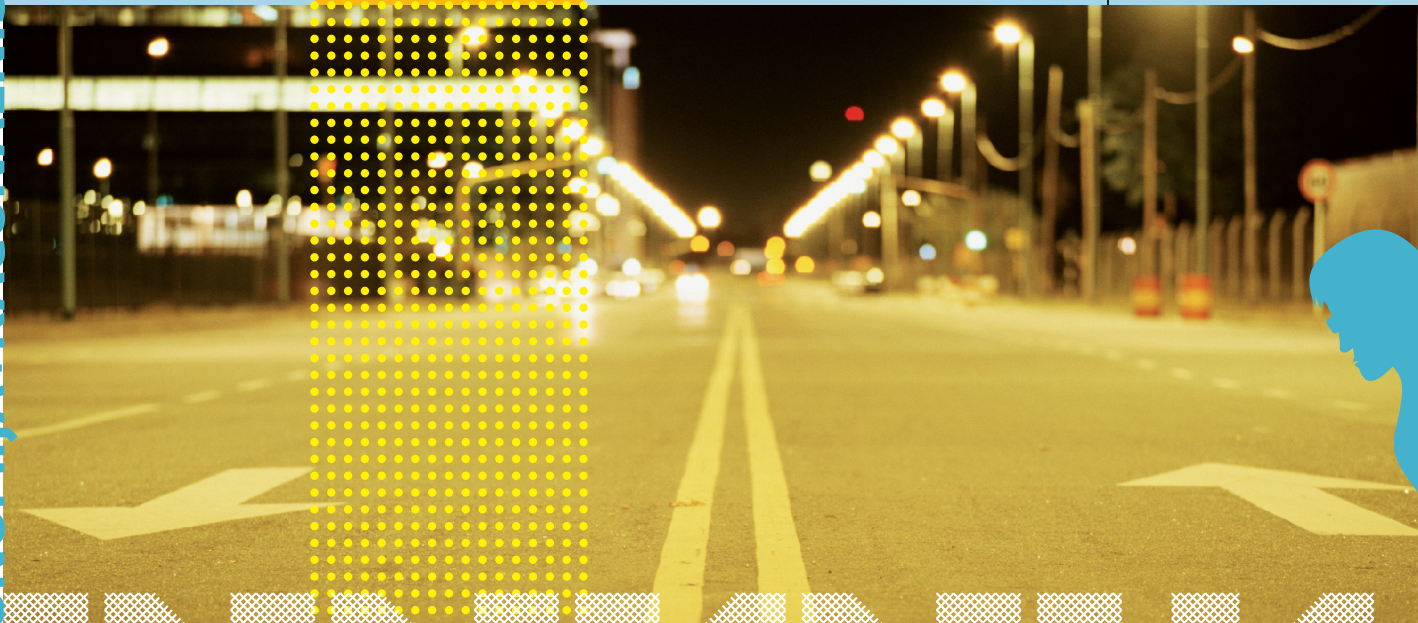




PRESEK

- IRACIONALNE ENAČBE
- KUHINJSKA POIZKUŠEVALNICA
- SVETLOBNO ONESNAŽENJE
- NAGRADNA KRIŽANKA



ISSN 0351-6652



9 770351 665418

Premagovanje prometa

☛ To ni vaša domišljija; promet RES postaja vedno hujši. Medtem ko se je v zadnjih 30 letih število prevoženih kilometrov več kot podvojilo, se je fizični cestni prostor povečal le za šest odstotkov. (Opomba prevajalca: podatki veljajo za ZDA, a bi do podobnih ugotovitev prišli tudi drugje.) Vendar gradnja novih cest ne daje zagotovila za olajšanje. Rezultat iz teorije prometa, ki je v nasprotju z intuicijo, pravi, da lahko nova cesta celo poveča prenatrpanost omrežja. Področja matematike, kot sta na primer teorija vrst in parcialne diferencialne enačbe, prispevajo k razumevanju prometa, ki je *vzvratni prenašalni val*—avtomobili se gibljejo naprej, medtem ko se prometni zastoj giblje nazaj.

Matematične raziskave prometa so relativno nove, toda ameriško državno poročilo je zaključilo, da bo informacijska revolucija—to je, kombinacija zmogljivejših računalnikov, telekomunikacij in boljših numeričnih metod—vplivala na transport ravno tako, kot sta na to vplivala izum avtomobila in izum motorja na reaktivni pogon. Analiziranje prometa (tako kot napovedovanje vremena) zahteva številne spremenljivke (voznikovo hitrost, dolžino potovanja, čas dneva in začetno točko) in vpleta teorijo kaosa (majhna sprememba na cesti lahko drastično spremeni potovalne pogoje). Za razliko od vremena pa se promet lahko v odgovor na napoved preusmeri na alternativne poti—danes z vozniki in v prihodnosti nemara s samimi avtomobili. ☛



POJASNILO: Gornji prispevek je prevod iz rubrike »The Mathematical Moments«, ki jo objavlja Ameriško matematično društvo AMS na spletni strani www.ams.org/mathmoments.

Presek

list za mlade matematike, fizike, astronome in računalnikarje
letnik 34, šolsko leto 2006/2007, številka 1

Uredniški odbor: Vladimir Batagelj, Tanja Bečan (jezikovni pregled), Mojca Čepič, Mirko Dobovšek (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) 2517 281.

Naročnina za šolsko leto 2006/2007 je za posamezne naročnike 4.000 SIT (16,69 EUR)—posamezno naročilo velja do preklica, za skupinska naročila učencev šol 3.500 SIT (14,61 EUR), posamezna številka 900 SIT (3,76 EUR), dvojna številka 1.650 SIT (6,89 EUR), stara številka 650 SIT (2,71 EUR), 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 3100 izvodov

© 2006 Društvo matematikov, fizikov in astronomov Slovenije – 1643

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). Zaželeno 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.

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

Premagovanje prometa	2
----------------------------	---

■ MATEMATIKA

Je lahko matura iz angleščine navdih matematikom ali matematični komentarji h knjigi »Skrivnostni primer ali kdo je umoril psa« – Prvi del: Praštevila (<i>Jasna Kos</i>)		4-6
Iracionalne enačbe (<i>Ajda Fošner</i>)		7-9
Tehtanje pobarvanih lesenih kock – rešitev nagradne naloge (<i>Marija Vencelj</i>)		10

■ FIZIKA

Žabice (<i>Janez Strnad</i>)	12-14
Vetromobil (<i>Branislav Čabrić, prevod Petar Pavešić</i>)	15 in 18
Kuhinjska poizkuševalnica – Ali teče, ali je trdno? (<i>Mojca Čepič</i>) ..	19

■ ASTRONOMIJA

Svetlobno onesnaženje – Prvi del (<i>Andrej Guštin</i>)	22-24
---	-------

■ RAČUNALNIŠTVO

Diffie–Hellmanov dogovor o ključu (<i>Aleksandar Jurišić</i>)	25-30
---	-------

■ RAZVEDRILO

Nagradna križanka (<i>Marko Bokalič</i>)	16-17
Rešitev nagradne križanke Presek 33/6	18

■ TEKMOVANJA

47. Mednarodna matematična olimpijada	9
42. tekmovanje za Zlata Vegova priznanja (<i>Klavdija Mlinšek</i>)	11
26. državno tekmovanje iz fizike za Stefanova priznanja (<i>Saša Kožuh</i>)	20-21
37. Mednarodna fizikalna olimpijada	20
41. področno tekmovanje za Srebrno vegovo priznanje	priloga
42. državno tekmovanje za Zlato vegovo priznanje	priloga

Je lahko matura iz angleščine navdih matematikom ali matematični komentarji h knjigi »Skrivnostni primer ali kdo je umoril psa«

JASNA KOS

PRVI DEL: PRAŠTEVILA

➔ Knjiga Marka Haddona *“Skrivnostni primer ali kdo je umoril psa”* je v Evropi požela velik uspeh in bila večkrat nagrajena. Gimnazijski maturantje ste morda že posegli po njej, saj je obvezno čtivo za maturo iz angleščine. Niste pričakovali, kajne, da boste naleteli na literaturo, v katero se prijetno vpletajo matematični pojmi, računi, primeri in modeli. Vsa ta matematična šara se v literarnem delu pojavlja tako nevsiljivo, da ne odvrne od branja še tako zadržega sovražnika matematike. “Kakšno protislovje”, boste odvrnili. Ne, ni tako, samo malo bolj poglobljeno se ozrimo na te matematične vložke in tudi matematiki bomo imeli dovolj dela, če se jih nekoliko podrobneje lotimo.

Nekaj besed za uvod naj bo za vse tiste, ki knjige ne poznate. Zgodba, napisana v prvi osebi, pripoveduje o avtističnem 15-letniku Christopherju, ki ima rad matematiko, logiko, vzorce in rdečo barvo, ne mara pa rumene, strah ga je množice ljudi in dotikov. Christopher ne prepozna čustev, hkrati pa ima nadpovprečno razvite “savant”¹ sposobnosti na področju računanja na pamet in matematike. Se spomnite filma Rain Man? Glavni junak je imel enako razvojno motnjo - avtizem in tudi on je bil neverjetno



računsko spreten. Iz “realnega sveta” pa omenimo sedemindvajsetletnega Angleža, rekorderja v recitiranju decimalk števila pi. To je Daniel Tammet, ki je marca 2004 brez napake naštel na pamet prvih 22511 decimalk števila pi, kar je trajalo nekaj več kot pet ur.

Značilno je, da osebe z avtistično motnjo ne morejo filtrirati kopice podatkov, ki vsak trenutek prihajajo iz okolice v možgane, in izločati nepotrebnih. Tako milijoni informacij povzročajo pravi kaos v njihovi glavi. Christopher se zapre pred zunanjim svetom in se umiri tako, da ponavlja potence števila 2, njegov rekord je 2^{45} . Včasih na pamet rešuje kvadratne enačbe z dvo ali tromestnimi koeficienti ali našteva praštevila. Našteti zna vsa praštevila do 7507.

“Zaporedje in določanje praštevil se ne podrejata vnaprej določenim vzorcem. Meni se zdijo podobna življenju. Videti so zelo logična, ne moreš pa jim določiti pravil, tudi če se ves čas ukvarjaš z njimi.” [1, str. 20]

Christopherja praštevila tako navdušujejo, da je celo poglavja oštevilčil z njimi. Bralcu razloži, da praštevila dobimo tako, da zapišemo vsa naravna števila večja od 1. Prvo število, to je 2, je praštevilo. Prečrtamo vse večkratnike števila 2 in prvo neprečrtano število, to je 3, je zopet praštevilo. Prečrtamo vse večkratnike števila 3, ... Vsem nam je ta postopek dobro poznan, to je Eratostenovo rešeto (Eratosten, 280–196 pr. n. št.). Postopek je malo zamuden. Z njim lahko izračunamo, koliko poglavij je v knjigi *“Skrivnostni primer ali kdo je umoril psa”*, če je zadnje poglavje oštevilčeno s številko 233. Če se vprašamo, koliko praštevil zna naštet Christopher, pa bomo raje pobrskali po spletu in poiskali tabelo praštevil, ali si pomagali s kakšnim računalniškim programom. Predlagam Derive in tri ukaze, ki pomagajo rešiti zastavljeno uganko:

- **PRIMEPI(x)** nam pove, koliko je praštevil, ki so manjša ali enaka x .
- **NTH_PRIME(n)** pove, katero je n -to praštevilo.
- **VECTOR(VECTOR(NTH_PRIME(n+m),m,0,90,10),n,1,10)** naredi tabelo prvih 100 praštevil.

Christopher ima sicer prav, ko trdi, da vzorcev v množici praštevil ni, kakšno zakonitost pa le lahko najdemo. Na primer, znameniti praštevski izrek:

Razmerje med številom praštevil, manjših ali enakih naravnemu številu n , in tem naravnim številom n , kar lahko imenujemo gostota praštevil v množici naravnih števil, je za velike n približno enaka $1 / \ln n$.

Izrek sta leta 1896 neodvisno dokazala Jacques Hadamard in C. J. de la Vallée Poussin. Več o tem lahko preberete v Preseku, letnik 24, št. 3, [2].

Kljub temu izreku, ki kaže na neko urejenost, moramo potrditi, da so praštevila v množici naravnih števil zelo nepravilno posejana.

Obstajajo poljubno dolgi odseki v zaporedju naravnih števil, na katerih ni nobenega praštevil.

Navedimo dokaz te trditve iz knjige profesorja Grassellija Osnove teorije števil [3]. Oglejmo si zaporedje naravnih števil $k! + 2, k! + 3, \dots, k! + k$, kjer je k naravno število večje od 2 in $k! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot k$ (preberemo k fakulteta ali k faktorialno). Nobeno izmed naštetih števil ni praštevilo. Prvi člen zaporedja je deljiv z 2, drugi člen s 3 in tako naprej do zadnjega člena, ki je deljiv s k . To pomeni, da je razmik med sosednjima praštevila vsaj $k-1$. Ker je k poljubno velik, je s tem trditev dokazana.

ln že nas je iz zgodbe in preproste omembe praštevil zaneslo v svet matematike. Problemi o praštevilih so resda enostavno zastavljeni, vendar težki za reševanje in mnogi med njimi še nerešeni. Kaj pa uporabnost?

“Praštevila so uporabna pri sestavljanju šifer in v Ameriki veljajo za vojaško tajnost in če odkriješ novo praštevilo, daljše od 100 mest, moraš o tem obvestiti CIA in ti bodo zanj plačali 10.000 dolarjev. Ampak od tega se ne bi dalo živeti.” [1, str. 21]

V tem citatu je nekaj netočnosti. Iskalci velikih praštevil se že približujejo praštevilo z 10 milijonov števkami in tudi nagrada za tako veliko praštevilo bo 10-krat večja. O tem smo brali v Preseku, letnik 32, št. 6, [4]. V lanski četrti številki Preseka smo iz-

1 savant sindrom = strokovni izraz, beseda savant je francoska in pomeni učen ali učenjak



→ vedeli, da je na novo odkrito praštevilo že kar blizu temu rekordu. Večina na novo odkritih praštevil pripada Mersennovim praštevilom, ime imajo po francoskem redovniku Marinu Mersennu iz 17. stoletja. To so praštevila oblike $M_n = 2^n - 1$. Niso pa vsa števila take oblike praštevila. Če je n sestavljeno število, je tudi $2^n - 1$ sestavljeno število. To lahko enostavno dokažemo, zadošča že poznavanje formule za razstavljanje razlike n -tih potenc, pri čemer je n naravno število. Postopek, s katerim pokažemo, ali je Mersennovo število praštevilo ali ne, se imenuje Lucas-Lehmerjev test. Osnovno idejo zanj je izdelal Edouard Lucas leta 1873, izboljšal pa jo je David Lehmer leta 1930. Končna ideja je naslednja:

Naj bo s funkcija iz množice $\mathbb{N} \cup \{0\}$ v množico $\mathbb{Z}$ podana z rekurzivno formulo:

- $s(0) = 4$,
- $s(n + 1) = (s(n))^2 - 2$.

Za vsako liho praštevilo n je $M_n = 2^n - 1$ praštevilo tedaj in le tedaj, ko je $s(n - 2) \equiv 0 \pmod{M_n}$.

Poskusite z opisano metodo ugotoviti, če je katero izmed Mersennovih števil M_{11} ali M_{13} praštevilo. Tudi tokrat vam predlagam Derive. Ukaz, s katerim izračunate ostanek pri deljenju števila a s številom b , je MOD(a, b).

Velika praštevila se res, tako kot trdi tudi Christopher, uporabljajo za šifriranje. Metoda šifriranja z javnim ključem je taka, da lahko prejemnik javno objavi števila, ki predstavljajo ključ za šifriranje, števila za dešifriranje pa pozna le sam. Ena takih je RSA metoda, ki so jo razvili leta 1978. Opisana je bila v Preseku, letnik 22, št. 6, [5]. Javni ključ je število, ki je zmnožek dveh velikih praštevil. Kdor bi hotel vdreti v sistem, bi moral število faktorizirati, kar pa je sila zamudno in pri res velikih praštevilih praktično nemogoče. Že od Evklida (350–300 pr. n. št.) do danes se matematiki ukvarjajo z ugotavljanjem praštevilstosti. Vedno bolj zmogljivi računalniki so v pomoč, ne gre pa brez matematičnega uma. Ko bo odkrit test, ki bo lahko v primernem času odgovoril na vprašanje, ali je dano veliko število praštevilo ali ne, bo RSA metoda le še zgodovina.

Kaj ni matematika čudovita veda? Logična je in

urejena, vedno se izkaže, da je tudi uporabna. Ljudje smo nepredvidljivi, za vsako našo kretnjo, izrazom ali pogledom je kup različnih pomenov. Pomen matematičnih znakov, izrazov, izrekov je en sam. Svet matematike ponuja Christopherju varnost, v tem svetu Christopher napreduje, je uspešen in srečen.

■ Literatura

- [1] M. Haddon, *Skrivnostni primer ali kdo je umoril psa*, Mladinska knjiga, Ljubljana, 2004.
- [2] G. Pavlič, *Porazdelitev praštevil v množici $\mathbb{N}$* , Presek 24(3) (1996/1997), str. 140–143.
- [3] J. Grasselli, *Osnove teorije števil*, DZS, Ljubljana, 1975.
- [4] C. Petr, *Odkrili dve novi Mersennovi praštevili*, Presek 32(6) (2004/2005), str. 9.
- [5] M. Vencelj, *Šifriranje z javnim ključem*, Presek 22(6) (1994/1995), str. 354–357.
- [6] M. G. Fung, *Read This!*, <http://www.maa.org/reviews/dogincident.html>
- [7] K. Devlin, *Nova zlata doba matematike*, Knjižnica Sigma 53, DMFA Slovenije, Ljubljana, 1993. ✕



Iracionalne enačbe

AJDA FOŠNER

■ Reševanje iracionalnih enačb

➔ Enačbi $\sqrt{x+6} = x+4$ pravimo *iracionalna enačba*, ker v njej spremenljivka x nastopa pod korenem. Čeprav je pri reševanju take enačbe postopek največkrat jasen, se pogosto zgodi, da ne pridemo do pravih rešitev. Zato je namen tega članka predstaviti ozadje in ključne korake reševanja iracionalnih enačb. Avtorica se je za to temo odločila po prebiranju članka *Iracionalne enačbe i neenadžbe* (N. Dmitroviča, Hrvatski matematički elektronski časopis 2 (2005), 1-10), ki med drugim opozarja na napake pri postopku iskanja rešitev iracionalnih enačb.

PRIMER 1. Pa si za začetek pogledjmo primer preproste iracionalne enačbe

$$\blacksquare \sqrt{x+6} = x+4. \quad (1)$$

Iščemo torej vsa taka realna števila x , ki zadoščajo zgornji enakosti. Kar sta leva in desna stran enaki, sta enaka tudi njuna kvadrata

$$\blacksquare x+6 = x^2+8x+16. \quad (2)$$

Zgornjo enakost preuredimo v $x^2+7x+10=0$ oziroma $(x+2)(x+5)=0$. Rešitvi enačbe (2) sta torej $x=-2$ in $x=-5$, vendar le prva reši tudi enačbo (1), kar lahko preverimo z direktnim vstavljanjem v enakost (1).

Že zgornji primer kaže na to, da so posamezni koraki reševanja iracionalnih enačb največkrat očitni, kljub temu pa je rešitev lahko napačna. Razlog za to je v tem, da iz $a=b$ res sledi $a^2=b^2$, vendar pa iz $a^2=b^2$ sledi, da je $a=b$ ali $a=-b$. Pri kvadriranju enačb se moramo torej zavedati, da so rešitve prvotne enačbe vsebovane v množici rešitev kvadrirane enačbe (množica rešitev prvotne enačbe

ni nujno enaka množici rešitev kvadrirane enačbe). Prav zaradi te lastnosti moramo pred kvadriranjem leve in desne strani enačbe določiti pogoje, s pomočjo katerih bomo prišli do pravih rešitev. Enako velja za iracionalne enačbe, v katerih namesto drugega korena nastopa koren s sodim eksponentom.

In kako določimo pogoje? Pogledjmo si kar na konkretnem primeru iracionalne enačbe

$$\blacksquare \sqrt{2x^2+x-1} = 1-2x. \quad (3)$$

Takoj lahko opazimo, da morajo rešitve te enačbe zadoščati pogoju $2x^2+x-1 = (2x-1)(x+1) \geq 0$. Torej mora biti $x \leq -1$ ali $x \geq 1/2$. Vendar to še ni vse. Ker je leva stran enakosti (3) nenegativno število, mora biti tudi desna stran nenegativna. Torej se drugi pogoj glasi $1-2x \geq 0$ oziroma $x \leq 1/2$.

Ko smo tako določili pogoje, enakost (3) kvadriramo:

$$\blacksquare 2x^2+x-1 = 4x^2-4x+1. \quad (4)$$

Opazimo lahko, da je pogoj $2x^2+x-1 \geq 0$ nepotreben, saj za vsako realno število x , ki zadošča enakosti (4), velja tudi $2x^2+x-1 \geq 0$. Namreč, $2x^2+x-1 = 4x^2-4x+1 = (1-2x)^2 \geq 0$. Če enačbo (4) preoblikujemo, dobimo $2x^2-5x+2 = (2x-1)(x-2) = 0$. Iz tega sledi, da je $x = 1/2$ ali $x = 2$. Ker pa mora biti $x \leq 1/2$ (glej drugi pogoj), je edina rešitev prvotne enačbe $x = 1/2$. Na podoben način bi poiskali pogoje in rešili iracionalno enačbo, če bi namesto drugega korena v enačbi nastopal koren s sodim eksponentom.

PRIMER 2. Zdaj pa že znamo rešiti malo težjo iracionalno enačbo

$$\blacksquare \sqrt{x^2-3x+3} + \sqrt{x^2-36} = x-1. \quad (5)$$





Takoj lahko zapišemo pogoj $x - 1 \geq 0$ oziroma $x \geq 1$. Ob upoštevanju te omejitve za x enačbo kvadriramo:

$$\blacksquare x^2 - 3x + 3 + \sqrt{x^2 - 36} = x^2 - 2x + 1.$$

Zgornjo enakost preuredimo in dobimo $\sqrt{x^2 - 36} = x - 2$. Pred kvadriranjem te enakosti moramo zapisati drugi pogoj $x - 2 \geq 0$ oziroma $x \geq 2$. Prvi ($x \geq 1$) in drugi pogoj ($x \geq 2$) nam skupaj povesta, da mora biti $x \geq 2$. Zdaj lahko ponovno kvadriramo:

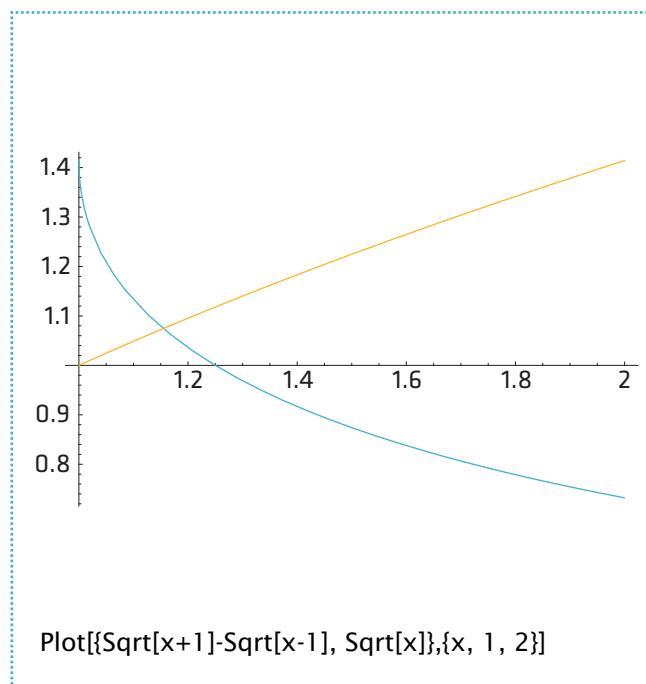
$$\blacksquare x^2 - 36 = x^2 - 4x + 4$$

oziroma $4x - 40 = 0$. Rešitev te enačbe je $x = 10$ in to je tudi rešitev prvotne enačbe (5), saj zadošča pogoju $x \geq 2$.

■ Reševanje iracionalnih enačb s pomočjo grafov funkcij

Naslednji primer nam bo pokazal, kako si lahko pri reševanju iracionalnih enačb pomagamo z grafi funkcij.

V nadaljevanju so na slikah z modro barvo narisani grafi funkcij leve strani enakosti, z rumeno barvo pa grafi funkcij desne strani enakosti. Pod vsako sliko je napisan tudi ukaz v programu Mathematica, ki nariše ustrezna grafa.



PRIMER 3. Poiskati želimo vsa realna števila x , za katera velja naslednja enakost

$$\blacksquare \sqrt{x+1} - \sqrt{x-1} = \sqrt{x}. \quad (6)$$

Narišimo v koordinatni sistem grafa funkcij

$$\blacksquare f_1(x) = \sqrt{x+1} - \sqrt{x-1} \quad \text{in} \quad g_1(x) = \sqrt{x}.$$

Iz slike lahko opazimo, da se grafa leve in desne strani enačbe (6) sekata v eni točki s pozitivno vrednostjo prve koordinate. To pomeni, da bomo imeli eno samo rešitev zgornje enačbe. Še več, ta rešitev bo pozitivno realno število.

Pri reševanju enačbe (6) bomo seveda obe strani enakosti najprej kvadrirali. Dobimo

$$\blacksquare x + 1 - 2\sqrt{(x+1)(x-1)} + x - 1 = x$$

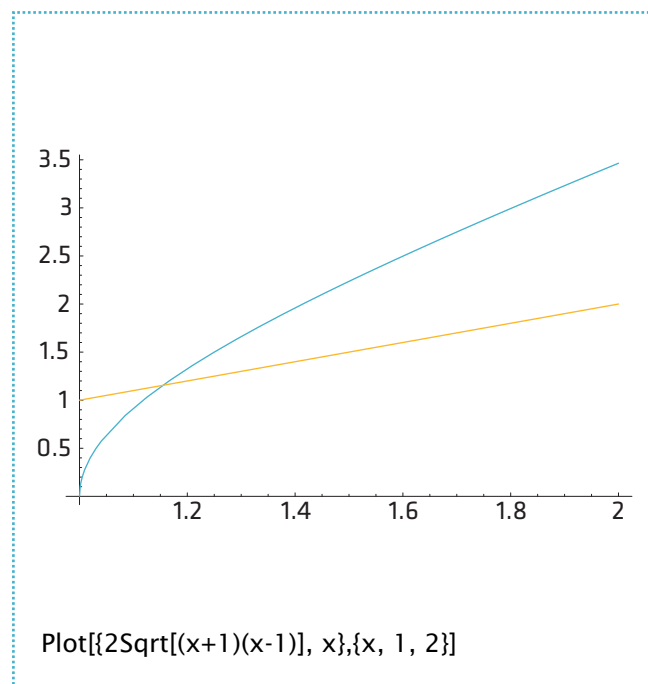
oziroma

$$\blacksquare 2\sqrt{(x+1)(x-1)} = x. \quad (7)$$

Poglejmo si grafa funkcij

$$\blacksquare f_2(x) = 2\sqrt{(x+1)(x-1)} \quad \text{in} \quad g_2(x) = x.$$

Tudi tukaj lahko opazimo, da se grafa leve in desne strani enačbe (7) sekata v eni sami točki s pozi-



tivno vrednostjo prve koordinate. Torej s kvadriranjem nismo dobili nobene dodatne rešitve oziroma je množica rešitev enačbe (7) enaka množici rešitev enačbe (6).

Na naslednjem koraku kvadriramo enakost (7), dobimo $4(x^2 - 1) = x^2$ in preuredimo

$$3x^2 = 4. \quad (8)$$

Pa narišimo v koordinatni sistem še grafa funkcij

$$f_3(x) = 3x^2 \quad \text{in} \quad g_3(x) = 4.$$

Takoj lahko opazimo, da smo dobili dve presečišči, kar pomeni, da ima enačba (8) dve različni rešitvi. Seveda, zgornjo enačbo rešita števili $2\sqrt{3}/3$ in $-2\sqrt{3}/3$. Ker pa že vemo, da v tem primeru prvotno enačbo reši pozitivno realno število, lahko takoj zapišemo, da je $x = 2\sqrt{3}/3$ edina rešitev enačbe (6). To lahko preverimo tudi z direktnim vstavljanjem v enačbo ali z določanjem pogojev, kot smo to naredili v prejšnjem poglavju.

Za konec omenimo še, da si pri risanju grafov lahko pomagamo z enostavnimi računalniškimi programi, kot so Graph, Derive, GnuPlot.

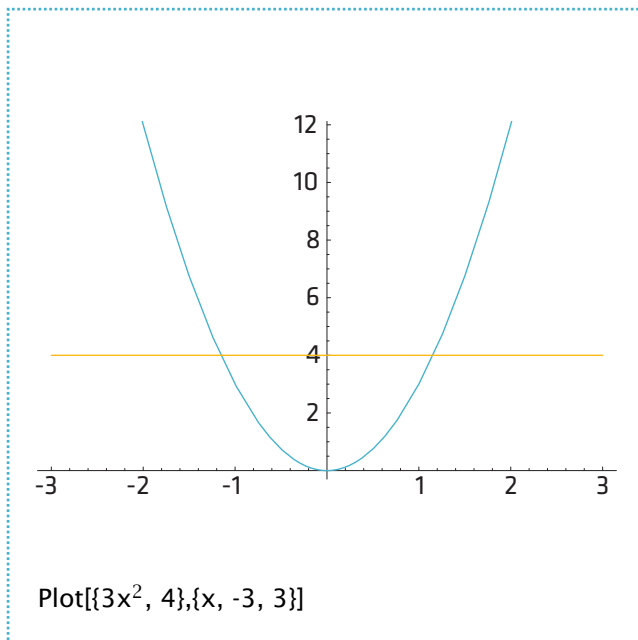
■ Za zaključek

Sami se lahko pozabavate z naslednjimi iracionalnimi enačbami:

1. $\sqrt{x} + \sqrt{x - \sqrt{1 - x}} = 1,$
2. $\sqrt{\sqrt{2x + 3} + \sqrt{4x - 3}} = \sqrt{6},$
3. $\sqrt{x}\sqrt{x} = \left(\frac{x}{2\sqrt{x}}\right)^3,$
4. $2\sqrt{5\sqrt[4]{x+1} + 4} - \sqrt{2\sqrt[4]{x+1} - 1} = \sqrt{20\sqrt[4]{x+1} + 5},$
5. $6\sqrt[3]{x-3} + \sqrt[3]{x-2} = 5\sqrt[6]{(x-2)(x-3)}.$

■ Literatura

- [1] N. Dmitrović, *Iracionalne jednadžbe i nejednadžbe*, Hrvatski matematički elektronski časopis 2 (2005), str. 1-10.
<http://web.math.hr/~mathe/dmitrovic/index.html>
- [2] F. Križanić, *Matematika 3*, DZS, Ljubljana, 1989.
- [3] P. Legiša, *Matematika: vektorji, potence in koreni, kvadratna funkcija*, DZS, Ljubljana, 1994. ✖



47. Mednarodna matematična olimpijada

☛ Če se letos poleti niste popolnoma izklopili, ste v medijih morali opaziti, da je letošnja Mednarodna matematična olimpijada potekala v Sloveniji. Glede na število udeležencev je bil to eden največjih dogodkov, kar jih je bilo organiziranih v Sloveniji in je predstavljal odlično mednarodno promocijo naše države. Da je bila celotna slika še lepša, so poskrbeli tudi naši tekmovalci, ki so dosegli odlične rezultate.

MATJAŽ BERČIČ (Gimnazija Škofja Loka) je osvojil **srebrno medaljo**, DAVID GAJSER (II. gimnazija Maribor), PETER LENDERO (ŠC Velenje - Splošna in strokovna gimnazija) in ŠPELA ŠPENKO (Gimnazija Bežigrad, Ljubljana) pa **bronaste medalje**. Uspeh naše ekipe sta s **pohvalama** dopolnila še URBAN JEZERNIK (I. gimnazija v Celju) in PRIMOŽ KOŽELJ (Gimnazija Bežigrad, Ljubljana).

Celotni slovenski ekipi čestitamo za dosežene rezultate, organizatorjem in vsem njihovim sodelavcem pa za odlično organizacijo olimpijade. ✖

Tehtanje pobarvanih lesenih kock

REŠITEV NAGRADNE NALOGE

MARIJA VENCELJ

➤ Pravilne rešitve nagradne naloge iz 6. številke 33. letnika Preseka so nam poslali: LUKA KRMPOTIČ, učenec OŠ Rogaška Slatina, JURE SENČAR iz Križevcev pri Ljutomeru, IVAN LISAC iz Kopra in NINO BAŠIČ iz Ljubljane.

Zadnja dva sta pot do rešitve tudi opisala. Ivan Lisac je dodal preprost računalniški program, s katerim si je pomagal, Nino Bašič pa je nalogo rešil z logičnim premislekom, napisal pa je tudi računalniški program, ki nas lahko privede do rešitve.

Vsi štirje prejmejo za nagrado enoletno naročnino na Presek.

Rešitev naloge

1. Ker so vse kocke narejene iz enakega lesa, imajo enako gostoto in zato lahko v pogoje 1 do 4 zastavljene naloge vstavimo namesto mas kar njihove prostornine.

Naj bo S rob srebrne kocke, Z zlate, $\check{S}$ škrlatne, R rumene, V vijolične, B bele, $\check{C}$ črne, C cinober, I indigo, O oranžne, M modre in F rob kocke fres barve. Iz pogojev 1 do 4 dobimo sistem enačb

$$\blacksquare R^3 + \check{C}^3 = Z^3 + C^3 \quad (1)$$

$$\blacksquare M^3 = F^3 + S^3 + V^3 \quad (2)$$

$$\blacksquare \check{C}^3 + O^3 + M^3 + V^3 = C^3 + Z^3 + I^3 + S^3 + B^3 + R^3 \quad (3)$$

$$\blacksquare Z^3 = I^3 + M^3 + R^3 \quad (4)$$

Sistem moramo rešiti s paroma različnimi naravnimi števili od 1 do 12.

Edina rešitev enačbe (1) je

$$\blacksquare 1^3 + 12^3 = 9^3 + 10^3,$$

od koder sklepamo, da je $R, \check{C}, Z, C \in \{1, 9, 10, 12\}$. Števila 1, 9, 10, 12 tudi ne morejo biti vrednosti drugih neznank.

Za rešitev enačbe (2) imamo tri možnosti:

$$\blacksquare 12^3 = 6^3 + 8^3 + 10^3$$

$$\blacksquare 9^3 = 1^3 + 6^3 + 8^3$$

$$\blacksquare 6^3 = 3^3 + 4^3 + 5^3$$

Ker M ne sme biti 9 ali 12, pride v poštev le tretja od navedenih možnosti. Torej je $M = 6$ in $F, S, V \in \{3, 4, 5\}$.

Ena od ostalih dveh možnosti je rešitev enačbe (4). Iz obeh sledi $I = 8$, saj so števila 1, 6 in 10 že oddana. Dodatno velja $(R, \check{C}) \in \{(1, 12), (10, 9)\}$.

Vstavimo v enačbo (3) izračunane vrednosti in upoštevajmo dobljene pogoje. Z nekaj poskušanja dobimo edino možnost za vrednosti nastopajočih neznank:

$$\blacksquare \check{C} = 12, O = 7, V = 3, C = 10, Z = 9, S = 4, B = 2, R = 1.$$

Določiti moramo še F in $\check{S}$, nezasedeni sta še števili 5 in 11. Iz pogoja za F , ki smo ga dobili iz rešitve enačbe (2), sledi $F = 5$ in od tod $\check{S} = 11$.

Če kocke postavimo po velikosti, si barve od največje proti najmanjši sledijo takole:

■ črna, škrlatna, cinober, zlata, indigo, oranžna, modra, fres, srebrna, vijolična, bela, rumena.

2. Odgovor podaja enakost

$$\blacksquare 1^3 + 2^3 + 4^3 + 8^3 + 9^3 + 12^3 = 3^3 + 5^3 + 6^3 + 7^3 + 10^3 + 11^3.$$



42. tekmovanje za Zlata Vegova priznanja

KLAVDIJA MLINŠEK

➔ Najboljši osmošolci in devetošolci s področnih tekmovanj so se v soboto, 22. aprila 2006, pomerili v sedmih regijah na državnem tekmovanju za zlato Vegovo priznanje. Nanj se po veljavnem pravilniku uvrsti 1 % vseh osmošolcev s posameznega področja in 1 % vseh devetošolcev s posameznega področja ter še učenci, ki jih na podlagi dosežkov na področnem tekmovanju izbere državna tekmovalna komisija.

Na področnem tekmovanju je sodelovalo 4826 učencev, od teh pa se jih je 638 uvrstilo na državno tekmovanje. Podelili smo 307 zlatih priznanj v osmem in devetem razredu, prejeli pa so jih učenci, ki so v osmem razredu prejeli najmanj 25 točk od 50 možnih in v devetem razredu najmanj 21 točk od 50 možnih. Nagrade so prejeli naslednji učenci:

1. NAGRADA

■ 8. razred

- NEJC JANŠA, OŠ Žirovnica

■ 9. razred

- TOMAŽ STEPIŠNIK PERDIH, OŠ Šmarje pri Jelšah

Najbolje uvrščene devetošolce smo v juniju povabili na tedensko poletno šolo matematike v Bohinj. Najbolje uvrščene tekmovalce v Mednarodnem matematičnem kenguruju iz 7., 8. in 9. razreda pa smo v začetku junija peljali na celodnevni izlet v okolico Salzburga.

2. NAGRADA

■ 8. razred

- MATEJA HRAST, OŠ Franceta Bevka, Tolmin
- KLEMEN KLOBOVES, OŠ Škofja Loka - Mesto
- NINA TROHA, OŠ Idrija

■ 9. razred

- SAMO KRALJ, OŠ Loka, Črnomelj
- JAN OGRIN, OŠ Karla Destovnika Kajuha, Ljubljana

3. NAGRADA

■ 8. razred

- LUKA KRMPOTIČ, VIZ I. OŠ Rogaška Slatina
- ŽIGA MARKUŠ, OŠ Janka Padežnika, Maribor
- KLEMEN ZAJC, OŠ Cerkno
- POLONA GAMS, OŠ Log - Dragomer
- ERIK GRABLJEVEC, OŠ Stična
- NIK JAZBINŠEK, OŠ Valentina Vodnika, Ljubljana
- KAJA SAJKO, VIZ II. OŠ Rogaška Slatina
- JAN SIMONČIČ, OŠ Majde Vrhovnik, Ljubljana
- BERNARD TRČEK, OŠ Horjul

■ 9. razred

- JADRAN KOTNIK, OŠ Šmartno pri Slovenj Gradcu
- PETER KOŽELJ, OŠ Majde Vrhovnik, Ljubljana
- ŠPELA POHLEVEN, OŠ Železniki
- JAN RAVNIK, OŠ Vič, Ljubljana
- ANJA ŠTUHEC, OŠ Trzin
- KATRA KOMAN, OŠ Cvetka Golarja, Škofja Loka
- TIM VODOVNIK, OŠ Frana Roša, Celje



Žabice

JANEZ STRNAD

Žabica: odboj vrženega kamna od vodne gladine.

Slovar slovenskega knjižnega jezika

➔ Kdo še ni z zanimanjem opazoval odbojev kamnov od vodne gladine, če kamnov že sam ni metal? Kamen je za metanje tem bolj pripraven, čim bolj je ploščat. Številni prispevki na spletu kažejo, da zbuja žabice veliko zanimanja. Pri tekmovanjih je dovoljeno uporabljati le kamne iz narave. Vodijske podatke o svetovnem rekordu, ki ga navaja tudi Guinnessova knjiga rekordov. Ta čas drži rekord Američan Kurt Steiner s štiridesetimi odboji. Posnetek njegovih metov si lahko ogledate na naslovu pastoneskipping.com/steiner.htm.

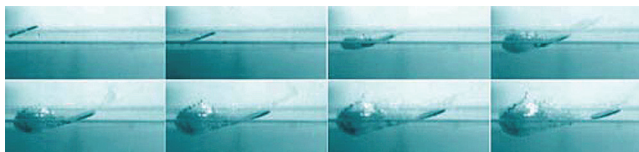
Fizikalno ozadje metanja žabic sta v revijah opisala Lyderic Bocquet z univerze Lyon-1 v Villeurbanne in Christopher Clanet z Inštituta za neravnostne pojave v Marseillu s sodelavci. Izdelali so napravo, ki meče aluminijeve ploščice z maso 15 g s hitrostjo do 10 m/s pod določenim kotom. Gibanju ploščice sledijo s hitro televizijsko snemalno kamero (slika 1, 2).

Hitrost ploščice mora preseči nekaj metrov na sekundo, da se ploščica odbije na gladini vode. Ploščica se mora okoli simetrijske osi tudi dovolj hitro vrteti, da kot vrtavka ohrani svojo lego v prostoru. Zato naprava ploščico še zavrti. Metalec zavrti kamen s sunkom prstov proti koncu meta.

Ploščica se giblje po paraboli in trči z gladino vode. Voda med trkom na ploščico deluje navzgor, da se ploščica odbije. Potem se ploščica znova giblje po paraboli, se odbije na gladini in pojav se ponovi. Vodoravna komponenta hitrosti ploščice se med trkom ne zmanjša izrazito, bolj opazno se pri vsakem trku zmanjša višina, do katere se dvigne ploščica nad gladino. Nazadnje se ploščica ne dvigne več iz vode



Slika 1. Stroboskopska fotografija ploščice, ki se je na začetku gibanja štirikrat odbila od gladine vode.



Slika 2. Osem sličic, ki si sledijo v časovnih razmikih po 6,5 tisočin sekunde, kaže trk ploščice z maso 15 g pri hitrosti 3,5 m/s z gladino vode. Ploščica se je dotikala gladine 32 tisočin sekunde, kar ustreza približno četrtini ocene za čas med dvema odbojema. Slika kaže, da ploščica pri gibanju navzdol odrine vodo, ki se nato dvigne v pljusk. Sliki sta vzeti iz članka v Physics World.

in potone. Z opazovanji so ugotovili, da število odbojev približno linearno narašča z začetno hitrostjo (slika 3). Odvisno je tudi od oblike in mase ploščice ter od kota, pod katerim ploščico vržemo. Pri hitrosti 10 m/s so dosegli 20 odbojev, tako da je bila za 40 odbojev potrebna po oceni začetna hitrost 20 m/s.

Privoščimo si nekaj ocen. Ploščico vrzimo z nagibom β proti vodoravnici. Voda deluje na ploščico s prečno silo F_p , ki jo razstavimo na vodoravno $-F_p \sin \beta$ in na navpično komponento $F_p \cos \beta$ (slika 4). V smeri ploščice v nasprotni smeri gibanja deluje voda z vzdolžno silo F_v , ki jo razstavimo na vodoravno $-F_v \cos \beta$ in navpično komponento $-F_v \sin \beta$. Sestavimo vodoravni komponenti v smeri osi x , ki jo položimo v nemoteno gladino vode $F_x = -F_p \sin \beta - F_v \cos \beta$, in navpični komponenti v smeri osi z $F_z = F_p \cos \beta - F_v \sin \beta$.

Hitrost ploščice glede na vodo je tolikšna, da velja kvadratni zakon. Sila vode na ploščico je sorazmerna z gostoto kinetične energije $\rho v^2/2$ in z delom ploščine S , na katerem se ploščica dotika vode. Pri tem je ρ gostota vode in $v^2 = v_x^2 + v_z^2$ kvadrat velikosti hitrosti vode glede na ploščico. Tako izrazimo komponenti sile vode na ploščico kot

$$\begin{aligned} F_x &= -\frac{1}{2}\rho v^2 S(c_p \sin \beta + c_v \cos \beta) = -\frac{1}{2}\rho v^2 S c_x, \\ F_z &= \frac{1}{2}\rho v^2 S(c_p \cos \beta - c_v \sin \beta) = \frac{1}{2}\rho v^2 S c_z. \end{aligned}$$

Številski koeficienta c_p in c_v se ne razlikujeta znatno od 1, vpeljali pa smo še njuni kombinaciji $c_x = c_p \sin \beta + c_v \cos \beta$ in $c_z = c_p \cos \beta - c_v \sin \beta$. Komponenti sile F_x in F_z se pojavita v drugem Newtonovem zakonu za gibanje težišča ploščice:

$$m a_x = F_x \quad \text{in} \quad m a_z = -m g + F_z.$$

a_x in a_z sta komponenti pospeška težišča v vodoravni in navpični smeri, m je masa ploščice in g težni pospešek. Kvadrat velikosti hitrosti $v^2 = v_x^2 + v_z^2$

poveže enačbi in zaplete reševanje.

Nalogo si lahko olajšamo s približkom, v katerem privzamemo, da je komponenta hitrosti v vodoravni smeri v_x veliko večja od komponente v navpični smeri v_z . S tem enačbi prenehata biti povezani in lahko rešimo drugo neodvisno od prve. Za začetek se omejimo na kvadratno ploščico s stranico b , tako da je v stiku z vodo del ploščine $S = -bz/\sin \beta$, $z < 0$. Drugo enačbo potem lahko zapišemo v obliki

$$a_z + \omega_0^2 z = -g$$

z $\omega_0^2 = \rho v_{x0}^2 c_z b / (2m \sin \beta)$. Enačba opisuje sinusno nihanje s krožno frekvenco ω_0 kot približek za gibanje po odsekih parabol. Začetnemu odmiku $z(t=0) = 0$ in začetni hitrosti $dz/dt(t=0) = v_{z0}$ ustreza rešitev

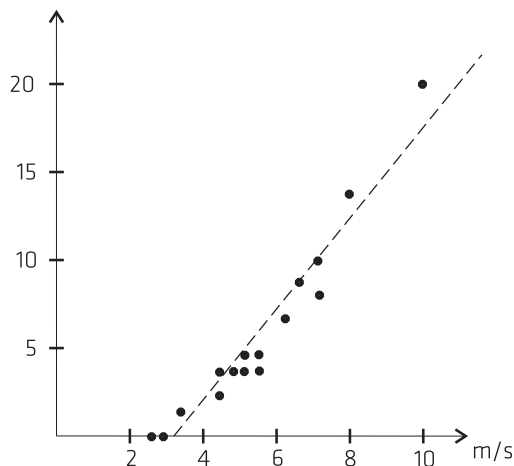
$$z = (g/\omega_0^2)(\cos \omega_0 t - 1) + (v_{z0}/\omega_0) \sin \omega_0 t.$$

V najnižji legi se ploščica dotika vode in v navpični smeri za trenutek obmiruje, ko je $dz/dt = 0$. Tedaj je

$$-z_0 = (g/\omega_0^2)(1 + \sqrt{1 + (\omega_0 v_{z0}/g)^2}).$$

Med zaporednima odbojema poteče čas $t_0 = 2\pi/\omega_0$, v katerem ploščica prepotuje razdaljo $l = t_0 v_{x0}$. Z ocenami $v_{x0} = 1$ m/s, $c_z = 1$, $b = 0,1$ m, $m = 0,1$ kg in $\beta = 10^\circ$ dobimo za ω_0 oceno 54 s^{-1} . Iz tega izhaja za čas med zaporednima odbojema ocena $t_0 = 0,12$ s in za razdaljo $l = 0,12$ m.





Slika 3. Število odbojev ploščice narašča približno linearno z začetno hitrostjo. Poskusi kažejo, da najmanjša potrebna začetna hitrost presega 3 m/s, kar je večje od obeh preprostih ocen. Slika je vzeta iz članka v *Journal of Fluid Mechanics*.

vsem teža ploščice. Kinetična energija ploščice se pri trku zmanjša za delo vzdolžne sile na poti med zaporednima trkoma l :

$$\frac{1}{2}mv_x^2 - \frac{1}{2}mv_{x0}^2 = -(c_x/c_z)mgl.$$

Veljati mora $v_{x0} > \sqrt{2glc_x/c_z}$. Za prvo silo uporabimo oceno $c_x/c_z \approx (\sin 10^\circ + \cos 10^\circ)/(\cos 10^\circ - \sin 10^\circ) = 1,4$ in z $l = 0,12$ m dobimo nekoliko večjo mejno hitrost 2 m/s.

S pojavi take vrste je mogoče raziskati podrobnosti pri trku hitrih teles z gladino vode. Ti pojavi imajo, žal, predvsem vojaški pomen, na primer pri raznih bombah in torpedih.

Bralec lahko najde več podatkov v člankih:

Literatura

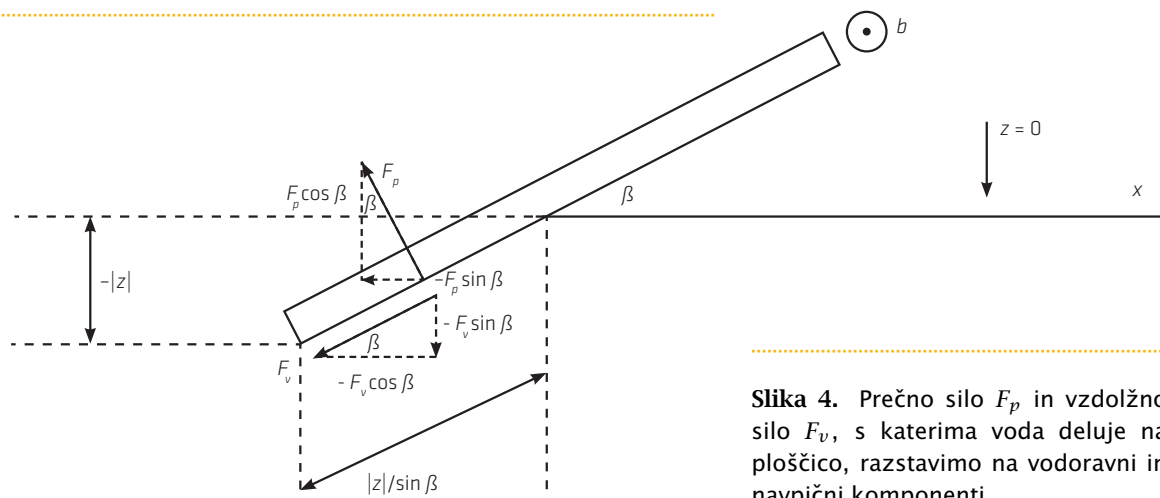
- [1] L. Bocquet, *The physics of stone skipping*, American Journal of Physics **71** (2003), str. 150-155.
- [2] Ch. Clanet, F. Hersen, L. Bocquet, *Secrets of successful stone-skipping*, Nature **427** (2004), str. 29.
- [3] L. Rosellini, F. Hersen, Ch. Clanet, L. Bocquet, *Skipping stones*, Journal of Fluid Mechanics **543** (2005), str. 137-146.
- [4] L. Boquet, Ch. Clanet, *The mystery of the skipping stone*, Physics World **19**(2) (2006), str. 29-31. ☒

Zahteva, da se vsa ploščica ne dotakne gladine, $|z_0| < b \sin \beta$, pripelje po daljšem računanju do spodnje meje za komponento hitrosti v vodoravni smeri:

$$v_{z0} > \sqrt{4mg/c_z \rho b^2 / \sqrt{1 - m \tan^2 \gamma_0 / b^3 c_z \rho \sin \beta}}.$$

Pri tem je $\tan \gamma_0 = v_{z0}/v_{x0}$. Z ocenami $m = 0,1$ kg, $b = 0,1$ m, $c_z = 1$, $\rho = 1000$ kg/m³ in $\beta = \gamma = 10^\circ$ dobimo za hitrost nekaj manj kot 1 m/s. Oblika izidov ostane v veljavi tudi pri krožni ploščici, čeprav je pri njej izraz za del ploščine, na katerem se ploščica dotika vode, bolj zapleten.

Ploščica ob trku z gladino zaradi vodoravne sile F_x izgubi del kinetične energije, ki je naložena v njeno gibanje v vodoravni smeri. Do ocene se dokoplremo z Newtonovim zakonom za vodoravno smer. Ugotovimo, da je vodoravna sila vode F_x z navpično silo F_z povezana takole $F_x = c_x F_z / c_z$. Navpično komponento sile v Newtonovem zakonu pa določa pred-



Slika 4. Prečno silo F_p in vzdolžno silo F_v , s katerima voda deluje na ploščico, razstavimo na vodoravni in navpični komponenti.

Vetromobil

BRANISLAV ČABRIĆ, prevod PETAR PAVEŠIĆ

❖ Vsakdanje izkušnje kažejo, da se ladjica, ki jo prosto izpostavimo vetru, giblje v smeri vetra. Če želimo, da se ladjica giblje proti vetru, potrebuje notranji pogon, ki bo preko propelerja in vode deloval na ladjico v smeri, nasprotni sili vetra. Ali je mogoče, da se brez tovrstnega pogona ladjica giblje proti vetru in pri tem uporablja samo energijo vetra? Vprašanje je navidez nesmiselno, saj se zdi, da nasprotuje fizikalnim zakonom. Kljub temu je gibanje ladjice proti vetru pri določenih pogojih mogoče.

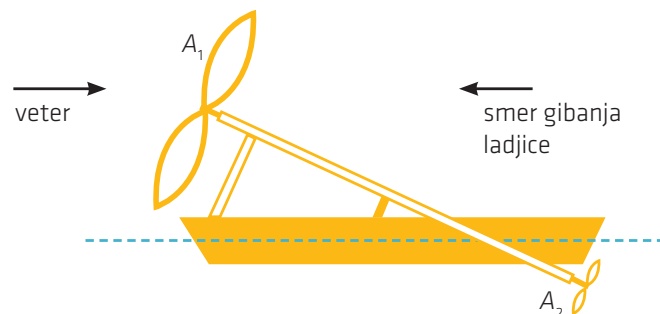
Spomnimo se najprej, da jadrnice lahko plujejo proti vetru, čeprav ne naravnost v veter, temveč pod določenim kotom. Pri tem izrabljajo za prenos energije vetra vodo in kobilico. Podobno velja tudi za jadrnice na snegu.

Leta 1975 je S. Martin [1] opisal ladjico, ki lahko pluje naravnost proti smeri, iz katere piha veter. B. L. Blackford [2] pa je leta 1978 razložil fizikalne osnove, na katerih sloni gibanje ladjice. Ladjico so uspešno zgradili in preskusili njene lastnosti (slika 1).

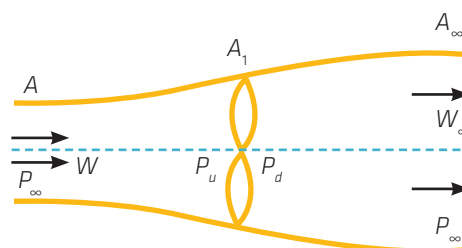
Gibanje ladjice naravnost proti vetru lahko razložimo na podlagi treh osnovnih načel mehanike: a) ohranitve energije, b) ohranitve gibalne količine in c) ohranitve mase [3]. Na sliki 2 je prikazan propeler (vetrница) v zraku pri hitrosti vetra W . Naj bo ploščina lika, ki ga med vrtenjem pokrije propeler, enaka A_1 , preseka, ki ju oklepajo ustrezne tokovnice daleč pred in za propelerjem, pa A in A_∞ .

Tlak, daleč od propelerja, je P_∞ , neposredno pred in za propelerjem pa P_u in P_d . Hitrost vetra daleč pred propelerjem je W , za propelerjem je W_∞ , na propelerju samem pa $W(1 - a)$, kjer je $0 < a < 1$ faktor zmanjšanja hitrosti vetra. Na podlagi zakona o ohranitvi mase sledi

$$\blacksquare AW = A_1 W(1 - a) = A_\infty W_\infty. \quad (1)$$



Slika 1. Skica ladjice, ki se lahko giblje naravnost proti vetru. Na isti osi sta dva propelerja z efektivno ploščino A_1 v zraku in A_2 v vodi.



Slika 2. K izpeljavi formule za moč, dobljene iz vetra.

Z uporabo Bernoullijeve enačbe za gibanje zraka ($P + \rho W^2/2 = \text{konst.}$) za področje pred in za propelerjem dobimo

$$\blacksquare P_\infty + \frac{1}{2}\rho_1 W^2 = P_u + \frac{1}{2}\rho_1 |W(1 - a)|^2 \quad (2)$$

$$\blacksquare P_\infty + \frac{1}{2}\rho_1 W_\infty^2 = P_d + \frac{1}{2}\rho_1 |W(1 - a)|^2, \quad (3)$$

kjer je ρ_1 gostota zraka. Iz enačb (2) in (3) sledi enačba za razliko pritiskov:

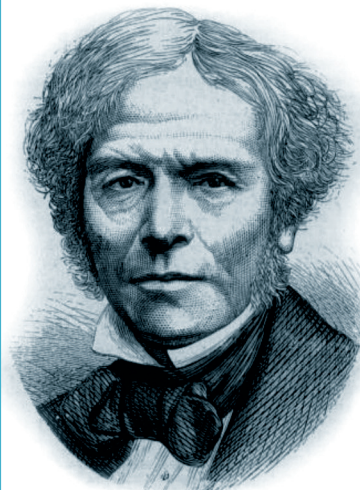
$$\blacksquare \Delta P = P_u - P_d = \frac{1}{2}\rho_1 (W^2 - W_\infty^2),$$

iz nje pa enačba za silo, s katero veter deluje na propeler:

$$\blacksquare F_w = A_1 \Delta P = \frac{1}{2}\rho_1 A_1 (W^2 - W_\infty^2). \quad (4)$$



A map of Cuba is shown with the word "HAVANA" written across the northern part of the island. A large black question mark is placed on the eastern side of the island.



RAZPIS

Med poslanimi praviilnimi rešitvami bomo izžrebali 3 reševalce, ki bodo prejeli knjigo **Nova zlata doba matematike**.

Zaporedne številke, ki so razporejene v križanki, določajo nagradno geslo, ki ga napišite na priloženo dopisnico. Ne pozabite nanjo napisati tudi svojega naslova. Dopisnico nam pošljite do 15. oktobra 2006.

$$\blacksquare \quad F_w = \rho_l A W^2 - \rho_l A_\infty W_\infty^2. \quad (5)$$

$$\blacksquare F_w = 2\rho_1 A_1 W^2 a(1-a). \quad (6)$$

$$\blacksquare \quad P_w = F_w W(1 - a) = 2\rho_1 A_1 a(1 - a)^2 W^3. \quad (7)$$

Iz pogoja, da je moč maksimalna, tj., $\partial P_W / \partial a = 0$, dobimo optimalno vrednost parametra a , $a_{opt} = 1/3$. Za izkoristek pa dobimo

kjer je P_0 moč vetra pred propelerjem. V praksi, pri zelo dobro narejenih propelerjih, lahko dosežemo okoli 60 % do 70 % vrednosti 16/27.

- [1] S. Martin, Scientific American **233**(12) (1975), str. 125.
- [2] B. L. Blackford, *The physics of a push-me pull-you boat*, American Journal of Physics **46**(10) (1978), str. 1004–1006.
- [3] F. Kraš, A. Rubčić, *Bespogonsko gibanje vozila direktno protiv struje vjetra ili vode*, Mat. fiz. list **34**(1) (1983-84), str. 10–14.

Za nagradno križanko iz prejšnje številke smo prejeli 11 pravih rešitev. Nagradno geslo se je glasilo **Računalništvo**. Žreb je nagrade razdelil med naslednje nagrajence:

Nagrajenci so razpisane nagrade prejeli po pošti.

[illegible]

Ali teče, ali je trdno?

MOJCA ČEPIČ

☛ Za večino snovi, s katerimi se srečujemo v vsakdanjem življenju, lahko brez pretiranega miselnega napora povemo, ali tečejo ali ne. Nekatere snovi, npr. mast, vosek, ali voda, celo spremenijo svoje "tekočnostne" lastnosti in tečejo pri višjih temperaturah in so trdne pri nižjih. Vendar lahko v kuhinji najdemo mnoge snovi, ki jih ne moremo enostavno opredeliti. Ena od njih je gotovo majoneza. S počasnim iztiskanjem iz tube lahko oblikujemo okraske, ki ostanejo nespremenjeni in ne stečejo tudi nekaj dni, a vendar lahko majonezo z žlico enostavno premešamo in je nikakor ne bi mogli uvrstiti med trdne snovi.

Kuhinja pa skriva še druga presenečenja. Poskusite se poigrati z mešanico, ki jo naredimo na naslednji način.



■ Potrebujemo

- približno 4 velike žlice škrobne moke (npr. Gustin),
- kozarček vode,
- žličko za mešanje,
- gumijaste rokavice,
- delovni prostor, ki ga ni težko pomiti.

Manjši kozarček (kak dl, drugače boste potrebovali preveč škrobne moke) napolnimo z vodo do polovice. V vodo postopoma dosipamo škrobno moko in POČASI (poudarek je na POČASI) mešamo z žličko, da razbijemo grudice škrobne moke. Mešati POČASI pomeni, da v kozarčku z vilico ali žličko enkrat zakrožimo v približno dveh sekundah. V zmes dodamo toliko škrobne moke, da je zmes po videzu podobna nestepeni sladki smetani. Pri POČASNEM mešanju naj se zmes zdi nekoliko gostejša od sladke smetane. Sedaj naj se poizkušanje začne.

Poskusi!

- Poskusite žličko sunkovito potegniti iz kozarca!
- Poskusite žličko sunkovito potisniti v zmes!
- Potolcite z žličko po površini zmesi!
- Z žličko zajemite nekoliko zmesi in jo dvignite nad kozarček! Opazujte curek zmesi, ki odteka z žličke!

Natakните si gumijasto rokavico in s prsti zajemite nekoliko zmesi! Poskusite jo stisniti, zgnesti!

Opišite, kaj se je dogajalo pri poskusih! Posnemite fotografije svojih poizkušanj in jih pošljite na Presekov elektronski naslov. Postavite nam vprašanja, poskusili bomo odgovoriti nanje.

V naslednji številki pa preberite še nekaj več o škrobovi mešanici in "čudnih" lastnostih še nekaterih drugih snovi iz kuhinje. ☘

26. državno tekmovanje iz fizike za Stefanova priznanja

SAŠA KOŽUH

➔ Oddelek za fiziko Pedagoške fakultete v Mariboru, Oddelek za fiziko Pedagoške fakultete v Ljubljani, Društvo matematikov, fizikov in astronomov Slovenije in Zavod Republike Slovenije za šolstvo so bili organizatorji 26. tekmovanja iz fizike za osnovnošolce. V predavalnicah in laboratorijih Pedagoške fakultete v Mariboru in Pedagoške fakultete v Ljubljani se je 1. aprila 2006 na državnem tekmovanju pomerilo 138 učencev iz osmih razredov in 140 učencev iz devetih razredov. Tekmovalci so reševali tri teoretične in dve eksperimentalni nalogi. Naloge za področno in državno tekmovanje sta pripravila Zlatko Bradač iz Pedagoške fakultete v Mariboru in Mirko Cvahte iz Zavoda RS za šolstvo, pri organizaciji sta sodelovala Saša Kožuh in Jelka Sakelšek, za računalniško podporo tekmovanja je skrbel Matjaž Željko.

Na državnem tekmovanju so v kategoriji osmih razredov prvo nagrado osvojili trije tekmovalci, drugo nagrado en tekmovalec in tretjo nagrado pet tekmovalcev. Zlato Stefanovo priznanje je osvojilo 95 tekmovalcev. V kategoriji 9. razredov sta prvo na-

grado osvojila dva tekmovalca, drugo nagrado štirje tekmovalci in tretjo nagrado štirje tekmovalci. Zlato Stefanovo priznanje je osvojilo 96 tekmovalcev. Na spletni strani www.dmfa.si so objavljeni podrobnejši rezultati.

Pred državnim tekmovanjem je bilo na dvanajstih mestih po vsej Sloveniji 21. marca 2006 organizirano področno tekmovanje. Skupaj je tekmovalo 797 učencev v osmem razredu in 865 učencev v devetem razredu, skupaj 1662 učencev. Podeljenih je bilo 1372 srebrnih Stefanovih priznanj. Tekmovalci so na področnih tekmovanjih reševali 5 teoretičnih nalog.

Šolskega tekmovanja 7. marca 2006 se je udeležilo preko 9.000 učencev. Na šolskem tekmovanju so tekmovalci reševali 5 teoretičnih nalog.

Letos je tekmovanje prvič potekalo po novem načinu: učenci so na področnem in državnem tekmovanju tekmovali posamično, doslej so 25 let tekmovali v dvojicah. Zaradi večjega števila sprejetih tekmovalcev na državnem tekmovanju je bilo to tekmovanje letos prvič hkrati v Mariboru in Ljubljani.

37. Mednarodna fizikalna olimpijada

➔ Letos je Mednarodna fizikalna olimpijada potekala v daljnem in vročem Singapurju.

Tudi letos so se naši tekmovalci zelo dobro odrezali, MATIJA VIDMAR (Gimnazija Bežigrad, Ljubljana) je osvojil **bronasto medaljo**, MATJAŽ GOMILŠEK (II. gimnazija Maribor), ŽIGA PAVLIN (Gimnazija Bežigrad, Ljubljana), VASJA SUSIČ (Gimnazija Bežigrad, Ljubljana) in GAŠPER ZADNIK (Gimnazija Vič, Ljubljana) pa **pohvale**.

Celotni slovenski ekipi čestitamo za dosežene rezultate. ✖

1. NAGRADA

■ 8. razred

- PAVEL KOS, OŠ Koseze, Ljubljana
- TADEJ NOVAK, OŠ Orehek
- BLAŽ REPAS, Prva OŠ Slovenj Gradec

■ 9. razred

- FILIP KOZARSKI, OŠ Preserje pri Radomljah
- PETER KOŽELJ, OŠ Majde Vrhovnik, Ljubljana

2. NAGRADA

■ 8. razred

- TINA GRABNAR, OŠ Bojana Iliča, Maribor

■ 9. razred

- BLAŽ KNAVS, OŠ Sava Kladnika, Sevnica
- JURIJ KRAJČIČ, OŠ in vrtec Škofljica
- ŽIGA AVSEC, OŠ Gornja Radgona
- JOŠT STERGAR, OŠ Valentina Vodnika, Ljubljana

3. NAGRADA

■ 8. razred

- REBEKA JEREB, OŠ Škofja Loka - Mesto
- KLEMEN KLOBOVES, OŠ Škofja Loka - Mesto
- MAJA PETEK, OŠ Franceta Prešerna, Maribor
- NINA TROHA, OŠ Idrija
- ALEŠ VIGALI, OŠ II Murska Sobota

■ 9. razred

- AJDA KOŠIR, OŠ Naklo
- DAMJAN LAŠIČ JURKOVIČ OŠ T. Čufarja, Ljubljana
- MATIJA OBLAK, OŠ Ivana Tavčarja, Gorenja vas
- JAN OGRIN, OŠ Karla Destovnika Kajuha, Ljubljana

VEČ NA www.dmfa.si



Svetlobno onesnaženje

PRVI DEL

ANDREJ GUŠTIN

➔ Od babic in dedkov pogosto slišimo o dobrih starih časih. Pogosto pripovedujejo tudi o tem, kako so kot otroci v poletnih nočeh ležali pod jasnim nebom in občudovali migetave zvezde ter Rimsko cesto med njimi. Zvezde so se jim včasih zdele tako blizu, da bi jih lahko prijeli. Menda pa niti zvezdnato nebo ni več tako kot nekoč. Naši stari starši se v tem primeru ne motijo. Množica luči, ki se ob mraku prižgejo na naših cestah, ulicah, dvoriščih in reklamnih napisih, je kriva, da vidimo vse manj zvezd. Temu pravimo svetlobno onesnaženje, ki je za astronomijo zelo velika nadloga.

■ Vse manj zvezd

Svetlobno onesnaženje je poenostavljeno povedano povečana svetlost neba zaradi umetne razsvetljave. Svetloba iz svetilk, ki se širi po ozračju, se deloma sipa na njegovih sestavinah—molekulah, pršnih delcih, vlagi. Sipani del ne pobegne v vesolje, temveč se vrne nazaj proti tlorisu in nebo ni videti "črno". Pojav sipanja svetlobe v ozračju najlepše spoznamo z baterijsko svetilko, ko v vlažni noči z njo posvetimo v nebo. Pojavi se dokaj svetel snop svetlobe in se zdi, kot bi bila naša svetilka ročaj dolge svetleče palice. Podobno se od vsake luči, ki stoji na planem, delež svetlobe razprši v nebo. O posledicah tega se lahko prav enostavno prepričamo. Če živimo v kraju z obsežnejšo javno razsvetljavo in se v jasni noči brez Lune ozremo v nebo, vidimo le peščico najsvetlejših zvezd in planete. Šibkejših zvezd ni mogoče videti, saj je ozadje neba svetlejše od njih. Če se odpravimo v kak bolj oddaljen kraj daleč od umetne razsvetljave, vidimo mnogo več zvezd, načeloma bi jih lahko prešteli ne-

kaj več kot 2000. Žalostno je, da pri nas ni kraja, kjer bi lahko opazovali s svetlobnim onesnaženjem neokrnjeno nebo.

Svetlobno onesnaženje jezi predvsem astronome, saj zaradi njega ne morejo opazovati zelo šibkih nebesnih teles. Observatorije sicer postavljajo daleč od mest in večjih naselij, toda v Sloveniji moteča umetna svetloba seže v še tako oddaljen kotiček. Resne raziskave so pokazale še eno žalostno posledico razsvetljave. Ta namreč vpliva na življenje nočnih živali. V nekaterih primerih tako drastično, da ima za posledico izumiranje posamezne vrste.

■ Neekološko osvetljevanje

Nočna razsvetljava kaže na standard in razvitost družbe. Danes si ne moremo niti zamišljati, da bi živeli v mestih brez luči, se sprehajali po temačnih ulicah in podobno. Vprašamo pa se lahko, ali je razsvetljava smotrno urejena. Ali mogoče po nepotrebnem



Slika 1. Nebo nad astronomskim observatorijem Golovec v neposredni bližini Ljubljane je zaradi mestnih luči tako svetlo, da je vidna le peščica najsvetlejših zvezd. Foto: Pobuda za temno nebo.

ne izgubljam preveč svetlobe v nebo? V zadnjih letih se je razsvetljava po Sloveniji močno razmahnila. Čeprav ni nikjer zbranih natančnih podatkov o številu javnih luči, ocene kažejo, da se pri nas vsako noč prižge približno 250.000 svetilk. To je po številu na prebivalca približno 20 odstotkov več kot v nekaterih najbolj razvitih evropskih državah. Pri nas se je v zadnjem času uveljavila logika, da moramo osvetliti prav vse. Glavna težava je ta, da luči znaten delež svetlobe pošiljajo naravnost v nebo, kar predstavlja čisto izgubo in bistven prispevek k svetlobnemu onesnaženju neba.

Svetilke javne razsvetljave delimo v tri vrste: nezasenčene, delno zasenčene in popolnoma zasenčene, tako imenovane ekološke svetilke. Že na osnovi enostavne logike je okoljsko in drugače najmanj sprejemljiva nezasenčena svetilka, katere glavna predstavnica je okrogla buča. Ta navzgor pošlje polovico svetlobe. Če bi to polovico svetlobe preusmerili navzdol, bi za enako osvetljenost tal zadoščala polovico

šibkejša žarnica. Delno zasenčene svetilke so nekoliko boljše, saj oddajajo v nebo le nekaj odstotkov celotne emisije. Te tudi prevladujejo v populaciji svetilk javne razsvetljave v Sloveniji. Prepoznamo jih po tem, da so na vrhu zastrte, spodnji del pa je zaprt z izbočenim steklom. V steklu se svetloba lomi in kljub zgornjemu senčilu se je v nebo preusmeri do 20 odstotkov. Navidez majhna izguba pa se pri velikem številu tovrstnih svetilk pretvori v velike številke. Najbolj sprejemljiva je popolnoma zasenčena svetilka, ki svetlobe ne seva nad vodoravnico in na širše okolje vpliva le preko odboja svetlobe od tal (običajno med 5 in 10 odstotki izseva). Oblikovana je tako, da ima zgoraj senčilo, spodaj pa ravno steklo. Delež ekoloških svetilk v Sloveniji je majhen in ne dosega 10 odstotkov.

Pri izgubah svetlobe v nebo moramo upoštevati še nagib svetilk. Tudi popolnoma zasenčena svetilka, ki je postavljena pod kotom glede na vodoravnico, bo določen delež svetlobe brez potrebe poslala v





Slika 2. Zaradi neprimerne javne razsvetljave je nočno nebo nad Slovenijo močno svetlobno onesnaženo tudi daleč od večjih naselij. Foto: Pobuda za temno nebo.

→ nebo. Posebno moteči so reflektorji in druga svetila za osvetljevanje stavb, cerkva in spomenikov. Večina teh je pri nas postavljena tako, da objekt osvetljuje od spodaj navzgor, pri čemer močni svetlobni snopi sijejo mimo objektov v nebo. Take svetlobne stožce lahko vidimo tudi več deset kilometrov daleč.

■ Spremljanje svetlobnega onesnaženja

V Sloveniji je skupina astronomov in drugih državljanov, ki so zaskrbljeni zaradi naraščajočega svetlobnega onesnaženja našega nočnega neba, organizirala POBUDO ZA TEMNO NEBO. Namen pobude je opozoriti strokovno in širšo javnost na problem svetlobnega onesnaženja in njegov negativen vpliv na astronomska opazovanja in okolje nasploh ter doseči zakonsko ureditev, ki bi omejevala onesnaženje na razumno mero. Člani pobude skrbijo tudi za stalno merjenje svetlobnega onesnaženja. Leta 2005 so člani Pobude pričeli z rednim snemanjem neba iz

več lokacij po Sloveniji. S standardizirano opremo dokumentirajo stanje svetlobnega onesnaženja neba nad obstoječimi astronomskimi observatoriji ter na lokacijah, kjer bi se zaradi relativno temnega neba še lahko izvajala astronomska opazovanja. Meritve kažejo, da se je kvaliteta nočnega neba nad Slovenijo v zadnjem desetletju močno poslabšala. Celo nad najbolj oddaljenimi in redko poseljenimi področji zahodne in južne Slovenije je ponoči nebo presemetljivo svetlo. Dejavnosti pobude in številne koristne informacije o svetlobnem onesnaženju dobite na spletnem naslovu www.temnonebo.org.

V prihodnji številki Preseka bomo spoznali, kako je mogoče zmanjšati svetlobno onesnaženje in kako ga z enostavnim astronomskim opazovanjem ozvezdja Orion meriti. ☒

Diffie-Hellmanov dogovor o ključu

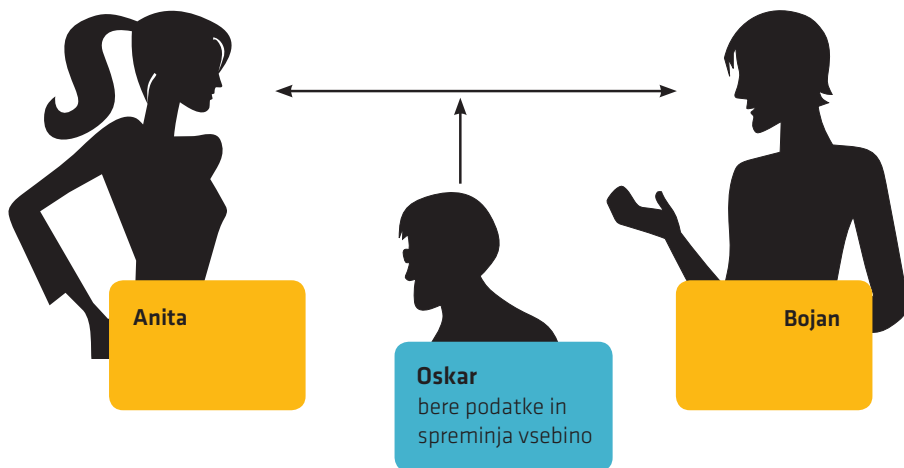
ALEKSANDAR JURIŠIĆ

➔ Ali je mogoče, da se dve osebi, ki se želita pogovarjati po javnem kanalu (npr. po telefonu ali na medmrežju), preko njega dogovorita o skrivnem ključu?

Le-tega naj bi poznali samo oni dve in ga uporabili za šifriranje svojih pogovorov. Če sta se že prej srečali na štiri oči, potem bi se gotovo lahko spomnili česa, kar je skupno samo njima ter na osnovi tega sestavili skrivni ključ. Dovolj bi bilo že, da bi se npr. spomnili knjige, ki sta jo takrat prebirali, in si izbrali za relativno varno geslo npr. deveti odstavek v tretjem poglavju. Četudi bi prisluškovalec vedel, da gre za deveti odstavek v tretjem poglavju, nikakor ne bi mogel ugotoviti, za katero knjigo gre. Tako pridobljena informacija mu brez knjige ne bi bila v kdo ve kakšno pomoč. Naj zveni še tako neverjetno, a ljudje so dolga leta uporabljali prav takšne kodne knjige za zaščito svojih zaupnih pogovorov. Odkar pa so pri Googlu začeli skenirati skoraj vse knjige po vrsti in odkar je mogoče prav hitro preveriti več milijonov gesel, pa tak pristop ni nujno dovolj varen.

Kaj pa, če se naši osebi nista še nikoli srečali na štiri oči in če je poleg njiju (na javnem kanalu) vedno še nekdo, ki jima utegne kaliti srečo (glej sliko 1)? Ali se lahko potem preko javnega kanala dogovorita o skupnem ključu, ki bi bil znan le njima? Rekli boste, da je to vendar nemogoče, saj sogovornik ne more ločiti drugega sogovornika od prisluškovalca. Na srečo je tak dogovor o ključu iskal tudi **Whitfield Diffie**. Verjel je, da so ga v črnih kabinetih (ki so jih za potrebe lastne varnosti in vohunjenja ustanovile različne države) že našli, da pa si ne želijo, da bi o njem



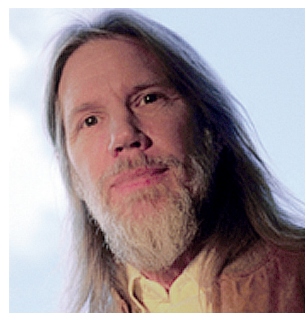


Slika 1. Anita, Bojan ter napadalec Oskar

→ kaj več vedeli običajni ljudje. Ena izmed največjih takih organizacij je ameriška NSA (No Such Agency – morda že veste, kaj ta kratica pomeni v resnici). Tam dela največ matematikov na svetu, vendar pa so rezultati njihovega dela strogo zaupne narave, saj jih uporabljajo v vojaške oziroma vohunske namene. Diffija je bilo kar groza, da bi na tak način zadrževali razvoj vsega človeštva. Zato si je za osrednjo nalogo zadal, da se bo dokopal do teh skrivnosti in jih posredoval vsem ljudem. Temu cilju je podredil svoje življenje. Kriptologi so ga imeli večinoma že za malce trčenega, saj niso verjeli, da je kaj takega sploh mogoče. Ko je Diffie nekega dne izvedel, da se z istim problemom ukvarja tudi **Martin Hellman**, ki je živel na čisto drugem koncu ZDA, je nemudoma sedel v avto in se z vzhodne obale odpravil živeti v njegovo bližino (San Francisco). Sledilo je obdobje skupnega iskanja rešitve in čez nekaj let se jima je zares posrečilo. Najprej sta rešila Diffijev problem, ki je osrednja tema tega sestavka, kmalu zatem pa sta skupaj z **Ralphom Marklom** prišla do revolucionarnega koncepta **kriptosistemov z javnimi ključi**, ki ga bomo spoznali v tretjem delu. Čeprav sta rešitev iskala tako dolgo, pa se je **Diffie-Hellmanov dogovor o ključu** (na kratko **DH-protokol**) izkazal za zelo enostavnega in elegantnega. Predstavimo ga!

Najprej se Anita in Bojan dogovorita, kako bosta računala, na primer, katero število α bosta uporabljala. Takemu številu bomo rekli **generator**. Kmalu bo postalo jasno, zakaj je tako. Anita si naključno izbere svoje zasebno število a , Bojan pa svoje naključno zasebno število b . Nato izračunata vsak svojo potenco $A := \alpha^a$ in $B := \alpha^b$ ter si ju izmenjata preko javnega kanala. Končno izračunata skupni tajni ključ $\alpha^{ab} = K = \alpha^{ba}$, Anita z $B^a = (\alpha^b)^a$, Bojan pa z

$A^b = (\alpha^a)^b$ (glej sliko 4). Če je bil namen dogovora o ključu med Anito in Bojanom pošiljanje zaupnega sporočila, potem po zgoraj opisanih dveh izmenjavah sledi še tretja, v kateri Anita s skupnim tajnim ključem zašifrira in pošlje zaupno sporočilo, ki ga na drugi strani Bojan brez težav odšifrira. Popolnoma brez matematike lahko opišemo podoben protokol, ki sta ga predlagala **Massey** in **Omura**. Tudi zanj potrebujemo tri izmenjave sporočil (glej sliko Protokol Massey-Omura). V digitalnem svetu, kjer si seveda ne želimo fizičnih ključavnic, si namesto njih lahko omislimo dve obrnljivi funkciji, ki med seboj komutirata, to pomeni, da velja pravilo o zamenjavi.



Slika 2. Whitfield Diffie

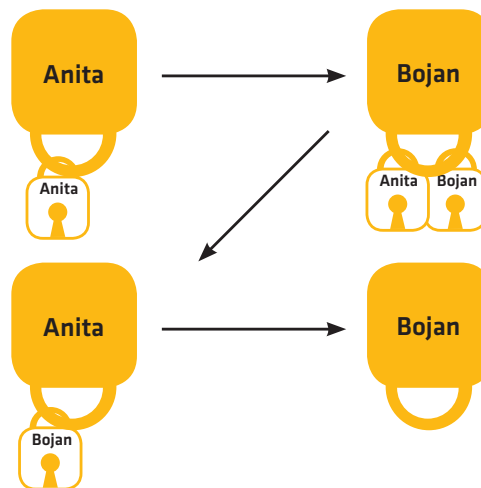


Slika 3. Martin Hellman

Slika 4. Diffie-Hellmanov dogovor o ključu: Anita in Bojan si izbereta vsak svoje naključno število a in b ter si na koncu delita skupni ključ, ki ga izračunata iz izmenjanih potenc: $(\alpha^a)^b = (\alpha^b)^a = \alpha^{ab} = K$.

■ Protokol Massey-Omura

- 1. korak:** Anita zaklene sporočilo v škatlo s svojo ključavnico ter vse skupaj pošlje Bojanu.
- 2. korak:** Bojan prejme pošiljko, prepozna Anitino ključavnico, doda še svojo ključavnico in vrne pošiljko Aniti.
- 3. korak:** Anita prejme pošiljko, prepozna svojo in Bojanovo ključavnico ter odklene in odstrani svojo ključavnico. Nato še drugič pošlje pošiljko Bojanu.
- 4. korak:** Bojan prejme pošiljko, odklene in odstrani svojo ključavnico ter pride do sporočila.



■ Učinkovitost

Kaj je tako posebnega pri DH-protokolu? Najprej moramo znati učinkovito izvesti vse potrebne računske operacije. V našem primeru je to potenciranje elementa α . Če želimo izračunati α^n , kjer je $n \in \mathbb{N}$, potem lahko to storimo z $n - 1$ množenji:

$$\blacksquare ((\dots((\alpha * \alpha) * \alpha) * \dots) * \alpha) * \alpha.$$

Žal s tem ne moremo biti zadovoljni, saj čas računanja merimo v odvisnosti od dolžine zapisa števil, s katerimi imamo opravka. Naj bo dolžina največjega zapisa enaka k . Produkt dveh števil v dvojiškem zapisu lahko izračunamo v grobem s k^2 operacijami (premisljaj zakaj!). Problem pa je v tem, da iz

$$\blacksquare 2^k \approx n$$

sledi, da moramo opraviti eksponentno mnogo množenj. Eksponentni algoritmi so izredno počasni (glej zapis Zgodba iz antične Indije), v praksi pa je pogosto $k > 100$, tako da takšno računanje potence v nobenem primeru ne pride v poštev.

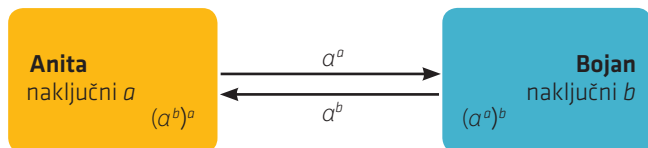
■ Zgodba iz antične Indije

O njej smo v Preseku že pisali (A. Lipovec, *Kaj imajo skupnega Gari Kasparov, Jamie Oliver in ozonske luknje?* Presek 33(1) (2005/2006), str. 4–6), zato le na kratko omenimo, da naj bi na prvo polje šahovnice položili eno zrno riža, na drugo polje dve, na tretje štiri (za vsako naslednje polje podvojimo število zrn). Šahovnica ima 64 polj, kar pomeni, da bi morali nanjo postaviti

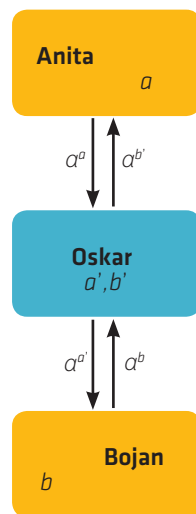
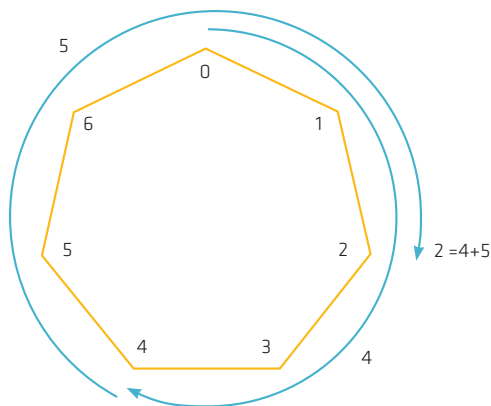
$$\blacksquare 1 + 2 + 2^2 + \dots + 2^{63} = 2^{64} - 1 \text{ zrn riža.}$$

Za kriptografijo je zelo pomembno, da razumemo velike številke. Ali si vsaj v grobem lahko predstavljamo, koliko riža bi to bilo? Recimo, da lahko poje povprečen človek pol kg riža na dan. To je kar precej, ko je riž enkrat kuhan. Koliko zrn napolni čajno žličko? Približno 330, za pol kg riža pa jih potrebujemo nekaj čez 80 oziroma $27.500 = 2,75 \times 10^4$ zrn riža. Na svetu je danes 6,6 milijarde = $6,6 \times 10^9$ ljudi. Če bi vsi ljudje jedli samo riž, bi torej lahko pojedli $2,75 \times 10^4 \times 6,6 \times 10^9 \approx 1,8 \times 10^{14}$ zrn riža na dan.

Sedaj pa se vrnimo k številu $2^{64} - 1 \approx 1,8 \times 10^{19}$ zrn in ga delimo s številom $1,8 \times 10^{14}$ zrn, ki jih poje človeštvo na dan. Dobimo 100.000 dni, kar pomeni, da bi lahko svet jedel riž s šahovnice tako dolgo, dan za dnem oziroma $100.000/365 \approx 274$ let!



Slika 5. Računanje po modulu 7



Slika 6. Napad srednjega napadalca na DH-protokol. Pri tem napadu nasprotnik Oskar prestreže Anitino javno vrednost α^a in pošlje svojo javno vrednost $\alpha^{a'}$ Bojanu. Ko Bojan pošlje svojo javno vrednost α^b , jo Oskar prestreže in zamenja s svojo javno vrednostjo $\alpha^{b'}$ ter jo pošlje naprej Aniti. Tako delita Anita in Oskar skupen skrivni sejni ključ $K_{ab'} = \alpha^{ab'}$ ter Bojan in Oskar drugi skrivni sejni ključ $K_{a'b} = \alpha^{a'b}$. Po tej izmenjavi Oskar preprosto odšifrira sporočila poslana s strani Anite ali Bojana, jih prebere in po potrebi spremeni, preden jih zopet zašifrira in pošlje naprej.



Pa si pogledjmo zapis števila n v dvojiškem sistemu:

$$n = n_k 2^k + \dots + n_1 2^1 + n_0 2^0, \text{ kjer je } n_i \in \{0, 1\}.$$

Potem velja

$$\alpha^n = \alpha^{n_k 2^k} * \dots * \alpha^{n_1 2^1} * \alpha^{n_0 2^0}. \quad (1)$$

Potence $\alpha^2, \alpha^{2^2}, \dots, \alpha^{2^k}$ izračunamo s k kvadriranjem (v ta namen kvadriramo $\alpha^{2^{i-1}}$, da dobimo α^{2^i}). S tem smo dobili vse faktorje v (1). Potem pa za izračun produkta iz (1) potrebujemo še največ k množenj. Skupaj nanese $2k$ množenj oziroma v grobem k^3 procesorskih operacij, kar pomeni, da je naše računanje učinkovito in s tem tudi DH-protokol.

Varnost

Kako je z možnimi napadi na DH-protokol? Bralci, ki se še niste srečali s funkcijami, lahko preskočite ta razdelek. Na prvi pogled se zdi, da je dovolj, da znamo učinkovito izračunati bodisi $\log_\alpha A = a$ bodisi $\log_\alpha B = b$. Če bi bila α , a in b realna števila, potem to ne bi smel biti problem, vsaj od takrat naprej, ko so ljudje sestavili dobre logaritemske tablice, da o današnjih računalnikih niti ne govorimo. Vendar pa si kriptografi namesto obsega realnih števil v praksi raje izberemo diskretno grupo, v kateri ne znamo učinkovito izračunati logaritma poljubnega njenega elementa (glej zapis Problem diskretnega logaritma (DLP)). Spomnimo se, da smo, ne tako dolgo nazaj, v Preseku pisali o računalih nove dobe (1. del, Presek 30 (2002/2003), str. 226-231 in 2. del, Presek 30 (2002/2003), str. 291-296), kjer smo vpe-

ljali nekaj zanimivih grup. Pa DLP ni edini razlog za uporabo diskretnih grup. Če računamo z običajnimi tipi števil, celimi, racionalnimi ali realnimi števili, se zna zgoditi, da bodo rezultati izračunov hitro zrastle preko vseh meja (glej zapis Zgodba iz antične Indije) oziroma bomo zaradi omejene velikosti prisiljeni nenehno zaokrožati. V kriptografiji je učinkovitost osrednjega pomena, približki pa ne zadoščajo (predstavljajte si, da vam bankomat ali pa prenosni telefon odgovori, da danes nista povsem zadovoljna z vašim geslom, pa naj si bo to zato, ker še vedno računata, ali pa se jima zdi geslo samo približno pravilno).

Tako si za računanje raje omislimo končne množice kot pri številčnici na uri. Tak zgled so kolarji $\mathbb{Z}_n$, $n \in \mathbb{N}$, v katerih računamo po modulu števila n . Za elemente vzamemo $\{0, 1, \dots, n-1\}$, računamo pa tako, da seštejemo ali zmnožimo dve števili tako, da pravi rezultat nadomestimo z njegovim ostankom pri deljenju z **modulom** n . Na primer, za $n = 7$ velja $4 +_7 5 = (4 + 5) \bmod 7 = 2$ in $5 *_7 4 = (5 \cdot 4) \bmod 7 = 6$, saj ima število 9 pri deljenju s 7 ostanek 2, število 20 pa ostanek 6 (glej sliko 5). Če želimo v taki množici še deliti z vsakim neničelnim številom, si moramo za modul n izbrati praštevilo p . Tako v resnici delamo v praštevilskem obsegu $\mathbb{Z}_p$ oziroma za potrebe DH-protokola kar v njegovi podgrupi $(\mathbb{Z}_p \setminus \{0\}, *)$, ki ji pravimo **multiplikativna podgrupa** (oznaka $\mathbb{Z}_p^*$). Za vsak element $\alpha \in \mathbb{Z}_p^*$, za katerega velja $D(\alpha, p-1) = 1$, potence $\alpha, \alpha^2, \dots, \alpha^{p-1}$ pretečejo vse elemente grupe $\mathbb{Z}_p^*$ (zadnji element je seveda enota, saj Fermatov izrek za izbrana α in p pravi $\alpha^{p-1} \equiv 1 \pmod{p}$). (Glej članek D. Pagona, *Kongruence in Eulerjev izrek*, Presek 15 (1987/1988), str. 194-196), tj. α generira grupo

■ Problem diskretnega logaritma (DLP)

Za dano grupo G in elementa $\alpha, \beta \in G$, kjer je red elementa α enak n , poišči učinkovito metodo, ki določi celo število x , $0 \leq x \leq n - 1$ (če obstaja), tako da je $\alpha^x = \beta$. Število x imenujemo **diskretni logaritem** števila β pri osnovi α .

Požrešna metoda za reševanje DLP, ki računa zaporedne potence elementa α , t. j. $\alpha, \alpha^2, \alpha^3, \dots$ in jih primerja z β , ni bila zanesljiva za n nad 2^{40} , danes pa verjetno za n pri 2^{80} (odvisno koliko opreme in časa imamo na voljo).

Metoda mali-veliki korak je v nekaterih grupah še vedno najboljša metoda (izboljšati je mogoče le njeno prostorsko zahtevnost), odpove pa pri dvakrat večjih eksponentih, ki smo jih omenili pri požrešni metodi. Pri tej metodi si najprej naredimo tabelo na enak način, kot smo začeli pri požrešni metodi, le da se ustavimo pri k -ti potenci, kjer je k celi del kvadratnega korena iz n . Lahko si predstavljamo, da smo z malimi koraki prehodili in s tem pokrili lok dolžine k na zgoraj omenjenem krogu, ki ga sestavljajo potence elementa α . Nato pa zaporedoma pregledujemo, katerega izmed elementov $\beta, \beta\alpha^k, \beta\alpha^{2k}, \dots, \beta\alpha^{k \cdot k}$ najdemo v tej tabeli (enega bomo zagotovo, saj pravkar omenjenega loka ne moremo preskočiti s korakom dolžine k). Ko se to zgodi, velja

$$\beta(\alpha^k)^j = \alpha^i,$$

od koder dobimo $\log_\alpha \beta = i - k * j \bmod n$.

$$\blacksquare \quad a\alpha + kn = 1$$

za a (in k). To pa znamo učinkovito rešiti z razširjenim Evklidovim algoritmom, saj je $D(\alpha, n) = 1$ (glej članek M. Juvana, *O Evklidovem algoritmu*, Presek 21 (1993/1994), str. 116-121). Izbira najboljše grupe G za DH-dogovor o ključu, v kateri bo računanje potenc učinkovito, razkritje DLP pa nedosegljivo, je izredno občutljiva naloga, ki jo zmorejo opraviti le izkušeni kriptologi.

■ Aktivni srednji napadalec

Zgoraj predstavljeni Diffie-Hellmanov protokol imenujemo tudi **neoverjeni** Diffie-Hellmanov protokol. Pri njem udeleženci namreč ne morejo z gotovostjo ugotoviti izvora javnih vrednosti ostalih udeležencev (t. j. potenc, ki si jih morajo izmenjati). Zato je neoverjeni Diffie-Hellmanov protokol ranljiv na napad, ki ga imenujemo **napad srednjega napadalca** (angl. *middle man attack*, glej sliko 6). Besedno zvezo "*napad srednjega napadalca*" uporabljamo za opis napada, kadar Oskar sedi na sredini komunikacijskega kanala/poti med Anito in Bojanom ter oba prelišči. Je pomemben napad, zaradi katerega je potrebno dopolniti in spremeniti številne komunikacijske protokole. Vendar pa je, kot pravi B. Schneier, to tudi napad, ki ga lahko uporabimo v vsakdanjem življenju.

Premožna gospa želi najti pomoč pri pospravljanju hiše in v časopisu objavi oglas, da rabi pomoč. Ko se javi primerna oseba, jo gospa vpraša po priporočilih, da preveri njene izkušnje in zanesljivost. Ker pa gospa v resnici sploh ni lastnica hiše, ampak gre za staro znanko policije, sama uporabi pravkar pridobljena priporočila in si z njimi najde zaposlitev pomočnice v bogati hiši.

Službo je dobila z dobrimi priporočili—pa saj so vendar prava, čeprav niso njena—in nato odnese iz hiše vso zlatnino in ostale vrednosti.

Seveda lahko ta postopek lažna gospa-pomočnica ponovi tudi večkrat.

Kaj se je zgodilo v zgornjem primeru? Navidezna gospa-pomočnica se je postavila na sredino komunikacije med pravo pomočnico ter pravo gospo in se

$\mathbb{Z}_p^*$. Multiplikativna grupa poljubnega končnega obsega je torej **ciklična**. V grupi obstaja namreč tak element, da so vsi elementi njegove potence, zato lahko njene elemente predstavimo na krogu, tako kot smo to storili na sliki 5.

Morda se na prvi pogled zdi, da bi lahko namesto $\mathbb{Z}_p^*$ uporabljali kar grupo $(\mathbb{Z}_n, +_n)$, $n \in \mathbb{N}$. Potem bi namesto potence α^a v DH-protokolu zapisali večkratnik $V = a\alpha$, kjer je $\alpha \in \mathbb{Z}_n$, $D(\alpha, n) = 1$ in $a \in \mathbb{N}$. Vendar pa v tem primeru poznamo algoritem, ki nam iz večkratnika V izračuna a . V ta namen je namreč potrebno rešiti naslednjo diofantsko enačbo





predstavila vsaki kot tista druga. Pomočnica pošlje priporočila nekomu, ki ni prava gospa. Prava gospa preveri priporočila, ne da bi preverila, da v resnici ne pripadajo lažni pomočnici.

Napad srednjega napadalca je uspešen zato, ker Diffie-Hellmanov protokol ne preveri identitete udeležencev v protokolu oziroma njihovih javnih vrednosti. Rešitev tega problema lahko dosežemo tako, da se udeleženci in javne vrednosti, ki nastopajo v protokolu, ustrezno overijo z digitalnimi certifikati. To pa je že nova zgodba, ki si jo lahko ogledate v tretjem delu hkrati z zgodbo o volku in sedmih kozličkih.

■ Naloge

1. Funkcija $f(x) = \log_{\alpha} x$ nam pove, kateri eksponent moramo uporabiti na α , da dobimo x . Določi definicijsko območje realnih funkcij $f(x)$ in $g(y) = \alpha^y$. Prepričaj se, da je $\alpha^{\log_{\alpha} x} = x$ in $\log_{\alpha}(\alpha^x) = x$, kar pomeni, da sta funkciji $f(x)$ in $g(x)$ **inverzni**.
2. Preveri enakost

$$1 + 2 + 2^2 + \dots + 2^{63} = 2^{64} - 1,$$

tako da levo stran pomnožiš z $(2 - 1)$ in odpraviš oklepaje. Bi znal to enakost posplošiti?

3. Ali se lahko domisliš še kakšne zanimive zgodbe, ki bi nazorno ponazorila hitro rast eksponentne funkcije? Pomisli, npr. koliko prednikov bi imel v času, ko je bila zgrajena puljska arena (pred približno 2000 leti), če si med njimi

nobena dva iz iste generacije ne bi bila v sorodu? (Glej <http://hr.wikipedia.org/wiki/Pula>)

4. Oцени, koliko riža potrebujemo, da pokrijemo cel svet (vključno z oceani), če meri polmer zemlje 6400 km?
5. Oцени, koliko besed lahko "obdeli" tvoj ali pa šolski PC v eni uri? Kolikšna je velikost največjega števila, ki bi ga še lahko zapisal v spomin svojega ali šolskega računalnika?
6. Kolikšna je dolžina produkta dveh binarnih števil, katerih zapisa sta dolga m in n ?
7. Koliko operacij potrebuješ za izračun produkta dveh 100-bitnih binarnih števil s procesorjem/vodilom svojega ali šolskega računalnika?
8. Pri učinkovitem algoritmu računanja potence α^n , $n \in \mathbb{N}$, smo vnaprej izračunali potence α^2 , α^{2^2} , α^{2^3} , ...
Poišči učinkovit algoritem za potenciranje, ki potrebuje bistveno manj spomina. (Namig: en tak algoritem je znan pod imenom **kvadriraj in zmnoži**, njegov spomin pa je neodvisen od števila n .)
9. Poišči čim več parov funkcij, za katere velja pravilo o zamenjavi.
Ali znaš s takim parom sestaviti digitalno različico protokola Massey-Omura, ki bo varna?
- 10.* Ni se težko prepričati, da je ciklična grupa z n elementi izomorfna grupi $(\mathbb{Z}_n, +_n)$. Kaj lahko poveš o relaciji med zahtevnostjo problema diskretnega logaritma v poljubni ciklični grupi G z n elementi in problema iskanja izomorfizma med grupo G in aditivno grupo $(\mathbb{Z}_n, +)$? *

Stare številke revije Presek

Če želite dopolniti svojo zbirko revij Presek, so nekatere stare številke še vedno na voljo. Na spodnjem naslovu najdete seznam razpoložljivih števil in naročilnico:

<http://www.presek.si/staro.htm>

Za individualne naročnike revije Presek, člane DMFA, dijake in študente je cena stare številke 520 SIT (2,17 EUR), za vse ostale pa 650 SIT (2,71 EUR).

Izkoristite možnost dodatnih popustov pri večjem naročilu!

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



Knjižnica Sigma

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. Najnovejša izdaja je že osemdeseta po vrsti!



Borut Zalar:

TEŽIŠČA IN VZTRAJNOSTNI MOMENTI

120 strani
format 14×20 cm
mehka vezava

2.000 SIT
(8,35 EUR)

**ŽE OSEMDESETA IZDAJA
V KNJIŽNICI SIGMA!**

Ciril Dominko in Bojan Golli:

REŠENE NALOGE IZ FIZIKE Z DRŽAVNIH TEKMOVANJ – 3. del

Prva knjiga:

VADEMEKUM IN NALOGE

Druga knjiga:

NAMIGI IN REŠITVE

skupaj 424 strani
format 14×20 cm
mehka vezava

cena kompleta: 5.000 SIT (20,86 EUR)



Robert B. Banks:

LEDENE GORE, PADAJOČE DOMINE in druge prigode iz uporabne matematike

1. in 2. del

skupaj 348 strani
format 14×20 cm
mehka vezava

cena kompleta: 5.000 SIT
(20,86 EUR)

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 pri 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.



je revija, ki jo berejo
po vsem vesolju →

Pridruži se nam tudi ti!



Revija Spika je mesečnik; izhaja 15. v mesecu. Na leto izide deset enojnih in dvojna poletna številka (julij/avgust). Celoletna naročnina (za leto 2006) je 9.220,00 SIT, polletna naročnina za prvo polletje je 5.200,00 SIT, za drugo polletje pa 4.950,00 SIT.

Spika vsak mesec prinaša:

- novice
- efemeride Sonca, Lune in planetov
- napoved meteorskih rojev in drugih nebesnih dogodkov
- zanimive prispevke o planetih, zvezdah, galaksijah...
- prispevke za resne opazovalce neba in začetnike
- poučne, a zabavne vaje za šolo in dom
- astronomijo za najmlajše

Ilustracije: TBC'93

CAMBIO d.o.o., Koprška 94, 1000 Ljubljana
tel.: 01/256-07-11, e-naslov: spikar@siol.net

