$ . To je posledica dejstva, da je zaporedje parnosti  $Z_{n-1}$  začetni odsek zaporedja  $Z_n$ . ✖

## Nekaj nalog za počitnice

MATJAŽ KOVŠE, GAŠPER MEKIŠ,  
GORDANA RADIĆ in SIMON ŠPACAPAN



➔ Izgleda že ne tako. Vprašanje pa je, kaj pa sploh počne? Večina bi verjetno takoj pomislila, da je to kakšna matematična "čudakinja", ki dan in noč sedi za pisalno mizo in rešuje matematične naloge. Matematika je pač veda, ki večini ljudi ni preveč pri srcu. Predpostavljamo, da za vas to ne velja. Po vsej ver-

jetnosti spadate med tisto trohico ljudi, ki jim matematika ne dela težav, in zaradi tega nimate takšnih asociacij. Po možnosti vam je matematika "fajn" in vam je reševanje takšnih in drugačnih nalog v veliko veselje in vam celo predstavlja nekakšen izziv.

In prav zaradi takšnih kot ste vi, smo se tudi letos odločili in sestavili kup zanimivih problemov. Neka-teri so zelo enostavni, pri drugih pa se lahko zgodi, da bodo zahtevali malo več časa za premislek. Prva polovica nalog je namenjena vsem bralcem, medtem ko je za drugo polovico nalog včasih potrebno srednješolsko znanje. Pri nalogah 14–18 predpostavljamo, da oba igralca igrata optimalno, torej najboljše možno. Ker je Bine kavalir, igro zmeraj prične Anica.

No, in kaj počnete sedaj? Nič pametnega? Potem pa hitro svinčnik v roke in se lotite reševanja. Saj boste videli, da ni težko. In prosim, ne sedet za mizo tako dolgo kot gospa na začetku tega prispevka. Privoščite si kakšen premor, dobite se s prijatelji, pojedite s fantom ali s punco na sprehod. Skratka, imejte kar se da lepe in nepozabne počitnice.

P.S.: Ste opazili, da je uvodni stavek anagram?

1. Izmed 200 obiskovalcev plaže jih 160 govori slovensko, 180 angleško in 140 italijansko. Najmanj koliko obiskovalcev plaže govori vse tri jezike?

2. Drevesa v sadovnjaku so razvrščena v (kvadratni obliki) v  $n$  vrstic in  $n$  stolpcev. Lastnik sadovnjaka je povečal število vrstic in število stolpcev za ena in pri tem dodal 29 novih dreves. Koliko dreves je v sadovnjaku po povečanju?

3. Lojzka, Štefka in Marička so tekmovali na državnem tekmovanju iz matematike in se uvrstile na tri zaporedna mesta. Produkt njihovih mest je 504. Koliko je vsota njihovih mest?

4. Poslovnež ima naloženih za 50000 € delnic v dveh delniških skladih. Nato prenese tretjino naložbe prvega sklada iz prvega v drugi sklad, zatem pa še prenese naložbo v vrednosti 7000 € spet iz prvega v drugi sklad. Na koncu sta naložbi v obeh skladih iste vrednosti. Koliko denarja je imel poslovnež na začetku naloženega v prvem skladu?

5. Andrej, Bojan, Ciril in Dominik so med sabo tekmovali v znanju matematike. Andrej je rekel: "Nisem bil niti prvi, niti zadnji," Bojan: "Nisem bil za-

dnji," Ciril: "Bil sem zadnji." Dominik pa je izjavil: "Bil sem prvi." Nobena dva nista zasedla istega mesta in natanko trije so povedali resnico. Kdo je končal prvi in kdo zadnji? Odgovor utemelji.

6. Marička je študentka Fakultete za naravoslovje in matematiko, rojena v 20. stoletju. Katerega leta se je rodila, če je leta  $x^2 - 19$  imela  $x - 23$  let?

7. Babica je s prodajo jagod zaslužila  $X$  €. Razdelila jih je trem vnukom. Če je dala najstarejšemu polovico in še 1 €, srednjemu polovico preostale polovice in še 1 €, ostanek pa je razdelila na pol in dala najmlajšemu eno polovico in še 3 €, potem je porabila ves denar. Koliko denarja je zaslužila?

8. Vsak dan se kmet Marko odpravi na tržnico prodajati krompir. V ponedeljek ga je vzel s seboj 80 kg. V torek zjutraj je stehal, koliko kilogramov mu je še preostalo od prejšnjega dne. Ker se mu je zdelo, da je ostalo premalo, se je odločil da bo to količino podvojil. Do konca dneva je prodal enako količino kot dan prej. Naslednji dan pa se je Marko odločil, da bo količino krompirja, ki je ostala od torka, potrojil. Tudi v sredo je prodal enako količino kot v ponedeljek in torek. Koliko krompirja je prodal vsak dan, če je v sredo prodal ves krompir, ki ga je imel s seboj?

9. Koti v trikotniku so v razmerju 3 : 4 : 5. Kako dolga je najdaljša stranica, če najkrajša meri 1 meter?

10. V nekem razredu ima 9 učencev dobre ocene pri fiziki, 13 pri kemiji in 14 učencev ima dobre ocene pri biologiji. Štirje učenci imajo dobre ocene hkrati pri fiziki in kemiji, trije hkrati pri fiziki in biologiji ter šest učencev ima dobre ocene hkrati pri kemiji in pri biologiji. V razredu je tudi zelo priden učenec, ki ima dobre ocene pri vseh treh predmetih, ter štirje učenci, ki imajo slabe ocene pri vseh treh predmetih. Koliko učencev ima slabe ocene pri fiziki?

11. Na okroglem obroču imamo  $n$  ključev enake oblike,  $n \geq 3$ . Če vsak ključ pobarvamo s svojo barvo, potem lahko ključ ločimo med seboj. Najmanj koliko barv potrebujemo, da bomo ključ ločili med seboj? Pri tem moramo upoštevati, da se obroč s ključi lahko vrti ali obrne.





12. Na vsakem polju šahovnice velikosti  $9 \times 9$  se nahaja po ena čebelica. Čez čas se vse čebelice pomaknejo po diagonali na eno izmed sosednjih polj. Pri tem se lahko zgodi, da eno polje zasede več čebelic. Lahko pa tudi katero izmed polj ostane prazno. Poišči najmanjše možno število praznih polj.

13. Šahovska pravila nekoliko spremenimo tako, da v vsaki potezi igralec naredi dva legalna premika svojih figur. Pokaži, da obstaja strategija za igralca z belimi figurami, ki mu zagotavlja vsaj neodločen rezultat.

14. Anica in Bine menjaje postavljata bele in črne konje na nezasedena polja šahovnice, ki še niso napadena z nasprotnikovim konjem, torej konjem nasprotne barve. Poraženec je tisti, ki ne more več postaviti novega konja na šahovnico. Ali obstaja strategija za Anico ali Bineta, ki zagotavlja zmago?

15. Anica in Bine menjaje postavljata bele in črne tekače na nezasedena polja šahovnice, ki še niso napadena z nasprotnikovim tekačem, torej tekačem nasprotne barve. Pri tem lahko oba postavljata tekače na polja obeh barv. Poraženec je tisti, ki ne more več postaviti novega tekača na šahovnico. Ali obstaja strategija za Anico ali Bineta, ki zagotavlja zmago?

16. Anica in Bine menjaje rišeta diagonale pravnega 2006-kotnika. Pri tem morata upoštevati pravilo, da lahko povežeta dve oglišči, če nova diagonala ne seka katere izmed že narisanih diagonal znotraj 2006-kotnika. Poraženec je tisti, ki ne more narisati nove diagonale. Ali obstaja strategija za Anico ali Bineta, ki zagotavlja zmago?

17. Igra se prične s številom  $n = 2$ . Anica in Bine menjaje prištevata nek pravi delitelj<sup>1</sup> števila  $n$  k trenutnemu številu  $n$ . Cilj igre je doseči število, ki bo večje od 2007. Ali obstaja strategija za Anico ali Bineta, ki zagotavlja zmago?

18. Anica in Bine menjaje vstavlja znake  $+$ ,  $-$  in  $\times$  na katerakoli prosta mesta med števila

$$1 \quad 2 \quad 3 \quad \dots \quad 99 \quad 100.$$

Pokaži, da lahko Anica vedno doseže, da je rezultat: (a) liho število, (b) sodo število.

19. V vrsti stoji 2007 škatel. Škatla na  $k$ -tem mestu vsebuje  $k$  kroglic. Na vsakem koraku lahko izberemo poljubno število škatel in iz vseh izbranih škatel odstranimo enako število kroglic, kot smo izbrali škatel. Najmanj koliko korakov je potrebnih, da izpraznimo vse škatle?

20. Ali lahko tlakujemo pravokotnik sestavljen iz  $66 \times 62$  kvadratkov s pravokotniki sestavljenimi iz  $12 \times 1$  kvadratkov?

21. Računalniška trgovina ima razprodajo: disketa stane 1 €, zgoščenska 3 € in DVD stane 4 €. Kako naj kupimo 30 medijev, tako da bomo porabili točno 50 € in kupili vsaj en medij iz vsake skupine?

22. Peter si je pri prijatelju izposodil  $xyzu$  €, (kjer so  $x, y, z$  in  $u$  števke) in kasneje pozabil, koliko si je izposodil. Prijatelj, ki je zagrizen matematik, mu je dolg posredoval s sistemom enačb:

- $x + y + z + u = 10$
- $-2x + 3y - z + 2u = 9$
- $3x + 8y - z - 3u = 4$
- $-x + 4y - 12z + u = -25$ .

Da bi dobil denar za pokritje dolga, se je prijavil za delo v tujini, kjer je v enem tednu zaslužil natanko trimestno vsoto denarja. Kolikšen bo tedenski zaslužek so mu povedali s pomočjo naslednje naloge: Trimestno število ima vsoto števk enako 12. Če zamenjamo enice in desetice, bo nastalo število manjše za 36, in če zamenjamo enice in stotice bo novo število večje za 99.

Peter bo v tujini delal 5 tednov. Ali bo v tem času zaslužil dovolj, da bo lahko pokrtil dolg?

23. Naj bo  $f(x)$  funkcija, za katero za vse  $x$  iz  $\mathbb{R}$  velja  $5f(x) + 2f(2-x) = 3x - 5$ . Izračunaj  $f(4)$ .

24. Poenostavi izraz

$$\frac{\sqrt{\sqrt{5}+2} + \sqrt{\sqrt{5}-2}}{\sqrt{\sqrt{5}+1}}$$

do oblike

<sup>1</sup>pravi delitelj števila  $n$  je delitelj števila različen od  $n$



$$\blacksquare \frac{a + b\sqrt{c}}{d},$$

kjer so  $a, b, c$  in  $d$  cela števila.

25. Poišči vse realne rešitve sistema enačb

$$\blacksquare \begin{cases} x^2y + xy^2 = 1 \\ x^3 + y^3 = 5. \end{cases}$$

26. Pokaži, da je število  $13^{123456} - 1$  deljivo s 17.

27. Oče petih sinov poseduje posestvo, ki meri  $3 \text{ km}^2$ . Oče, ki ni ravno vešč računanja, želi razdeliti posestvo med svoje sinove. Vsakemu naroči, da si naj izmeri del posestva v velikosti  $1 \text{ km}^2$ . Dokaži, da se vsaj dvema sinovoma njuna dela prekrivata za vsaj  $1/5 \text{ km}^2$ .

28. Poišči takšen  $n \in \mathbb{N}$ , za katerega velja

$$\blacksquare 3! \cdot 5! \cdot 7! = n!$$

29. Naj bo  $f(x) = (x - 1)/(x + 1)$ . Izrazi  $f(2x)$  s pomočjo  $f(x)$ .

30. Poišči vsa cela števila, pri katerih funkcija  $f(x) = x^2/(x + 3)$  zavzame celoštevilске vrednosti.

31. Poišči vse pare naravnih števil  $x, y$ , za katere velja enakost  $4^x + 5 = 9^y$ .

32. Naj bo  $f: \mathbb{N} \rightarrow \mathbb{N}$ , ki zadošča enakosti  $f(f(n)) + 2f(n) = 3n + 4$  za vsak  $n \in \mathbb{N}$ . Poišči  $f(2007)$ .

33. Poišči vsa praštevila  $p$ , za katera so števila  $p + 2$ ,  $p + 8$ ,  $p + 14$  in  $p + 56$  tudi praštevila.

34. Za  $x \in \mathbb{R}$  naj bo  $\lfloor x \rfloor$  največje celo število, ki je manjše ali enako  $x$ , in naj bo  $\{x\} = x - \lfloor x \rfloor$ . Naj bo  $p$  praštevilo in  $s$  celo število  $0 < s < p$ . Dokaži, da obstajata celi števili  $m$  in  $n$ , za kateri velja  $0 < m < n < p$  in

$$\blacksquare \left\{ \frac{sm}{p} \right\} < \left\{ \frac{sn}{p} \right\} < \frac{s}{p}$$

natanko tedaj, ko  $s$  ne deli  $p - 1$ .



Rešitve nalog bomo v juliju objavili na Presekovi domači strani [http:// www.presek.si](http://www.presek.si) ☒



# Kvantna kriptografija

## DRUGI DEL - VARNA IZMENJAVA KLJUČA

MARKO ŽNIDARIČ

### ■ Kvantna kriptografija

☉ Osnovna ideja kvantne varne komunikacije oz. natančneje, kvantne izmenjave ključa je, da si Anja in Boštjan, še preden začneta s pošiljanjem šifriranih sporočil, po t.i. kvantnem kanalu izmenjata skrivni ključ. Kvantni kanal je povezava med Anjo in Boštjanom, po kateri si izmenjujeta kvantne delce. Kasneje si bomo podrobneje ogledali primer, pri katerem je kvantni kanal kar navadno telekomunikacijsko optično vlakno, po katerem Anja pošlje Boštjanu fotone, torej posebej oblikovane pulze svetlobe. Končni produkt tega prvega kvantnega dela komunikacije je ta, da imata oba enako skrivno geslo, pri čemer lahko absolutno zagotovita, da je le-to res znano samo njima, četudi je pošiljanju fotonov nekdo "prisluškoval". Nadaljnji postopek, po tem ko imata skupni ključ, je popolnoma klasičen. Za šifriranje uporabita enega izmed algoritmov z zasebnim ključem, najboljši kar Vernamov postopek, ki je edini dokazano varen. Kot bomo videli, nam varnost prvega dela, torej kvantne izmenjave ključa, zagotavlja kvantna fizika. Varnost izmenjave ključa torej ne temelji na nepreverjenem matematičnem dejstvu, npr. na težavnosti faktorizacije kot pri RSA, temveč na fizikalnih zakonih. RSA zaščito lahko tudi zloмимо, če le imamo dovolj hiter računalnik. Vdor v kvantno izmenjavo ključa pa je v nasprotju s fizikalnimi zakoni. Kvantna varna komunikacija torej odpravi glavno pomanjkljivost Vernamovega šifriranja, to je problem varne izmenjave ključa. Oglejmo si podrobneje, kako je zagotovljena varnost kvantne izmenjave ključa.

+ = vodoravna ali navpična polarizacija

$\leftrightarrow = 0$

$\updownarrow = 1$

x = polarizacija pod kotom 45° ali 135°

$\nearrow = 0$

$\searrow = 1$

Slika 1. Slovarček polarizacij

Princip je enak kot pri kvantnih bankovcih. Temelj je spoznanje, da kvantnih sistemov ni mogoče pomeriti, ne da bi jih pri tem zmotili. Temu je ekvivalentna izjava, da jih ni mogoče klonirati. Kloniranje kvantnega sistema bi pomenilo, da bi stanje sistema popolnoma verodostojno skopirali. Če bi bilo kloniranje mogoče, bi lahko meritve opravljali, ne da bi sistem zmotili. Sistem bi enostavno klonirali, potem pa opravili meritve na podvojeni kopiji. Stanje te kopije bi se ob meritvi sicer spremenilo, vendar pa bi stanje prvega sistema ostalo nedotaknjeno. To pa je v nasprotju z zakoni kvantne fizike. Pri kvantni varni komunikaciji za izmenjavo ključa ponavadi uporabimo fotone, ki jih pošiljamo po optičnem vlaknu. Fotoni so lahko v dveh osnovnih ortogonalnih stanjih, ki ju določa smer linearne polarizacije. Dve različni polarizaciji fotona nam pri kvantni komunikaciji predstavljata dve različni vrednosti bita, torej 0 in 1. Dogovoriti se je seveda potrebno, katera smer polarizacije bo pomenila katero vrednost (vodoravna polarizacija nam npr. pomeni vrednost 0, navpična pa 1). Izkaže se, da za uspešno kvantno izmenjavo

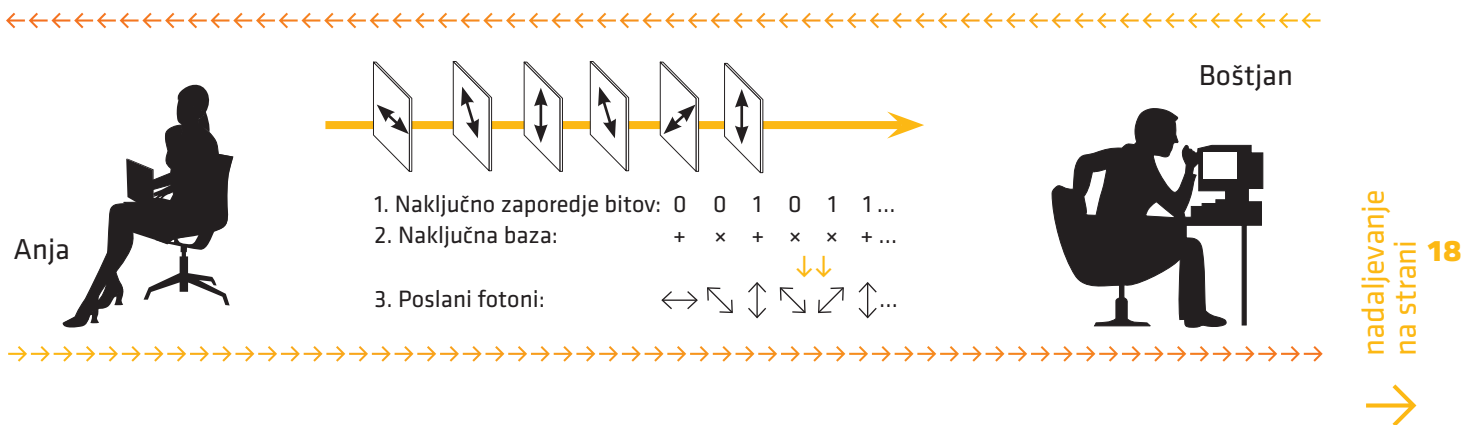
ključa ni dovolj, da pošljamo le vodoravno ali navpično polarizirane fotone. Anja mora pošiljati tudi fotone, ki so polarizirani pod kotom  $45^\circ$  ali  $135^\circ$ . Z drugimi besedami, potrebujemo dve bazi, v katerih bomo pošiljali fotone. Anja bo izbirala med navpično bazo, to bomo označili na kratko s + in bo pomenila fotone z navpično ali vodoravno polarizacijo, in diagonalno bazo, na kratko  $\times$ , ki bo pomenila fotone polarizirane v diagonalni smeri pod kotom  $45^\circ$  ali  $135^\circ$  (glej sliko 1). Izbira, katero bazo bo Anja uporabila za posamezni foton, mora biti naključna. Na drugi strani optičnega vlakna mora Boštjan te fotone detektirati, ter, če hoče ugotoviti ali dani foton predstavlja stanje 0 ali 1, tudi ugotoviti, v kateri smeri so ti fotoni polarizirani. Polarizacijo fotona ugotovimo na enostaven način. Če je Anja poslala foton v + bazi, potem Boštjan ta foton enostavno pošlje skozi polarizator, ki prepušča le svetlobo polarizirano v navpični smeri. Če je polarizator foton prepustil, potem je bila polarizacije fotona navpična, torej 1, sicer pa 0. Podobna zgodba je tudi v primeru, da Anja uporabi  $\times$  bazo, Boštjan pa ima polarizator obrnjen v diagonalni smeri. Zanimivo vprašanje pa je, kaj se zgodi, če smer Boštjanovega polarizatorja ni skladna z Anjino izbiro baze, Anja npr. pošlje foton v  $\times$  bazi, Boštjanov polarizator pa je obrnjen v navpični smeri. Kvantni račun pokaže, da bo v tem primeru Boštjan v polovici primerov izmeril 0, v polovici pa 1! Kaj bo izmeril za konkretni foton, ne moremo napovedati, vse, kar vemo, so verjetnosti. Ta nedoločenost je ključna za varnost kvantne izmenjave ključa. Eden izmed bolj znanih kvantnih protokolov za izmenjavo ključa se imenuje BB84, po odkriteljih Brassardu in Bennettu ter letu objave 1984.

## ■ Protokol BB84

Postopek izmenjave ključa poteka v več korakih. Anja pošilja polarizirane fotone Boštjanu, ta pa meri njihovo polarizacijo.

1. Anja ima zaporedje naključnih bitov, ki jih želi poslati Boštjanu.
2. Anja za vsak bit naključno izbere + ali  $\times$  bazo. Izbira, katero bazo uporabi za posamezni foton, je naključna in znana samo njej. Tudi Boštjan ne ve, ali je dani foton poslan v + ali  $\times$  bazi.
3. Glede na vrednost bita in izbrano bazo Anja pošlje ustrezno polariziran foton (slika 2).
4. Ker Boštjan ne ve, v kateri bazi je poslan posamezni foton, lahko le ugiba. Tako za vsak foton naključno izbere bazo, v kateri bo opravil meritev.
5. Boštjan izmeri foton v izbrani bazi.
6. Iz rezultatov meritev dobi Boštjan niz bitov (slika 3). Ker je v polovici primerov izbral bazo, ki ni kompatibilna z Anjino, ta niz ni enak Anjinemu.

**Slika 2.** Anja generira naključni niz bitov. Vsak foton pošlje v naključno izbrani bazi.



# Nagradna križanka



|                                         |                           |                                 |                                                |                       |                                       |                                     |                                                                          |                                               |                                                       |                      |                                                      |                                                                                   |                    |                                               |                            |
|-----------------------------------------|---------------------------|---------------------------------|------------------------------------------------|-----------------------|---------------------------------------|-------------------------------------|--------------------------------------------------------------------------|-----------------------------------------------|-------------------------------------------------------|----------------------|------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------|-----------------------------------------------|----------------------------|
| AVTOR MARKO BOKALIČ                     | NEMŠKI MATE-MATIK (DAVID) | STARO-GRŠKI MATE-MATIK IN FIZIK | PRIMORSKI PRISLOV ALI VEZNIK                   | ISLANDIJA PO ANGLEŠKO | NEKDANJI KITAJSKI DRŽAVNIK (SHAOQI)   | INDIJAN. LJUDSTVO IZ SREDNJE MEHIKE | 7. GRŠKA ERKA AMERIŠKI IGRALEC (RYAN)                                    |                                               |                                                       |                      | LETOVIŠČE NA BRAČU. BOLEZEN, KI JO PRENAŠA MUHA CECE |                                                                                   |                    | KRAJ NA LASTOVU                               |                            |
| IRSKI MATE-MATIK (WILLIAM ROWAN)        |                           |                                 |                                                |                       |                                       |                                     |                                                                          | VPISO-VANJE PODATKOV RIMSKA 50                |                                                       |                      |                                                      |                                                                                   | BRITANSKA KRALJICA | SL. KIPAR (JANEZ) PRIPRAV-LJALNO URLENJE      |                            |
| NE MORE-MO JIH ZAPISATI V OBLIKI ULOMKA |                           |                                 |                                                |                       |                                       | 9                                   |                                                                          |                                               |                                                       |                      |                                                      |                                                                                   |                    |                                               |                            |
| LIDJUA HREN                             |                           |                                 | ŠVIC. MA-TEMATIK (LEONHARD) REKA V SZ. NEMCIJI |                       |                                       |                                     |                                                                          | KRAJ PRI LJUBLJANI<br>POPIŠ ZALOG IN SREDSTEV |                                                       | 1                    |                                                      | PRIVRŽENEC LACA-NOVIH NAZOROV<br>POŠTNO IN LOVSKO TROBILO<br>POD ZA SUŠENJE ZRNJA |                    |                                               |                            |
| MESTO NA OBROBJU JURE V SZ. ŠVICI       |                           |                                 |                                                |                       | PREHITER SRČNI UTRIP                  |                                     |                                                                          |                                               |                                                       |                      |                                                      |                                                                                   |                    |                                               | GRADBENI MATERIAL IZ GLINE |
| IGRALKA THOMPSON                        |                           | 4                               |                                                |                       | DELOVNA VNEMA<br>INFRA-RDEČA SVETLOBA |                                     |                                                                          |                                               | FILOZOF. POJEM<br>NAJVEČJA REKA V MJANMARU            |                      |                                                      |                                                                                   |                    | IME DVEH RIMSKIH VOJSKO-VODIJ                 | MEDNA-RODNA SMUČAR. ZVEZA  |
| SLOVENSKI PEVEC (VILI)                  |                           |                                 |                                                |                       |                                       |                                     | TABLETKA ZA MOŠKO SPOLNO MOČ<br>BILL CLINTON<br>FR. FIZIK IN KEMIČ (GAY) |                                               |                                                       |                      |                                                      |                                                                                   |                    | KROGLA<br>VAS PRI GEOMETR. SREDIŠČU SLOVENIJE |                            |
| TOMAŽ DOMICELJ                          |                           |                                 | NOGO-METAŠ, KI RAD PREIGRAVA                   |                       |                                       |                                     |                                                                          |                                               | LANI UMRLI SL. PREVA-JALEC (JANKO)<br>ZNAK 72. IPRILI | 1. KOOR-DINATA TOČKE |                                                      |                                                                                   |                    |                                               |                            |

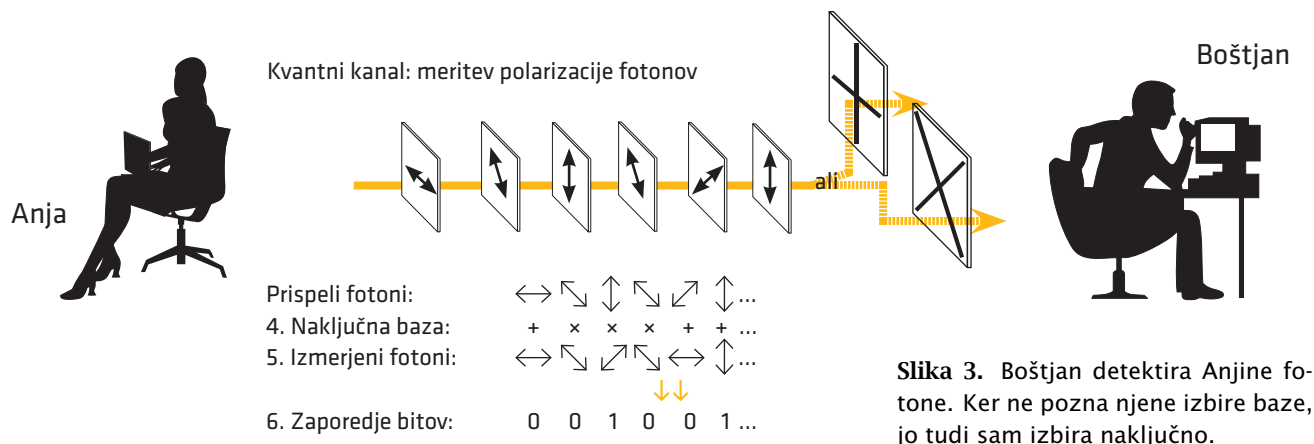


|                                                          |                                              |  |  |   |  |                                                          |                                           |  |  |                                |
|----------------------------------------------------------|----------------------------------------------|--|--|---|--|----------------------------------------------------------|-------------------------------------------|--|--|--------------------------------|
| K                                                        |                                              |  |  | 8 |  | LETALSKI<br>VIJAK,<br>PROPELER                           |                                           |  |  |                                |
|                                                          | BITJE,<br>KI VZBUJA<br>ODPOR<br>ALI<br>STRAH |  |  |   |  | VZOREC,<br>OBLIKA                                        |                                           |  |  | VILIČASTA<br>RIBJKA<br>KOŠČICA |
|                                                          |                                              |  |  |   |  |                                                          | TON MED<br>D IN E                         |  |  |                                |
|                                                          | MUSLI-<br>MANSKO<br>MOŠKO<br>IME             |  |  |   |  | AM. FIZIK,<br>NOBELOVEC<br>2002<br>(RAYMOND)<br>NEZNANEC |                                           |  |  |                                |
|                                                          | HRIBOVJE<br>NA BELG.-<br>FRANC.<br>MEJI      |  |  |   |  |                                                          | SKANDI-<br>NAVSKA<br>DRŽAVA               |  |  |                                |
| MESTO NA<br>VZH. OBALI<br>POLOTOKA<br>YORK V<br>AVSTRAL. |                                              |  |  |   |  |                                                          | GRŠKI<br>FILOZOFOV,<br>PLATONOV<br>TEKMEC |  |  |                                |

|                                                        |                                                        |                                                          |                                                  |                                                                                   |                                              |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
|--------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------|--------------------------------------------------------|--------------------------------------------------------|---------------------------------------------------|----------------------------------------------------------|----------------------------------------------------|--------------------------------------------------------|---------------------------------------|----|------------------------------------------------------------------------------------|---------------------------------------------|---------------------------------------|------------------|
| ZMAGA<br>PRI JUDU<br>Z METOM<br>TEKMECA<br>NA HRBET    | RUSKI<br>FIZIK<br>GINZBURG<br>NOBELOVEC<br>2003        | JAPONSKO<br>MESTO,<br>ZNANO PO<br>"OKOLJSK-<br>SPORAZUMU | UMRLI<br>FILMSKI<br>PRODU-<br>CENT<br>SPELLING   |  |                                              |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        |                                       |    |  |                                             |                                       |                  |
| 5                                                      |                                                        |                                                          |                                                  |                                                                                   |                                              |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
| PLAČILO,<br>NAGRADA<br>TRAVNA<br>PLANJAVA<br>(SPANSKO) |                                                        |                                                          |                                                  |                                                                                   |                                              |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
|                                                        |                                                        | POSODICA<br>ZA IZDELA-<br>VO FORME<br>ZOBNIH<br>PROTEZ   | PALMA IZ<br>JV. AZIJE<br>Z<br>UŽITNIMI<br>SEMENI | TELE-<br>VIZIJA                                                                   |                                              |                                                        | ROPARSKA<br>POVODNA<br>KUNA                            | ZAKON<br>O DOPOL-<br>NITVAH<br>VELJAVN.<br>ZAKONA | SLIKANJE<br>ZVOČNIH<br>POJAVOV<br>Z JEZIKOV,<br>SREDSTVI | HENRY                                              | ROSVITA<br>PESEK                                       | DRŽAVA<br>V JUGO-<br>ZAHODNI<br>AZIJI |    |                                                                                    |                                             |                                       |                  |
|                                                        |                                                        |                                                          |                                                  | SLOVENSKI<br>IGRALEC<br>(PAVLE)<br>MEHIŠKO<br>LETOVIŠČE                           |                                              |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        |                                       |    | RAZELEK-<br>TRENJE<br>V PLINIH<br>OZRAČJA                                          | VELETOK<br>V IRAKU,<br>SOTOČNICA<br>EVFRATA | KOVINSKI<br>DELI<br>OHIŠJA<br>NAPRAVE | ZNAK<br>ZA RADIJ |
|                                                        | MESTO<br>NA KRETI<br>ODRSKO<br>GLASBENO<br>DELO        |                                                          |                                                  |                                                                                   |                                              |                                                        |                                                        |                                                   | 6                                                        | VEČDIMEN-<br>ZIONALNA<br>TVORBA<br>?,<br>DIE, DAS  |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
|                                                        |                                                        |                                                          |                                                  |                                                                                   | DIFE-<br>RENČNI<br>KOLIČNIK                  |                                                        |                                                        |                                                   |                                                          |                                                    | GRŠKO-<br>RIMSKO<br>UMETNO-<br>STNO<br>OBDOBJE         |                                       |    |                                                                                    |                                             |                                       |                  |
|                                                        |                                                        |                                                          | 7                                                | DOMENA<br>METEO-<br>ROLOGOV<br>AVANS,<br>NAPLAČILO                                |                                              |                                                        |                                                        |                                                   |                                                          |                                                    | LADJSKI<br>ALI LETAL<br>TOVOR<br>KOŠARKAR<br>DELIBAŠIČ |                                       |    |                                                                                    |                                             | PLAVALCA<br>CROCKER<br>IN<br>THORPE   |                  |
| DEL<br>DIRKE<br>EVROPSKA<br>VESOLJSKA<br>AGENCIJA      |                                                        |                                                          |                                                  |                                                                                   |                                              | ZVOČNI<br>ZNAK ZA<br>NEVARNOST<br>BIVALNI<br>AVTOMOBIL |                                                        |                                                   |                                                          |                                                    | ITAL.<br>IGRALEC<br>(GINO)<br>ZNAK ZA<br>TANTAL        |                                       | 10 |                                                                                    |                                             |                                       |                  |
|                                                        |                                                        |                                                          |                                                  | ČASO-<br>MERILNA<br>NAPRAVA<br>DEKLICE                                            |                                              |                                                        | ZNAK<br>ZA ASTAT<br>ON PO<br>NEMŠKO                    |                                                   |                                                          | NAŠA<br>ZAHODNA<br>SOSEDA<br>GL. MESTO<br>KOLORADA |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
|                                                        |                                                        | HIDRO-<br>CENTRALA<br>NA SOČI<br>PREDSTOJ.<br>KAPITLJA   |                                                  |                                                                                   |                                              |                                                        |                                                        | POLJSKO-<br>NEMŠKA<br>REKA<br>FIZIK<br>MOLJK      |                                                          |                                                    |                                                        |                                       |    | ZAČETNIK<br>BOLGAR.<br>DINASTIJE<br>KONEC<br>12. STOL.                             |                                             |                                       |                  |
|                                                        | SL. ROKO-<br>METAŠ<br>(IZTOK)<br>TELOVADNO<br>OBLAČILO |                                                          |                                                  |                                                                                   | VRSTA<br>ŠTIRI-<br>KOTNIKA<br>VOLT-<br>AMPER |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
| KRAJ OB<br>DOLENJSKI<br>AVTOCESTI<br>PRI<br>KRŠKEM     |                                                        |                                                          |                                                  |                                                                                   |                                              |                                                        | 9. GLASB.<br>INTERVAL<br>SREDINA<br>RIMSKEGA<br>MESECA |                                                   |                                                          |                                                    |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
| DRŽAJ<br>RIMSKA 6                                      |                                                        |                                                          |                                                  | KEMIČNI<br>DODATEK<br>IZDELKU<br>ALFRED<br>NOBEL                                  |                                              |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        | OZNAKA<br>HRVAŠ.<br>MESTA<br>KUTINA   |    |                                                                                    |                                             |                                       |                  |
| 12                                                     |                                                        |                                                          |                                                  |                                                                                   | MLAD<br>PRAŠIČEK                             |                                                        |                                                        |                                                   |                                                          | 11                                                 |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |
|                                                        |                                                        |                                                          |                                                  |                                                                                   | SLOVENSKI<br>PESNIK<br>(JANEZ)               |                                                        |                                                        |                                                   |                                                          |                                                    |                                                        |                                       |    |                                                                                    |                                             |                                       |                  |

## NAGRADNI RAZPIS

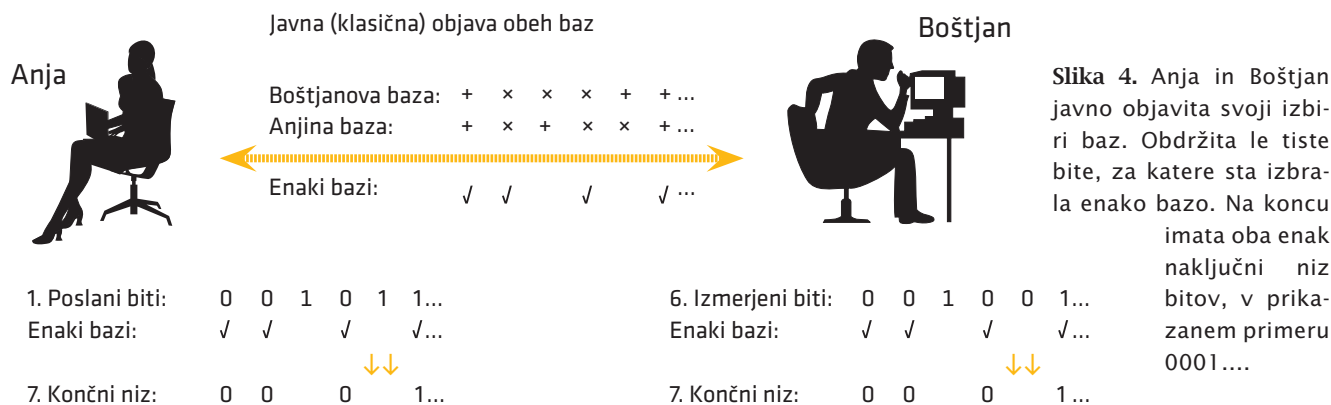
➔ Črke iz označenih polj po vrsti zapišite na Preseku priloženo dopisnico, dodajte tudi svoje ime, priimek in naslov. Dopisnice pošljite na Presekov naslov (poština je že plačana) do 15. junija 2007, ko bomo izžrebali pet nagrajencev, ki bodo prejeli **Presekovo majico** (na dopisnici označite želeno velikost, M, L, XL). ✕



7. Anja in Boštjan po javnem kanalu, npr. telefonu, objavita, v katerih bazah sta pošiljala oz. detektirala fotone. Nato oba obdržita le tiste bite, za katere sta izbrala enako bazo (slika 4).

Ker je v polovici primerov Boštjanova izbira baze napačna, je dobljeni niz bitov krajši kot pa začetni Anjin. V povprečju bo pol krajši. Če bi Anja in Boštjan primerjala svoja niza bitov, preden sta zavržla neskladne, bi ugotovila, da se razlikujeta v 25% primerov (v polovici napačnih izbir baz). Kako je z varnostjo? Recimo, da je pošiljanju fotonov prisluškovala Eva. Njena strategija je, da pomeri vse Anjine fotone in nato Boštjanu pošlje foton v stanju, kot ga je izmerila. Ker tudi Eva ne pozna Anjine izbire baze, tudi sama le-to izbira naključno. V po-

lovici primerov bo pravilna, v polovici pa ne. Verjetnost, da bo Boštjan izmeril enako vrednost bita, kot ga je poslala Anja, je sedaj enaka 62,5% (ko Eva izbere kompatibilno bazo, je ta verjetnost 75%, sicer pa 50%). Končna Anjina in Boštjanova niza se bosta torej v primeru Evinega prisluškovanja razlikovala v 37,5% bitov. Verjetnost za različne bite se je ob prisluškovanju povečala iz 25% na 37,5%. To povečanje napak pa lahko Anja in Boštjan zaznata in temu ustrezno ukrepata. Dejstvo je, da Eva ne more prisluškovati, ne da bi jo pri tem odkrili. Kvantna mehanika namreč pravi, da bodo Evin meritve spremenile stanja fotonov in tako vnesle dodatne napake, ki jih lahko zaznamo. Po koncu celotnega kvantnega protokola imata Anja in Boštjan niz naključnih bitov, ki





so znani samo njima in ki potem služijo za Vernamovo šifriranje.

## ■ Tehnologija

Kvantna kriptografija, za razliko od kvantnih računalnikov in kvantne teleportacije, ni samo domena laboratorijskih poskusov, temveč je že komercialno dostopna. Pred nekaj leti je podjetje idQuantique iz Ženeve ponudilo prvi plug&play sistem za kvantno izmenjavo ključev. Podobne izdelke ponuja tudi ameriški MagicQ, svoje pa razvija tudi NEC. Vsi ti sistemi delujejo na principu pošiljanja fotonov po optičnih vlaknih. Za sedaj so razdalje, na katerih delujejo, omejene pod 100 km. Da zagotovimo 100% varnost, morajo biti izpolnjeni določeni tehnični pogoji, ki potem omejujejo razdaljo, na kateri zadeva še deluje. Problem je v neidealnih polarizatorjih, izkoristku merilcev fotonov, absorpciji svetlobe v optičnih vlaknih. Polprevodniški detektorji fotonov so danes sposobni detektirati posamezni foton z nekaj 10% učinkovitostjo, poleg tega imajo tudi lastni šum, kar pomeni, da včasih zaznajo foton, ko le-tega sploh ni bilo. Pulzi svetlobe, ki jih pošiljamo po optičnih vlaknih, morajo biti zelo šibki. V posameznem pulzu namreč ne sme biti več kot le en foton. Če bi imeli v pulzu dva fotona, bi lahko Eva enega pomečila, drugega pa nemotenega poslala naprej Boštjanu. V tem primeru Evinega prisluškovanja ne bi mogli odkriti. Ker je v uporabljenih pulzih le en samcat foton, se le-ta slej ko prej absorbira v optičnem vlaknu. Vse te težave skupaj nam omejijo končni doseg na okoli 100 km. ☒



Slika 5. Komercialni sistem za kvantno kriptografijo Vectis podjetja IdQuantique.

# Kdaj nas pri plavanju (ne) zebe?

MITJA ROSINA

➔ Če je okolica zelo hladna, toplota hitro prehaja od nas na okolico in nas zebe. Najprej zaznamo ohladitev na koži (čutnice v koži), potem pa se začne mraz v globino, saj se kri, ki je nekoliko ogrela površino, vrača ohlajena proti notranjim organom.

Če smo dovolj oblečeni, pa nas ne zebe, saj telo kuri hrano, da vzdržuje delovanje organov in mišic (*osnovni metabolizem*); pri tem se sprošča toplota. To toploto je treba odvesti, ustrezna temperaturna razlika med telesom in okolico pa je dobrodošla. Oblečemo se torej toliko, da temperaturna razlika poganja ravno pravišen toplotni tok.

Še večjo temperaturno razliko pa zdržimo, če se gibljemo in opravljamo delo. Mehanski izkoristek energije, ki jo daje hrana, je namreč le kakih 25%, medtem ko gre 75% v toploto.

Na mehanski izkoristek vpliva dvoje. Najprej potrebujemo banke (*mitohondrije*), ki zamenjajo bankovce (energijo vskladiščeno v molekuli *sladkorja*) v drobiž (molekule *adezin-trifosfata* (ATP)). Bankovec bi bil prevelik zalogaj, kovanci ATP pa so ravno pravišnji za posamezne živčne in mišične sunke. Ena molekula sladkorja nabije do 40 molekul adezin-difosfata (ADP) v energijsko bogatejši ATP (kemijsko formulo za ADP in ATP najdeš npr. na naslovu <http://sl.wikipedia.org/wiki/Nukleotid>). Za živčni ali mišični impulz pa se ta energija sprosti s kemično



→ reakcijo  $ATP \rightarrow ADP + \text{še kaj}$ . Toda banka vzame 50% provizije, pol energije molekule sladkorja gre v toploto in le pol v nabijanje  $ADP \rightarrow ATP$ . Toda veseli bodimo, da banko (mitochondrije) sploh imamo.

Za še manjši mehanski izkoristek pa je kriv tudi način krčenja mišičnih vlaken. Mišice izkoristijo za opravljanje dela le polovico energije, ki jo nudi ATP. Skupni izkoristek je torej  $pol \times pol = \text{četrť}$ . Tudi tu se ne gre pritoževati. Odpadna toplota nas greje!

Zanimivo je, zakaj ni evolucija preskrbela v telesu pečice, ki bi nas grela, ko nas zebe in se nam ne ljubi delati. Kar sedli bi, kurili sladkor in bi nam bilo toplo. Toda gorje, ko bi pokurili vso zalogo sladkorja v telesu! Narava nas torej prisili, da v mrazu nekaj ukrenemo, da gremo na toplo ali da si preskrbimo kurjavo in hrano.

V vodi so toplotne izgube pri dani temperaturni razliki večje kot na zraku, ker je voda boljši prevodnik toplote od zraka, in ker pri kopanju nismo oblečeni. V topli vodi lenarimo, v hladni pa moramo zelo intenzivno plavati. Zanimive so osebne izkušnje, pri kateri temperaturi lenarimo, pri kateri plavamo počasi, hitro, divje. Za ilustracijo bomo obdelali zgled iz svojih osebnih izkušenj. Pri zgledu bomo priredili vrednosti količin za nekoga s telesno maso 66 kg (namesto mojih 79 kg).

Če mirujemo, porabimo za osnovni metabolizem dober watt na kg telesne mase. Vrednost je odvisna od telesne mase, višine, starosti in spola. Rezultate empirične formule najdete zase na medmrežju (recimo <http://www.room42.com/nutrition/basalphp4>, ali pa poiščite z Googlom “basal metabolism calculator”). Ker se v vodi vedno nekoliko gibljemo, bomo za oceno zaokrožili predlagano vrednost (moški 66 kg, 180 cm, 18 let) na 100 W.

Intenzivnost plavanja smo ocenili po občutku s primerjavo z močjo pri hoji v hrib. Te ni težko izračunati, če vemo, kako hitro se dvigamo. Pri planinskem koraku se dvigamo 360 m/h (0,1 m/s). Pol tega, 180 m/h, je sprehod, dvojna hitrost 720 m/h (0,2 m/s) pa je že zelo naporna, trojno zmoremo le zelo kratek čas, ali pa če smo trenirani športniki. V tabeli navajamo rezultate svojih opazovanj. Naj poudarimo, da se rezultati za različne osebe lahko precej razlikujejo, odvisni pa so tudi od tega, kako močno nas še dodatno greje sonce.

Za mehansko moč plavanja  $P$  v wattih uporabimo za primerjavo moč pri vzponu v hrib ( $P_{vzpon} = mgv_z$ ,  $m = 66$  kg) in navajamo hitrost vzpona  $v_z$ .

Za toplotni tok ( $\dot{Q} = \dot{Q}_{plavanje} + \dot{Q}_0$ ) pa vzamemo trikratno mehansko moč ( $\dot{Q}_{plavanje} = 3P$ ) in prištejemo toplotni tok  $\dot{Q}_0 = 100$  W zaradi osnovnega metabolizma. Telesno temperaturo smo zaokrožili na  $T_0 = 36^\circ\text{C}$ . V tabeli podajamo temperaturo vode  $T$  in temperaturno razliko  $\Delta T = T_0 - T$ . Zvezo med toplotnim tokom in temperaturno razliko smo zaokrožili na linearno funkcijo, čeprav to ni čisto res. Za grobo oceno pa je najbrž dovolj dobro. Tabela torej pove, kako intenzivno moramo plavati, da nas ne zebe, niti nam ni prevroče.

Ne pozabite, navedena hitrost  $v_z$  ni hitrost plavanja, temveč primerjalna hitrost, kako hitro bi morali za isti napor hoditi v hrib. Iz hitrosti plavanja bi bilo namreč dosti težje izračunati moč. Moč pri raznih športih merijo tako, da nataknejo športniku masko in merijo porabo kisika; iz tega je mogoče sklepati na porabo sladkorja ter s tem na porabo energije. V našem primeru naj zadošča le ocena moči.

Opazujte se še vi in pri tem izmerite temperaturo vode in ocenite intenzivnost plavanja! ☘

| $P$ [W] | $v_z$ [m/s] | $\dot{Q}$ [W] | $T$ [ $^\circ\text{C}$ ] | $\Delta T$ [ $^\circ\text{C}$ ] | intenzivnost plavanja |
|---------|-------------|---------------|--------------------------|---------------------------------|-----------------------|
| 0       | 0           | 100           | 33 $^\circ$              | 3 $^\circ$                      | namakanje             |
| 33      | 0,05        | 200           | 30 $^\circ$              | 6 $^\circ$                      | zelo lagodno          |
| 66      | 0,1         | 300           | 27 $^\circ$              | 9 $^\circ$                      | lagodno               |
| 99      | 0,15        | 400           | 24 $^\circ$              | 12 $^\circ$                     | naporno               |
| 132     | 0,2         | 500           | 21 $^\circ$              | 15 $^\circ$                     | zelo naporno          |
| 165     | 0,25        | 600           | 18 $^\circ$              | 18 $^\circ$                     | le kratek čas         |

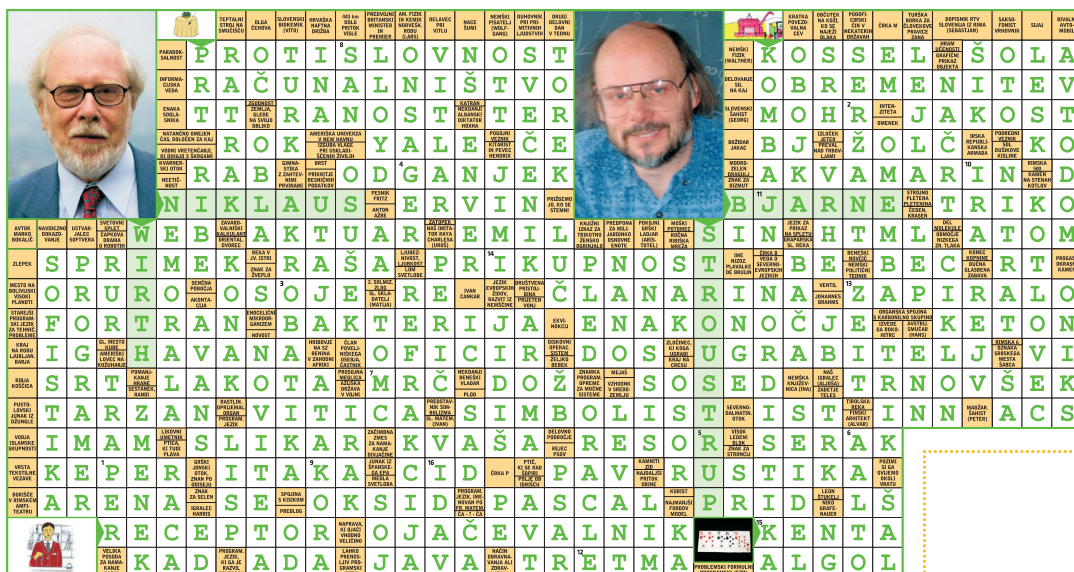
## MARIJA VENCELI

Posamezno črko morate zamenjati z isto desetiško števkco, ne glede na to, v katerem od obeh računov se nahaja. Različne črke pomenijo različne številke in, kot je pri kriptaritmi v navadi, nobeno od nastopajočih števil se ne začneja z nič. Po zamenjavi vseh črk s števkami morate dobiti pravilna računa seštevanja.

Rešitve naloge pošljite najkasnje do petka, 29. junija 2007, na naš naslov:

DMFA - založništvo, Presek, p.p.2964, 1001 Ljubljana

Izmed reševalcev, ki **bodo poslali pravilno rešitev in na kratko opisali tudi premislek, s katerim so do rešitve prišli**, bomo izžrebali tri nagrajence, ki bodo za nagrado prejeli enoletno naročnino na Presek. ❌



REŠITEV  
NAGRADNE  
KRIŽANKE  
PRESEK 34/5

➤ Za nagradno križanko iz prejšnje številke smo prejeli 14 pravih rešitev. Nagradno geslo se je glasilo **Programski jezi-ki**. Izžrebani reševalci, MARJAN GRILJ iz Domžal, EVA LORENČIČ iz Pesnice pri Mariboru in MARIJA MARC iz Ajdovščine so razpisane nagrade prejeli po pošti. ❌

# Kartezijev plavač

## ODGOVOR NALOGE

MOJCA ČEPIČ



☉ Verjetno z izdelavo Kartezijevega plavača niste imeli težav. Če je bil obtežen tako, da je komaj kupal iz vode, potem je gotovo deloval. Ali je bil videti nekako takole kot moj na sliki?

Če ste se s plavačem igrali in med igranjem še igranje odgovorili na vprašanja zastavljena v poizkuševalnici, bi verjetno radi tudi vedeli, zakaj tako. Verjetno ste nekatere odgovore našli že sami, a vseeno, poskusimo dogajanja razložiti po vrsti.

Kaj se zgodi s plavačem, če plastenko stisneš? Kaj se zgodi s plavačem, če plastenko spet spustiš?

Ob stisku plastenke plavač potone, ko stisk popusti, se spet dvigne. V plavaču je namreč ujet zrak. Ko plastenko stisnemo, se tlak v plastenki poveča in stisne zrak v plavaču. Vanj vdre nekoliko vode iz okolice. Če obravnavamo plavač kot sestavljeno telo iz slamice, sponk, zraka in vode v slamici, se njegova teža poveča, prostornina pa ne. Zato se poveča tudi povprečna gostota plavača. Ko postane večja od vode, plavač potone. Njegova gostota je bila že pred vdorom vode skoraj enaka kot voda, saj je bil načrtno narejen tako, da je le majhen delež plavača gledal iz vode. Bil je "slab plavalec". Ni se bilo potrebno pretirano truditi, da bi ga s stiskanjem potopili.

Podobno, ko stisk popusti, se tlak v plastenki zmanjša, zrak v plavaču se zopet raztegne, izrine nekaj vode iz slamice in povprečna gostota plavača postane manjša od vode. Plavač se ponovno dvigne pod zamašek.

Ali lahko potopiš plavača, če plastenko stisneš na spodnjem delu? Ali je stisk plastenke odvisen od mesta, kjer plastenko stisneš?

Za preizkuševalca je morda zanimivo, da plavač potone, tudi če steklenico stisnemo na dnu. Vsakdanje izkušnje nam namreč pravijo, da bi moral še

trdneje ostati v gornjem delu plastenke, saj naj bi ga tja "potisnili" z vodo vred. Pa ni tako. Pascal je pokazal, da so mirujoče tekočine čudna zadeva. Če na enem mestu povečamo tlak, se tlak enako poveča povsod po mirujoči tekočini. Tako lahko s stiskanjem plastenke na kateremkoli mestu dosežemo povečanje tlaka in plavač potone.

Kaj pa občutki v roki? Ali je lažje stisniti plastenko spodaj ali zgoraj, na ožjem ali širšem delu? Iz področja fizike zahajamo na področje fiziologije. Platenka je majhna, zato ne moremo pričakovati velikih razlik med gornjim in spodnjim delom plastenke. A vendar je marsikomu z majhno roko lažje stisniti plastenko v ožjem delu. Kot smo omenili že prej, učinek je enak.

Ali lahko obdržiš plavača na neki vnaprej izbrani globini dalj časa? Kakšni so tvoji občutki, medtem ko plavač lebdi v sredini plastenke?

Kdor se je poskušal s to nalogo, je ugotovil, da plavača sicer lahko obdržimo na poljubni globini, a ga je ves čas treba aktivno nadzirati. Z aktivnim nadzorom mislimo na povečevanje stiska, kadar plavač uhaja navzgor, in na popuščanje stiska, kadar plavač uhaja navzdol. Zakaj tako? Plavač, ki lebdi na sredini plastenke, je v labilni legi. To sicer pomeni, da sta vzgon in teža plavača izenačena, a vsaka najmanjša motnja oz. tresljaj premakne plavača nekoliko iz lebeče lege. Če se plavač premakne navzgor, se zrak nekoliko razpne, izrine malo vode iz slamice in vzgon postane večji od teže. Plavač se dviguje k višjim legam, zrak se vedno bolj razpenja in neravnovesje postaja vedno večje, dokler ne zadene v zamašek plastenke. Podobno se zgodi, če se plavač nekoliko potopi. Tedaj se zrak v slamici nekoliko dodatno stisne, voda dodatno napolni slamico in teža plavača postane večja od



vzgon. Plavač tone, opisano neravnovesje narašča, dokler se plavač ne opre ob dno posode.

Še nekaj besed o plavaču za poznavalce. Namesto navadne vode je pol plastenke napolnjene s slano raztopino, ki ima večjo gostoto kot neslana voda. Če plastenke ne stresamo, ostane slana voda na dnu zelo dolgo. Sedaj s stiskom (običajno) plavača ne moremo več potopiti do dna. Še več, pri stiskanju plastenke oz. povečevanju tlaka v plastenki se umiri v bližini meje med slano in neslano vodo. S povečevanjem tlaka lahko poskušamo plavača potisniti nekoliko globlje, a do dna ga potisnejo le silaki. Plavača tudi ni potrebno nadzirati. Ob stisku se v določeni globini umiri sam od sebe. Zakaj tako?

Od dna plastenke navzgor se gostota vode zvezno zmanjšuje. Plavač, ki ga s povečevanjem tlaka poskušamo potopiti, tako prehaja iz področja manjše gostote v področje večje gostote. Izpodrinjena voda ima zato vedno večjo težo in vzgon na plavač narašča. Zato moramo povečevati stisk (tlak v plastenki), da se povečuje tudi povprečna gostota plavača. Kljub majhnim razlikam v gostoti, so za ustrezne spremembe povprečne gostote plavača potrebne precej velike sile. Tudi plavačeva lega v bližini ne ravno ostre meje med slano in neslano vodo ni več labilna, temveč stabilna. Če stisk nekoliko popustimo, se plavač premakne v področje manjše gostote, če stisk povečamo, pa v področje večje gostote.

Upam, da vam je bilo igranje s plavačem všeč. Ker se bliža poletje, naj povem še to. Kartezijev plavač pogosto omenjajo kot model rib, ki imajo mehur. Ribji mehur je kožna vrečka, napolnjena s plinom (ni nujno enake sestave kot zrak), ki pri mnogih kostnicah leži tik pod hrbtenico. Kadar boste na morju čistili ribe, si tega ne pozabite ogledati. Ribji mehur pomaga ribi pri spuščanju in dvigovanju. Če se riba namerava dvigniti, mehur nekoliko bolj napolni s plinom, da se njegova prostornina poveča in se povprečna gostota ribe zmanjša. Riba se začne brez truda dvigovati. A dvig mora skrbno nadzirati, saj bi se prostornina mehurja lahko zaradi manjšega tlaka v manjših globinah preveč povečala. Ko doseže željeno globino, ponovno zmanjša prostornino mehurja. Zato da ostane v isti globini, mora ves čas aktivno plavati, saj bi jo, podobno kot lebdečega plavača brez nadzora, lahko odneslo navzgor ali navzdol. Podobno se riba tudi spušča; zmanjša prostornino mehurja, potone do zelene globine, nato pa mehur spet napolni do prostornine, ki izenačuje vzgon in težo. ☒



# Odkrivanje planetov s spektroskopskim merjenjem radialne hitrosti zvezd

NIKOLAJ ŠTRITOF

☉ Ponavadi pozabljamo, da poleg planetov tudi Sonce kroži okoli skupnega težišča vseh teles v Osončju. Največji vpliv na Sončevo kroženje ima Jupiter, ki je planet z največjo maso. Morebitni opazovalci pri drugih zvezdah, ki bi orbito Jupitra videli s strani, bi lahko izmerili, kako se Sonce giblje v smeri proti in stran od nas. To je tako imenovana sprememba radialne hitrosti in se pri Soncu spreminja z amplitudo  $K = 12,5 \text{ m/s}$  in s periodo  $P = 11,9$  let. Prvi eksoplanet 51 Pegaza b (51 Peg b) so odkrili prav z metodo merjenja radialne hitrosti.

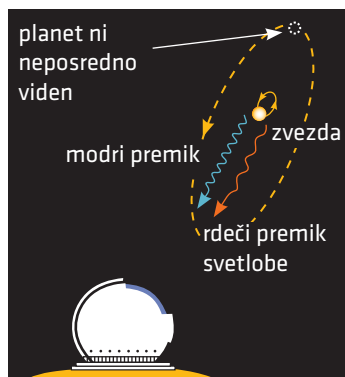
Podobno kot Sonce tudi druge zvezde opletajo okoli skupnega težišča s planeti. Spremembe radialne hitrosti zvezd se kažejo v Dopplerjevem pojavu pri spektralnih črtah v njihovi svetlobi, kar je mogoče meriti s spektroskopi (glej okvirček). Na ta način so poskušali najti planete pri drugih zvezdah že v sedemdesetih letih preteklega stoletja, vendar so bili spektroskopi premalo občutljivi, natančni in obdelava prezahtevna. V osemdesetih so začeli iskati rjave pritlikavke, to so majcene zvezde, z masami med 1,3% in 8% Sončeve mase, ki imajo premajhno temperaturo v sredici, da bi se v njih zlival vodik. Za planetne sisteme so astronomi takrat mislili, da so močno podobni našemu Osončju, da so veliki planeti daleč od zvezd, kar je bil glavni vzrok, da je bilo iskanje planetov in rjavih pritlikavk takrat neuspešno.

Švicarja Michel Mayor in Didier Queloz sta v začetku devetdesetih let prejšnjega stoletja sodelovala pri švicarsko-francoskem spektroskopskem projektu Elodie na observatoriju Haute-Provence. Sprejela sta izziv iskanja rjavih pritlikavk, saj sta se že prej izu-

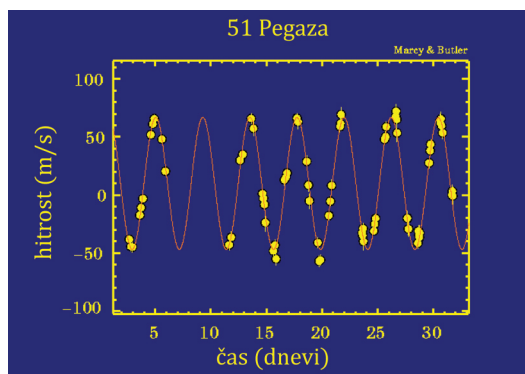
rila pri odkrivanju dvozvezdij z večjimi masami. Mayor in Queloz sta radialno hitrost zvezd merila z natančnostjo 20 – 30 m/s in sproti obdelovala podatke. Tako je Queloz konec 1994 opazil, da se zvezdi 51 Peg, ki sta jo namenila za testiranje, že v eni noči spreminja radialna hitrost. Vendar sta kmalu morala prenehati z opazovanji, saj ozvezdje Pegaz pozimi ni vidno. Morala sta počakati do februarja 1995, ko sta lahko določila periodo  $P = 4,23$  dni. Do avgusta sta zbrala dovolj podatkov, da sta lahko potrdila odkritje prvega eksoplaneta. Na objavo rezultatov sta morala čakati do novembra 1995, ker ju je k temu zavezoval dogovor s prestižno znanstveno revijo Nature. Toda v astronomski srenji se je o odkritju že šušljalo in na veliko komentiralo, saj je bil to izjemen dosežek.

Zvezda 51 Peg je podobna Soncu, okoli nje kroži na oddaljenosti  $a = 0,052$  astronomske enote (7,8 milijona kilometrov) planet z maso 0,47 mase Jupitra, temperatura na njem je 1200 stopinj Celzija. Nenavadna bližina masivnega planeta pri zvezdi je bila ob odkritju veliko presenečenje. Temu tipu planetov danes pravimo *vroči jupitri*. Kmalu so sledila še druga odkritja planetov na različnih oddaljenostih od materinske zvezde. Sedaj je znanih 216 planetov (april 2007), od tega so jih kar 204 odkrili s spektroskopsko metodo merjenja radialnih hitrosti. Astronomi so odkrili tudi več planetov v okolici ene zvezde, v dveh sistemih celo štiri planete.

Ta bogata bera planetov pa je prinesla še eno skrivnost, odkrili so zelo malo rjavih pritlikavk. Pričakovali bi, da jih je vsaj toliko kot planetov ali masivnejših zvezd s periodami od nekaj dni do nekaj let



Slika 1. Zvezda zaradi prisotnosti planeta kroži okoli skupnega težišča. Posledica tega gibanja je Dopplerjev premik v svetlobi zvezde. Ko se ta giblje proti opazovalcu na Zemlji, pride do modrega premika, ko se giblje stran pa do rdečega premika (ilustracija: George Mason Uni).



Slika 2. Prvi planet zunaj Osončja (51 Pegaza b) so astronomi odkrili z meritvami radialne hitrosti zvezde. Periodične spremembe hitrosti zvezde proti in stran od opazovalca kažejo na prisotnost sicer nevidnega spremljevalca. S to metodo je planetu mogoče določiti periodo, ekscentričnost orbite in spodnjo mejo za maso (ilustracija: Marcy in Butler).

okoli materske zvezde. Pa so jih odkrili le prgišče. To pomanjkanje so poimenovali “puščava rjavih pritlikavk”. Na večjih oddaljenostih, periode več desetletij ali stoletij, pa so jih odkrili kar nekaj.

Sedaj odkrijejo od 20 do 30 tujih planetov na leto. Odkrili so zelo masivne orjake z velikostjo 10 Jupitrovih mas, ki so na meji z rjavimi pritlikavkami, in tudi že zelo majhne planete, ki imajo približno 10 mas Zemlje, nekakšnih tujih neptunih. Astronomi upajo, da bodo že v bližnji prihodnosti s spektroskopsko radialno metodo zaznali superzemlje, ki imajo maso od 2 do 4 mase Zemlje. Nekoč pa naj bi zaznali še manjše objekte, podobne našemu domačemu planetu. ☒

Če okoli zvezde kroži planet, potem tudi zvezda kroži okoli težišča zvezda – planet. Hitrost gibanja zvezde astronomi merijo s pomočjo Dopplerjevega pojava. V astronomiji je pojav, ki ga je odkril Christian Doppler (1803–1853), izredno pomembno orodje za ugotavljanje narave objektov v vesolju. V vsakdanjem življenju ga vsi poznamo, ko poslušamo sireno rešilnega avtomobila. Ko se nam ta približuje, je njen ton višji kot takrat, ko se oddaljuje. Enako kot za zvočila velja za svetlobne izvire. Spektralne črte v svetlobi zvezd, ki se nam približujejo, so premaknjene proti krajšim valovnim dolžinam oz. višjim frekvencam – modri premik. Če se oddaljujejo, so črte premaknjene proti daljšim valovnim dolžinam oz. nižjim frekvencam – rdeči premik. Velikost tega premika je odvisna od hitrosti in ga opisuje enačba

$$\Delta\lambda/\lambda = v/c,$$

$\Delta\lambda$  je sprememba valovne dolžine,  $\lambda$  je valovna dolžina mirujočega svetila,  $v$  je hitrost svetila in  $c$  je svetlobna hitrost. Tako izmerjeni hitrosti  $v$  zvezde rečemo radialna hitrost, saj na spremembo valovne dolžine vpliva le komponenta hitrosti v radialni smeri, torej v smeri opazovalec-svetilo.

Sam Doppler je menil, da so zvezde različnih barv, od modrih do rdečih, ker se ene gibljejo z veliko hitrostjo – nekaj 10% svetlobne hitrosti proti nam, druge stran od nas. Danes vemo, da so tipične hitrosti zvezd v Sončevi okolici od 10 km/s do 40 km/s premajhne v primerjavi s svetlobno hitrostjo, da bi to prispevalo k spremembi njihove barve.

Kroženje zvezde okoli težišča je torej mogoče zaznati v majhnih premikih spektralnih črt. Za meritve tako majhnih sprememb je potreben izredno natančen spektroskop, ki more izmeriti spremembo valovne dolžine za vsega 0,003% ali manj. Žal pa mase planetov odkritih z metodo radialne hitrosti astronomi ne morejo natančno določiti. Z njo namreč merijo spreminjanje hitrosti samo v smeri gledanja (glej sliko 2), kar pa je le komponenta celotne hitrosti, ki je odvisna od nagiba orbite planeta glede na smer opazovanja. Nagib pa s to metodo ni neposredno merljiv in ga je v nekaterih primerih mogoče izmeriti z drugimi astronomskimi metodami.

# Izmerimo svetlobno onesnaženje v svojem kraju

ANDREJ GUŠTIN

➤ Pri nas je problematika svetlobnega onesnaženja slabo znana, zato smo jo letos nekoliko obširneje predstavili tudi v Preseku, med drugim tudi z vajo merjenja mejne vizualne magnitude zvezd v Orionu (*Presek*, 34, št. 2). Na naš poziv sta se odzvali dve skupini s po štirimi opazovalci, in sicer iz Šolskega centra Postojna in Gimnazije Ptuj. Medtem pa drugod po svetu že dalj časa poteka ozaveščanje in izobraževanje o svetlobnem onesnaževanju. Med take aktivnosti sodi tudi mednarodna šolska akcija *GLOBE at Night*, v okviru katere slovenski predstavniki žal ne nastopajo organizirano.

GLOBE at Night poteka v okviru mednarodnega izobraževalnega in znanstvenega programa GLOBE (Global Learning and Observations to Benefit the Environment), ki sta ga ustanovila NASA in ameriški NSF (National Science Foundation), podpirajo pa ga ameriška vlada, nekatere univerze in inštituti. GLOBE je namenjen osnovnošolski in srednješolski mladini ter ima za cilj spoznavanje znanstvenih metod. Med drugim se učenci naučijo zbirati znanstveno relevantne podatke o ozračju, vodah in drugih z Zemljo povezanih področij. Učenci se naučijo svoje meritve in podatke sporočati po medmrežju, znanstvene projekte objavljati, analizirati podatke in sodelovati z znanstveniki in drugimi udeleženci projekta. Trenutno je v program vključenih 36.000 mentorjev in 19.000 šol iz 109 držav, ki so s svojimi učenci do začetka leta 2007 prispevali 16 milijonov meritev. Poleg učiteljev aktivno sodelujejo tudi starši. Žal pa v projekt GLOBE, kot že rečeno, zaenkrat Slovenija še ni vključena.

GLOBE at Night je vsakoletna akcija, ki je namenjena spremljanju svetlobnega onesnaženja in je le-

tos potekala med 8. in 21. marcem. V njej je sodelovalo skoraj 20.000 učencev in njihovih staršev, učiteljev ter mentorjev. Opazovanja so bila podobna tistim, ki smo jih predlagali v vaji *Izmerimo svetlobno onesnaženje v svojem kraju*, prilagojena različnim starostim otrok, a vseeno pomembna za spoznavanje in razumevanje problematike vplivov umetne razsvetljave na izgled nočnega neba. Opazovalci so na razpolago dobili karte ozvezdja Orion, oceniti pa so morali mejno magnitudo, torej najšibkejše zvezde, ki so jih še videli. Svoja opažanja so vpisali v pripravljen obrazec in jih poslali na GLOBE. Tako vsako leto nastane svetovna karta svetlobnega onesnaženja. Na spletnem naslovu [www.globe.gov/GaN](http://www.globe.gov/GaN) najdete več o tem.

Čeprav število in porazdelitev lokaciji opazovanj, ki so nam jih poslali dijaki in njihovi mentorji iz Postojne ter Ptuja, ni reprezentančno za vso Slovenijo, kažejo na veliko svetlobno onesnaženost našega neba. V idealnih pogojih brez Lune bi morali videti zvezde približno 6,5. magnitude, kar pomeni, da jih je nad obzorjem naenkrat vidnih približno 4000. Postojnski dijaki so ob povsem jasnem vremenu opazovali v Postojni in njeni širši okolici (Knežak, Prestanek), razmeroma daleč od cestnih luči (od 30 do 500 metrov) in v nočeh brez Lune. V povprečju so videli zvezde do 4. magnitude. Takih zvezd pa je hkrati nad obzorjem približno 450. Ptujski dijaki so opazovali v nekoliko slabših pogojih, saj je bila Luna tedaj nad obzorjem, v povprečju bližje javni razsvetljavi (od 20 do 150 metrov), a so kljub temu videli zvezde do 5. magnitude. Načeloma bi v isti noči videli približno trikrat več zvezd kot njihovi postojnski kolegi. Svetlobno onesnaženje v bližini mest

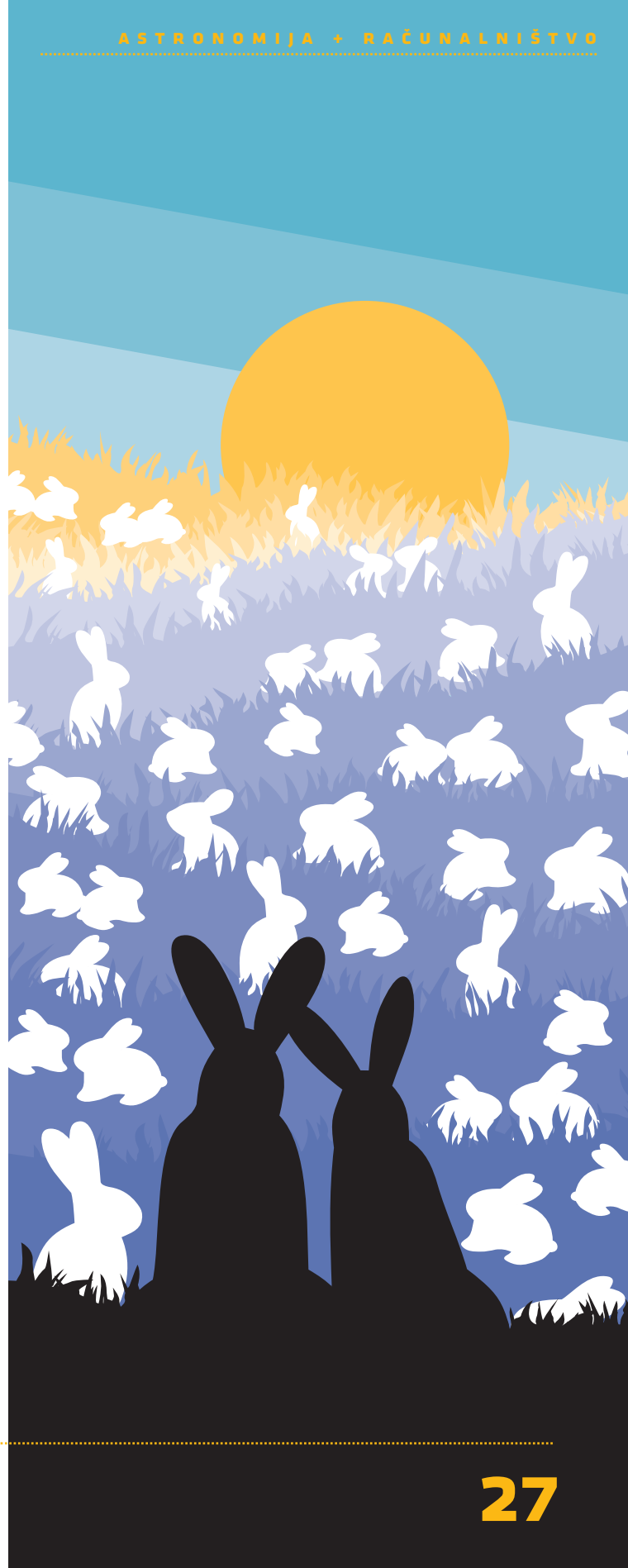


- mejna magnituda 7      ● mejna magnituda 4      ● mejna magnituda 1
- mejna magnituda 6      ● mejna magnituda 3
- mejna magnituda 5      ● mejna magnituda 2

**Slika 1.** Nočni pogled na Evropo razkrije veliko svetlobno onesnaženost. Kljub noči je obris kontinenta jasno viden, saj ga s svetlobo zaznamujejo večja in manjša mesta ter glavne prometnice. Na karto so vrisane meritve učencev (barvaste točke), ki so v okviru projekta GLOBE at Night leta 2006 opazovali vizualno mejno magnitudo zvezd. Očitno prevladujejo področja, kjer je mejna magnituda vsega 3 in je na nebu videti le peščico zvezd. Astronomska opazovanja so tam zelo motena (ilustracija: GLOBE).

ni presenetljivo, bolj vznemirja dejstvo, da je nebo močno svetlobno onesnaženo tudi daleč od strnjenih naselij, o čemer pričajo podatki iz okolice Postojne. Tako stanje potrjujejo tudi natančnejše meritve članov Pobude za temno nebo, ki se z monitoringom svetlobnega onesnaženja ukvarjajo strokovno. Za to so zagotovo krive nezasenčene in delno zasenčene svetilke, ki sevajo pod ostrimi koti nad vodoravnico. Ta svetloba po ozračju naredi dolgo pot in onesnažuje nebo nad kraji, kjer ni močne javne razsvetljave in drugih svetlobnih virov.

Upamo, da bosta primera iz Postojne in Ptuja vzpodbudila tudi druge šole k sodelovanju pri meritvah svetlobnega onesnaženja v Sloveniji in da se bomo lahko prihodnje leto priključili mednarodni akciji GLOBE at Night.



# Hitro do Da Vincijeve šifre

ALEKSANDER VESEL

## ■ Nenavadno zaporedje

- 1, 1, 2, 3, 5, 8, 13, 21, ...

so številke, ki jih začudeno opazuje junak Da Vincijeve šifre, ene od največjih svetovnih uspešnic zadnjih let. Mnenja o kakovosti knjige so precej deljena, mi pa si bomo raje poglobljevali samo zaporedje in poskušali odkriti, kako lahko s pomočjo računalnika izračunamo poljubni člen tega zaporedja. Zgornja števila imajo zanimivo lastnost, ki je ni težko uganiti: vsako število (razen prvih dveh) je vsota predhodnjih dveh števil. Običajno je v matematični literaturi dodana na začetku zaporedja še ničla, tako da dobimo:

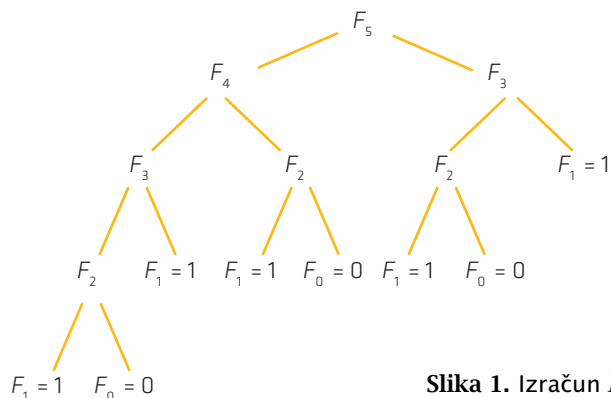
- 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

Zgornje zaporedje običajno označimo z  $F_n$  in formalno definiramo na naslednji način:

- $F_0 = 0$ ,
- $F_1 = 1$ ,
- $F_n = F_{n-1} + F_{n-2}$ ,  $n \geq 2$ .

To slavno zaporedje je leta 1202 zapisal Leonardo Fibonacci kot odgovor na vprašanje, koliko parov zajcev nastane v enem letu iz začetnega enega para. Pri tem je predpostavil, da ima par zajcev vsak mesec dva mladička (torej en par) in da mladički po enem mesecu postanejo plodni. Opazimo lahko, da imamo po enem mesecu dva para zajcev, po dveh pa tri. Tretji mesec dobi potomca spet prvi par, prav tako pa tudi par, ki je bil rojen prvi mesec, zato število parov naraste na pet. S podobnim razmislekom ugotovimo, da imamo po četrtem mesecu osem parov itd.

Opisi zaporedja  $F_n$  so se pojavili že v nekaterih


Slika 1. Izračun  $F_5$ 

starejših spisih, pa tudi po letu 1202 so ga nekateri odkrivali "na novo". Konec 19. stoletja je prišlo do pomembnih rezultatov, povezanih z zaporedjem, in od takrat je to zaporedje znano kot *Fibonaccijevo zaporedje*, njegovi členi pa Fibonaccijeva števila.

Znano je, da je s Fibonaccijevim zaporedjem tesno povezano število

- $\phi = \frac{1}{2}(1 + \sqrt{5}) \approx 1,618$ .

Velja namreč, da lahko  $n$ -ti člen zaporedja izračunamo tudi tako, da vrednost izraza  $\phi^n / \sqrt{5}$  zaokrožimo na najbližje celo število.

Zanimivo je, da se število  $\phi$  pojavlja na zelo različnih področjih; poleg tega, da ga najdemo v matematiki, ga srečamo še v računalništvu, fiziki in nekaterih drugih znanostih, zelo pomembno pa je tudi v umetnosti, kjer ga običajno imenujejo *zlati rez*. Mnogi umetniki so namreč mnenja, da je razmerje določeno z zlatim rezom, estetsko najbolj dovršeno razmerje. Zato ni čudno, da so razmerje zlatega reza uporabili tudi nekateri oblikovalci spletnih strani. O pomembni vlogi zlatega reza piše tudi Da Vincijeva šifra, a ker gre za leposlovno delo, je priporočljivo biti do trditev v knjigi nekoliko zadržan.

## ■ Počasi do rešitve

Kot smo že napovedali, bomo poskusili poiskati računalniški program, ki izračuna splošni člen Fibonaccijevega zaporedja. Če je neko zaporedje definirano tako, da je  $n$ -ti člen zaporedja izražen s predhodnjimi členi, potem pravimo, da je *rekurzivno* definirano. Če je podano zadostno število začetnih členov, potem rekurzivna definicija omogoča, da izračunamo poljubni člen zaporedja. Za primer poskušajmo izračunati  $F_5$ . Vemo, da velja  $F_5 = F_4 + F_3$ ,



in ker  $F_4$  še ne poznamo, uporabimo  $F_4 = F_3 + F_2$ . Nadaljujemo z  $F_3 = F_2 + F_1$ , v naslednjem koraku pa pridemo do začetnih členov  $F_2 = F_1 + F_0 = 1 + 0 = 1$ . Ko imamo vrednost  $F_2$ , lahko izračunamo  $F_3$ , nato  $F_4$  in na koncu še  $F_5$ . Celoten postopek izračuna kaže slika 1. Za izračun katerega od kasnejših členov zaporedja bi potrebovali precej več dela, zato je računalniški program seveda dobrodošel.

Delo nam olajša dejstvo, da večina sodobnih prevajalnikov podpira rekurzivne podprograme. Pravimo, da je podprogram *rekurziven*, če kliče samega sebe. Tudi programski jezik pascal in na pascalu zasnovani sodobni programski jeziki (npr. Turbo Delphi) podpirajo rekurzijo. Izračun  $n$ -tega člena Fibonaccijevega zaporedja je šolski primer elegantne uporabe rekurzivnega klica podprograma, saj problem reši z enim samim pogojnim stavkom.

```
function Fib(n: integer): integer;
begin
  if (n = 0) or (n = 1) then Fib := n
  else Fib := Fib(n-1) + Fib(n-2);
end;
```

Rešitev ni samo kratka, ampak tudi zelo pregledna, saj neposredno sledi definiciji. A lepota in uporabnost ne gresta vedno skupaj in tako je tudi v zgornjem primeru. Začetne vrednosti zaporedja lahko s funkcijskim podprogramom Fib sicer razmeroma hitro in natančno izračunamo, pri malo večjem  $n$  pa se stvari zapletejo. Težave se lahko pojavijo že pri izračunu vrednosti  $F_{40}$ , saj računanje na manj zmogljivem računalniku traja kar nekaj časa, pri  $F_{47}$  pa naš elegantni podprogram popolnoma odpove.  $F_{47} = 2971215073$  je namreč že zelo veliko število, večje od  $2^{31} - 1 = 2147483647$ , kar je največja vrednost, ki jo lahko shranimo v spremenljivko celoštevilskega tipa integer. Novejši programski jeziki sicer poznajo tudi 64 bitne celoštevilske podatkovne tipe, ki omogočajo računanje s precej večjimi vrednostmi (običajno do  $2^{63} - 1$ ), a tudi če ga uporabimo, je z zgornjim podprogramom možen izračun le do člena  $F_{96}$ . Na podobno omejitev naletimo tudi, če poskusamo izračunati  $F_n$  s pomočjo števila  $\phi$ .

Rešitev problema bomo poiskali tako, da bomo dolga cela števila v računalniku predstavili nekoliko drugače. Spomnimo se, da v vsakdanjem življenju zapisujemo števila kot zaporedja znakov oz. natančneje, števk. Sodobni programski jeziki imajo zelo

dobro podprto delo z zaporedji znakov oz. z nizy, kot zaporedja znakov tudi imenujemo. V pascal-skih programskih jezikih uporabljamo za predstavitev niza podatkovni tip *string*. Celo število lahko v niz torej čisto naravno shranimo, več problemov pa imamo z izvedbo računskih operacij, ki jih moramo v tem primeru realizirati sami. Na srečo za izračun Fibonaccijevih števil potrebujemo samo seštevanje, zato naša naloga ni pretirano zahtevna. Problem rešimo podobno kot pri pisnem seštevanju, ki smo se ga naučili v prvih razredih osnovne šole: najprej seštejemo enice obeh seštevancev in dobimo enico rezultata, morebiten prenos pa nato upoštevamo pri seštevanju desetic. Postopek ponavljamo, dokler ne izčrpamo števk obeh seštevancev. Račun je nekoliko zahtevnejši, ker so številke predstavljene kot znaki, zato moramo dejanske vrednosti najprej izračunati. Vsak znak je v računalniku predstavljen s posebnim celim številom oz. s tako imenovano ASCII vrednostjo. V pascal-skih jezikih uporabljamo za izračun ASCII vrednosti znaka funkcijo *ord*. Pri tem nam pomaga dejstvo, da so številke predstavljene z zaporednimi ASCII vrednostmi: tako je *ord('0')* = 48, *ord('1')* = 49 in *ord('9')* = 57. Če z *a[i]* in *b[i]* označimo istoležne številke obeh seštevancev, s *p* pa vrednost prenosa (*p* je enak 0 ali 1), potem lahko izračunamo njun seštevek (označimo ga z *v*) na naslednji način:

$$v = (\text{ord}(a[i]) - \text{ord}('0')) + (\text{ord}(b[i]) - \text{ord}('0')) + p.$$

Vrednost *v* lahko presega 9, zato moramo poiskati vrednost ostanka pri deljenju *v* z 10 (operacija *mod*), za izračun prenosa pa poiščemo vrednost po celoštevilskem deljenju z 10 (operacija *div*). Izračunano vrednost *v* nato spet pretvorimo v številko (znak) s funkcijo *chr*. V podprogramu je uporabljena funkcija *length*, ki vrne dolžino niza oz. število znakov v nizu, s simbolom *+* pa opišemo operacijo, s katero zlepimo dva ali več nizov.

```
function plus(a,b: string): string;
var i: integer;
    p,v: integer;
    la,lb: integer; { dolžini niza a in b }
    c: string; { začasni rezultat }
begin
  p := 0; { prenos je najprej enak 0 }
  c := ""; { prazen niz }
  la := length(a); lb:=length(b);
```





```

if la > lb then b := '0' + b;
    { želimo enako dolga niza }
for i := la downto 1 do begin
    v := ord(a[i]) + ord(b[i]) - 2*ord('0') + p;
    p := v div 10; { prenos }
    v := v mod 10; { vrednost i-te številke }
    c := chr(ord('0')+v) + c;
    { i-to številko pripnemo na začetek niza }
end;
if p = 1 then plus := '1' + c else plus := c;
end;

```

Zgornji funkcijski algoritem sedaj uporabimo na naslednji način:

```

function Fib2(n: integer): string;
begin
    if (n = 0) or (n = 1) then Fib2 := chr(ord('0') + n)
    else Fib2 := plus(Fib2(n-1),Fib2(n-2));
end;

```

Problem predstavitve velikih števil s podprogramom Fib2 rešimo, problema počasnosti pa ne. Ravno nasprotno; seštevanje, ki smo ga izvedli sami v podprogramu plus, je precej bolj počasno od običajnega seštevanja. Posledica tega je, da je podprogram Fib2 še počasnejši od podprograma Fib. Za izračun  $F_{40}$  s Fib2 je na srednje zmogljivem računalniku potrebno približno tri minute, za izračun  $F_{41}$  šest minut, za izračun  $F_{42}$  enajst minut, za izračun  $F_{43}$  18 minut, za izračun  $F_{44}$  pa že 28 minut. Pri izračunu  $F_{50}$  pa je avtor tega prispevka po približno desetih urah obupal in ugasnil računalnik ter kasneje raje na roke izračunal, da bi program tekel zagotovo več kot en dan.

### ■ Hitra rešitev

Za razmislek o hitrejši programski rešitvi si pogledajmo še enkrat izračun  $F_5$  na sliki 1. Slika ponazarja računanje  $F_5$  po definiciji in zato opisuje tudi delovanje funkcijskih podprogramov Fib in Fib2. Pozoren bralec je že verjetno opazil, da je postopek računanja prikazan na sliki 1 zelo zamuden. Podprogram mora tako za izračun  $F_5$  izračunati  $F_3$  dejansko dvakrat,  $F_2$  pa kar trikrat. Pri kasnejših členih Fibonaccijevega zaporedja je odvečnost računanja samo še bolj izrazita: za izračun  $F_{10}$  je tako potrebno 34 krat izračunati  $F_2$ , 21 krat  $F_3$ , 13 krat  $F_4$ , osemkrat  $F_5$ , petkrat  $F_6$ , trikrat  $F_7$  in dvakrat  $F_8$ . Oči-

tno gre za časovno zelo potraten postopek. (Mimo grede: poskusite pokazati, da je število izračunov posameznega člena zaporedja iz zgornjega primera spet Fibonaccijevo število.) Pravzaprav sta podprograma tudi dober primer upravičenosti načela: ne računaj ničesar več kot enkrat! To pa seveda ne pomeni, da je rekurzija v splošnem neuporabna, saj obstaja veliko problemov, pri katerih jo lahko zelo koristno uporabimo.

Poskusimo se računanja zaporedja lotiti še enkrat, najprej brez računalnika tako, da sproti zapisujemo zaporedne člene zaporedja. Začnemo seveda z 0 in 1, ko ju seštejemo dobimo 1, nato seštejemo 1 in 1 ter dobimo 2, nato 1 in 2 da dobimo 3 itd. Če torej sproti zapisujemo zaporedna Fibonaccijeva števila, lahko pridemo do rešitve hitro in brez nepotrebnega dodatnega dela. Pravzaprav se pokaže, da v resnici ni potrebno shranjevati vseh izračunanih števil, temveč le zadnji dve. Rezultat tega razmisleka je spodnji podprogram, v katerem v spremenljivki  $f1$  in  $f2$  shranimo zadnje oz. predzadnje izračunano število.

```

function Fib3(n: integer): string;
var f1,f2,z: string;
    i: integer;
begin
    if (n = 0) or (n = 1) then Fib3 := chr(ord('0') + n)
    else begin
        f1 := '1'; { F1 = 1 }
        f2 := '0'; { F0 = 0 }
        for i := 2 to n do begin
            z := f1; { začasno shrani F(n-1) }
            f1 := plus(f1,f2); { izračuna F(n) }
            f2 := z; { shrani F(n-1) (v naslednjem
                                koraku postane F(n-2)) }
        end;
    end;
    Fib3 := f1;
end;

```

Program izračuna  $F_{1000} = 43466557686937456435688527675040625802564660517371780402481729089536555417949051890403879840079255169295922593080322634775209689623239873322471161642996440906533187938298969649928516003704476137795166849228875$  v manj kot sekundi, za izračun  $F_{10000}$  pa potrebuje 14 sekund. Za lažjo predstavbo povejmo, da je  $F_{10000}$  število z natančno 2090 števki! ✖

# Predstavitev nove knjige

DOMINIK BENKOVIČ



➔ Jeffrey Rosenthal je profesor na Oddelku za statistiko Univerze v Torontu. Leta 2005 je izdal knjigo z naslovom *Ko strela udari: Skrivnostni svet verjetnosti*. Knjiga govori o tem, kako se v vsakodnevnem življenju nprestano srečujemo s situacijami, ki so povezane s slučajnostjo in negotovostjo. Zorni kot verjetnosti nam po avtorjevih besedah lahko pomaga, da najdemo smisel takih situacij, se izognemo nepotrebnim strahovom, posežemo po priložnostih, ki jih slučajnost ponuja in uživamo v negotovih situacijah, ki so pred nami. Zaradi tega je knjiga v Ameriki nemudoma postala zelo priljubljena. Omenjeno delo je sedaj na voljo tudi širšemu krogu slovenskih bralcev. Leta 2006 je namreč pri založbi DMFA izšel slovenski prevod, ki ga je pripravil profesor Matjaž Omladič. Knjiga ima 261 strani in je razdeljena na 17 poglavij. Na kratko predstavimo njeno vsebino.

V začetnem delu knjige nas avtor seznani s slučajnostjo in verjetnostjo, ki nastopa vsepovsod okoli nas. Nadaljevanje je namenjeno igranju na srečo: kockanju, loteriji, družabnim igram s kartami. Tu s pomočjo zakona velikih števil najdemo odgovor, zakaj na dolgi rok igralnice vedno služijo in se ne

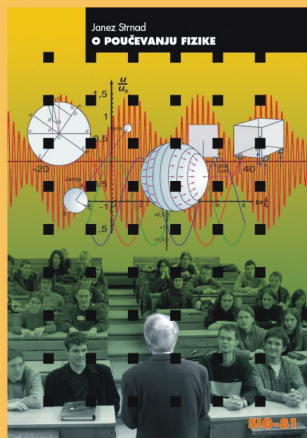
splača igrati iger na srečo. Na konkretnih primerih so lepo predstavljene slučajnostne strategije, kjer igramo igro tako, da je v povprečju ne izgubljam. Preko aktualnih "ameriških" tem, kot so umori in terorizem, spoznamo merjenje trendov in regresijo. Na konkretnih primerih je predstavljena teorija funkcij uporabnosti, ki nam omogoča, da se v življenju lažje odločamo. Posebno poglavje je namenjeno dogodkom z majhno verjetnostjo, kot so npr., da vas ob nevihti udari strela, da strmoglavi letalo, s katerim ravnokar letite na počitnice. Po avtorjevih besedah se nam takih dogodkov ni potrebno bati, ker se ti preprosto ne bodo zgodili. Na primerih anket javnega mnenja in medicinskih raziskavah spoznamo uporabnost in slabost statističnega sklepanja. Namreč, javnomnenjske ankete pomembno vplivajo na družbo in predvsem politiko, zato je pomembno, da jih razumemo. Slučajnost lahko prinese veliko težav, ki so povezane predvsem z negotovostjo, v marsičem pa je slučajnost ravno naš prijatelj. Zato se slučajnost pogosto uporablja tudi za doseganje pravičnosti, o čemer govori posebno poglavje. Poučni so tudi primeri uporabe verjetnosti in slučajnosti v biologiji, genetiki in epidemiologiji. Tako preko modela širjenja virusnih boleznih, naraščanja števila prebivalstva in širjenja verižnih pisem spoznamo dejitveni proces. V knjigi najdemo odgovor, kako se z verjetnostjo borimo proti nezaželeni elektronski pošti in kako slučajnost uporabljamo pri šifriranju in varovanju podatkov. Avtor zaključuje delo z vzroki za slučajnost in negotovost, kjer izvemo, da je slučajnost vgrajena že v same temelje vesolja. Po teoriji kvantne mehanike vesolje deluje na podlagi verjetnosti in negotovosti. Zato slučajnost in negotovost ni posledica naše nevednosti!

Vsako poglavje je popestrjeno s kakšno avtorjevo osebno prigodo ali anekdoto, zato je branje še toliko bolj zanimivo. Sama knjiga je pisana poljudno in zelo razumljivo. Ker je za razumevanje večine primerov potrebno samo osnovno matematično znanje, knjigo toplo priporočam v branje vsakomur, tudi osnovnošolcem. ☒



# Novosti v Knjižnici Sigma

Že od leta 1959 nam Knjižnica Sigma prinaša poljudna in strokovna besedila za popularizacijo področij matematike, fizike, astronomije in računalništva. Vključuje tako zbirke nalog z različnih tekmovanj, dopolnilne učbenike, priročnike in drugo zanimivo branje domačih avtorjev, kot tudi nekaj prevodov znanih tujih avtorjev. Najnovejši dve knjižici sta izšli konec leta 2006.



Janez Strnad:

## O POUČEVANJU FIZIKE

320 strani  
format  $14 \times 20$  cm  
mehka vezava

12,49 EUR  
(2.993,10 SIT)



Jeffrey S. Rosenthal:

## KO STRELA UDARI

Skrivnostni svet  
verjetnosti

264 strani  
format  $14 \times 20$  cm  
mehka vezava

12,49 EUR  
(2.993,10 SIT)

Robert B. Banks:

## LEDENE GORE, PADAJOČE DOMINE in druge prigode iz uporabne matematike

skupaj 348 strani  
format  $14 \times 20$  cm  
mehka vezava

cena kompleta:  
20,86 EUR (4.998,89 SIT)



Borut Zalar:

## TEŽIŠČA IN VZTRAJNOSTNI MOMENTI

120 strani  
format  $14 \times 20$  cm  
mehka vezava

8,35 EUR  
(2.000,99 SIT)



Poleg omenjenih lahko v Knjižnici Sigma najdete še več kot 40 drugih del. Podrobnejše predstavitve so na spodnjem naslovu, kjer lahko vse knjige tudi naročite s popustom:

<http://www.knjiznica-sigma.si/>

Individualni naročniki revije Presek, člani DMFA, dijaki in študentje imate ob naročilu pri DMFA-založništvo 20 % popusta na zgornje cene – izkoristite ga!

Dodatne informacije lahko dobite v uredništvu Preseka po telefonu (01) 4766 553 ali 4232 460.