



PRESEK LETNIK 38 (2010/2011) ŠTEVILKA 1



PRESEK



- MAVRICA
- GALILEI IN POSPEŠEK
- DIGITALNI PODPIS
- NAGRADNA KRIŽANKA

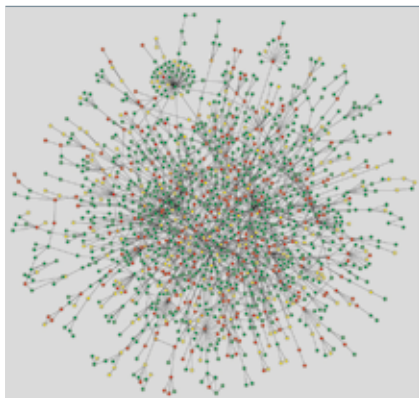


ISSN 0351-6652



9 770351 66581 4

Ustvarjanje povezav



→ Skupnost ljudi, nevroni v možganih in spletne strani, skupaj z njihovimi povezavami, so primeri omrežij. Matematiki proučujejo lastnosti omrežij, na primer število in porazdelitev povezav, da bi odkrili, kaj lahko te lastnosti razkrijejo o notranji naravi omrežja. Na primer, barve na spodnji sliki nakazujejo, kako razdiralna je lahko odstranitev vozlišča za omrežje v primeru žive celice. Odkritje in potrditev omrežnih lastnosti, kot je omenjena, je pomembno za uporabo pri zelo majhnih in ogromnih omrežjih, kot tudi pri zaščiti računalnikov in ljudi pred virusi. Zarodek študija omrežij je fraza „šest stopenj ločenosti“, ki izvira iz študije povezanosti igralcev preko skupnega nastopanja v filmih. V poskusu, ki so ga izvedli v 1960-ih, je bilo 100 slučajno izbranih ljudi iz Srednjega zahoda v ZDA (the Midwest) povezanih z borznim posrednikom iz Massachusettsa (preko prijatelja od prijatelja od prijatelja ...) v povprečju v šestih korakih. Da so bili ljudje na pol poti preko države tako tesno povezani, je bilo presenetljivo odkritje, ki je pokazalo, da lahko celo veliko omrežje predstavlja „majhen svet“ („small world“). Danes raziskovalci za analizo omrežij uporabljajo parametre iz teorije grafov in teorije verjetnosti, da bi ugotovili, ali je zamotano omrežje, najsi bo to omrežje političnega vpliva ali pa igralci povezani s Kevinom Baconom, res majhen svet.



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 38, šolsko leto 2010/2011, številka 1

Uredniški odbor: Vladimir Batagelj, Tanja Bečan (jezikovni pregled), Vladimir Bensa, Mojca Čepič, Mirko Dobovišek, Vilko Domajnko, Darjo Felda (tekmovanja), Bojan Golli, Andrej Guštin (astronomija), Marjan Jerman (matematika), Martin Juvan, Maja Klavžar, Damjan Kobal, Andrej Likar (fizika), Matija Lokar, Aleš Mohorič (odgovorni urednik), Marko Petkovšek (glavni urednik), 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

Elektronska pošta: presek@dmfa.si

Naročnina za šolsko leto 2010/2011 je za posamezne naročnike 16,69 EUR – posamezno naročilo velja do preklica, za skupinska naročila učencev šol 14,61 EUR, posamezna številka 3,76 EUR, dvojna številka 6,89 EUR, stara številka 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): SKBAS12X, IBAN: SI56 0310 0100 0018 787.

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

Založilo DMFA-založništvo

Tehnična urednica Tadeja Šekoranja

Oblikovanje in ilustracija Polona Šterk in Ines Kristan

Tisk Tiskarna Pleško, Ljubljana

Naklada 1700 izvodov

© 2010 Društvo matematikov, fizikov in astronomov Slovenije – 1787

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

Poštšina 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 odgovornemu uredniku 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

- 2** Ustvarjanje povezav

MATEMATIKA

- 4-12** Mavrica
(*Marija Vencelj*)

FIZIKA

- 12-15,18** Galilei in pospešek
(*Janez Strnad*)
- 18-20** Kaj se hitreje kotali? –
Poizkuševalnica v kuhinji – odgovor naloge
(*Mojca Čepič*)
- 21** Opazuj svoje drevo, kako spreminja barve –
Poizkuševalnica v naravi
(*Mojca Čepič*)
- 21-22** Razmisli in poskusi
(*Mitja Rosina*)

ASTRONOMIJA

- 23-24** Tekmovanje iz znanja astronomije – drugič
(*Andrej Guštin*)

RAČUNALNIŠTVO

- 25-29** Zaupati ali ne zaupati – Digitalni podpis v
kriptografiji, 4. del
(*Aleksandar Jurišić in Jasmina Veselinović*)

RAZVEDRILO

- 16-17** Nagradna križanka
(*Marko Bokalič*)
- 30** Rešitev nagradne križanke Presek 37/6
(*Marko Bokalič*)
- 20, 29** Sudoku

TEKMOVANJA

- priloga** 46. tekmovanje iz matematike za Vegovo
priznanje – področno tekmovanje
- priloga** 46. tekmovanje iz matematike za Vegovo
priznanje – državno tekmovanje

SLIKA NA NASLOVNICI: Če se boste med poletnimi počitnicami kdaj dolgočasil, vas vabimo, da preverite izsledke kakšnega od člankov iz te številke. Fotografija na naslovnici se tokrat navezuje na članek iz fizike.

OBVESTILO: Bralce vabimo, da nam na naslov presek@dmfa.si pošljejo slike svojih, doma narejenih mavric. Najboljšo sliko bomo objavili v naslednji številki, pripravili pa smo tudi lepe nagrade. Navodila za „izdelavo“ mavrice so na koncu članka o mavrici.



Mavrica



MARIJA VENCELJ

→ Mavrica je svetlobni pojav v ozračju, ki ga opazovalec dojema kot del svetlobnega kolobarja, v katerem si sledijo barve v značilnem spektralnem zaporedju. Nastane kot posledica loma in odboja sončne svetlobe na kapljicah vode v Zemljini atmosferi.

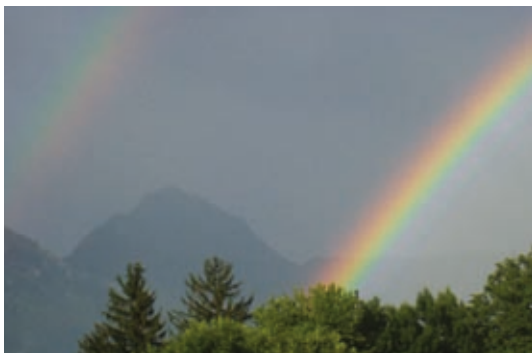
Mavrica

Mavrico lahko opazujemo, kadar je pred nami dežna zavesa ali oblak in prihaja sončna svetloba iz za našega hrbta pod nizkim kotom nad obzorjem. Najbolj spektakularna je, kadar je nebo pred nami temno, zakrito z dežnimi oblaki, za nami pa je v smeri sonca jasno nebo. Rezultat je bleščeča **glavna mavrica** na kontrastnem temnem ozadju. Ima obliko večjega ali manjšega dela večbarvnega kolobarja, ki je na zunanji strani rdeč in na notranji vijoličen (slika na naslovnici).

Drugi mavrični pojavi so šibkejši in jih ne opazimo vedno. Nad glavno mavrico vidimo včasih še **stransko mavrico**, v kateri se vrste barve v obratnem vrstnem redu kot v glavni mavrici – od rdeče na notranjem do vijolične na zunanjem robu. Če je v ozadju modro nebo, jo vidimo slabo ali sploh ne.

Zlahka opazimo, da je področje med obema mavričnima lokoma nekoliko temnejše kot okoliško nebo. Ta pojav je opazen celo, če stranska mavrica ni vidna. Glavna mavrica ima tedaj temnejšo in svetlejšo stran (slika 1). Temno področje nad lokom glavne mavrice se imenuje **Aleksandrov temni pas** po grškem filozofu Aleksandru iz Afrodisia, ki je pojav opisal pred več kot dva tisoč leti.

Redkeje kot stransko mavrico opazimo dodatno **zaporedje nejasnih lokov**, ki leže na notranji strani glavne mavrice in so izmenično rožnati in zeleni. Še redkeje se taki loki pojavijo na zunanji strani stranske mavrice. Oboji so vidnejši v bližini mavričnega vrha. Pozornost, ki so jo zbudili, je imela velik vpliv

**SLIKA 1.**

Izrazit Aleksandrov temni pas mavrice s Storžičem v ozadju (foto Agata Tiegl).

na razvoj teorije mavrice. Na sliki na naslovnici jih vidimo na notranji strani glavne mavrice.

Z letala imamo včasih priložnost videti popoln mavrični kolobar s senco letala v središču (slika 2). Tega pojava ne smemo zamenjati s precej manjšo **glorijo**, ki ni dosti večja od opazovalčeve sence, ki jo obdaja (slika 3).

**SLIKA 2.**

Iz letala posneta mavrica nad Melbournom v Avstraliji. Višje je opazovalec, več spodnjega dela ima „njegova mavrica“ (vir Wikipedia, AlterVista).

**SLIKA 3.**

Glorija, posneta z Mizaste gore nad Cape Townom v Južni Afriki. Opazovalčeva (fotografova) senca je obdana z majhnim mavričnim krogom (foto Matjaž Vencelj).

Včasih lahko pri močni mesečini vidimo **lunino ali nočno mavrico**. Ker človeško oko pri šibki svetlobi slabo loči barve, jo dojemamo kot bel lok.

Kaj je mavrica?

Naše fizikalno in matematično znanje je preskromno, da bi lahko povzeli vso znano teorijo mavrice. Zato se bomo omejili na njeno osnovno analizo, ki temelji na odboju in lomu sončnega žarka na dežni kapljici.

Mavrica ni svetlobni efekt na določenem mestu na nebu. Njena **navidezna lega je odvisna od opazovalčevega položaja in smeri sončnih žarkov**. Če med dežjem ali kmalu po njem posije sonce na steno iz dežnih kapljic, se svetloba na njih lomi in odbija. Vendar doseže opazovalčeve oči samo svetloba iz nekaterih žarkov, ki zadenejo kapljico. In ta svetloba daje mavrico za tega opazovalca.

Opazovalec vidi mavrico vedno na strani, nasprotni od sonca. Mavrična loka sta dela dveh večbarvnih krožnih kolobarjev, ki imata skupno središče na podaljšku zveznice med opazovalčevo glavo in njeno senco. To lepo prikazuje slika na naslovnici, na kateri ob sredini spodnjega roba vidimo senco fotografove glave. Poltrak od opazovalčeve glave skozi njeno senco ima smer sončnih žarkov. Vrh glavne mavrice se boči približno 40° – 42° nad tem poltraktom, vrh stranske pa je okrog 50° – 53° nad njim. Če je sonce več kot 42° nad obzorjem, je torej glavna mavrica pod obzorjem in je navadno ne vidimo. Izjema je, če je opazovalec visoko nad tlemi, npr. v letalu ali na visoki gori. V podobno izjemnih razmerah je bila posneta tudi slika 4.

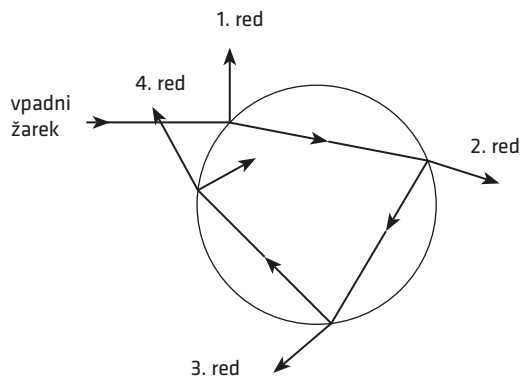
**SLIKA 4.**

Mavrica globoko v dolini Pišnice, fotografirana s ceste, ki pelje z Vršiča v Kranjsko Goro. Slika je bila posneta julijskega dne zgodaj popoldne, ko je visoko poletno sonce sijalo čez gorske robove za hrbti opazovalcev (foto Agata Tiegl).

→ Razloge za tako natančno določeno lego mavrice glede na opazovalca in smer sončnih žarkov si bomo ogledali v nadaljevanju. Razložili bomo tudi njene barve.

Pot in razklon sončnega žarka v dežni kapljici

Za začetek pogledjmo, kako se odbija in lomi svetloba, ki v zraku naleti na dežno kapljico. Predpostavili bomo, da ima kapljica obliko majhne kroglice. Žarek, ki zadene njeno površino, se delno odbije, delno lomi. Lomljeni žarek potuje skozi kapljico do nasprotna stene, kjer se spet delno odbije, del pa lomljen zapusti kapljico (slika 5).



SLIKA 5.

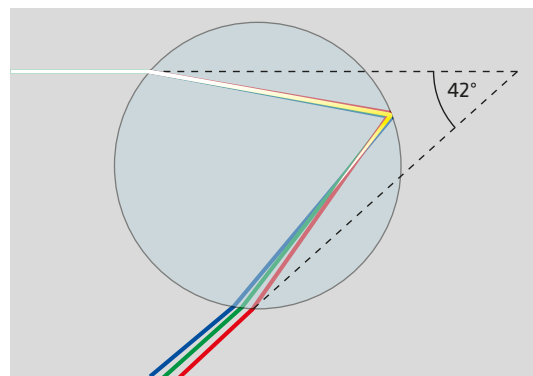
Vpadni žarek in žarki vseh redov, ki izvirajo iz njega, ležijo v isti ravnini. To je ravnina glavnega krogelnega kroga kapljice, na katero je žarek padel.

Prvi odbiti žarek imenujemo žarek prvega reda. Preostala svetloba lomljena prodre v kapljico. Na nasprotni steni je del izstopi kot žarek drugega reda, del se je odbije nazaj v kapljico. Ko ta del spet zadene steno kapljice, prodre delno ven kot žarek tretjega reda, delno pa nadaljuje pot znotraj kapljice kot odbiti žarek. Tako se proces nadaljuje. Iz kapljice torej izvirajo žarki različnih redov. Za mavrico so pomembni žarki tretjega in četrtega reda. **Žarki tretjega reda** zapustijo kapljico po enem notranjem odboju in nam **dajejo glavno mavrico**. **Žarki četrtega reda** opravijo dva notranja odboja in so **izvor stranske mavrice**.

Naravna bela svetloba, ki prihaja od Sonca, je mešanica vijolične, modre, zelene, rumene, oranžne in rdeče svetlobe. Vsaka od teh barv se nekoliko dru-

gače lomi; pri enakem vpadnem kotu imajo rahlo različne lomne kote. Posledica tega je, da se žarek bele svetlobe **razkloni** na barvne komponente. Pri tem je od prvotne smeri najmanj odklonjena rdeča, najbolj vijolična sestavina.

Pri dežni kapljici se žarki vseh redov, od drugega dalje lomijo dvakrat: enkrat ob vstopu v kapljico, drugič pri izstopu iz nje. Razen pri žarku, ki gre skozi središče kapljice, pride zaradi dvojnega loma do povečanega razklona svetlobe (slika 6). Opazovalec, ki gleda v dežno zaveso ali oblak, vidi večbarvne vse tiste kapljice, skozi katere vodi opisana pot svetlobe natanko v njegovo oko. Žarki drugega reda niso zanimivi, ker gledamo pri njih skoraj natanko v sonce. Povedali smo že, da dajejo žarki tretjega in četrtega reda glavno in stransko mavrico. Pri več kakor treh notranjih odbojih pa je izguba svetlobe že prevelika, da bi kaj videli.



SLIKA 6.

Skica poti in razklona enega od žarkov tretjega reda. Zaradi preglednosti so vrisane le tri barvne komponente.

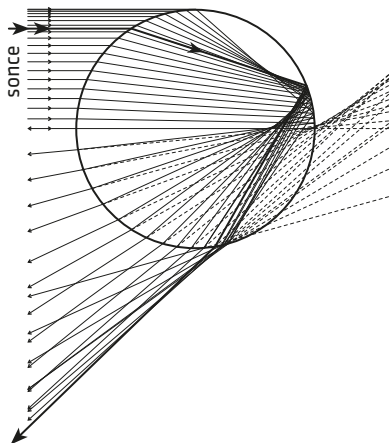
Mavrični kot

Po odbojnem zakonu leži odbiti žarek v ravnini, ki jo določata vpadni žarek in pravokotnica na odbojno ploskev v vpadni točki. Podobno sledi **iz lomnega zakona**, da leže vpadni in lomljeni žarek ter pravokotnica na mejno ploskev v isti ravnini.

Ker potekajo vse pravokotnice na krogelno površino skozi središče kroglice, leži prvi par lomljenega in odbitega žarka v ravnini, ki jo določata vpadni žarek in središče kroglice. Drugi par takih žarkov leži v ravnini prvega lomljenega žarka in središča kroglice.

Ta ravnina seveda sovпада s prvo. Podobno sovпада z njo ravnina tretjega para ustreznih žarkov. To pomeni, da leže poti vseh žarkov, ki izvirajo iz istega vpadnega žarka, v isti ravnini. Zasedovanje svetlobe skozi kapljico je zato **ravninski problem**, kar precej poenostavi obravnavo mavrice.

V nadaljevanju bomo začasno privzeli, da je svetloba, ki zadene kapljico, enobarvna, torej bomo zanemarili razklon. Na sliki 7 je skica žarkov tretjega reda iz skupne ravnine, ki poteka skozi središče kapljice. Žarek, ki pade na kapljico pravokotno, gre skozi središče kapljice, se na notranji steni odbije nazaj proti soncu in izhaja kot žarek tretjega reda za 180° odklonjen od prvotne smeri. Z oddaljevanjem od tega žarka se odklon žarkov tretjega reda od prvotne smeri najprej manjša do nekega najmanjšega odklona (ta žarek je na sliki narisana poudarjeno), nato pa spet raste. Črtkano so narisane navidezne poti žarkov, kot jih dojemata naše oko. S slike razberemo marsikaj. Če naj žarek tretjega reda zadene naše oko, se moramo nahajati na isti strani kapljice kot sonce. To pomeni, da moramo biti obrnjeni tako, da imamo sonce za hrbtom. Poleg tega **mavrice ne bomo našli prav visoko na nebu. Najvišja možna smer je določena s smerjo najmanjšega odklona žarkov tretjega reda od prvotne smeri.** Na sliki 7 je označena s poudarjeno črtkano črto. Kot, ki ga ta smer oklepa s smerjo sončnih žarkov, imenujemo **mavrični kot glavne mavrice**.



SLIKA 7.

Skica poti žarkov tretjega reda v eni od ravnin skozi središče kapljice. Žarki, ki padejo na spodnjo polovico kapljice, zaradi preglednosti niso narisani. Iz kapljice izstopajo v smereh navzgor in ustvarjajo spodnji mavrični kolobar za dvignjenega opazovalca (kot na sliki 2).

Izračun mavričnega kota¹

Če je mavrica vidna, mavrični kot lahko izmerimo. Poiskali ga bomo tudi po matematični poti.

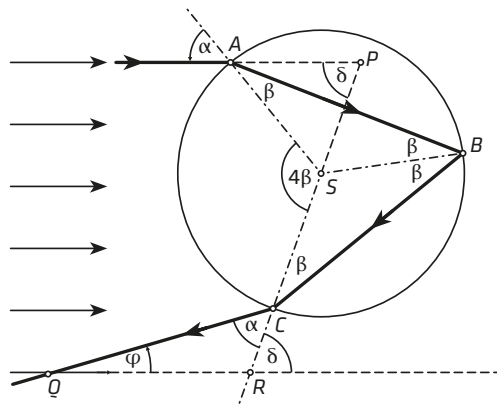
Na sliki 8 je narisana pot enega samega žarka tretjega reda skozi dežno kapljico. Naj bosta α in β njegov vpadni in lomni kot v točki A. Zaradi odboja v točki B in ponovnega loma v točki C ter lastnosti krožnice se kota ponovita v točkah B in C, kot je vrisano. Nadalje smo s φ označili kot, suplementaren odklonu žarka od prvotne smeri. Poiščimo njegovo odvisnost od vpadnega kota α .

Pomožna kota pri P in R, ki smo ju označili z δ , sta enaka, ker sta izmenična ob vzporednicah. Trikotnik ASP ima pri S zunanji kot 4β in nepriležna notranja kota α in δ , trikotnik QRC pa pri R zunanji kot δ in nepriležna notranja kota φ in α . To pomeni

$$\blacksquare \delta = \varphi + \alpha = 4\beta - \alpha,$$

kar da

$$\blacksquare \varphi = 4\beta - 2\alpha.$$



SLIKA 8.

Natančna skica poti enobarvnega žarka tretjega reda skozi dežno kapljico.

¹Komur je račun pretežek, naj ga izpusti in upošteva samo rezultat.



Po lomnem zakonu je

$$\frac{\sin \alpha}{\sin \beta} = n$$

oziroma

$$\beta = \arcsin\left(\frac{1}{n} \sin \alpha\right),$$

kjer je n lomni količnik za prehod iz zraka v vodo.

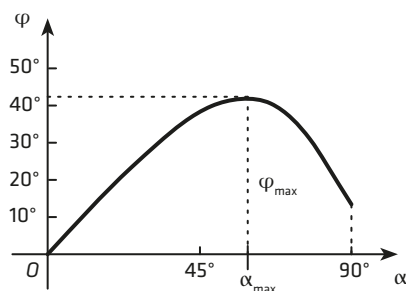
Sledi

$$\varphi = 4 \arcsin\left(\frac{1}{n} \sin \alpha\right) - 2\alpha. \quad (1)$$

Če v (1) vstavimo vrednost $n = \frac{4}{3}$, kar je približna povprečna vrednost lomnega količnika svetlobe za tak prehod, dobimo

$$\varphi = 4 \arcsin\left(\frac{3}{4} \sin \alpha\right) - 2\alpha, 0^\circ \leq \alpha \leq 90^\circ. \quad (2)$$

Funkcija (2) je narisana na sliki 9. Ustrezno opazovanjem, do katerih smo prišli pri risanju žarkov na sliki 7. Vidimo, da zavzame kot φ vrednosti od 0° do približno 42° . Pri tem ne prezrimo, da je φ odvisen le od velikosti vpadnega kota in nič od premera kapljice. Torej je tudi **največja možna vrednost kota φ za vse dežne kapljice enaka.**



SLIKA 9.

Odvisnost kota φ s slike 8 od vpadnega kota α .

Z nekaj več matematičnega znanja lahko to vrednost izračunamo. V ta namen poiščemo



ničle prvega odvoda funkcije (2) na intervalu $[0^\circ, 90^\circ]$. Imamo

$$\varphi' = \frac{4 \cos \alpha}{\sqrt{(\frac{4}{3})^2 - \sin^2 \alpha}} - 2 = 0,$$

kar da

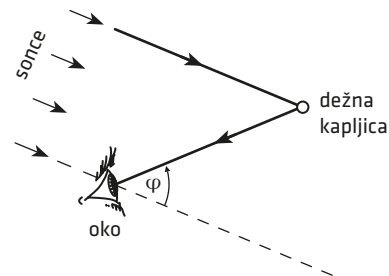
$$\sin \alpha_{\max} = \frac{2}{3} \sqrt{\frac{5}{3}}$$

in

$$\alpha_{\max} = 59,4^\circ, \quad \varphi_{\max} = 42,03^\circ.$$

Pomen mavričnega kota

Poglejmo ponovno sliko 8. Denimo, da narisani žarek zadene naše oko. Potem je kot φ enak kotu z vrhom v našem očesu, enim krakom v smeri sončnih žarkov (stran od sonca) in drugim krakom v smeri kapljice, iz katere žarek izhaja (slika 10). Ta kot lahko zavzame vrednosti od 0° do $\varphi_{\max}$. Ker je $\varphi_{\max}$ enak za vse kapljice, ustreza v prostoru temu pogoju **notranjost stožca z vrhom v našem očesu, osjo v smeri sončnih žarkov in kotom $\varphi_{\max}$ med osjo in stranico stožca.** V idealnem primeru, ko je opazovalec dovolj visoko in ves dopustni prostor zastira dežna zavesa, daje pojav vtis osvetljene krožne plošče v daljavi. V običajnih razmerah pa je več kot polovica tega stožca pod obzorjem. V zgornjem delu prihajajo do nas žarki tretjega reda, ki **jih dojemamo kot kos osvetljene polkrožne plošče.** Kolikšen je ta kos, je odvisno od višine sonca, konfiguracije obzorja in od obsega dežne zaves.



SLIKA 10.

Žarek tretjega reda po prehodu skozi kapljico zadene naše oko, če je kot med smerjo sončnih žarkov in smerjo proti kapljici enak kotu φ s slike 8.

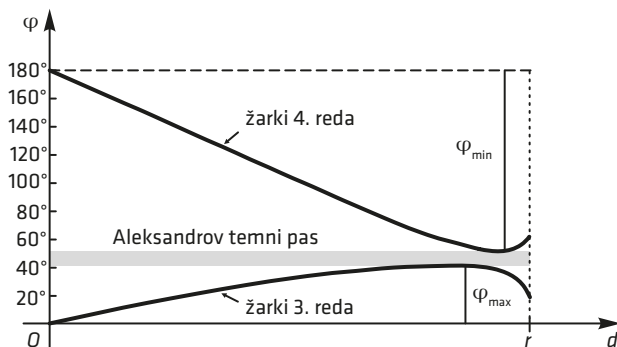
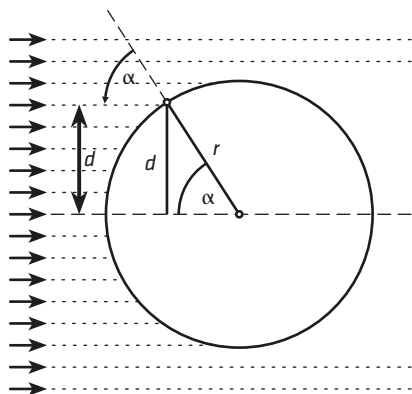
Porazdelitev svetlobe na mavrični plošči

Poglejmo, kako je s porazdelitvijo svetlobe na opisani navidezni plošči. Ker pripada dani kapljici ena sama ravnina, v kateri potuje žarek tretjega reda proti opazovalčevemu očesu, je tudi ta problem ravninski.

Sončna svetloba je v prostoru **enakomerno porazdeljena**. Za ravninski primer lahko to lastnost prikazemo s snopom med seboj enakomerno oddaljenih žarkov (slika 11). S slike vidimo, da temu ne ustreza enakomerna porazdelitev vpadnih kotov. **Pod manjšimi vpadnimi koti zadene kapljico več žarkov kot pod velikimi.** Enakomerna pa je porazdelitev oddaljenosti vpadnih žarkov od središča kapljice. Na sliki 11 je ta razdalja označena z d . Zavzame lahko vrednosti z intervala $[0, r]$, kjer je r polmer opazovane kapljice. Enako velikim intervalom spremenljivke d pripadajo enake količine vpadle svetlobe.

SLIKA 11.

Pod manjšimi vpadnimi koti zadene kapljico več svetlobe kot pod velikimi.



SLIKA 12.

Odvisnost smeri žarkov glavne in stranske mavrice od oddaljenosti žarka do središča kapljice s polmerom r .

Za opis svetlobe na navidezni svetli plošči v daljavi je zato primerneje v funkciji (2) zamenjati spremenljivko α s spremenljivko d . Opustimo analitičen zapis funkcije $\varphi(d)$, $d \in [0, r]$, pač pa si oglejmo njen graf na sliki 12. Na isti sliki je narisana tudi graf ustrezne funkcije za stransko mavrico.

Večjo koncentracijo svetlobe lahko pričakujemo v taki smeri φ , v kateri se združujejo žarki s širšega območja spremenljivke d . To je področje počasnega spreminjanja funkcije $\varphi(d)$, torej okolica maksimuma. S slike 12 razberemo, da za zelo širok interval spremenljivke d izhajajo žarki tretjega reda pod koti med 40° in 42° . Pri manjših vrednostih kota φ je svetlobe manj in je enakomernije porazdeljena. **Zato ima navidezna svetlobna plošča v bližini $\varphi_{\max}$, to je ob zunanem robu, svetel lok, ki blesti postopoma proti notranjosti in ostreje proti temni zunanji strani.** Zaradi tega dodatnega pomena kot $\varphi_{\max}$ res zasluži ime **mavrični kot**.

Kaj pa barve?

Pri izračunu mavričnega kota nismo upoštevali, da sestoji naravna bela svetloba iz barvnih komponent, saj smo funkcijo (2) dobili iz (1) z vstavljanjem $n = \frac{4}{3}$, približne povprečne vrednosti lomnega količnika za prehod svetlobe iz zraka v vodo. Dejansko pa bi morali vstaviti za vsako posamezno barvo njeno povprečno vrednost za n . Da ne bo preveč podatkov, navedimo le vrednosti za mejni barvi in pripadajoča mavrična kota:

barva	n	$\varphi_{\max}$
rdeča	1,329	$42,6^\circ$
vijolična	1,345	$40,3^\circ$

TABELA 1.

Vidimo, da je mavrični kot pri rdeči komponenti za dobri dve stopinji večji kot pri vijolični. Ko gremo v osnovnem spektru vidne svetlobe od vijolične preko modre, zelene, rumene in oranžne barve do rdeče, lomni količnik monotono pada. Pri tem mavrični kot monotono narašča od $40,3^\circ$ do $42,6^\circ$ glede na barve v istem vrstnem redu, kot si sledijo v osnovnem spektru.

Mavrica sestoji torej iz svetlobnih plošč različnih barv. Ker imajo skupno središče (na poltraku iz našega očesa v smeri sončnih žarkov), se v sredini prekrivajo in dajejo **belo ali svetlo sivo notranjost**



glavnega mavričnega loka. Posamezne barvne plošče so zaradi različnih mavričnih kotov različno velike. Največja je rdeča, najmanjša vijolična plošča. Zato rdeča plošča na zunanjem robu ni prekrita z drugimi barvami. To pojasnjuje, zakaj je rdeča barva v mavrici najčistejša. Ostale barve se bolj ali manj prekrivajo. Ker pa so njihovi močnejše obarvani zunanji robovi medsebojno rahlo premaknjeni, prevlada v mešanici na posameznem mestu ustrezna najmočnejša barva.

Lep lok glavne mavrice torej sestavljajo drug ob drugem nanizani barvni loki s skupno navidezno širino nekaj nad dvema stopinjama. V njem je vijolična barva najmanj izrazita, ker je prekrita z vsemi drugimi barvami. Včasih celo čisto zbledi. Ostale barve postajajo proti zunanjemu robu vse izrazitejše.

Stranska mavrica

Stransko mavrico obravnavamo podobno kot glavno, le da namesto žarkov tretjega reda analiziramo žarke četrtega reda. Odvisnost kota φ , ki ga merimo od istega poltraka kot pri žarkih tretjega reda, prikazuje zgornja krivulja na sliki 12.

Vidimo, da stranska mavrica ne oddaja nobene svetlobe v notranjost stožca, določenega s kotom $\varphi_{\min}$, ki meri približno 50° . To je **mavrični kot stranske mavrice**. Med posameznimi barvami ima najmanjši mavrični kot rdeča komponenta stranske mavrice, največjega vijolična. Zato si barve stranske mavrice slede od znotraj navzven v obratnem vrstnem redu kot pri glavni mavrici. Poleg tega so razlike med mavričnimi koti posameznih barv večje. Zato je stranska mavrica širša od glavne, je pa tudi bolj medla oziroma bleda. To lahko razložimo z večjo izgubo svetlobe pri žarkih četrtega reda v primerjavi z žarki tretjega reda. Delno pa pojasnjuje medlost tudi manj sploščeno teme zgornje krivulje na sliki 12.

Slika 12 pojasnjuje tudi **Aleksandrov temni pas**, temnejše področje med obema mavričnima lokoma. Vidimo, da žarki tretjega in četrtega reda ne prispevajo nič svetlobe v kote med 42° in 50° . Če ne bi bilo drugih žarkov, bi bilo to področje povsem črno.

Navidezna oddaljenost mavrice

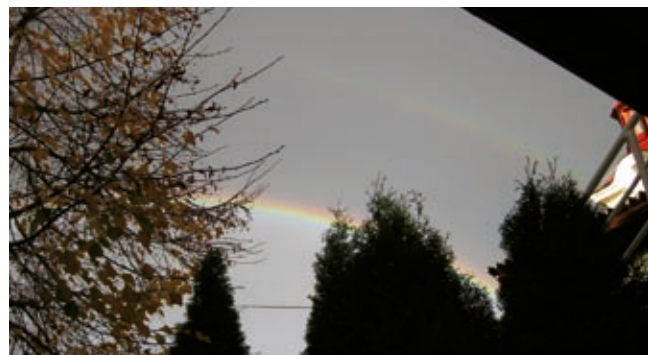
Dejstvo, da človek gleda z dvema očesoma, ima za

posledico globinski vid. To je sposobnost razločiti, da so predmeti od nas različno oddaljeni. Ker sta očesi postavljeni narazen, vidita isti predmet pod nekoliko različnima zornima kotoma. Bližje nas je predmet, večja je razlika med kotoma. Pri tem dobi vsako oko drugačno polpodobo predmeta. Možgani združijo obe polpodobi v eno samo in tako ustvarijo globinski vtis. Ta sega približno 1300 m daleč, nato pa se izgubi, ker postane razlika med zornima kotoma premajhna.

Mavrico zaznavata obe očesi pod mavričnim kotom, torej sta oba zorna kota enaka. Zato dojemamo mavrico kot zelo oddaljen predmet, četudi morda dežna zavesa, na kateri je mavrica nastala, blizu. Ta optična prevara je lahko moteča, kadar izza nedaleč nastale mavrice vidimo predmete, ki jih naš globinski občutek postavlja pred mavrico. Nenavaden občutek ustvarja tudi dejstvo, da se mavrica z opazovalcem premika glede na okolico. Zato je nikoli ne moremo doseči.

Pojavnost mavrice

Naravna mavrica se rada prikaže, če se po plohi hitro razjasni in nizko ležeče sonce obsije odhajajoče nevihtne oblake. V osrednji Sloveniji so zaradi prevladujočih zahodnih in jugozahodnih smeri vetra ti pogoji izpolnjeni najpogosteje pozno popoldne ob koncu vročinskih neviht. Večji verjetnosti za popoldansko kot dopoldansko mavrico botruje tudi dejstvo, da pade dopoldne navadno manj dežja kot popoldne. Izključena pa možnost dopoldanske mavrice seveda ni (slika 13).



SLIKA 13.

Jutranja mavrica na zahodnem nebu v okolici Ljubljane (foto Marija Vencelj).

Poleti okrog poldne v naših krajih naravna mavrica ni vidna, ker je sonce previsoko na nebu. Pa vendar se tudi to - sicer redko - lahko zgodi (slika 4).

Nedvisno od letnega časa in vremenskih razmer lahko mavrico opazimo v pršici fontan, škropilnikov ali slapov. Ker taka mavrica ni vezana na nevihte, jo veliko lažje in natančneje predvidimo.

V lepem vremenu si mavrico lahko napravimo sami, tako da s škropilko za zalivanje vrta ali pranje avtomobila naredimo zaveso iz vodnih kapljic. Dobljena mavrica je povsem enaka naravni. Le velikost mavričnega kolobarja je manjša, ker smo bližje odbojni steni iz vodnih kapljic (slika 14). Središče mavrice najdemo tako, da pogledamo v smeri svoje sence. Pri taki mavrici lahko tudi opazujemo, kako se premika glede na okoliške predmete, ko spreminjamo svoj položaj. Pojav je veliko izrazitejši kot pri naravni mavrici, saj se koti, odgovorni za mavrico, že pri majhnih premikih hitro spreminjajo. Poskusite!



SLIKA 14.

Mavrica, narejena na domačem vrtu (foto Marija Vencelj).

Zgodovina razlage mavrice

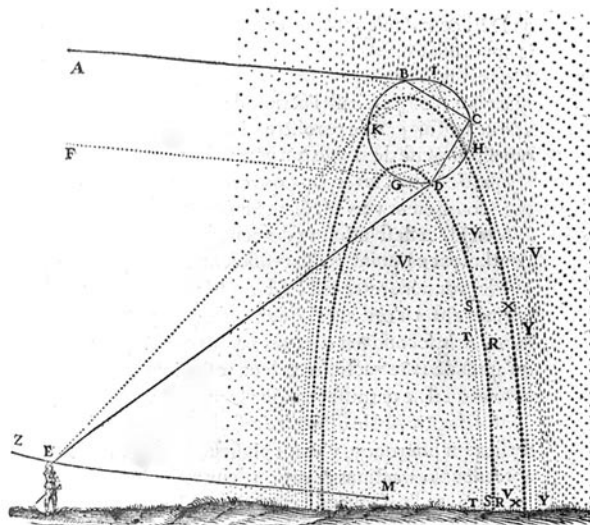
Prvi poskus znanstvene razlage mavrice zasledimo že okrog leta 1000. Veliki islamski učenjak Alhazen je domneval, da nastane mavrica pri **odboju** sončnih žarkov na oblaku z obliko vbočenega zrcala. Čeprav napačna, je bila ta domneva osnova kasnejšim praviim razlagam nastanka mavrice.

Da je mavrica posledica odboja **in loma** svetlobe, je že v 13. stoletju domneval poljski menih Witelo. Vendar je menil, da gre za lom in odboj na oblaku kot celoti.

Pomemben napredek pomeni trditev nemškega meniha Teodorica iz Freiburga v začetku 14. stoletja, da nastane mavrica zaradi loma in odboja sve-

tlobe **na posameznih vodnih kapljicah**. Opisal je lego glavne in stranske mavrice in razložil, zakaj je vrstni red barv v obeh mavricah medsebojno nasproten. Ker v njegovem času lomni zakon še ni bil znan, ni mogel razložiti, zakaj vidimo mavrico vedno pod istim kotom glede na smer sončnih žarkov. Do enakih zaključkov kot on je neodvisno prišel njegov sodobnik, perzijski astronom al-Farisi. Skupno jima je, da sta osnove črpala iz Alhazenove knjige Optika.

Njuno razlago je tristo let kasneje, kmalu po odkritju lomnega zakona, nadgradil francoski filozof, matematik in fizik René Descartes (slika 15). Natančno je opisal pot vzporednih sončnih žarkov, ki zadenejo kapljico pod različnimi vpadnimi koti, in razložil **mavrični kot** glavne in stranske mavrice.



SLIKA 15.

Descartesova skica razlage mavrice iz leta 1637. Žarek ABCDE prikazuje pot žarkov glavne mavrice, žarek FGHKE pot žarkov stranske mavrice.

Barvitost mavrice je postala razumljiva šele po letu 1666. Tedaj je angleški matematik, fizik in astronom Isaac Newton s svojim slavnim poskusom prehoda svetlobe skozi tristrano prizmo pokazal, da je bela svetloba mešanica vijolične, modre, zelene, rumene, oranžne in rdeče barve in da se vsaka teh barv nekoliko drugače lomi.

Tako so bili z metodo geometrijske optike, na katero smo se v tem prispevku omejili tudi mi, poja-



→ snjeni najbolj opazni mavrični pojavi. Ni pa moč z njo pojasniti navidezno manj pomembnih pojavov. Za njihovo razumevanje je treba upoštevati valovno naravo svetlobe. Angleški učenjak Thomas Young je leta 1804 z interferenco pojasnil pojav **dodatnih lokov**, ki leže na notranji strani glavne mavrice. Njegovo delo je kasneje dopolnil George B. Airy, ki je pokazal, da je jakost dodatnih lokov odvisna od velikosti dežnih kapljic. Čim manjše so kapljice, tem redkejši in zato jasneje vidni so dodatni loki. Ko kapljice dežja padajo, se večajo, zato dodatne loke lažje opazimo blizu vrha mavrice.

Moderni fizikalni opisi mavrice in sorodnih pojavov, npr. glorijs, temeljijo na Mieovem sipanju. To nastaja na zelo majhnih okroglih kapljicah, katerih velikost je približno enaka valovni dolžini vidne svetlobe, to je nekaj sto nanometrov.

× × ×



Galilei in pospešek



JANEZ STRNAD

→ Mednarodno leto astronomije 2009 so razglasili v spomin na leto 1609. Tedaj je Galileo Galilei med prvimi usmeril daljnogled v nebo in nebo prvi načrtno raziskal. Odkril je gore na Luni, zvezde v Rimski cesti, štiri Jupitrove Lune, pa še Saturnov obroč, ki ga s svojim daljnogledom ni mogel razločiti od planeta, Venerine mene in Sončeve pege. Leta 1609 je Johannes Kepler odkril prva dva zakona o gibanju planeta po elipsi. Galilei je dosegel veliko tudi v fiziki, tako da nekateri v njem ne vidijo samo „očeta opazovalne astronomije“, ampak tudi „očeta fizike“. Med drugim je odkril zakon o padanju in z njim zajel gibanje izstrelkov. Povejmo nekaj o tem.

Padanje kamna in kotaljenje kroglice po blagem klanecu je enakomerno pospešeno gibanje. Galilei je tako gibanje prištel k „lokalnim gibanjem“, to je gibanjem na Zemlji, da ga je razlikoval od gibanja planetov. Lokalnim gibanjem je leta 1638 posvetil tretje in četrto poglavje, to je zadnji poglavji, v knjigi *Razprave in matematični dokazi o dveh novih znanostih, ki zadevata mehaniko in lokalna gibanja*. Po Evklidovem in Arhimedovem zgledu je svoje ugotovitve oblikoval kot *izreke*. Kot prve tri izreke je v tretjem poglavju navedel:

1. Čas, v katerem telo iz mirovanja z enakomernim pospešenim gibanjem preide določeno razdaljo, je enak času, v katerem bi telo prešlo to razdaljo z enakomerno hitrostjo, katere vrednost je enaka povprečju največje hitrosti in hitrosti, tik preden se je pospeševanje začelo.

2. Razdalje, ki jih preleti telo, padajoče iz mirovanja, so v razmerju kvadratov časov, v katerih preleti te razdalje.

3. Če se telo iz mirovanja giblje po klanecu in pada navpično iz enake višine, sta časa v razmerju dolžine klanca in navpičnice.

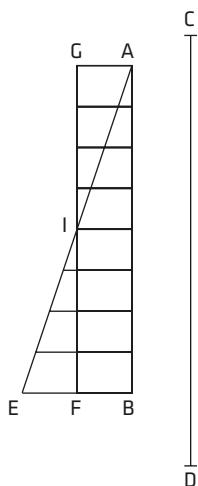
Prvi izrek iz četrtega poglavja se je glasil:

1'. Izstrelek, ki se giblje enakomerno v vodoravni smeri in hkrati enakomerno pospešeno v navpični smeri, opiše tirnico, ki je polovica parabole. Dandanes te ugotovitve v nekaj vrsticah izpeljemo iz Newtonovega zakona, potem ko na klanecu razstavimo težo na komponenti v smeri klanca in pravokotno na klanec.

V prevodih Galilejeve knjige zaman iščemo en sam podatek o pospešku. V prvi izdaji iz leta 1638 pa sta dva podatka, iz katerih je mogoče izračunati pospešek prostega padanja. Po prvem podatku pade telo iz višine 200 vatlov v manj kot desetih srčnih utripih in po drugem iz višine 100 vatlov v petih sekundah. Prvi podatek da za pospešek prostega padanja več kot $4,0 \text{ m/s}^2$ in drugi $5,6 \text{ m/s}^2$. To je precej manj od pravega pospeška $g = 9,807 \text{ m/s}^2$ v Padovi, kjer je Galilei izvedel večino poskusov. Najbrž so zato v prevodih podatka izpustili.

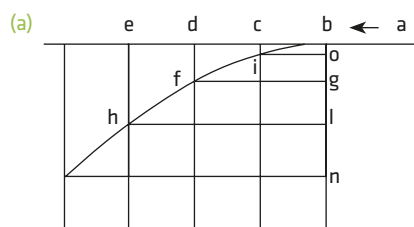
➤ Iz enačbe $y = \frac{1}{2}gt^2$, v kateri so y višina in t čas ter g pospešek prostega padanja, izračunamo pospešek $g = 2y/t^2$. Če računamo z 72 utripi v minuti, to je 60-ih sekundah , desetim utripom ustreza čas $10 \cdot 60 \text{ s} / 72 = 8,3 \text{ s}$. Vatel (braccio) so uporabljali za merjenje dolžine blaga. Zanj danes navedejo $0,7 \text{ m}$, nekdanj pa je meril lahko tudi manj. Prvi podatek da za pospešek $g = 4,0 \text{ m/s}^2$. Če bi upoštevali krajši vatel, bi bil pospešek še manjši. Ker je navedeno, da je čas krajši od desetih utripov, je pospešek večji od $4,0 \text{ m/s}^2$. Z drugim podatkom dobimo pospešek $5,6 \text{ m/s}^2$.

Galilei se je lahko oprl le na geometrijo in sorazmerje. Tedaj niso poznali pojma funkcije in niso pisali enačb s simboli za količine. Obstajale so že me-



SLIKA 1.

V Galilejevem času še ni bilo pojma funkcije. Z risbo, v kateri še ni koordinatnih osi, je Galilei utemeljil trditev, da je pri enakomernem pospešenem gibanju povprečna hitrost enaka polovici vsote začetne in končne hitrosti.



SLIKA 2.

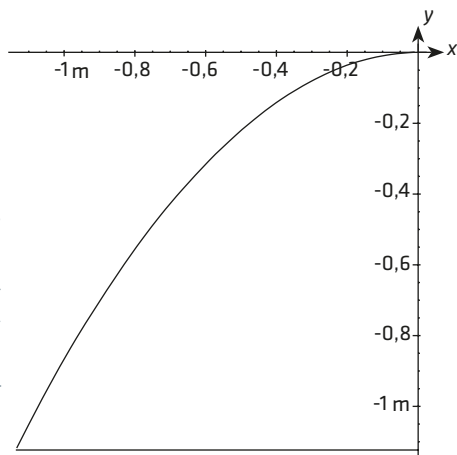
Tako je Galilei izračunal tirnico telesa pri vodoravnem metu (a) in zaznamoval polovico parabole ab, bc je dolžina, ac višina, ae vzvišenost, vodoravna črta ad pa kaže smer začetne hitrosti (b). Ta in prejšnja slika sta iz angleškega prevoda Galilejevih *Razprav in matematičnih dokazov o dveh novih znanostih*.

hanične ure, večinoma na cerkvenih stolpih, z enim samim kazalcem. Na dan so zaostale ali prehitete do četrte ure. S tako uro ni bilo mogoče meriti sekund, čeprav so enoto že poznali. Galilei ni mogel meriti kratkih časov pri prostem padanju. Pomagal si je tako, da je „razredčil“ težni pospešek. Namesto prostega padanja je opazoval kotaljenje kroglic po blago nagnjenem klanecu. Po izreku 3 je s tem pospešek zmanjšal v razmerju med višino in dolžino klanca. Galilei še ni imel izdelanega pojma sile in ni poznal zakona gibanja. Zato po podatkih pri kotaljenju kroglic po klanecu in nihanju nitnega nihala ni mogel izračunati pospeška prostega padanja.

Galilei se je prepričal, da je kotaljenje kroglice po klanecu enakomerno pospešeno gibanje s sorazmernostjo med potjo in kvadratom časa: $s/s_1 = t^2/t_1^2$. Čase je primerjal z opazovanjem srčnega utripa ali

**SLIKA 3.**

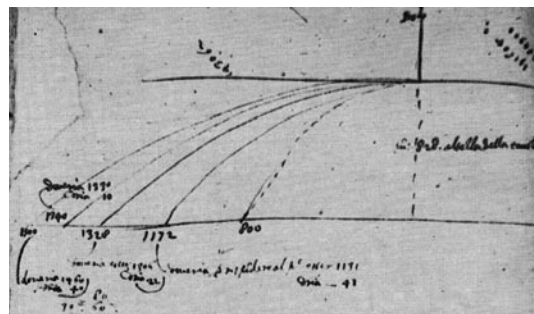
Risba parabole vodnega curka pri preprostem poskusu. Os x smo obrnili v levo, da parabola ustreza paraboli na Galilejevi sliki.



razmikov med poki, ko je kroglica preskakovala vrvice, s katerimi je ovil klanec. Vrvce je premikal, dokler si poki niso sledili v enakih časovnih razmikih. Pri tem si je pomagal s petjem, ki mu ni bilo tuje, saj sta bila oče in brat glasbenika. Z ritmičnim petjem je mogoče držati takt na desetino sekunde natančno. Natančneje je primerjal čase tako, da je pustil vodo teči iz posodice skozi slamico na dnu v spodnjo posodo. Slamico je odprl, ko se je gibanje začelo, in zaprl, ko se je končalo. Razmerje časov je bilo enako razmerju tež vode, ki se je natekla iz posodice v posodo in ki jih je stehal z natančno tehtnico. Poskus je ponavljal, da je izboljšal natančnost. V novejšem času so poskus večkrat izvedli z napravami, ki jih je imel na voljo Galilei, in podprli njegove ugotovitve.

Zaradi težav pri merjenju časa se Galilei ni izogibal samo podatkom za pospešek, ampak tudi podatkom za čas in hitrost. Polovico parabole pri vodoravnem metu je označil z *dolžino* (amplitudo) x , *višino* y in *vzvišenostjo* (sublimnostjo) Y . Pri paraboli s temenom v izhodišču je x abscisa in y ordinata točke na paraboli, Y pa višina, iz katere bi moralo telo navpično pasti, da bi doseglo začetno hitrost v vodoravni smeri. Abscisa je $x = v_x t$ s konstantno komponento hitrosti v_x v vodoravni smeri, ordinata pa $y = \frac{1}{2}gt^2$ s spremenljivo navpično komponento hitrosti $v_y = gt$. Os y usmerimo navpično navzdol. Vzvišenost je $Y = \frac{1}{2}v_x^2/g$. Vsota ordinate in vzvišenosti $y + Y = \frac{1}{2}(v_y^2 + v_x^2)/g$ določa kvadrat velikosti hitrosti telesa $v^2 = v_x^2 + v_y^2$ v končni točki.

Iz enačbe za absciso izračunamo čas $t = x/v_x$, vstavimo v enačbo za ordinato in dobimo enačbo parabole $y = \frac{1}{2}gx^2/v_x^2$. Za nagib y tirnice v končni točki velja $\tan y = v_y/v_x = gt/v_x = gx/v_x^2$, tako da

**SLIKA 4.**

Risba iz Galilejeve neobjavljene zapuščine opiše vodoravni met kroglic. Vzeta je iz članka Draka in MacLachlana *Galileo's discovery of the parabolic trajectory* v *Scientific American* 323 (1975) 102 (3).

je $Y = \frac{1}{2}x/\tan y$. Z nekaj računanja ugotovimo, da je $y + Y = x/\sin 2y = y/\sin^2 y$. Galilei ni uporabljal razmerij stranic v pravokotnem trikotniku, današnjih kotnih funkcij, ki so jih tedaj že uvajali astronomi. Vseeno je sestavil obsežne tablice za dolžino x in višino y v odvisnosti od nagiba y pri konstantni velikosti končne hitrosti ter višine y in vzvišenosti Y v odvisnosti od nagiba pri konstantni dolžini x . Pri tem je nagib spreminjal v korakih po 1° . Lahko si mislimo, koliko truda ga je to stalo, ker ni uporabljal enačb s simboli za količine, ampak le sorazmerje in lastnosti parabole, ki jih je dobro poznal. Zaradi tega toliko više cenimo Galilejeve dosežke. Pisanje enačb s simboli in znanje o funkcijah danes močno olajšata delo.

Galilei bi mogel natančneje ugotoviti pospešek prostega padanja. Opišimo, kako bi to lahko naredil. Iz šobe na cevi brizga curek vode. Najprej izmerimo prostornino vode V , ki se nateče v posodo v $t = 60$ s. Hitrost vode v šobi je $v_x = V/(tS)$, če je $S = \pi R^2$ presek šobe s premerom $2R$. Cev postavimo tako, da curek iz nje izteka v vodoravni smeri. Izmerimo vodoravno razdaljo x od šobe do točke, v kateri curek zadene vodoravno podlago v višini y pod šobo. To vstavimo v enačbo za tirnico in izračunamo pospešek:

$$g = \frac{2yv_x^2}{x^2}.$$

Poskus naredimo na vrtu. Zalivanju namenjeno cev pritrdimo na lestev s šobo v višini $y = 1,12$ m. Cu-

rek naravnomo tako, da zadene tla v enaki vodoravni razdalji $x = 1,12$ m. V minuti se je z njim v posodo nateklo 2,5 l vode. Premer curka je bil malo manjši od 5 mm. Upoštevamo 4,8 mm, kar je lahko nenatančno za enoto na zadnjem mestu. Za hitrost curka da to $v = V/(t\pi r^2) = 2,5 \cdot 10^{-3} \text{ m}^3/[60 \text{ s} \cdot \pi \cdot (2,4 \cdot 10^{-3} \text{ m})^2] = 2,3 \text{ m/s}$. Za $x = y$ sledi iz zapisane enačbe pospešek prostega padanja $g = 2v^2/x = 2 \cdot (2,3 \text{ m/s})^2/(1,12 \text{ m}) = 9,4 \text{ m/s}^2$. S premerom curka 4,7 mm bi dobili pospešek $10,3 \text{ m/s}^2$, s premerom 4,9 mm pa $8,7 \text{ m/s}^2$. Dobljeni pospešek je manjši od pravega $9,8 \text{ m/s}^2$. Izid je nenatančen predvsem zaradi tega, ker premera curka pri poskusu nismo mogli izmeriti natančneje. Vseeno pa je izid precej natančnejši od Galilejeve ocene.

Podobno bi lahko ravnal Galilei. Že Leonardo da Vinci je opazoval vodne curke v obliki parabole. Galilei pa ne bi mogel izmeriti časa v sekundah. Za pospešek bi navedel $9,3$ vatla/utrip². Sekunde so začeli meriti proti koncu 17. stoletja po zaslugi angleških urarjev potem, ko je Christiaan Huygens leta 1657 patentiral uro na nihalo.

R. G. Mentzer je v članku *Measuring the acceleration due to gravity. An experiment Galileo could have run*, The Physics Teacher 22 (1984) 580–581 opisal poskus, ki bi ga tudi lahko izvedel Galilei. Kroglico so spustili po klanecu, na 2 m dolgi vodoravni poti izmerili hitrost njenega težišča in jo nato pustili, da je padla. Višino kroglice so v različnih razdaljah ugotavljali tako, da so pri različnih razdaljah postavili navpično merilno palico s papirjem in kopirnim papirjem. Na mestu, na katerem je kroglica zadela palico, je nastala sled. Merjenje s curkom je preprostejše.

Za kotaljenje kroglic dobimo iz zakona o vrtenju, ki ga Galilei tudi še ni poznal:

$$\begin{aligned} M &= J\alpha, \quad mgr \sin \beta = \left(\frac{2}{5}mr^2 + mr^2\right)\alpha, \\ a &= \alpha r = \frac{5}{7}g \sin \beta \end{aligned}$$

Pri tem je M navor teže glede na trenutno mirujočo os v točki, v kateri se kroglica dotika tal in okoli katere se v trenutku vrti, β pa je nagib klanca. Teža prijmlje v središču kroglice. J je vztrajnostni moment kroglice s polmerom r okoli te osi, α kotni pospešek pri vrtenju okoli te osi in $a = \alpha r$ pospešek težišča kroglice.

Nihajni čas nitnega nihala z dolžino l pri majhnih amplitudah je $t_0 = (2\pi)\sqrt{l/g}$. Galilei je vedel za sorazmernost nihajnega časa s $\sqrt{l}$, a ni poznal enačbe, ker ni poznal zakona gibanja.

Stillman Drake in James MacLachlan sta v Državni centralni knjižnici v Firencah raziskovala neobjavljene Galilejeve zapiske. Pri tem sta naletela na podrobna opisa dveh zanimivih poskusov. Pri prvem je Galilei spuščal bronaste kroglice po nagnjeni deski z žlebom, ki je bil na koncu ukrivljen, da je kroglica odletela v vodoravni smeri. Meril je vodoravno razdaljo x , v kateri so kroglice udarile na tla po padcu za višino $y_1 = 77,7$ cm. Kroglica je bila namazana s črnilom, tako da je bilo mogoče ugotoviti, kje je zadela tla. Pri tem je večal dolžino klanca in ugotavljal, kako se je večala dolžina x . Za dolžino klanca si je po vrsti izbiral podatke z okroglim številom *puntov*. 1 punto ustreza 0,938 mm (slika 4).

Drake in MacLachlan sta ponovila poskus in dobila Galilejeve izide z nagibom klanca $\beta = 30^\circ$. Namesto pospeška težišča kotaleče se kroglice $a = \frac{5}{7}g \sin \beta = 3,5 \text{ m/s}^2$ sta najboljše ujemanje dobila s pospeškom $a = 3,2 \text{ m/s}^2$. Morda je bil žleb tako širok, da se je kroglica vanj malo ugreznila in je bil polmer trenutno mirujoče točke manjši od polmera kroglice r . Z enačbami $t = \sqrt{2s/a}$ in $s = \frac{1}{2}v_0^2/a$ je sledilo

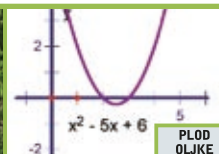
$$\blacksquare \quad x = \sqrt{2v_0^2 y_1 / g} = \sqrt{4a s y_1 / g}.$$

Po tej enačbi izračunani podatki so se od štirih Galilejevih izmerkov razlikovali za največ 2,8 %.

Na mestu, kjer je bil žleb ukrivljen, je kroglica poskočila. Morda je to Galileja napeljalo na drug poskus, pri katerem je pustil žleb raven, tako da je kroglica odletela z začetno hitrostjo v_0 poševno navzdol.

Poskusa sta pomembna. Nedvoumno sta pokazala, da je Galilei izvajal podrobne poskuse in pri njih meril razdalje na milimeter natančno. Ni obravnaval samo vodoravnega meta, ampak tudi poševni met. Zgodovinarji so večkrat menili, da je Galilei svoje „izmerke“ pravzaprav dobil z računom, češ da nekaterih sploh ne bi mogel tako natančno izmeriti. V opisanih poskusih Galilei ni mogel ničesar izračunati, zato je zagotovo zares izmeril. Pri tem ni mogel vedeti, koliko je pri gibanju po klanecu pospešek a manjši od pospeška g pri padanju. Pri kotaljenju kroglice po klanecu je odpovedal izrek 3. Morda je bil to razlog, da Galilei o opisanih poskusih ni poročal v *Dveh novih znanostih*. xxx

A diagram showing a beam of white light entering a triangular prism from the top. The light is dispersed into a spectrum of colors as it exits the bottom. The colors are labeled from top to bottom: vijolična (violet), modra (blue), zelena (green), rumena (yellow), oranžna (orange), and rdeča (red).

16

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 **3. oktobra 2010**, ko bomo izžrebali tri nagrajence, ki bodo za nagrado prejeli **Presekov paket**.

Kateri se hitreje kotali?

ODGOVOR NALOGE



MOJCA ČEPIČ

→ Pri iskanju odgovora na nalogo, je bilo treba narediti nekaj meritev. Lahko pa ste seveda dogajanje le opazovali in samo primerjali, tako, bolj na oko.

Mi smo se igrali z manjšim kozarcem za vlaganje, v katerem so bile predhodno kapre. Postopoma smo ga polnili z lečo. Pravzaprav ni pomembno, katero vrsto semen vzamemo, le rezultati se bodo morda nekoliko razlikovali. Za enoto polnjenja smo izbrali manjši kozarček za žgane pijače, ki ne služi prav pogosto svojemu osnovnemu namenu. Kozarec smo kotalili po jedilni mizi, čas pa smo merili z mobilom, saj imajo možnost štoparice danes že najenostavnejši modeli. Mizo smo podložili z revijami Monitor, katerih stari letniki so prav v teh dneh na poti v zbiralnik papirja. Stare revije so še posebej primerne, ker so približno enako debele in je z njimi mogoče precej natančno nagniti mizo na naklon, ki ga želimo. Postavitev poskusa in pripomočke si lahko ogledate na slikah 1 in 2. Revije pod mizo so bile pripravljene za meritev pri največjem naklonu. Kotalili smo manjši stekleni kozarec, večji stekleni kozarec je samo „zaloga“ leče, merili smo pa z majhnim kozarčkom na desni. Kozarec, ki smo ga kotalili, smo do vrha napolnili s sedmimi kozarčki leče. Stoli na koncu mize skrbijo le zato, da kozarec ni padal na tla.

Naloge smo se lotili po znanstveno. Izbrali smo neodvisno spremenljivko pri poskusu, torej fizikalno količino, katere vpliv na izid poskusa smo želeli raziskati. To je seveda bila količina leče v kozarcu, ki smo jo merili v številu „kozarčkov“. Izbrali smo tudi spremenljivko, na katero je vsebina kozarca vplivala



SLIKA 1.

Postavitev poskusa. Kup revij je bil visok 10,5 cm pri najvišjem podlaganju.



SLIKA 2.

Kozarec za kotaljenje (levo), zaloga leče (sredina) in merica (desno).

in jo je bilo najenostavneje meriti – čas kotaljenja po mizi. Seveda je vsebina kozarca vplivala tudi na druge spremenljivke, npr. na povprečno hitrost, vendar teh nismo neposredno merili. Zavedali smo se tudi kontrolnih spremenljivk, torej okoliščin, ki jih je bilo potrebno nadzorovati. Za vse poskuse je bila enako dolga pot kotaljenja in vsakič smo kozarec le spustili, da je bila njena začetna hitrost enaka nič. Naklon mize smo spremenili le za vsako serijo poskusov. Naklon je torej imel vlogo kontrolnega parametra.

Spodnja tabela kaže kar nekaj podatkov. Izmerili smo čas, ki ga je kozarec potrebovala za kotaljenje preko mize, izračunali pa smo tudi povprečno hitrost kozarca. Ker je na kotaljenje kozarca močno vplival naklon mize, smo poskuse ponovili pri nekaj različnih naklonih mize.

Pot, po kateri se je kotalil kozarec, je bila dolga $l = 148$ cm. Naklonski kot, izražen v stopinjah, smo izračunali kot $\arcsin(h/l)$.

št. meric	$h = 5,5$ cm; $\varphi = 2,1^\circ$		$h = 7$ cm; $\varphi = 2,7^\circ$		$h = 10,5$ cm; $\varphi = 4^\circ$	
	čas kotaljenja [s]	povpr. hitrost [cm/s]	čas kotaljenja [s]	povpr. hitrost [cm/s]	čas kotaljenja [s]	povpr. hitrost [cm/s]
0	3,9	37,9	3,2	46,7	2,7	54,4
1	9,0	16,5	4,5	33,0	3,3	44,6
2	∞	0	∞	0	5,5	27,1
3	∞	0	∞	0	10,5	14,1
4	∞	0	∞	0	7,7	19,8
5	∞	0	7,6	19,4	4,7	31,6
6	5,5	26,8	4,4	34,0	3,1	47,9
7	3,5	42,3	3,1	46,3	2,5	58,3

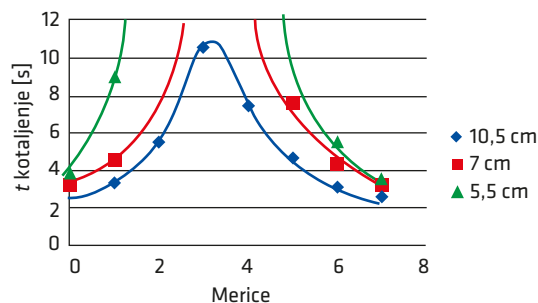
TABELA.

Na slikah 3 in 4 si lahko ogledamo tudi grafični predstavitev časov, ki jih je potreboval kozarec pri različnih meritvah, ter povprečnih hitrosti kozarcev, izračunanih iz časov.

Iz rezultatov lahko takoj razberemo nekaj zanimivih spoznanj:

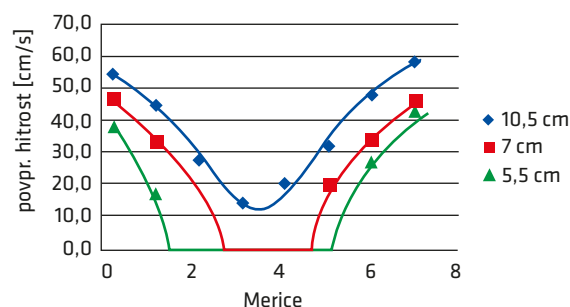
- Prazen in polni kozarec sta najhitrejši, še več, sta približno enako hitri; govorimo o povprečni hitrosti.
- Ko plastenko polnimo, povprečna hitrost nekaj časa upada, nato začne ponovno naraščati.
- Če je naklon mize premajhen, se kozarec, napolnjen z lečo, sploh ne zakotali.

Najprej razmislimo, kako smo zapolnili tabele s podatki, nato pa še, zakaj je obnašanje pravzaprav takšno. Običajno nismo navajeni, da bi okrogle za-



SLIKA 3.

Odvisnost časa kotaljenja kozarca od števila meric leče v kozarcu. Različne barve podajajo različne višine podlaganja.



SLIKA 4.

Odvisnost povprečne hitrosti kotaljenja kozarca od števila meric leče v kozarcu. Različne barve podajajo različne višine podlaganja.

deve kar mirovale na nagnjenih površinah.

Izračun povprečne hitrosti je enostaven. Povprečna hitrost je definirana kot razmerje

$$\bar{v} = \frac{\text{razdalja}}{\text{čas za razdaljo}} = \frac{l}{t}.$$

Gibanja kozarca ne moremo uvrstiti v eno od kategorij preprostih načinov gibanja, npr. enakomerno ali enakomerno pospešeno. Natančne analize kažejo, da je kotaljenje polnega in praznega kozarca enakomerno pospešeno, vidimo tudi, da se poln in prazen kozarec kotalita približno z enako povprečno hitrostjo. Za vse kozarce, v katerih se leča presipava, pa preprosti opisi gibanj ne veljajo. Včasih se gibljejo pospešeno, še večkrat pa se po začetnem pospeševanju gibljejo enakomerno. Vidimo tudi, da presipava-



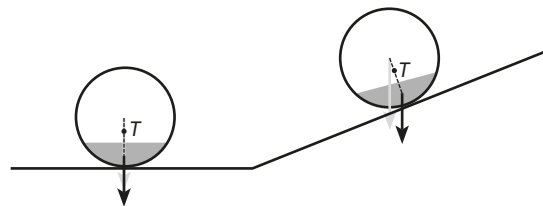
nje leče upočasni gibanje kozarca, saj so časi kotaljenja na pol polnih kozarcev najdaljši ali pa se kozarec sploh ne kotali.

Zakaj tako? Dokler je kozarec prazen, ga lahko obravnavamo kot kotaljenje praznega valja z dvema tankima valjema ob robovih. Ko je popolnoma poln in se leča v njem ne presipa, ga lahko obravnavamo kot valj z vstavkom polnega valja z manjšo gostoto od stekla. Natančnejši račun bi pokazal, da lahko pričakujemo za poln kozarec nekoliko večji pospešek kot za praznega. Da je to res, odražajo tudi meritve, saj so časi kotaljenja polnega kozarca nekoliko krajši od časov kotaljenja praznega kozarca.

Bolj zapletena je zadeva z deloma napolnjenim kozarcem. Vidimo dva pojava, ali zrna leče ob steni kozarca kar drsijo, kar je značilno za manjše količine leče v kozarcu, ali pa del zrn drsi, gornja plast zrn pa se presiplje. V obeh primerih prihaja med zrna leče do trenja, zato se del mehanske energije, ki je bila na začetku poskusa v obliki potencialne energije, pretvarja namesto v kinetično energijo kotaljenja tudi v notranjo. Če bi lahko temperatura zrn natančno merili, bi se le-tem temperatura nekoliko zvišala. Žal so take naprave precej zahtevne.

Energija se iz ene oblike mehanske energije (potencialne, kinetične ali prožnostne) lahko spreminja v drugo le, kadar ni trenja in je telo brez notranje strukture. Kadar pa so telesa sestavljena iz mnogih komponent, kot naš kozarec z lečo, navaden bicikel ali mi sami, lahko notranje gibanje komponent vpliva na zunanje sile, ki telesa pospešujejo ali zavirajo, pri tem pa del lastne energije pretvarja tudi v notranjo ali iz nje v mehansko, če k notranji energiji štejemo tudi kemijsko. Podobno dogajanje izkoristimo pri vožnji po klancu navzdol, ko kolo zaviramo s trenjem zavor ob obroče ali diske. Obratno pa lahko pretvorimo svojo notranjo energijo (npr. zajtrka) v svojo potencialno energijo pri hoji po stopnicah navzgor.

Še besedo o mirovanju na nagnjeni površini. Če je lepenje med koščki leče večje, kot so sile teže, ki poskušajo lečo premakniti drugo ob drugo ali ob steklu, prevelike, se leča v kozarcu ne premakne. Kozarec se nekoliko zakotali, a le toliko, da težišče leče ni več neposredno pod središčem kozarca, ampak se nekoliko premakne nazaj nad gornji del kozarca (kot kaže slika 5). Tako se navara, ki ju povzroča teža kozarca in teža leče, med seboj uravnovesita in kozarec ne zdrsne.



SLIKA 5.

Na ravni je leča razporejena pod težiščem kozarca, na klanecu pa sile lepenja med zrna leče ter zrna leče in stenami kozarca preprečijo premikanje zrn in prerazporejanje v nižje lege. S T je na sliki izenačeno težišče, s sivo puščico pa teža kozarca ter s črno teža leče. Slika je shematska.

xxx

Sudoku

	a	b	c	d	e	f	g	h	i
A	3					4	2	7	
B	1	9			2				4
C			2	8	3		5		
D			1	5		7	3		
E		3	8			2			1
F	9				8			6	5
G	7	6				5		8	
H			3	6			9	4	
I		1		9	7				2

xxx

www.presek.si

xxx

Opazuj svoje drevo, kako spreminja barve jeseni



MOJCA ČEPIČ

→ V prejšnji nalogi smo se ukvarjali z resnimi merjenji, v tej nalogi pa bomo izvedli opazovanje. Učitelji fizike pravimo temu „dolgotrajno opazovanje“ in s tem mislimo, da bomo določeno dogajanje opazovali dalj časa, vsaj nekaj dni, včasih tudi tednov, mesecev ali celo let.

Ko govorimo o dolgotrajnih opazovanjih, navadno opazujemo, pogosto pa tudi merimo, lastnost ali več njih pri določenem pojavu v naravi. Tokrat bi se radi osredotočili na barvo jesenskega listja. Ker pri tem opazovanju ne moremo ravno poskušati, bomo poskusili razloge za rezultate opazovanja pojasniti v odgovoru naloge. Z opazovanjem pa bi radi poiskali tudi morebitne namige, kaj na barvo drevesnega listja oziroma njen razvoj pravzaprav vpliva.

Za izvedbo naloge potrebujete digitalni fotoaparat. Seveda bi zadoščal tudi klasični aparat, a danes ga nima skoraj nihče več. V bližini svojega doma si izberite eno, dve ali več posameznih dreves in jih vsako zase slikajte vsak teden enkrat, najbolje na isti dan v tednu ob približno isti uri dneva. Za primerjavo, torej za študij vplivov na barve, lahko izberete drevo blizu cestne svetilke in enako drevo oddaljeno od svetlobe. Lahko preprosto izberete nekaj različnih vrst dreves, ki rastejo v enakih okoliščinah. Lahko primerjate drevesi enake vrste, ki raste na različnih nadmorskih višinah, če vključite v opazovanje katerega od prijateljev iz drugih krajev. Skratka, možnih primerjav ne manjka. Primerjave so tiste, ki v znanosti pripeljejo do mnogih novih spo-

znanj. Pošljite nam svoje serije fotografij z opisom vrste drevesa, okoliščin, v katerih je drevo rastle, in datumi slik. Opišite nam (na naslov presek@dmfa.si) tudi svoja opažanja, morda v povezavi z vremenom ali temperaturami.

xxx

Razmisli in poskusi



MITJA ROSINA



39. **Lok in frača.** Na jesenskih izletih si boste gotovo kdaj napravili lok s puščicami ali fračo. Poleg športnega užitka boste lahko tekmovali s prijatelji, naučili pa se boste tudi nekaj fizike.

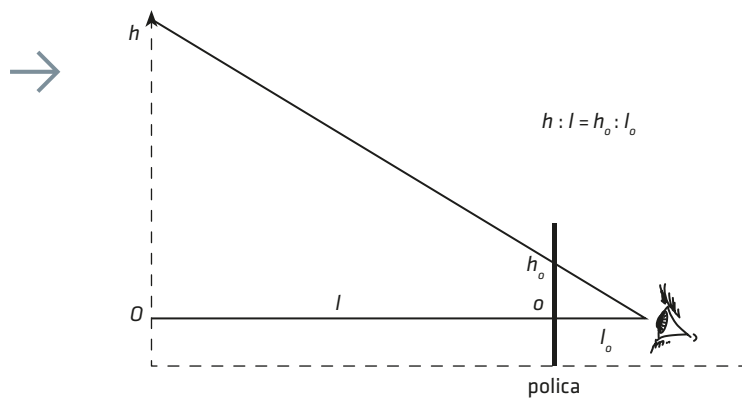
Na tetivo loka obesite tolikšno utež, da se bo lok napol toliko kot pri streljanju. S tem ocenite maksimalno silo, povprečna sila pri napevanju $\bar{F}$ je približno polovica tega. Opravljeno delo je torej $A = \bar{F} \cdot d$, kjer je d premik središča tetive. To delo prejme puščica, njena potencialna energija v najvišji točki je mgh . Stehajte maso puščice m in ocenite višino strele h . Pri meritvi višine naj vam pomaga prijatelj, ki opazuje pod kakšnim kotom vidi vrhno lego puščice. Izmerite, na kateri višini se ustrezna točka na palici navidezno prekriva s puščico, in uporabite sorazmerje pri podobnih trikotnikih (slika 1). Lahko pa streljate ob drevesu, si zapomnite, do katere veje je priletela puščica in naknadno izmerite višino te veje po opisani metodi ali kako drugače.

Preverite, ali se je vse delo izkoristilo za dvig puščice. Kaj mislite, kdo je „poneveril“ preostalo delo?

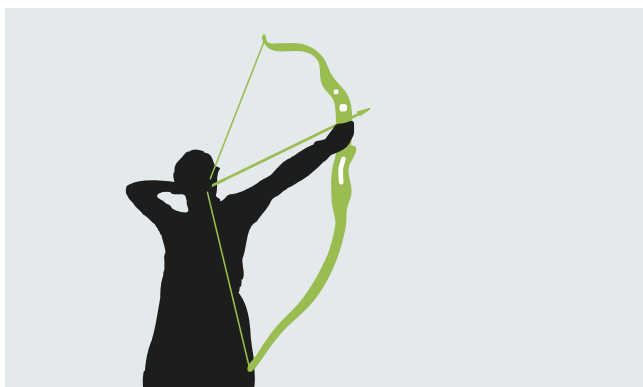
Priporočamo streljanje navzgor, ker je tako najlažje določiti energijo puščice, pa tudi najbolj varno je.

Podobne meritve in študijo lahko napravite tudi s fračo.

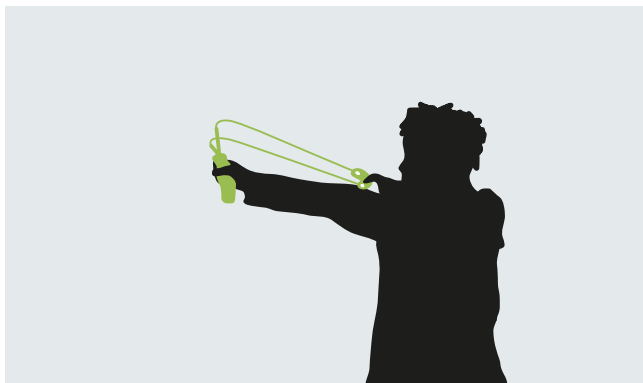
Odgovor na vprašanje iz prejšnje številke Preseka bo objavljen v naslednji številki, da boste imeli še nekaj časa za poskuse in razmislek.

**SLIKA 1.**

Določanje višine s podobnimi trikotniki.

**SLIKA 2.**

Lokostrelec, ki strelja navzgor.

**SLIKA 3.**

Otrok, ki strelja s fračo navzgor.

xxx



Tekmovanje iz znanja astronomije – drugič



ANDREJ GUŠTIN

→ Lani, v mednarodnem letu astronomije, smo pri DMFA uspešno začeli tekmovanje iz znanja astronomije za osnovne in srednje šole. Učence in dijake, ki želijo pokazati svoje astronomsko znanje, decembra ponovno čaka ta izziv. Zanje smo pripravili nekaj vprašanj, kakršna bodo na tekmovanju.

Mentorji, učenci in dijaki lahko obiščete tudi spletno stran www.astronomija2009.si, kjer je na podstrani *Tekmovanje iz astronomije* objavljenih še več astronomskih nalog z rešitvami, na *Forumu* pa lahko zastavljate vprašanja v zvezi s tekmovanjem, nalogami, načinom reševanja nalog, literaturo. Uradni kontakt s tajnico tekmovanja iz znanja astronomije je astronom.tek@gmail.com.

1. Na koliko ozvezdij je razdeljeno nebo?

2. V katerem ozvezdju je zvezda Sirij?

- a) Orion
- b) Veliki pes
- c) Mali pes
- d) Veliki medved

3. Severnica je najsvetlejša zvezda:

- a) v ozvezdju Veliki medved
- b) na nebu
- c) v ozvezdju Mali medved
- d) v ozvezdju Kasiopeja

4. Ozvezdje Orion leži na nebesnem ekvatorju. Ali je v naših krajih to ozvezdje lahko kdaj v zenitu?

5. Katere zvezde tvorijo tako imenovani Poletni trikotnik?

6. Kako se imenuje točka na nebesni krogli, ki leži nasproti zenita?

7. Janezek nebo opazuje na zemljepisni širini 46 stopinj. Koliko stopinj je tam zenit oddaljen od severnega nebesnega pola? Kam bi moral Janezek odpotovati, da bi zenit sovpadal z južnim nebesnim polom?

8. Kdaj v naših krajih Sonce zahaja točno na zahodu?

- a) vedno
- b) ob poletnem solsticiju
- c) ob jesenskem enakonočju
- d) ob zimskem solsticiju

9. Ali je lahko na severnem polu višina Sonca nad obzorjem 45 stopinj? Pojasni.

10. Katera izjava drži?

- a) Sonce je vedno na nebesnem ekvatorju.
- b) Sonce nikoli ni na nebesnem ekvatorju.
- c) Sonce je vedno na ekliptiki.
- d) Sonce je vedno na nebesnem ekvatorju in ekliptiki.

11. Skiciraj razporeditev Sonca, Zemlje in Jupitra, ko je Jupiter v opoziciji.

12. Kateri planet ima največjo tirno hitrost?

- a) Merkur
- b) Jupiter
- c) Zemlja
- d) Mars

13. Kaj pomeni, da je planet v periheliju?

- a) Da je najbližje Zemlji.
- b) Da je najdlje od Sonca.
- c) Da je najbližje Soncu.
- d) Da je med Soncem in Zemljo.

14. Luna na Zemlji ustvarja plimo in oseko. Zaradi tega se Luna

- a) približuje Zemlji in okoli nje kroži vse počasneje;
- b) približuje Zemlji in okoli nje kroži vse hitreje;





- c) oddaljuje od Zemlje in okoli nje kroži vse hitreje;
d) oddaljuje od Zemlje in kroži vse počasneje.

15. Kateri planet se na svoji poti okoli Sonca Zemlji najbolj približa?

16. Kaj ne sodi zraven?

- a) Vesta
b) Slovenija
c) Halley
d) Jurijvega

17. Kaj ne sodi zraven?

- a) Perzeidi
b) Atenci
c) Leonidi
d) Liridi

18. Kaj je na sliki? (Foto:

N. A. Sharp, REU program/NOAO/AURA/NSF)

- a) kroglasta kopica
b) planetarna meglica
c) galaksija
d) ostanek supernove



SLIKA.

19. Katero telo je najbolj oddaljeno?

- a) Andromedina galaksija
b) Pluton
c) Orionova meglica
d) kroglasta kopica M 13

20. Najboljša ocena starosti vesolja je:

- a) 5,7 milijarde let
b) 20,7 milijarde let
c) 10,7 milijarde let
d) 13,7 milijarde let

xxx



Zaupati ali ne zaupati – Digitalni podpis v kriptografiji, 4.del



ALEKSANDAR JURIŠIĆ IN JASMINA VESELINOVIĆ

→ Pred petdesetimi leti je imel malokdo doma telefon, danes pa le redkokateri učenec med poukom s svojim mobilcem ne pogleda na svetovni splet (npr. Facebook). Tako se nam vsaj navidezno zdi, da smo obkroženi s številnimi prijatelji. Pa vendar so ljudje že davno spoznali, da so človeški možgani sposobni res dobro razumeti največ 150 posameznikov in odnosov med njimi (npr. Robin Dunbar iz univerze v Liverpoolu). Tudi v podjetjih in vojski se število 150 izkaže za kritično, kadar obravnavamo najmanjšo neodvisno enoto. Ko se npr. z določeno znanstveno disciplino ukvarja več kot 200 raziskovalcev, se pogosto le-ta razcepi na dve ali več podpodročij. V vaseh, ki štejejo več kot 500 prebivalcev, se že pojavlja anonimnost, da o večjih mestih niti ne govorimo. V današnjem času medmrežja in potrošniške družbe bo zato vse pogostejše prihajalo do komuniciranja med ljudmi (celo med napravami), ki se ne poznajo. Kako si torej lahko zaupata dva, ki sta se začela pogovarjati preko mreže?

V tretjem delu [3] smo predstavili koncept *kriptosistemov z javnimi ključi*, ki so ga leta 1976 odkrili W. Diffie, M. Hellman in R. Merkle (zadnji je bil takrat še študent), in tudi idejo *digitalnega podpisa*. V tem sestavku bomo predstavili konkreten kriptografski protokol, ki omenjeno idejo uvaža v prakso. Po razmisleku o lastnostih lastnoročnega in digitalnega podpisa bomo opisali Elgamalovo shemo za digitalni podpis, ki je poleg RSA sheme [5] v praksi najbolj razširjena.

Bistveno se način zapisovanja informacij ni drastično spremenil. Medtem ko smo prej shranjevali in prenašali informacije na papirju, jih sedaj hranimo na diskih in v drugih elektronskih/magnetnih medijih ter jih prenašamo preko omrežij. Bistveno pa se je spremenila možnost kopiranja, prenašanja in spreminjanja informacij. Danes zlahka naredimo na tisoče kopij določene digitalne informacije in jih v trenutku prenesemo na različne konce sveta, pri tem pa se nobena kopija prav nič ne razlikuje od originala. Z informacijo na papirju je bilo vse to precej težje, če že ne nemogoče. Moramo pa danes poskrbeti, da bo varnost informacij neodvisna od fizičnega medija, ki jih je zapisal ali prenesel. Temeljiti mora izključno na digitalni vsebini, t. j. na številkah. Zato zna biti današnja tema zanimiva tudi za nas, Presekovce.



SLIKA 1.

Eno izmed osrednjih orodij za zaščito informacij je *podpis*. Le-ta preprečuje poneverjanje in je dokaz o izvoru, identifikaciji, pričanju. Podpis naj bi bil unikat vsakega posameznika, saj se z njim predstavljamo, nekaj potrjujemo, nekoga pooblašamo.



Z digitalnim podpisom potrjujemo izvor podatkov ali pa nekoga prepričamo, da je podpis opravil lastnik ustreznega zasebnega ključa.

Z razvojem digitalne informacije moramo ponovno obdelati bistvo podpisa. S pravo idejo lahko vplivamo na tok zgodovine, saj ni rečeno, da ne bi mogli dodati še kakšne nove lastnosti, na katero doslej še nihče ni pomislil, le-ta pa bi lahko vsem nam spremenila življenje oziroma vsaj navade.



→ (Stari) lastnoročni podpis

Na podiplomskem študiju mi je moral mentor na začetku vsakega semestra podpisati obrazec, na katerem so bili vpisani predmeti, ki sem si jih izbral za tisti semester. Ko sem že dobil podpis, sem na seznamu sosednjega oddelka za računalništvo opazil še dva zanimiva predmeta. Vpisal sem ju, saj je bil na obrazcu prostor ravno še zanju. Pa vendar sem pomislil tudi na to, da tak način morda ni ustrezen in sem mentorja obvestil o spremembi. Izkazalo se je, da bi moral mentorja v resnici še enkrat prositi za odobritev, ne pa samo obvestiti. Prav nič ni bil zadovoljen, da sploh lahko pride do takšnih zapletov. Kakšno leto kasneje sem izvedel, da mentorji dobijo kopije omenjenih obrazcev neposredno iz pisarne, kamor smo jih oddajali. Pogled v bližnjo prihodnost nam razkrije še nekaj pomanjkljivosti lastnoročnega podpisovanja:

- J: "Danes sem dobil podpis v šoli," pove Janezek sestri.
 S: "Kakšno neumnost si pa zopet naredil?"
 J: "Te nič ne briga, raje mi svetuj, kako naj prelisičim mamo."
 S: "Nad učiteljev podpis skopiraj obvestilo o športnem dnevu."
 J: "Odlična ideja, na ta način se bom zlahka rešil zagate, pa se smučat grem, namesto da bi šel v šolo."

SLIKA 2.



Janezek to naredi in mama pod digitalno obvestilo o smučarskem dnevu pripne svoj „digitalni“ podpis. Preden pa ga Janezek na ključku odnese v šolo, zopet zamenja obvestilo o športnem dnevu s prejšnjim besedilom. V resnici je škoda za starše še večja, saj ima sedaj Janezek mamin „digitalni“ podpis in ga bo odslej lahko izrabljal po mili volji. V času elektronskih medijev je zato izredno nevarno podpis skenirati (posneti) oziroma sprejemati skenirane podpise, ki so v resnici le posnetki. Postopek digitalnega podpisa mora biti dobro premišljen, saj moramo preprečiti spreminjanje vsebine podpisanega sporočila in ponarejanje oziroma kopiranje podpisa. Zgoraj opisani digitalni podpis ni več unikat, ki enolično določa

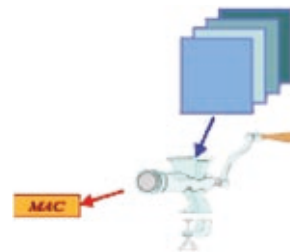
podpisnika. Z lahkoto ga kopiramo oziroma dodamo na poljubni dokument. Potrebujemo protokole, ki imajo podobne lastnosti kot trenutni „papirni protokoli“. Današnja družba ima enkratno priložnost, da vpelje nove in še učinkovitejše načine, ki nam bodo zagotovili boljšo varnost informacij.

➤ **Digitalni podpis naj bi bil nadomestek za lastnoročni podpis pri elektronski izmenjavi in digitalnemu hranjenju podatkov. Nastopa kot število oziroma, še bolj splošno, kot zaporedje bitov.**

Digitalni podpis mora imeti vse tiste dobre lastnosti, ki veljajo za lastnoročni podpis, poleg tega pa mora veljati, da vsebine digitalno podpisanega dokumenta ni mogoče spreminjati in podpisa ni mogoče kopirati in ne ponarejati. Obe obliki podpisovanja pa imata še nekaj pomembnih lastnosti:

- Lastnoročni podpis je fizično del podpisanega dokumenta.
- Lastnoročni podpis preverjamo s primerjanjem, digitalnega pa z algoritmom, ki ga izvaja računalnik. Rezultat tega preverjanja je odvisen od ključa ter dokumenta, ki smo ga podpisali.
- Digitalnega podpisa ne moremo razlikovati od njegove kopije, zato si želimo podpis, ki bo vedno drugačen (četudi podpisemo isto stvar).

SLIKA 3.



Povedali smo že, da je digitalni podpis odvisen od dokumenta, ki ga podpisujemo. Ker pa so dokumenti poljubno veliki, običajno iz dokumenta konstruiramo izvleček fiksne dolžine (lahko bi mu rekli tudi prstni odtis) in nato podpisemo le-tega. Tokrat se ne bomo spuščali v podrobnosti teh postopkov, ki jim rečemo *zgoščevalne funkcije*, pač pa omenimo le, da je mogoče priti do izvlečka z bločnimi simetričnimi šiframi, ki smo jih spoznali v prvem delu [1] (glej 2. in 3. nalogo).

(Novi) digitalni podpis

Shema za digitalni podpis je sestavljena iz treh delov:

- iz algoritma za generiranje ključa,
- algoritma za generiranje digitalnega podpisa in
- algoritma za preverjanje digitalnega podpisa.

SLIKA 4.



SLIKA 5.

Za lažje razumevanje definirajmo nekaj osnovnih pojmov:

- Pravilo $\text{sgn}_{Z(A)}$, ki sporočilo podpiše (angl. sign), imenujemo *funkcija za podpis* osebe A . Zasebni ključ $Z(A)$ varuje oseba A in ga uporablja le za podpisovanje dokumentov.
- Pravilu $\text{ver}_{J(A)}$, ki za dokument in njegov podpis preveri oz. verificira (angl. verify), t. j. priredi vrednost „veljaven“ oziroma „neveljaven“, rečemo *funkcija za preverjanje podpisov* osebe A . Javni ključ $J(A)$ pripada osebi A , a je vseeno javno znan. „Tretja“ oseba uporablja $\text{ver}_{J(A)}$ za preverjanje podpisov, ki jih je opravila oseba A .

Postopek pošiljanja digitalno podpisanega sporočila med Anito in Bojanom je naslednji:

1. Najprej si Bojan izbere svoj zasebni ključ $Z(B)$ ter sporoči Aniti ustrezni javni ključ $J(B)$.
2. Za podpis sporočila x , Bojan uporabi algoritem za generiranje digitalnega podpisa s svojim zasebnim ključem $Z(B)$ in izračuna podpis $\text{sgn}_{Z(B)}(x)$. Nato ga skupaj s sporočilom pošlje Aniti.
3. Če Anita pozna Bojanov javni ključ $J(B)$, lahko uporabi algoritem za preverjanje digitalnega podpisa $\text{ver}_{J(B)}$ ter tako preveri pristnost podpisa.

Vrstni red šifriranja in digitalnega podpisovanja je pomemben.

(a) Če hoče Anita poslati Bojanu podpisano, zašifrirano sporočilo, potem danemu čistopisu x najprej izračuna svoj podpis $y = \text{sgn}_{Z(A)}(x)$, nato zašifrira x in y z Bojanovo javno šifrirno funkcijo $e_{J(B)}$ in dobi $z = e_{J(B)}(x, y)$. Tajnopis z pošlje Bojanu. Ta ga odšifrira s svojo zasebno odšifrirno funkcijo $d_{Z(B)}$ in dobi par (x, y) . Potem uporabi Anitino javno funkcijo $\text{ver}_{J(A)}$, da preveri, ali je $\text{ver}_{J(A)}(x, y) = \text{veljaven}$.

(b) Če pa bi Anita najprej zašifrirala sporočilo x in potem podpisala rezultat, bi izračunala $z = e_{J(B)}(x)$ in $y = \text{sgn}_{Z(A)}(z)$ ter par (z, y) poslala Bojanu. Bojan bi z odšifriranjem tajnopisa z dobil $x = d_{Z(B)}(y)$, nato bi preveril podpis y na x z uporabo funkcije $\text{ver}_{J(A)}$. Če prestreže takšen par (z, y) Oskar, nastane problem, saj lahko zamenja Anitin podpis s svojim $y' = \text{sgn}_{Z(O)}(z)$, čeprav ne pozna čistopisa x . Ko pošlje par (z, y') Bojanu, bi ta lahko mislil, da mu je sporočilo x poslal Oskar.

Zato priporočamo najprej podpisovanje in nato šifriranje sporočil (glej 4. nalogo).

Če veljata naslednji dve lastnosti:

- Anita je edina, ki lahko podpiše sporočilo, torej edina, ki zna pri danem x izračunati y , tako da je $\text{ver}_{Z(A)}(x, y) = \text{veljaven}$,
- Bojan se je sposoben prepričati, ali gre za Anitin podpis ali pa gre za ponaredek,

potem rečemo, da je algoritem digitalnega podpisa *varen*. V naslednjem razdelku bomo predstavili konkretne opise funkcij **sgn** in **ver**, ki ju imamo za varne.

Elgamalov digitalni podpis

Opišimo Elgamalovo shemo za digitalni podpis (1985), ki temelji na težavnosti *problema diskretne logaritma* (oznaka DLP) v grupi $\mathbb{Z}_p^*$ in Diffie-Hellmanovega dogovora o ključu, ki smo ju opisali v drugem delu [2]. Spomnimo se, da smo za praštevilo $p \in \mathbb{Z}$ označili obseg z elementi $0, 1, \dots, p-1$ in operacijama $+_p, *_p$, kjer oznaka p pri $+$ in $*$ pomeni, da običajno vsoto oziroma produkt nadomestimo z ustreznim ostankom pri deljenju s p . V $\mathbb{Z}_p$ vedno obstaja tak element α , ki generira multiplikativno grupo $\mathbb{Z}_p^* = (1, \dots, p-1, *_p)$, t. j. množica $\alpha^0, \alpha^1, \dots, \alpha^{p-2}$ pokrije vse elemente v $\mathbb{Z}_p^*$ DLP v $\mathbb{Z}_p^*$



→ je, da za dani generator α in $\beta = \alpha^a$, kjer je a neko naravno število, iščemo učinkovit način (algoritem) za izračun števila a .

Priprava	Naj bo p tako praštevilo, da je v obsegu $\mathbb{Z}_p$ težko rešiti DLP in α generator grupe $\mathbb{Z}_p^*$.
Generiranje ključev	Za (skriti) zasebni ključ $\alpha \in 0, \dots, p-1$ izračunaj javni ključ $\beta = \alpha^a \pmod{p}$.
Podpisovanje	Za sporočilo $x \in 0, \dots, p-2$ izberi naključno skrito naravno število $k \leq p-2$, tako da je $D(k, p-1) = 1$, nato pa z zasebnim ključem a izračunaj $\text{sgn}_a(x, k) = (y, \delta)$, kjer je $y = \alpha^k \pmod{p}$ in $\delta = (x - ay)k^{-1} \pmod{p-1}.$
Preverjanje podpisa	(y, δ) sporočila x z javno trojico (p, α, β) : $\text{ver}_\beta(x, y, \delta) = \text{veljaven} \iff \beta^y y^\delta \equiv \alpha^x \pmod{p}.$

TABELA.

Elgamalov algoritem



SLIKA 6.

Taher Elgamal (iz Egipta).



SLIKA 7.

Pierre de Fermat je znan tudi po naslednjemu izreku [4]: Za praštevilo p in $a \in \mathbb{Z}_p^*$ velja $a^{p-1} \equiv 1 \pmod{p}$.

Za pravilnost preverjanja glej 5. nalogo. Zgornji podpis je nedeterminističen (odvisen od naključnega števila k), torej sploh ni natanko določen. Če torej isti dokument podpišemo vsaj dvakrat, bo z veliko verjetnostjo podpis vsakič drugačen. Poudarimo tudi, da podpisnik izračuna podpis z uporabo tako tajne vrednosti a , ki je del ključa, kot tajnega naključnega števila k , ki se sme uporabiti samo za podpis *ene*ga sporočila x (preverjanje pa je opravljeno samo z uporabo javnih informacij). Če namreč naključno število k ne ostane skrito, ali pa se isto število k uporabi v podpisih dveh različnih sporočil (v tem primeru ga je možno zlahka izračunati), lahko napadalec iz druge enačbe algoritma za podpisovanje izra-

čuna tajno vrednost a in ponaredi podpis (glej 6. in 7. nalogo). Elgamalovo shemo za podpis imamo za varno. Do danes namreč še nikomur ni uspelo učinkovito izračunati par (y, δ) brez računanja diskretnega logaritma. Lahko pa se zgodi, da bomo nekoč ugotovili, da se pri iskanju para (y, δ) problemu diskretnega logaritma sploh ne moremo izogniti.

Kako bi lahko ponaredili podpis, ne da bi vedeli za vrednost skritega števila a ?

(a) Za dano sporočilo x poišči tak par (y, δ) , da bo veljalo $\beta^y y^\delta \equiv \alpha^x \pmod{p}$:

- če izberemo y , potrebujemo $\delta = \log_y \alpha^x \beta^{-y} \pmod{p}$,
 - če izberemo δ , je potrebno rešiti enačbo $\beta^y y^\delta \equiv \alpha^x \pmod{p}$ po y ,
 - hkrati računamo y in δ
- (zaenkrat ni še nihče odkril hitrega postopka za reševanje zgornje enačbe).

(b) Za podpis (y, δ) poišči ustrezno sporočilo x , t. j. izračunaj: $x = \log_\alpha \beta^y y^\delta \pmod{p}$.

Omenimo še, da so Elgamalov digitalni podpis temeljito preučili tudi v ZDA, kjer na državnem nivoju neradi plačujejo patente (RSA je bil namreč takrat še patentiran). Na njegovi osnovi so sestavili Digital Signature Algorithm (DSA), ki ga je National Institute of Standards and Technology (NIST) sprejel za ameriški standard: Digital Signature Standard (DSS). Danes je vključen v večino varnostnih standardov.

Naloge

- (1.) RSA-podpis, ki je opisan v [5], je za razliko od Elgamalovega determinističen. Kako bi ga lahko spremenili v nedeterminističnega? Varnostno analiziraj svoj predlog.
- (2.) Kakšne lastnosti naj ima zgoščevalna funkcija, da ne bo ogrožena varnost podpisa?
- (3.) S prijateljem drug drugemu predlagajta način, s katerim bi iz dokumenta poljubne dolžine z bločno šifro skonstruirala izveček fiksne dolžine, nato pa poskusita predloge analizirati.
- (4.) V razdelku o digitalnem podpisu smo omenili ši-

frirno funkcijo $e_{J(B)}$, ki jo uporabi Anita, in Bojanovo odšifrirno funkcijo $d_{Z(B)}$. Elgamal je predlagal taki funkciji na osnovi DLP. Če je sporočilo m iz grupe G , ki je generirana z α , potem Anita izbere naključno naravno število k , ki je manjše od števila elementov v grupi G , ter z njim in Bojanovim javnim ključem $\beta = \alpha^b$ izračuna par $\alpha^k, m\beta^k$ ter ga pošlje Bojanu. Opiši odšifrirno funkcijo.

(5.) Prepričaj se, da je opisano preverjanje Elgamalovega podpisa pravilno. (Namig: pomagaj si s Fermatovim izrekom, da bo jasno, zakaj računamo δ po modulu $p - 1$.)

(6.) Podpisovalec ni bil pazljiv in je ponesreči izgubil naključno število k , ki ga je uporabil pri Elgamalovem podpisu. Uporabi njegovo napako za izračun zasebnega ključa a .

(7.) Generator naključnih števil je tako počasen, da se je podpisovalec odločil uporabiti število k dvakrat. Ali lahko uporabiš njegovo napako za izračun zasebnega ključa a ?

(8*) Predlagaj novo različico Elgamalovega podpisa, kjer ne bomo več potrebovali računanja inverza (k^{-1}), ki ga ponavadi izračunamo z razširjenim Evklidovim algoritmom.

(9.) Hkratno računanje vrednosti x, y in δ : naj bosta i in j takšni števili, da velja $0 \leq i, j \leq p - 2$ in $D(j, p - 1) = 1$. Prepričaj se, da potem števila

$$\gamma \equiv \alpha^i \beta^j \pmod{p}, \quad \delta \equiv -\gamma j^{-1} \pmod{p - 1}$$

in

$$x \equiv -\gamma i j^{-1} \pmod{p - 1}$$

zadoščajo enačbi za preverjanje Elgamalovega podpisa: $\beta^y \gamma^\delta \equiv \alpha^x \pmod{p}$.

(10*) Ali lahko pri veljavnem podpisu (γ, δ) za x najdemo še kakšen podpis za kakšno drugo sporočilo x' ?

Odgovor je „DA“. Naj bodo h, i in j takšna števila, da velja $0 \leq h, i, j \leq p - 2$ in $D(h\gamma - j\delta, p - 1) = 1$. Potem se prepričaj, da je par (λ, μ) veljaven podpis

za x' , kjer je

$$\lambda = \gamma^h \alpha^i \beta^j \pmod{p}, \quad \mu = \delta \lambda (h\gamma - j\delta)^{-1} \pmod{p - 1}$$

in

$$x' = \lambda (hx + i\delta) (h\gamma - j\delta)^{-1} \pmod{p - 1}.$$

V drugem razdelku je v tretji točki „ČE“, zaradi katerega še nismo povsem rešili problema identifikacije Bojana. Ta se je le prenesla na prepoznavanje Bojanovega javnega ključa. Če se morata Anita in Bojan prej sestati, da bi si izmenjala javna ključa, potem bi se lahko ob tej priložnosti dogovorila za skupen ključ za kakšno simetrično šifro. Več o tem, kako lahko s certifikati in z infrastrukturo javnih ključev rešimo ta problem, pa v zadnjem (5.) delu.

Literatura

- [1] A. Jurišić in U. Perko, *Klasične šifre in zdravstvena kartica, prvi del*, Presek 33/1 (2005-06), str. 22-24
- [2] A. Jurišić, *Diffie-Hellmanov dogovor o ključu, drugi del*, Presek 34 (2006-07), str. 25-30.
- [3] A. Jurišić, *Poštni nabiralnik in kriptografski protokoli, kriptosistemi z javnimi ključi, tretji del*, Presek 36/2 (2008-09), 22-26.
- [4] D. Pagon, *Kongruence in Eulerjev izrek*, Presek 15/4 (1987/88), str. 194-196.
- [5] M. Vencelj, *Šifriranje z javnim ključem*, Presek 22/6 (1994/95), str. 354-357. xxx

REŠITEV SUDOKU

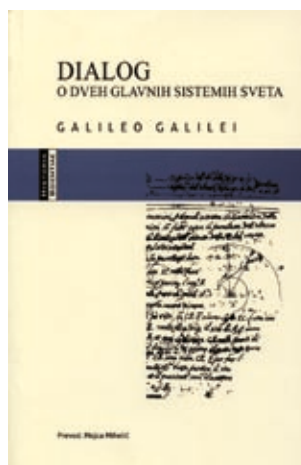
	a	b	c	d	e	f	g	h	i
A	3	8	6	1	5	4	2	7	9
B	1	9	5	7	2	6	8	3	4
C	4	7	2	8	3	9	5	1	6
D	6	4	1	5	9	7	3	2	8
E	5	3	8	4	6	2	7	9	1
F	9	2	7	3	8	1	4	6	5
G	7	6	9	2	4	5	1	8	3
H	2	5	3	6	1	8	9	4	7
I	8	1	4	9	7	3	6	5	2



ANDREJ GUŠTIN

Galileo v slovenščini

→ Pri Založbi ZRC SAZU je tik pred poletjem izšel prevod znamenitega *Dialoga o dveh glavnih sistemih sveta*, ki ga je leta 1632 izdal Galileo Galilei, poleg tega pa še delo Matjaža Vesela *Kopernikanski Manifest Galilea Galileija*, ki je pravzaprav spremna beseda k Galilejevemu „Dialogu“. Znameniti Toskanec, ki je v začetku 17. stoletja odigral eno od osrednjih vlog znanstvene renesanse, spomnite se preteklega mednarodnega leta astronomije, ki je bilo razglašeno v čast štiristoletnici prvih Galilejevih teleskopskih opazovanj, je z „Dialogom“ poskušal dokazati in javnosti predstaviti pravilnost Kopernikovega heliocentričnega sistema. Galilej je to dokazovanje spretno zavil v pogovor med tremi možakarji, Salvatijem, Galilejevim „alter egom“, ki podaja dokaze v prid Kopernikovi teoriji, Simplicijem, ki v sebi združuje vse Galilejeve nasprotnike, in bistrim beneškim gospodom Sagredom, ki naj bi bil nekakšen razsodnik med njima, a skoraj vedno sprevidi pravilnost kopernikanske teorije in zmotnost aristotelizma. Galilej je bil izjemen retorik in pisec, ki je z očitnim



namenom razširjanja lastnih idej pisal v toskanščini, jeziku, ki ga je bolj kot latinščino razumela širša publika. V političnem smislu pa si je Galilej z „Dialogom“ zabil avtogol, saj je služil kot kronski dokaz pri obtožbi cerkvenih oblasti, da razširja neresnice o ustroju sveta. Galilejevo zgodbo na kratko povzema Veselova knjižica, ki postreže tudi s kratkimi opombami k razpravam v „Dialogu“. V tej spremni knjigi bi si sicer želeli podrobnejših fizikalnih razlag pojavov, o katerih razpravljajo trije možakarji, saj bi tako sodobnemu bralcu besedilo postalo še bolj zanimivo. XXX

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 2,17 EUR, za vse ostale pa 2,71 EUR.

Izkoristite dodatni popust pri večjem naročilu!

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



Knjižnica 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.

Jože Grasselli:

ELEMENTARNA TEORIJA ŠTEVIL

168 strani
format 14 × 20 cm
mehka vezava

14,99 EUR

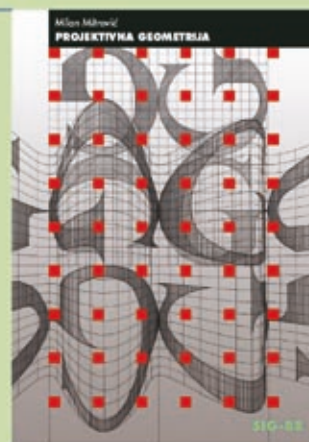


Milan Mitrović:

PROJEKTIVNA GEOMETRIJA

158 strani
format 14 × 20 cm
mehka vezava

20,99 EUR



Janez Strnad:

MALA ZGODOVINA VESOLJA

270 strani
format 14 × 20 cm
mehka vezava

20,99 EUR



Roberto Lucchetti:

STRAST DO TRILČKOV

Nekaj matematičnih
zamisli

152 strani
format 14 × 20 cm
mehka vezava

18,69 EUR

Poleg omenjenih lahko v Knjižnici Sigma najdete še več kot 45 drugih del. Podrobnejše predstavitev so na spodnjem naslovu, kjer lahko vse knjižnice 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.