

**PRESEK LETNIK 50 (2022/2023) ŠTEVILKA 5**

- STOŽNICA SKOZI PET TOČK
- KAJ POVEJO KRIVULJE ZA MTF O FOTOGRAFSKEM OBJEKTIVU
- MOJA IZKUŠNJA OPAZOVANJA EKSOPLANETA
- (DIGITALNI) KLJUČI

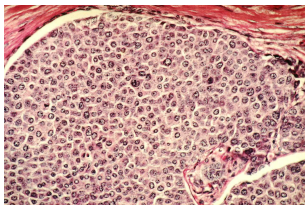
ISSN 0351-6652



9||770351||665050|

Uporaba matematike pri raziskovanju rakavih obolenj

↓ ↓ ↓



→ Raziskovanje rakavih obolenj je zahteven proces. Na tumorje v človeškem telesu vplivajo različne stvari: kisik, ki ga prinese kri, energija, dostavljena v obliki glukoze,

in številne celice in kemikalije v okolju. Ustrezne pogoje je težko posnemati v laboratoriju, opazovanje resničnih bolnikov pa je lahko boleče in invazivno. Matematični modeli dajejo raziskovalcem možnost, da nekatere eksperimente izvedejo virtualno in tako proučujejo različne procese veliko hitreje in ceneje kot sicer. Toda ti modeli ne morejo delovati sami zase. Potrebujejo resnične podatke in njihove napovedi morajo biti pozorno testirane z eksperimenti in kliničnimi poskusi.

V enem od obetavnih primerov tovrstnih raziskav so laboratorijski znanstveniki gojili tumorje obdane z novim tipom celice, matematiki pa so pridobljene podatke uporabili za simulacijo obnašanja celic pod različnimi pogoji. Rezultati so nakazali, da bi lahko zavrla rast tumorja z uporabo že obstoječega zdravljenja. Zdaj je treba s kliničnimi testiranjmi zagotoviti, da je rezultate iz modelov mogoče prenesti v resničnost.

Več informacij najdete v člankih R. P. Araujo, D. L. S. McElwain, *A history of the study of solid tumour growth: The contribution of mathematical modelling*, Bull. Math. Biol. **66** 2004, 1039–1091, in J. Wang, A. Delfarah, P. E. Gelbach, E. Fong, P. Macklin, S. M. Mumenthaler, N. A. Graham, S. D. Finley, *Elucidating tumor-stromal metabolic crosstalk in colorectal cancer through integration of constraint-based models and LC-MS metabolomics* Metabolic Engineering **69** 2022, 175–187. Slika: dr. Cecil Fox, National Health Institute, ID 2288.

Izvirno besedilo: Using Math to Support Cancer Research, Mathematical moments from the AMS. Prevod in priredba: B. Kuzman.

KOLOFON

→

Presek

list za mlade matematike, fizike, astronome in računalnikarje letnik 50, šolsko leto 2022/2023, številka 5

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

Dopisi in naročnine: DMFA-založništvo, Presek, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana, telefon (01) 4766 633, telefaks (01) 4232 460, 2517 281.

Internet: www.presek.si

Elektronska pošta: info@dmfa-zaloznistvo.si

Naročnina za šolsko leto 2022/2023 je za posamezne naročnike 22,40 EUR – posamezno naročilo velja do preklica, za skupinska naročila učencev šol 19,60 EUR, posamezna številka 6,00 EUR, stara številka 4,00 EUR, letna naročnina za tujino pa znaša 30 EUR.

Transakcijski račun: 03100-1000018787.

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

Založilo DMFA-založništvo

Oblikovanje Tadeja Šekoranja

Tisk Collegium Graphicum, Ljubljana

Naklada 900 izvodov

© 2023 Društvo matematikov, fizikov in astronomov Slovenije – 2166

ISSN 2630-4317 (Online)

ISSN 0351-6652 (Tiskana izd.)

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

Poština plačana pri pošti 1102 Ljubljana.

NAVODILA SODELAVCEM PRESEKA ZA ODDAJO PRISPEVKOV

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

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

Prispevke pošljite odgovornemu uredniku na naslov uredništva DMFA-založništvo, Presek, p. p. 2964, 1001 Ljubljana ali na naslov elektronske pošte info@dmfa-zaloznistvo.si.

Vsak članek se praviloma pošlje vsaj enemu anonimnemu recenzentu, ki oceni primernost članka za objavo. Če je prispevek sprejet v objavo in če je besedilo napisano z računalnikom, potem uredništvo prosi avtorja za izvirne datoteke. Le-te naj bodo praviloma napisane v eni od standardnih različic urejevalnikov TeX oziroma LaTeX, kar bo olajšalo uredniški postopek.

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

Kazalo

MATEMATIČNI TRENUTEK

- 2** Uporaba matematike pri raziskovanju rakavih obolenj

UVODNIK

- 4** Pouk računalništva
(*Nino Bašič*)

MATEMATIKA

- 5-7** Stožnica skozi pet točk
(*Marko Razpet*)
- 13-14** GeoGebrin kotiček – Krivulja prislonjene lestve
(*Boštjan Kuzman*)

FIZIKA

- 9-12** Kaj povejo krivulje za MTF o fotografskem objektivu
(*Peter Legiša*)

ASTRONOMIJA

- 18-19** Moja izkušnja opazovanja eksoplaneta
(*Neja Pisk*)

RAČUNALNIŠTVO

- 20-26** (Digitalni) ključ
(*Aleksandar Jurišić in Klemen Klanjšček*)

RAZVEDRILO

- 28** Rešitev nagradne križanke Presek 50/4
(*Marko Bokalič*)
- 15** Bilo je nekoč v reviji Presek – Razpis tekmovanja srednješolcev iz matematike in fizike v letu 1980/81
- 16-17** Nagradna križanka
(*Marko Bokalič*)
- 27-31** Izbrane slike in fotografije v petdesetih letih Preseka – nadaljevanje
(*Nada Razpet, Marko Razpet in Andrej Likar*)

TEKMOVANJA

- 7-8** Tekmovanje π
(*Nežka Mramor Kosta in Jasna Prezelj*)
- priloga** 58. tekmovanje iz matematike za Vegovo priznanje – državno tekmovanje
- priloga** 66. matematično tekmovanje srednješolcev Slovenije – državno tekmovanje
- priloga** 22. matematično tekmovanje za dijake srednjih tehniških in strokovnih šol – državno tekmovanje
- priloga** 22. matematično tekmovanje za dijake poklicnih šol – državno tekmovanje

zgornji desni pa 9999. Frekvenco PINa predstavimo z ustrezno barvo: višja je rumena, pa vse do bele, nižja pa oranžna, od svetlo do temno vijolične in črne. Skala je logaritmčna. Zvezda severnica (tj. beli kvadrater) na sliki seveda predstavlja najbolj popularen PIN 1234 (3,9 % – a kot kaže, mu popularnost vendarle pada). Sledijo mu letnice oblike 199? (3,5 %), 19?? (10,9 %), in 20?? (7,4 %). Tudi ponavljanje prvih dveh števk je zelo pogosto (4,1 %) – zato izstopa diagonala $x = y$. Poleg tega je delež PIN-ov sestavljenih le iz samo ene števke (1,2 %). Če bi bili vsi PIN-i enako možni, bi mogle biti ti deleži zaporedoma enaki 0,01 %, 0,1 %, 1 %, 1 %, 1 %, in 0,1 %.

SLIKA NA NASLOVNICI: Grafična predstavitev štirimestnih PIN-ov (ki potrjuje pregovor, da je slika vredna vsaj 1000 besed). Prvi dve števki uporabimo za x -koordinato, zadnji dve pa za y -koordinato. Levi spodnji kvadrater predstavlja 0000,

Pouk računalništva



NINO BAŠIČ, UREDNIK ZA RAČUNALNIŠTVO

→ Pred nekaj tedni sem po naključju zašel na spletno stran <https://www.racunalninstvo-in-informatika-za-vse.si/>. Gre za iniciativo, ki si prizadeva za uvedbo obveznega predmeta *Računalništvo in informatika* v slovensko šolstvo (od vrtca pa vse do srednje šole). Z njimi se strinjam. Zakaj? Čas, ki prihaja, bodo krojile digitalne valute, internet stvari (IoT), kvantni računalniki in umetna inteligenca (samo pogledjte, koliko se danes razpravlja o OpenAI oziroma ChatGPT!). Še pred nekaj leti so bili npr. samovozeči avtomobili znanstvena fantastika, toda zdaj postajajo realnost, pa če si to želimo ali pa ne. Da ne bomo povsem izgubljeni v tem svetu, je pomembo, da poglobljeno razumemo te tehnologije. Bralca pozivam, da tudi sam obišče omenjeno spletno stran. Pričujoči zapis pa je predvsem moja osebna izkušnja in pogled na vse skupaj. Mimogrede, zame sta pojma *računalništvo* in *informatika* sopomenki in tako povsem zamenljiva. To je tisto, čemur v angleščini pravimo *computer science*. Gre za področje znanosti, ki se ukvarja s študijem tako teoretičnih kot tudi praktičnih vidikov računalništva in med drugim vključuje programiranje, študij algoritmov in podatkovnih struktur, računalniško arhitekturo in omrežja, kibernetsko varnost, podatkovno znanost in umetno inteligenco.

Moja računalniška pot se je začela v zgodnjih devetdesetih letih. Takrat doma še nismo imeli računalnika, kaj šele interneta. Prvi stik z računalnikom sem imel na šolskem krožku v osnovni šoli, ki ga je vodila knjižničarka. Na računalnikih je bil nameščen operacijski sistem Windows 3.11. Spomnim se, da smo urejali besedila v MS Wordu, iskali literaturo na COBISSu (na bizarno počasnem internetu za današnje pojme) in igrali minolovca. Krožek je bil seveda zelo koristen za mladino, ki se je prvič srečala z računalnikom. V okviru rednega pouka nismo imeli skoraj nobenih računalniških vsebin. Pravo veselje se je zame začelo, ko je na šoli tečaj računalništva ponudil ZRI (Zavod za računalniško izobraževanje Ljubljana). Tu je bil poudarek na programiranju v jeziku Pascal. Živo se spominjam rumenega besedila na modrem ozadju: uporabljali smo razvojno okolje

Turbo Pascal 6.0. Zagnali smo ga kar z disket, ki jih je prinesel učitelj. Programiranje me je takrat povsem prevzelo. ZRI sem nato obiskoval vse do konca srednje šole. Za srednješolce je bil pouk, ki ga je vodil dr. Jelko Urbančič, na sedežu ZRI na Pržanu. Tu smo se osredotočali na algoritme, Pascalu pa sta se pridružila še jezika C in Python. Številni vrstniki, ki sem jih tam spoznal, so danes izjemni računalničarji. Nekateri so vodilni razvijalci pri velikih podjetjih, drugi so osnovali svoja lastna podjetja, tretji pa smo zajadrali v akademske vode. ZRI je tako zapolnil praznino, ki je nastala v šolskem sistemu. Po drugi strani smo na gimnaziji imeli informatiko samo v prvem letniku. Bežno se spominjam, da je imel učbenik modre platnice, programiranju pa je bilo namenjeno zgolj eno kratko poglavje na koncu. Ne spomnim se drugih vsebin, ki jih je ta učbenik vključeval, vem pa, da se mi je zdel nadvse dolgočasen.

Ko sem pripravljaval tale uvodnik, sem s presenečenjem ugotovil, da je že v sedemdesetih letih obstajal učbenik *Uvod v računalništvo* (I. Bratko in V. Rajkovič). Obiskal sem knjižnico Gimnazije Koper, ki hrani en izvod. V tem učbeniku, ki je po mojem mnenju prekleto dobro napisan, je izdatni del namenjen programiranju (v jeziku FORTRAN). Obstaja tudi verzija iz osemdesetih let, z naslovom *Računalništvo s programskim jezikom Pascal*, kjer je FORTRAN nadomeščen s Pascalom. Moj zaključek je, da ima na Slovenskem računalništvo zelo trdno in bogato tradicijo. To dopolnjujejo tudi tekmovanja iz znanja računalništva, ki obstajajo že mnogo let. Žal pa je računalništvo v šolah znova in znova potisnjeno nekam na obrobje. Naši računalniški strokovnjaki seveda ostajajo neumorni. Pred nekaj leti je npr. izšel moderen elektronski učbenik za gimnazije *Informatika 1* (<https://lusy.fri.uni-lj.si/ucbenik/book/index.html>). Sam se udeležujem kot član komisij za računalniška tekmovanja in sicer pripravljam naloge ter ocenjujem rešitve tekmovalcev. Zato vem, da imamo v Sloveniji veliko talentirane mladine in predanih mentorjev. Imamo vse pogoje, da bi postali velika sila na področju računalništva. A kaj, ko našim odločevalcem uspeva vse zreducirati na »dvig digitalnih kompetenc«, s čimer celotno stroko pomnožijo z 0. Si torej v svetu, ki prihaja, sploh ne želimo aktivno sodelovati, ampak bi radi zgolj nemo opazovali dogajanje nekje z obrobja?

× × ×

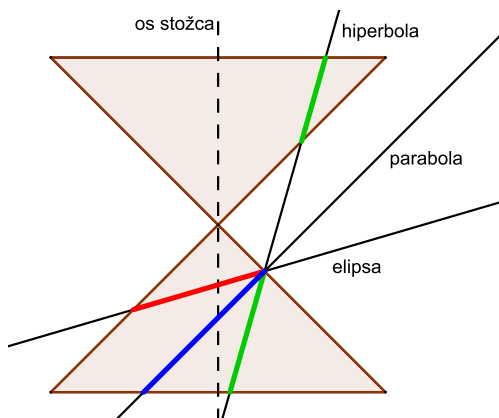
Stožnica skozi pet točk

↓↓↓

MARKO RAZPET

→ Stožnice so ravninske krivulje, ki nastanejo s presekom dvojnega stožca z ravnino. Zato se tudi tako imenujejo. Prave stožnice so elipsa, hiperbola in parabola. Tudi krožnica je stožnica, saj jo imamo lahko za poseben primer elipse. Na sliki 1 je poenostavljen prikaz nastanka pravih stožnic.

Vendar ni vsak presek dvojnega stožca z ravnino prava stožnica. Če se presečna ravnina stožca samo dotika vzdolž ene od njegovih tvorilk, je presek kar ta tvorilka, torej premica. Če presečna ravnina vsebuje os stožca, je presek unija dveh njegovih tvorilk, torej dveh sekajočih se premic. Če ravnina preseka stožec samo v njegovem vrhu, je presek točka. To so izrojeni ali degenerirani primeri stožnic, rečemo jim *izrojene stožnice*. Na sliki 2 je prikaz nastanka izrojnih stožnic.



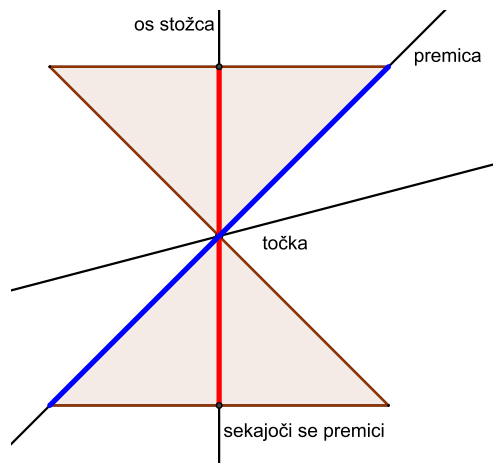
SLIKA 1.

Nastanek pravih stožnic.

V pravokotnem kartezijskem koordinatnem sistemu Oxy imajo vse stožnice enačbo

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0, \quad (1)$$

pri čemer so koeficienti A, B, C, D, E in F realna števila. Pri tem A, B in C niso vsi hkrati enaki 0. Vsaj



SLIKA 2.

Nastanek izrojnih stožnic.

en od teh je različen od 0 in z njim lahko (1) delimo in dobimo enakovredno enačbo s petimi koeficienti. Prav tako dobimo enakovredno enačbo, če (1) pomnožimo s poljubnim od 0 različnim številom. S petimi točkami pa je na splošno stožnica, prava ali izrojena, določena, morda ne ravno enolično. Problem določitve enačbe stožnice skozi pet točk nas privede do sistema petih linearnih enačb s petimi neznankami, ki pa bi se mu radi izognili.

Enačba (1) je po obliki algebrska enačba druge stopnje, zato uvrščamo stožnice med algebrske krivulje druge stopnje. V enačbi (1) se lahko skriva katera koli stožnica, prava ali izrojena, lahko pa tudi dvojica vzporednih premic ali celo prazna množica.

Primeri.

- $x^2 + y^2 - 1 = 0$ - krožnica;
- $4x^2 + 5y^2 - 2 = 0$ - elipsa;
- $4x^2 - 5y^2 - 2 = 0$ - hiperbola;
- $y^2 - 2x = 0$ - parabola;
- $4x^2 - 9y^2 = (2x - 3y)(2x + 3y) = 0$ - sekajoči se premici;
- $4x^2 + 12xy + 9y^2 = (2x + 3y)^2 = 0$ - dvojna premica;





- $x^2 + 2xy + y^2 + x + y = (x + y)(x + y + 1) = 0$ - vzporedni premici;
- $x^2 + y^2 = 0$ - točka $(0, 0)$;
- $x^2 + y^2 + 1 = 0$ - prazna množica.

Oglejmo si, kako pridemo do enačbe stožnice skozi pet danih točk $T_k(x_k, y_k)$, kjer je $k = 0, 1, 2, 3, 4$. Obravnavajmo primer, ko sta trojki (T_0, T_1, T_3) in (T_0, T_2, T_4) nekolinearni oziroma ko se dajo točke preindeksirati tako, da to drži. Trojka točk je nekolinearna, če njene točke ne ležijo na isti premici.

Kako najdemo enačbo stožnice skozi pet točk? Najprej poiščemo enačbe štirih premic, ki so določene z dvojicami točk $(T_1, T_2), (T_3, T_4), (T_1, T_3)$ in (T_2, T_4) . Njihove enačbe v implicitni obliki naj bodo $p_{i,j}(T) = p_{i,j}(x, y) = a_{i,j}x + b_{i,j}y + c_{i,j} = 0$ za dvojice $(i, j) \in \{(1, 2), (3, 4), (1, 3), (2, 4)\}$. Pri tem koeficienta $a_{i,j}$ in $b_{i,j}$ nista hkrati enaka 0. Veljajo seveda enakosti $p_{i,j}(T_i) = p_{i,j}(T_j) = 0$ za navedene dvojice. Nato zapišemo enačbo

$$P(T) = p_{1,2}(T)p_{3,4}(T) - \lambda p_{1,3}(T)p_{2,4}(T) = 0, \quad (2)$$

ki je po obliki algebrska enačba druge stopnje in s tem enačba algebrske krivulje druge stopnje. Pri tem je λ parameter, ki ga bomo izbrali tako, da bo tudi točka T_0 zadoščala enačbi (2), torej $P(T_0) = 0$. Očitno je $P(T_k) = 0$ za $k = 1, 2, 3, 4$. Pri tem pa $p_{1,3}(T_0)p_{2,4}(T_0) \neq 0$, ker trojki (T_0, T_1, T_3) in (T_0, T_2, T_4) nista kolinearni. Če izberemo

$$\lambda = \frac{p_{1,2}(T_0)p_{3,4}(T_0)}{p_{1,3}(T_0)p_{2,4}(T_0)},$$

velja $P(T_k) = 0$ za $k = 0, 1, 2, 3, 4$ in dobili smo enačbo stožnice skozi pet danih točk, in sicer do neničelnega faktorja natančno. Tudi implicitne enačbe sodelujočih premic so določene samo do neničelnega konstantnega faktorja natančno, kar pa ne vpliva na končni rezultat, o čemer se ni težko prepričati.

1. naloga.

Poiščimo enačbo stožnice, ki poteka skozi točke

$$T_0(0, 0), T_1(4, 0), T_2(6, 2), T_3(0, 4), T_4(-1, 3).$$

Brez težav najdemo enačbe premic:

$$\begin{aligned} p_{1,2}(x, y) &= x - y - 4 = 0, \\ p_{3,4}(x, y) &= x - y + 4 = 0, \\ p_{1,3}(x, y) &= x + y - 4 = 0, \\ p_{2,4}(x, y) &= x + 7y - 20 = 0. \end{aligned}$$

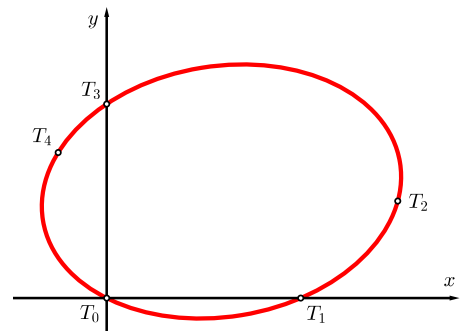
Iskana krivulja ima enačbo

$$\begin{aligned} P(x, y) &= (x - y - 4)(x - y + 4) - \\ &\quad \lambda(x + y - 4)(x + 7y - 20) = 0. \end{aligned}$$

Ker mora veljati še $P(T_0) = P(0, 0) = 0$, dobimo enačbo $-16 - 80\lambda = 0$ z rešitvijo $\lambda = -1/5$, kar vstavimo v enačbo iskane krivulje. Poenostavimo in na koncu dobimo

$$3x^2 - xy + 6y^2 - 12x - 24y = 0.$$

Iskana stožnica je elipsa (slika 3).



SLIKA 3.

Elipsa skozi pet danih točk.

V primeru, ko je vsaj ena od trojk (T_0, T_1, T_2) in (T_0, T_3, T_4) kolinearna, trojki (T_0, T_1, T_3) in (T_0, T_2, T_4) pa nekolinearni, poiščemo enačbo premice $a_{1,2}x + b_{1,2}y + c_{1,2} = 0$ skozi T_1 in T_2 ter enačbo premice $a_{3,4}x + b_{3,4}y + c_{3,4} = 0$ skozi T_3 in T_4 . Izrojena stožnica je kar unija teh dveh premic, njena enačba pa se glasi $(a_{1,2}x + b_{1,2}y + c_{1,2})(a_{3,4}x + b_{3,4}y + c_{3,4}) = 0$.

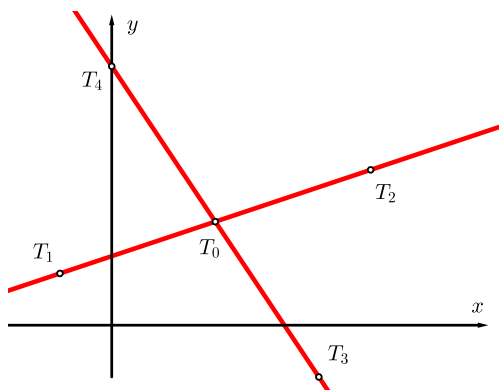
V preostalih primerih enačba izrojene stožnice ni do konstantnega faktorja enolično določena.

2. naloga.

Poiščimo še enačbo stožnice, ki poteka skozi točke

$$T_0(2, 2), T_1(-1, 1), T_2(5, 3), T_3(4, -1), T_4(0, 5).$$

Prve tri točke ležijo na premici $x - 3y + 4 = 0$, zadnji dve pa na premici $3x + 2y - 10 = 0$ (slika 4). Iskana izrojena stožnica ima enačbo $(x - 3y + 4)(3x + 2y - 10) = 3x^2 - 7xy - 6y^2 + 2x + 38y - 40 = 0$.



SLIKA 4.

Še en primer izrojene stožnice.

3. naloga.

Poiščimo še enačbo stožnice, ki poteka skozi točke

- $T_0(0, 0), T_1(1, 0), T_2(2, 0), T_3(3, 0), T_4(3, 3)$.

Prve štiri točke ležijo na premici $y = 0$. Premica skozi T_4 ima enačbo $k(x - 3) - y + 3 = 0$, kjer je k poljubna konstanta. Vseh pet točk najdemo na izrojeni stožnici $(k(x - 3) - y + 3)y = 0$, pa tudi na $(x - 3)y = 0$, kjer vzamemo navpično premico skozi T_4 . Rešitev je nešteto.

Domače naloge.

- Poišči stožnico, ki poteka skozi točke

- $T_0(0, 0), T_1(1, 1), T_2(-2, 0), T_3(4, 3), T_4(-3, 2)$.

(Rezultat: hiperbola z enačbo $22x^2 - 16xy - 31y^2 + 44x - 19y = 0$.)

- Poišči stožnico, ki poteka skozi točke

- $T_0(0, 1), T_1(-2, 0), T_2(-5, -2), T_3(0, -2), T_4(1, 0)$.

(Rezultat: parabola z enačbo $x^2 - 2xy + y^2 + x + y - 2 = 0$.)

- Poišči še stožnico, ki poteka skozi točke

- $T_0(-2, 0), T_1(1, 1), T_2(4, 2), T_3(3, -1), T_4(2, 3)$.

(Rezultat: izrojena stožnica, dvojica sekajočih se premic, z enačbo $(x - 3y + 2)(4x + y - 11) = 0$.)

× × ×

Tekmovanje π

↓↓↓

NEŽKA MRAMOR KOSTA IN JASNA PREZELJ

→

Letošnji Mednarodni dan matematike je potekal pod sloganom *Matematika za vsakogar* in res bi matematika ta dan lahko dosegla vsakogar, saj so ji slovenski mediji namenili razveseljivo veliko pozornosti. Na Društvu matematikov fizikov in astronomov Slovenije smo poleg že tradicionalnega likovnega natečaja za čim lepše porisano matematično tablo, ki se zaključuje konec meseca marca, učencem in dijakom letos ponudili še en izziv – poiskati čim boljši približek števila π (ki mu je 14. marec ali v angleškem datumskem zapisu 3.14., posvečen) z mehaničnimi pripomočki in z merjenjem, tehtanjem in preštevanjem. Na razpis, ki je bil objavljen že v prejšnji številki Preseka, smo prejeli pet izvirnih in zanimivih rešitev. Prav vse si zaslužijo pohvalo in nagrado za domiselnost in zgledno skupinsko delo.

Najbolj izdelano rešitev so prispevali učenci 8a. razreda OŠ Cerkvenjak-Vitomarci pod mentorstvom učitelja Stanislava Toplaka. Oceno števila π so dobili s preštevanjem kvadratkov kvadratne mreže, ki skupaj pokrivajo četrtno kroga z znano ploščino, izboljšali pa so jo tako, da so na robu lika uporabili finejšo mrežo (slika 1).

Rezultat računa: 3,1410. Posebno pohvalo si zaslužijo za oceno in analizo napake svojega približka.

Najbolj izvirno rešitev naloge so prispevali Neža, Živa, Tamara Elena, Domen, Niko in Matjaž, učenci 8. razreda OŠ Globoko pod mentorstvom učiteljice Danijepe Pezdirc. Izmerili so obseg in premer kroga na šolskem športnem igrišču in še 41 okroglih predmetov, ki so jih našli doma – od majhnih, kot so smoki, kabel, baterija, ..., do krožnikov, ponev, globusa ... Tako so dobili celo vrsto približkov števila π s povprečno vrednostjo 3,1243.

→



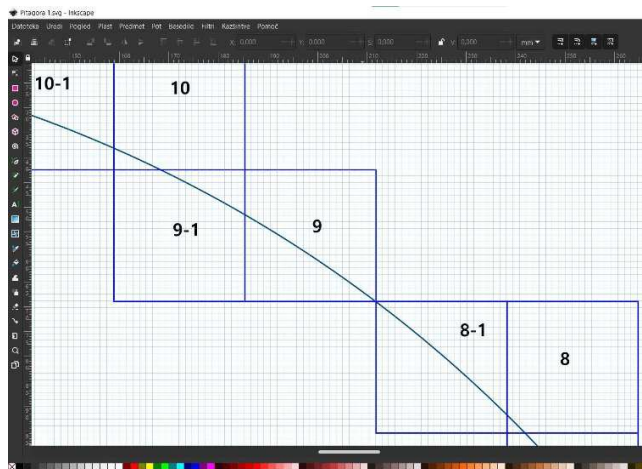
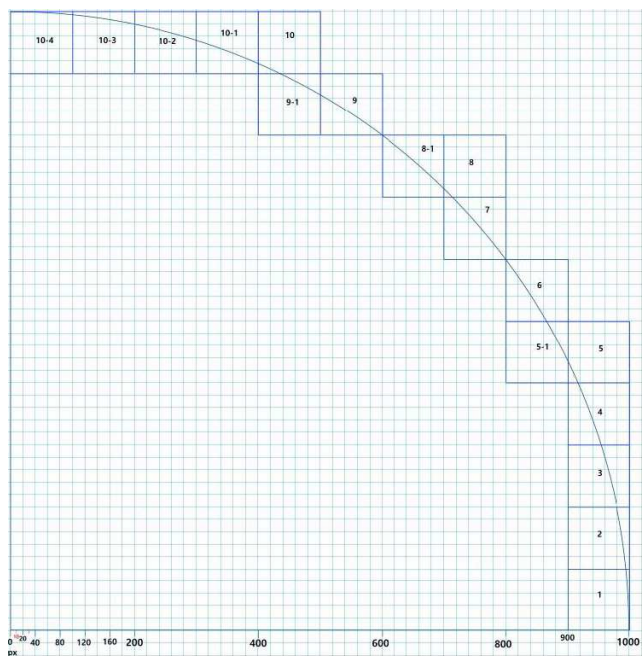
Učenci 8. razreda OŠ Gradec, Mia, Iris, Tjaša, Jona in Lovro, so pod mentorstvom učiteljice Astrid Žibert približek števila π izračunali s pomočjo geometrijske konstrukcije poljskega duhovnika Adama Kochanskega iz 17. stoletja. Pri različnih polmerih kroga so dobili pet različnih približkov, najboljši (ob nekoliko nerealni predpostavki, da lahko načrtamo

krog s polmerom 10 km) je 3,14153334, kar se ujema s π celo na prvih štirih decimalkah.

Skupina devetošolcev z OŠ Šmartno pod Šmarno goro je z mentorico Bojano Novak izdelala kartonast kvader, ki je imel za osnovno ploskev kvadrat, in valj, ki je imel za osnovno ploskev krog s polmerom enakim dolžini stranice kvadrata. Vanju so natresli riž, testenine in frnikule. Vse so prešteli in stehtali, nato pa izračunali količnike in dobili povprečni približek 3,13908709. Zanimivo je, da so pri rižu in testeninah s tehtanjem dobili boljše približke kot s preštevanjem.

Prav posebno pohvalo pa si zaslužijo učenci 4. razreda Waldorfske šole Savinja, ki so, čeprav še ne poznajo decimalnih števil, pod mentorstvom razredničarke Nine Kociper približek števila π dobili tako, da so primerjali število velikih palic mikado, ki jih lahko zložiš v valj (41) in v kvader, ki gre vanj (13). Dobili so približek 3,153, kar res ni slabo za velike mikado palice (slika 2)!

Vsem, učenkam, učencem, mentoricam in mentorjem hvala, da ste se lotili našega izziva in iskrene čestitke!



SLIKA 1.



SLIKA 2.

× × ×

Kaj povejo krivulje za MTF o fotografskem objektivu

↓↓↓

PETER LEGIŠA

→

Kontrast in modulacija

Na sliki 1 imamo svetlo in temno površino drugo ob drugi. Naj bo E_t svetlost temnejšega dela in E_s svetlost svetlejšega dela. Za mero kontrasta med obema površinama vzamemo **modulacijo**

$$M = \frac{E_s - E_t}{E_s + E_t}. \quad (1)$$

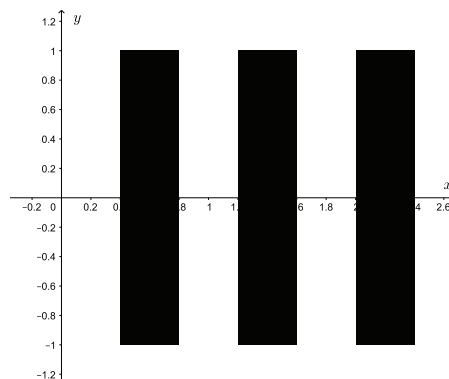
Vrednosti za M leže med 0 in 1.

Obstajajo še druge mere za kontrast, a mi se bomo držali gornje. Kontrast je pomemben tudi v vsakdanjem življenju. Pri branju si želimo kar se da velik kontrast med črkami in podlago. Črne črke na modri podlagi pomenijo kljub razliki v barvi majhen kontrast in težave pri branju. Še večja polomija so rumene črke na beli podlagi - kontrast je premajhen, tudi razlika v barvi je premajhna.

Pri večini fotografij si želimo visok kontrast in številne podrobnosti. Izjeme so recimo »zasanjane« meglene scene.

Pri testiranju fotografskih objektivov velikokrat slikajo površino - tarčo, na kateri so črni vzorci na beli podlagi. Denimo, da imamo črne stolpce, ločene z belimi prostori enake širine - kot na sliki 2. Ta tarča je že stara, a je prav primerna za razlago. En stolpec in skladen beli prostor ob njem sta en **črtni par** ali en **cikel**. Če je $E_t = 0$, je modulacija med obema pravokotnikoma 1.

Na sliki, ki jo naredi objektiv, bo kontrast zmanjšan: črnina ne bo čisto črna in se bo na robovih stolpca prelivala v belino. Prav tako vmesni prostori ne bodo povsem beli. To bo bolj očitno pri tankih stolpcih in v vogalih slike.



SLIKA 2.

Črni stolpci na beli podlagi.

Primer imamo na fotografiji 3, kjer je s tri desetletja starim širokokotnim zoomom 20-35 mm 1:3.5-



SLIKA 3.

Močno povečan vogal fotografije.



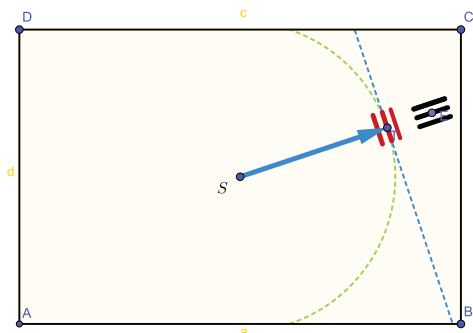
SLIKA 1.

Kontrast med temnejšo in svetlejšo površino.



4.5 pri goriščni razdalji 20 mm in povsem odprti zaslonki slikana tarča v spodnjem levem vogalu vidnega polja. Tarča je obešena tako, da je pol črnih paličic približno vzporednih zveznici s središčem slike. Objektiv je bil ročno izostren na tarčo, druge dele slike smo ignorirali. Poudarimo, da gre za manj kot pol odstotka površine celotne fotografije.

Smer od središča S slike do točke T na sliki 4 je **radialna** ali **sagitalna** smer. Latinska beseda *sagitta* pomeni puščico ali strelo. Na sliki 4 je ta smer narisana s puščico v modri barvi. Pravokotno na sagitalno smer pa poteka **tangentna** ali **meridionalna** smer skozi točko T . Rdeče imamo narisani tangentialni vzoreček okrog točke T . Črno pa imamo narisani sagitalni vzoreček okrog točke E , ki je bližje robu. **Število črtnih parov preslikanega vzorca na milimeter slike na tipalu (filmu) je frekvenca vzorca.**



SLIKA 4.

Rdeči vzoreček je tangentialen, črni sagitalen.

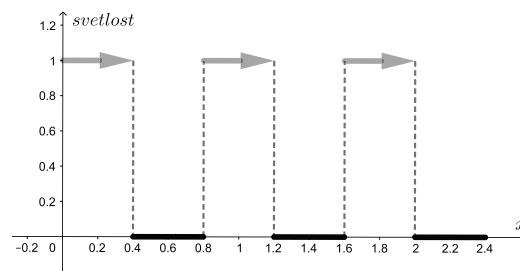
Vidimo, da je naša fotografija 3 razmazana v radialni smeri. Če dobro pogledamo, so robovi obarvani: na eni strani vijolično, na drugi zeleno. To je posledica *disperzije* svetlobe. Steklo in plastika lomita različne barve nekoliko različno, dolge valovne dolžine navadno manj od kratkih.

Manjše paličice, ki imajo tangentialno smer, so na sliki pošteno obledele. Večje paličice v tangentialni smeri so malo obledele in so se malo razmazale. Prostor med manjšimi paličicami je daleč od beline. Kontrast manjših tangentialnih vzorcev je tako bistveno zmanjšan. Modulacijo preslikanega vzorca treh paličic izračunamo po formuli 1, kjer je E_t izmerjen v najtemnejšem delu slike paličice, E_s pa v najsveblejšem delu sredi med paličicami.

Paličice, ki potekajo v radialni smeri, so jo precej bolj odnesle, razmazane so le na koncih. Edino pri najbolj drobnih vzorcih je kontrast v obeh smereh tako zmanjšan, da paličic praktično ne ločimo več. Višja frekvenca vzorca pomeni manjšo modulacijo slike.

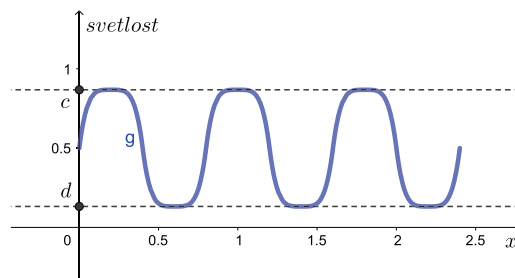
Faktor prenosa modulacije - MTF

Vrnimo se k sliki 2. Denimo, da se gibljemo po osi x in rišemo svetlost dela tarče (sustav treh črtnih parov) v vsaki točki. Če je svetlost črnih delov (idealizirano) 0, dobimo sliko 5. Modulacija te tarče je 1.



SLIKA 5.

Svetlost vzorca s slike 2.

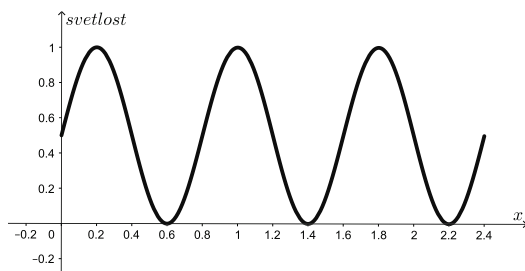


SLIKA 6.

Spreminjanje svetlosti preslikanega vzorca s slike 2.

Na sliki tarče merimo svetlost vzdolž slike osi x . Dobimo periodičen graf – nekaj takega kot na sliki 6. Nekoliko spominja na sinusoido. Modulacija, to je modulacija med najbolj temnimi in najbolj svetlimi deli slike, je enaka $(c - d) / (c + d)$ in je manjša kot 1.

V tridesetih letih prejšnjega stoletja je *Helmut Friese*, ki je delal pri firmi *Zeiss-Ikon*, prišel na nasled-

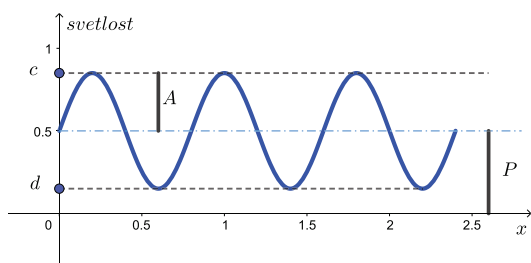


SLIKA 7.

Sinusno spreminjanje svetlosti vzorca.

njo idejo ([3, str. 30]). Tarčo na sliki 2 nekoliko spremenimo, tako da namesto oglatega grafa svetlosti dobimo sinusoido kot na sliki 7. Na tarči imamo zvezne prehode od bele do črne – kot bi se vzorec s slike 2 na poseben način razmazal v vodoravni smeri. Ekstremni vrednosti za svetlost se pri tem ohranita, tako da je modulacija M_1 tarče na sliki 7 blizu 1. En polni nihaj je en cikel. Na sliki 7 imamo tri cikle.

Frieser je opazil, da se svetlost slike – ne glede na napake lečja – v tem primeru spreminja tudi sinusno. To velja lokalno in bomo uporabili na majhnem delu slike okrog točke T . Svetlost preslikanega sinusnega vzorca je sinusoida, kot recimo na sliki 8. **Število ciklov na milimeter slike na tipalu (filmu) je frekvenca f vzorca.**



SLIKA 8.

Spreminjanje svetlosti preslikanega sinusnega vzorca.

Modulacijo slike, ki pride skozi lečje, izračunamo po formuli

$$M_2(f) = \frac{c - d}{c + d} = \frac{A}{P}, \quad (2)$$

kjer je c največja in d najmanjša vrednost sinusoide na sliki 8. In: $P = (c + d)/2$ je povprečna vrednost

sinusoide, $A = (c - d)/2$ pa *amplituda* sinusoide.

Količnik

$$K(f, T) = \frac{M_2(f)}{CM_1(f)}$$

je **faktor prenosa modulacije ali MTF** v točki T pri frekvenci f . Navadno je $M_1(f)$ konstanten, neodvisen od f . Normalizacijski faktor C določimo tako, da je pri frekvenci 0 vzorca zapisani količnik enak 1 (vira [1, str. 143] in [2]). Torej je

$$\frac{M_2(0)}{CM_1(0)} = 1 \quad \text{in od tod} \quad C = \frac{M_2(0)}{M_1(0)}.$$

(Po domače: če imamo zraven našega sinusnega vzorca večjo črno in večjo belo ploskev, je C modulacija med slikama teh ploskev.)

Število $K(f, T)$ je med 0 in 1 in je **mera za zmanjšanje kontrasta na sliki glede na original**.

Oznaka MTF je okrajšava za **Modulation Transfer Factor**.

Zdaj imamo že toliko izkušenj, da vemo, da bomo v točki T morali posebej obravnavati MTF za sagitalen tarčni vzorec in posebej za tangenten vzorec. In to vsaj pri dveh frekvencah. Kot minimum vzamejo recimo frekvenci 10 in 30 ciklov na mm slike. Kakovost upodabljanja v dani točki bo torej ocenjena z najmanj štirimi podatki.

Če je MTF pri frekvenci 10 visok, to je blizu 1, to navadno interpretirajo kot dober kontrast v dani točki. Visoko vrednost pri frekvenci 30 ali 40, 50 ciklov na mm pa interpretirajo kot visoko ločljivost. Navadno je najtežje doseči dobre vrednosti pri povsem odprti zaslonki, zato se skoraj vedno omejijo na ta primer.

Večina fotografiov ve, da je kakovost fotografije najboljša v sredini in večinoma pada proti robovom. Najslabša je navadno v vogalih. Torej je treba izmeriti MTF v več točkah, od sredine proti vogalu.

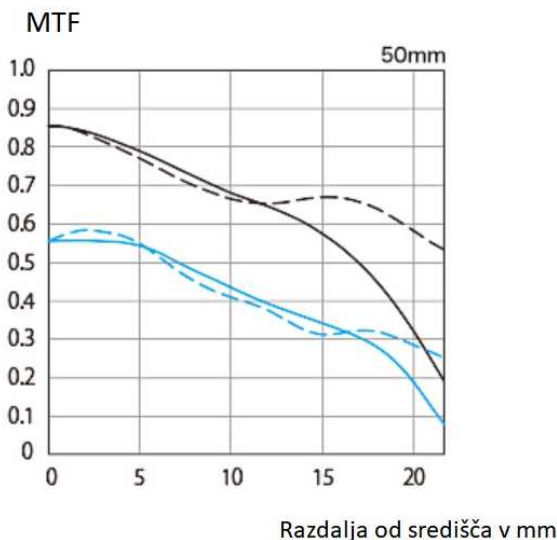
Postopek pri neposrednem merjenju je približno takle. Izberejo frekvenco f . Izostrijo sredino slike in tam določijo MTF. Nato se pomikajo v več korakih proti vogalu in na vsakem koraku izmerijo MTF, ne da spreminjali izostritev. Podatke vnesejo v graf, kjer je na abscisni osi razdalja od središča slike do točke v milimetrih. Pri polnem formatu s tipalom velikosti 24 mm × 36 mm je vogal od središča oddaljen

$$\sqrt{12^2 + 18^2} \approx 21,6 \text{ mm.}$$





Vrednosti povežejo – sagitalne vrednosti s polno, tangentne s črtkano črto. Dobijo dve lomljeni črti, ki ju večkrat zgladijo. Tako nastaneta dve **funkciji prenosa modulacije** pri frekvenci f , ki ju prav tako označimo z MTF – angleško **Modulation Transfer Function**.



SLIKA 9.

Novi proizvajalec prikaz MTF za polno odprti objektiv Canon EF 50 mm f/1.4 USM pri frekvencah 10 (črno) in 30 (modro). Črtkano tangentna smer, polno radialna.

Firmi Zeiss in Leica dejansko dajeta take izmerjene grafe za svoje objekte, Zeiss denimo pri 10, 20 in 40 ciklih na mm. Leica pa pri frekvencah 5, 10, 20 in 40 mm^{-1} . Drugi proizvajalci dajejo **izračunane** prikaze MTF za svoje objekte. Programi, ki izračunajo MTF lečja, so zelo olajšali delo konstruktorjem. Izračunani prikazi so bolj optimistični od izmerjenih.

MTF prikaze kakovosti objektivov je smiselno primerjati le v okviru enega proizvajalca. So prav koristna informacija pri odločitvi o nakupu. Na spletu jih najdemo pod »MTF chart« in oznako objektiva.

Canon je leta 2018 spremenil metodologijo, tako da je primerjava med prikazi pred tem datumom in po njem otežena. Novi kriteriji so strožji, dajejo pa le podatke pri frekvencah 10 in 30 na milimeter in povsem odprti zaslonki. Na sliki 9 imamo tako novi prikaz MTF s strani <https://canon.jp/> za tri dese-



SLIKA 10.

Fotografija vogalne tarče s Canon EF 50 mm f/1.4 USM.

tletja stari 50 milimetrski objektiv, pri zaslonkem številu 1,4.

Na abscisni osi je razdalja od središča slike. Črni krivulji sta pri frekvenci 10, modri pri frekvenci 30 mm^{-1} . Kakovost slike stran od središča pada in je v vogalih nizka. Pri frekvenci 10 je blizu roba tangentni kontrast precej višji od radialnega – črtkana črna črta je nad polno. To se ujema s fotografijo tarče v vogalu spodaj levo s tem objektivom na sliki 10. (Gre za približno odstotek površine celotne fotografije.)

Pri zaslonkih številih od 5,6 do 8 so za ta sede- mlečni objektiv krivulje MTF bistveno višje in drugačne in rezultati fotografiranja odlični. O tem več drugič.

Danes dobimo objekte 50 mm f/1,4, ki so zelo dobri ali odlični že pri polni odprtini. So pa mnogo bolj zapleteni, večji, težji in dražji.

Literatura

- [1] S. F. Ray, *Applied Photographic Optics*, 2nd ed., Focal Press, Oxford 1995, 586 str.
- [2] Imatest: *Sharpness: What is it and How it is Measured*, <https://www.imatest.com/docs/sharpness/>
- [3] H. H. Nasse, *How to Read MTF Curves II*, Carl Zeiss Camera Lens Division, March 2009, 31 str., https://lenspire.zeiss.com/photo/app/uploads/2018/04/CLN_MTF_Kurven_2_en.pdf

× × ×

Krivulja prislonjene lestve

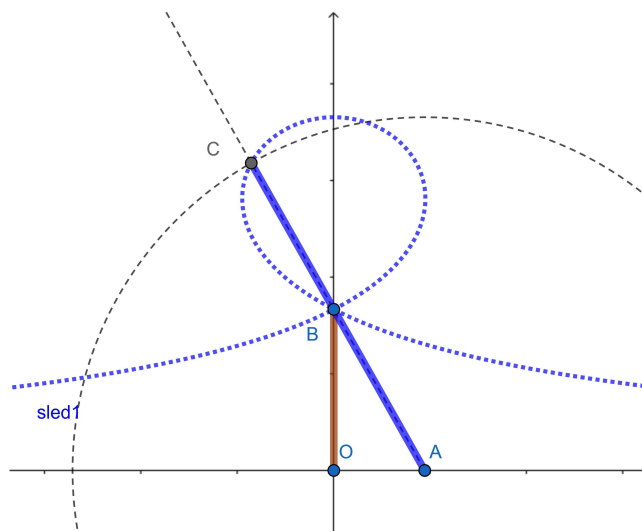
↓↓↓

BOŠTJAN KUZMAN

→ Pomlad je prišla in delo na vrtu kliče tudi matematike. V tokratnem kotičku si bomo ogledali skoraj vsakdanji problem: do kod seže prislonjena lestev. Natančneje, s pomočjo GeoGebre bomo narisali krivuljo, ki jo opiše vrh v fiksni točki prislonjene lestve, če njen spodnji del prosto premikamo po vodoravni površini. Problem bomo rešili na dva načina: najprej zgolj z uporabo preproste geometrijske konstrukcije, nato še z izračunom parametrične enačbe krivulje, za katerega bomo uporabili Pitagorov izrek in podobnost trikotnikov.

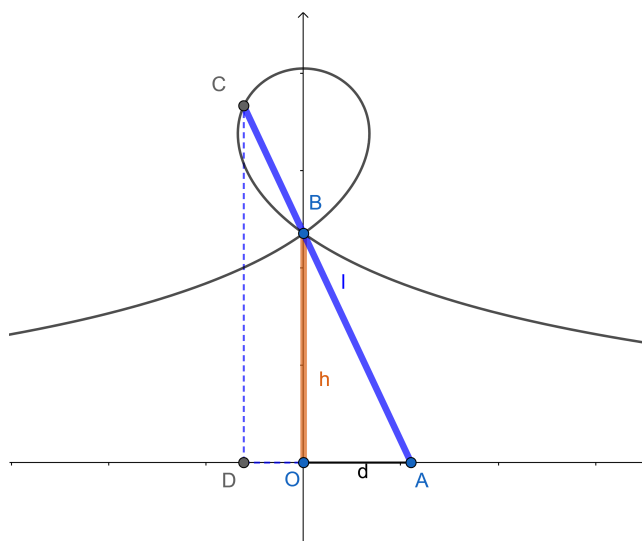
Problem bomo reševali kar v ravnini. Lestev in njeno oporo bosta predstavljali daljici. Opišimo zaporedje korakov za geometrijsko konstrukcijo:

- Vstavimo drsnik z imenom l , ki predstavlja dolžino lestve. Zavzame naj vrednosti med 0 in 10.
- Z orodjem za dodajanje točke in klikom na ustrezno koordinatno os vstavimo poljubno točko A na osi x in poljubno točko B na osi y . Označimo še točko $O = (0, 0)$.
- Narišemo daljico OB . Ta predstavlja oporo, na katero bomo prislonili lestev.
- Narišemo poltrak iz točke A skozi točko B in krožnico s središčem A in polmerom l .
- Označimo s C presečišče poltraka in krožnice. Našo lestev dolžine l zdaj predstavlja daljica skozi A in C . (Po potrebi povečajmo l , da bo lestev res prislonjena na oporo.)
- Zdaj lahko opazujemo gibanje točke C , ki predstavlja vrh lestve, v odvisnosti od pomikanja točke A po vodoravni površini.
- Daljice in točke po želji odebelimo in pobarvamo, ter z risalne površine skrijemo vse nepotrebne elemente.
- Če želimo, lahko narišemo krivuljo gibanja vrha lestve po točkah s pomočjo vklopa sledi točke C , ali pa narišemo celotno krivuljo vnaprej z ukazom $\text{Sled}(C, A)$ (slika 1).



SLIKA 1.

Geometrijska konstrukcija točke C in njena sled glede na točko A .



SLIKA 2.

Določanje koordinat točke C s pomočjo podobnih trikotnikov.



- Zanimivo je opazovati, kako se spreminja oblika krivulje, če spreminjamo dolžino lestve l ali višino opore (točka B).
- Pozorni bralec je seveda opazil, da lahko vrh lestve v resnici opiše le zanko, ne pa tudi levega ali desnega kraka krivulje na sliki, saj v tem primeru vrh lestve nima več opore in bi lestev padla na tla.

Kot smo napovedali na začetku, je naloga zanimiva in dovolj enostavna tudi za reševanje s pomočjo enačb. Namesto geometrijske konstrukcije točke C s pomočjo presečišča poltraka in krožnice lahko izračunamo njene koordinate v odvisnosti od položaja točke A . Oglejmo si skico na sliki 2.

Naj bo točka $C = (x_C, y_C)$ krajišče lestve in naj bo $D = (x_C, 0)$ njena pravokotna projekcija na vodoravno os. Zaradi podobnosti trikotnikov $\triangle AOB$ in $\triangle ADC$ velja $|AD| : |AC| = |AO| : |AB|$. Torej je $|AD| = \frac{l \cdot d}{\sqrt{h^2 + d^2}}$, kjer je h dolžina daljice $|OB|$ oziroma višina opore, d pa dolžina daljice OA oziroma x -koordinata točke A . Zato se x -koordinata točke C izraža kot

$$x_C = d - |AD| = d - \frac{l \cdot d}{\sqrt{h^2 + d^2}}.$$

Še enostavneje dobimo y -koordinato točke C iz zveze $|DC| : |AC| = |OB| : |AB|$ in torej

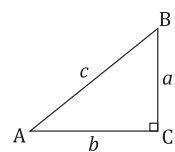
$$y_C = \frac{l \cdot h}{\sqrt{h^2 + d^2}}.$$

Izračun lahko uporabimo pri izdelavi modela tako, da ponovimo prve tri korake prejšnje konstrukcije in označimo daljici $d = \text{Daljica}(0, A)$ in $h = \text{Daljica}(0, B)$, nato pa direktno vnesemo še točko C z ukazom $C = (d - l \cdot d / \sqrt{h^2 + d^2}, l \cdot h / \sqrt{h^2 + d^2})$. Potem lahko podobno kot prej model še dopolnimo z dodatnimi daljicami, risbo sledi in podobno.

Nadebudni bralci in bralke pa lahko poskusijo krivuljo narisati še na tretji način s pomočjo ukaza **Krivulja** za risanje parametričnih krivulj.

× × ×



K	A	N	S	A	S	D	R	N	I	K	A	R	O	B	E	S	P	I	E	R	R	E	J	E	N	I	S	E	J	
K	R	V	O	P	R	E	L	I	T	J	E	R	N	I	L	U	S	T	R	A	C	I	J	A	I	L	I	Č	N	O
I	K	O	N	O	S	K	O	P	E	N	C	I	J	A	N	L	E	V	I	U	K	A	N	C	O	V	P	A	K	
H	A	N	O	J	T	V	A	S	T	E	R	A	R	M	L	T	K	R	Č	E	T	O	S							
A	S	T	E	R	O	I	D	T	E	R	A	R	M	L	T	K	R	Č	E	T	O	S								
K	I	L	A	N	O	S	R	O	S	I	C	A	I	N	O	V	A	T	I	V	N	O	S							
A	R	A	N	Ž	E	R	K	A	S	T	O	A	R	E	I	T	E	R	P	O	A	N	T	A						
P	I	N	J	A	E	R	E	P	S	I	N	A	I	K	O	S														
U	S	E	R	S	K	I	N	E	F	E	R	M	A	T	M	E	R	A												
Ž	S	T	A	N	G	A	V	O	N	J	S	O	P	L	E	S	A	L	E	C										
K	O	N	K	O	R	D	A	N	C	A	C	V	E	T	A	N	I	T	I											
A	R	I	A	N	A	Č	A	K	Š	O	T	R	O	K	A	N	I	S												

REŠITEV NAGRADNE KRIŽANKE PRESEK 50/4

→ Pravilna rešitev nagraadne križanke iz četrte številke Preseka letnika 50 je **Včrtani lik**. Med pravilnimi rešitvami smo izžrebali naslednje reševalce: Katarina Šipeč iz Kranja, Tadeja Bone iz Ajdovščine in Neža Korenjak iz Mengša, ki bodo nagrade prejeli po pošti.

× × ×

Razpis tekmovanja srednješolcev iz matematike in fizike v letu 1980/81

LETNIK 8, ŠTEVILKA 3, 1980/81

↓↓↓

→ Tekmovanji iz matematike in fizike za srednješolce tradicionalno potekata v marcu ali aprilu in imata od vseh srednješolskih tekmovanj v Sloveniji najdaljšo tradicijo. V 1980-tih letih so šole z običajno pošto poslale tekmovalni komisiji prijavo za predtekmovanje (današnje šolsko tekmovanje) in nato same izbrale dijake, ki so se uvrstili na republiško (današnje državno) tekmovanje. Republiško tekmovanje je bilo vsako leto izvedeno v drugem kraju. Ker so bila potovanja po Sloveniji takrat počasnejša, so dijaki z učitelji v ta kraj običajno prispeli že dan pred tekmovanjem in tam prenočili, predtekmovalni večer pa so si popestrili z družabnimi igrami in kvizi. Tako je bilo tekmovanje namenjeno tudi tkanju vezi in prijateljstev med dijaki iz različnih delov Slovenije. Republiško tekmovanje je običajno potekalo na soboto dopoldan, tekmovalci so si nato ogledali kakšno lokalno podjetje ali naravno znamenitost, komisija pa je izdelke ocenila v nekaj urah, da so bili rezultati slovesno razglašeni še isto popoldne.

Za tekmovanji sta v šolskem letu 1980/81 skrbela **Marko Petkovšek** in **Bojan Golli**, ki sta v naslednjih desetletjih ogromno prispevala k naši reviji, pa tudi k razvoju in popularizaciji matematike in fizike med mladimi v Sloveniji. Žal sta se oba poslovila v mesecu marcu 2023. Presekovi bralci ju bomo skupaj z lepimi trenutki iz matematičnih in fizikalnih tekmovanj ohranili v prijetnem spominu.

RAZPIS TEKMOVANJA SREDNJEŠOLCEV IZ MATEMATIKE IN FIZIKE V ŠOLSKEM LETU 1980/81

Urniki za to šolsko leto je naslednji:

Matematika: predtekmovanje bo 7. marca (sobota) od 9. do 11. ure, tekmovanje pa 4. aprila (sobota) od 10. do 12. ure.

Fizika: predtekmovanje bo 11. aprila (sobota) od 9. do 11. ure, tekmovanje pa 16. maja (sobota) od 10. do 12. ure.

Republiško tekmovanje iz matematike bo v Ljubljani, v prostorih I. gimnazije - Bežigrad, iz fizike pa v Velenju, v prostorih Rudarskega šolskega centra. Na predvečer republiškega tekmovanja iz fizike bo družabna prireditev z merjenjem znanja srednješolskih skupin iz fizike. O podrobnostih tega tekmovanja bomo obvestili šole posebej.

Želimo, da bi se predtekmovanj udeležile vse srednje šole v Sloveniji. Zato pozivamo tudi dijake, da opozorijo svoje učitelje na ta razpis. Profesorje matematike in fizike pa seveda prosimo, da sodelujejo pri izvedbi predtekmovanj, vzpodbujajo dijake in jim svetujejo pri pripravah. Predvsem jih prosimo, da sodelujejo z republiškima komisijama pri izdelavi nalog. Za vse predloge in pripombe bomo zelo hvaležni, naslovite pa jih na komisijo za popularizacijo, z navedbo za matematiko oz. fiziko. Mladim nadebudnežem želimo v letošnjem tekmovalnem ciklusu čimveč dobrih idej ob reševanju nalog!

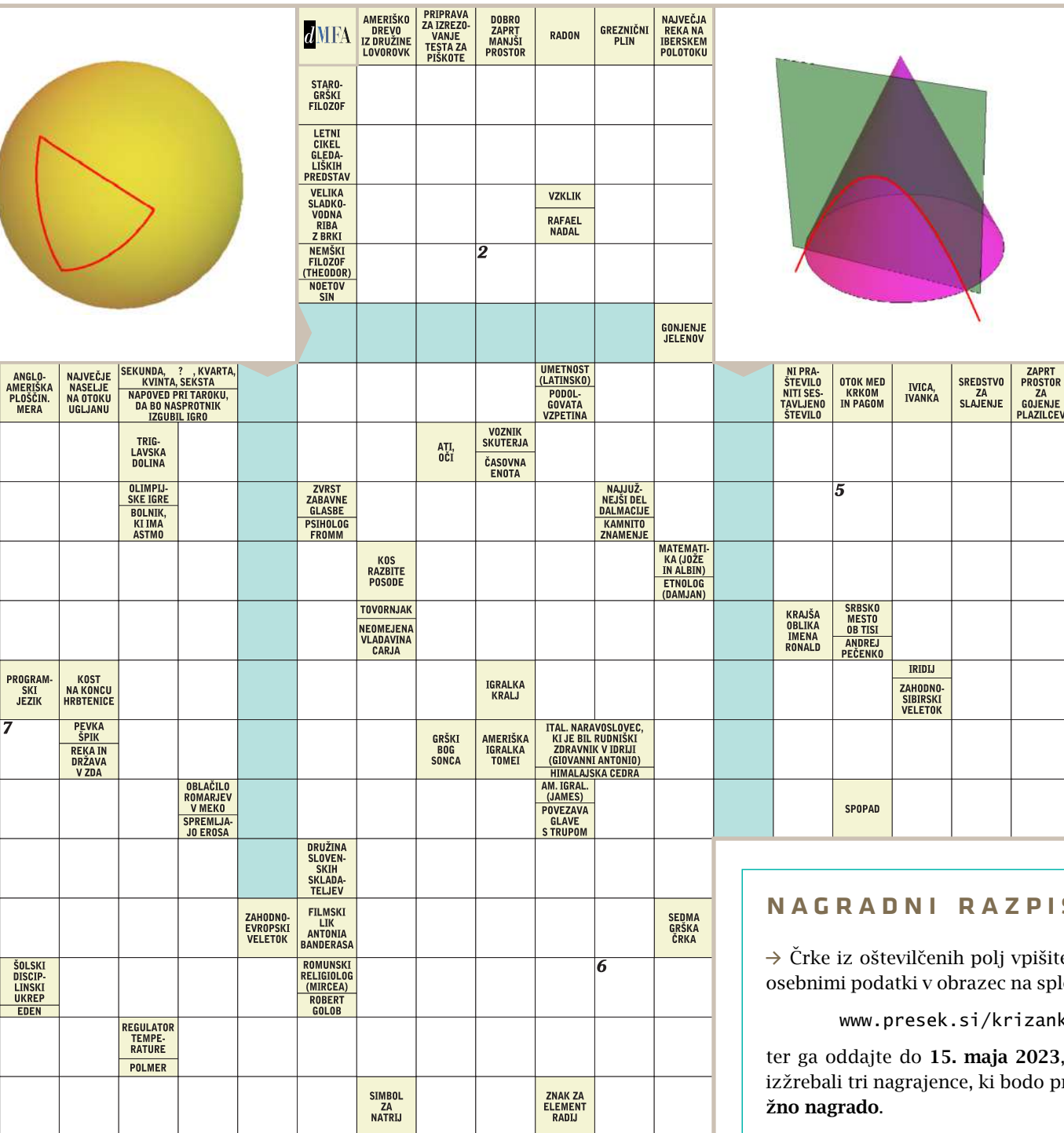
Marko Petkovšek, Bojan Golli



XXX

EIA RESOLUTION + CHART 1956

16



NAGRADNI RAZPIS

→ Črke iz oštevilčenih polj vpišite skupaj z osebnimi podatki v obrazec na spletni strani

www.presek.si/krizanka

ter ga oddajte do **15. maja 2023**, ko bomo izžrebali tri nagrajence, ki bodo prejeli **knjižno nagrado**.

Moja izkušnja opazovanja eksoplaneta

↓↓↓

NEJA PISK

→ Med 26. in 31. avgustom 2022 je v Hiši mladih v Ajdovščini potekala Prva šola astronomije GoChile. Šole se nas je udeležilo 16 dijakov in dijakinj iz cele Slovenije. Vodilo nas je sedem mentorjev. V šoli smo v dvojicah delali projekte s pomočjo teleskopa GoChile. Projekti so bili s področij astrofotografije, opazovanja eksoplanetov, spremenljivih zvezd, asteroidov, oddaljenih galaksij ter razsutih kopic. V tem prispevku bom predstavila svoj projekt opazovanja prehoda eksoplaneta.

Opazovanja smo izvajali s teleskopom v Čilu. Leta 2021 sta Fakulteta za naravoslovje v Novi Gorici in astronomska revija Spika na observatorij El Sauce postavila dva teleskopa v okviru pedagoško-raziskovalnega projekta GoChile. Čile so izbrali, saj ima kar 300 jasnih noči na leto in ker v gorovju, kjer sta teleskopa postavljena, ni svetlobnega onesnaženja. Manjši teleskop GoT2, ki je namenjen širokokotnemu opazovanju (predvsem fotografiranju večjih meglic in razsutih kopic), je lečni teleskop velikosti 72 mm. Večji 400-milimetrski zrcalni teleskop GoT1 pa je namenjen podrobnemu opazovanju temnejših objektov in raziskovanju meglic, galaksij, zvezd in objektov Osončja. Oba teleskopa upravljamo na daljavo.

Eksoplanet Wasp 145 Ab

Jaz sem v dvojici z Larisso Stepanovo opazovala prehod eksoplaneta prek gostujoče zvezde. Eksoplaneti so planeti zunaj našega Osončja, ki lahko krožijo okoli druge zvezde ali pa se gibljejo prosto med zvezdami. Astronomi so prve eksoplanete odkrili v devetdesetih letih, do sedaj pa so jih našli že več kot pet tisoč. Nekateri so po masi in velikosti podobni

planetom našega Osončja, drugih, kot na primer super Zemelj in mini Neptunov, pri nas ne najdemo. Na nekaterih eksoplanetih so odkrili led in vodo, našli naj bi tudi lavo. Eden izmed ciljev raziskovanja eksoplanetov je odkriti življenje zunaj naše Zemlje.

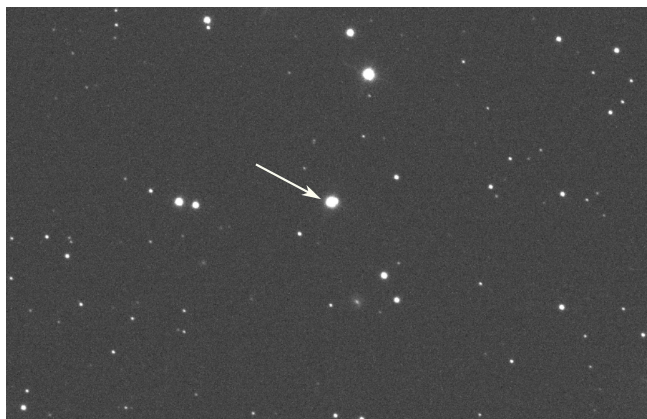
Ko sva se odločili za temo, sva si morali najprej izbrati planet, ki ga bova opazovali. To sva naredili s pomočjo Nasinega spletnega arhiva o eksoplanetih¹, kjer sva izbirali med tisočimi planeti. Prvi kriterij pri najini izbiri je bil seveda, da je planet viden iz Čila. Naprej se je izbor redčil še z magnitudo, saj z našim teleskopom lahko dobro vidimo le zvezde z najtemnejšo magnitudo 17, za opazovanje eksoplaneta pa je bolje, če je zvezda nekoliko svetlejša. Kot zadnji kriterij pa je bil čas prehoda. To je čas, ki ga planet potrebuje, da prečka vidno površino gostujoče zvezde. Poskušali sva izbrati krajši čas, saj nisva imeli možnosti in časa opazovati daljšega prehoda. Tako sva si izbrali eksoplanet Wasp-145 Ab.

Eksoplanet Wasp-145 Ab spada v skupino vročih Jupitrov. Za njih je značilno, da so po velikosti podobni Jupitru in se gibljejo na majhni oddaljenosti od zvezde, zaradi česar imajo zelo kratko obhodno pot. Zaradi svoje velikosti ti planeti med prehodom med zvezdo in nami občutno spremenijo navidezni sij zvezde, zato jih lažje detektiramo z majhnim teleskopom.

Opazovanje, analiza in rezultati

Opazovali sva 28. avgusta med 3:48 in 5:05 po UT času. Začeli sva pol ure pred prehodom planeta in končali pol ure po koncu prehoda. Opazovanje sva izvedli s teleskopom GoT1, pri čemer sva uporabili filter L (ki prepusti celotno območje vidne svetlobe), posamezna osvetlitev pa je trajala 60 sekund. Planet

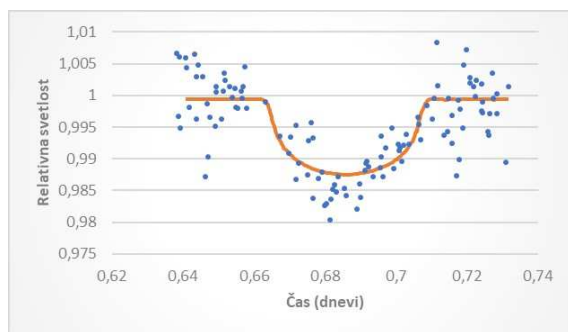
¹<https://exoplanetarchive.ipac.caltech.edu/cgi-bin/TransitView/nph-visibletbls?dataset=transits>


SLIKA 1.

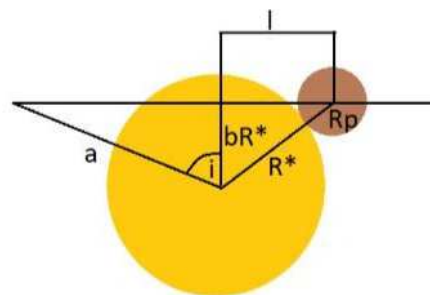
Zvezda Wasp-145 A in okoliško zvezdno polje.

je med opazovanjem dosegel najvišjo točko na nebu, zato se je med opazovanjem teleskop moral obrniti (t. i. obrat na meridianu). Zaradi tega sva izgubili nekaj podatkov. Po končanem opazovanju sva s pomočjo programa Astro Pixel Processor kalibrirali fotografije. Za tem sva naredili astrometrijo v programu ASTAP. Ta program je orientiral vse posnete slike ter vsakemu objektu na sliki dal natančne koordinate, da sva lahko potem slike primerjali med sabo. V predzadnji fazi projekta sva s pomočjo programa AstroImageJ prek primerjav z zvezdami v polju izmerili spreminjanje navideznega sija najine zvezde.

V programu AstroImageJ sva meritvam prilagodili tudi model spreminjanja svetlosti v primeru prehoda


SLIKA 2.

Potemnitev zvezde med prehodom eksoplaneta Wasp-145 Ab. Modre pike so najine meritve, oranžna črta pa model, prilagojen v programu AstroImageJ.


SLIKA 3.

Shematičen prikaz prehoda eksoplaneta. Označeni so parametri, ki jih lahko izmerimo z našimi podatki: razmerje velikosti radijev planeta (R_p) in zvezde (R_*), velika polos eliptične orbite (a) in inklinacija orbite (i).

eksoplaneta. Najboljši model nama je omogočil izračunati podatke, kot so čas prehoda, spremembo svetlosti oziroma globino prehoda, velikost planeta glede na zvezdo (ob znani velikosti zvezde), velikost velike polosi elipse, po kateri potuje planet okoli zvezde in inklinacijo orbite planeta. Ko sva vse te podatke izračunali, sva jih primerjali z rezultati v katalogu.

Najini podatki so se pri času prehoda, spremembi svetlosti, velikosti planeta in inklinaciji dobro ujemali, saj je razlika majhna glede na rezultate najdenih v katalogu. Čas prehoda se razlikuje za 0,0093 dneva, kar je posledica velike razsutosti meritev. Sprememba svetlosti med prehodom in posledično velikost planeta se zelo dobro ujemata z vrednostmi v katalogu. Pri velikosti velike polosi elipse in oddaljenosti od središča naši rezultati zelo odstopajo. Rezultata vrednosti inklinacije in oddaljenosti od središča nakazujeta, da ta dva parametra v prilagajanju modela nista skonvergirala, kar je posledica preslabe kvalitete podatkov. Ker program AstroImageJ ne poda napake, ne moreva soditi o resnični napaki najinih meritev.

S poletno šolo sem bila zelo zadovoljna, saj sem pridobila veliko novega znanja iz astronomije. Med delom na svojem projektu sem spoznala potek pridobivanja podatkov ter njihovo obdelavo. Na predavanjih so nam predavatelji dali predvsem veliko informacij na teoretičnem področju. Skozi cel tabor pa so nas vodili mentorji, ki so imeli veliko znanja in nam poskušali odgovoriti na vsa vprašanja.

× × ×

(Digitalni) ključi

↓ ↓ ↓

ALEKSANDAR JURIŠIĆ IN KLEMEN KLANJŠČEK

→ Šifre oziroma bolj splošno kriptosisteme pogosto kontroliramo s ključi, ki določajo pretvorbo podatkov. Seveda imajo tudi *ključi* lahko digitalno obliko. Ko bomo primerjali njihovo dolžino, bo to kar binarno zaporedje: 01001101010101 ... Pri tem se držimo *Kerckhoffsovega principa*, ki pravi:

»Napadalec« pozna kriptosistem oziroma postopke (algoritme), ki jih uporabljamo, ne pa tudi ključev.

Preden se poglobimo v kriptosisteme, in njihovo razbijanje, pomislimo na vsakdanje življenje. Najbolj pogosto uporabljamo posebne vrste ključev, ki jih imenujemo **gesla** in **PIN-i** (kratica pomeni Personal Identification Number, tj. osebno identifikacijsko število). Pri prvih radi uporabljamo čim širši nabor znakov, pri slednjih pa samo števke od 0 do 9 (saj običajno v tem primeru na tipkovnici ni drugih znakov).

V starih časih (tudi pr. n. št.), glej sliko 1, so imele mestne utrdbe stražarje, ki so varovali mestna vrata. Opremljeni so bili z orožjem in v nemirnih časih niso spustili noter nikogar, ki ni poznal pravičnega gesla.

Napadi na gesla

Gesla nam omogočajo kontrolo dostopa v večino računalnikov (danes sem štejemo tudi telefone). Skorajda ni osebe v modernem svetu, ki ne uporablja


SLIKA 1.

Kaj se je zgodilo s tistimi, ki so povedali napačno geslo? Pravilo je bilo: »Poskrbite zanje!«

gesel vsak dan in praktično povsod, npr. za prijavo v e-pošto, račun za družbena omrežja, do našega delovnega prostora, za dostop do shranjenih podatkov, denarja itd. Problem vohunove dileme pa ostaja v bistvu nespremenjen, glej sliko 2.

Kako vemo, ali lahko zaupamo tistemu, ki želi od nas geslo? Nas morda kdo posluša ali celo snema?

Zaupanje lahko dosežemo z digitalmi podpisi (in potrdili), glej Presekov članek [2]. Odgovor na drugo vprašanje predstavlja patentirana tipkovnica 4×3 (prikazana na zaslonu na dotik), ki vsakič naključno premeša številke na tipkah za vnos PIN-a, hkrati pa omogoča, da lahko te številke preberemo le pod skrajnim pravim kotom, glej [4]. Enostavnejši odgovor na obe vprašanji bomo predstavili v razdelku Predstavljanje in overjanje.

Če si geslo težko zapomnimo, je bolj verjetno, da ga bomo kmalu pozabili in s tem izgubili dostop. Nekateri sistemi nam sicer omogočajo ponastavitev gesla, a je ta pot lahko precej zamudna, skorajda v vseh primerih pa smo pri tem izpostavljeni določenim ranljivostim. Včasih si pomagamo tako, da si težko zapomnljiva gesla zapišemo, s čimer se seveda izpostavimo novim nepotrebnim tveganjem (zapis lahko nekdo najde in prebere).

Ko nastavljam geslo na računalniku, lahko nale-timo na veliko omejitev, kot npr.:

- imelo naj bi vsaj 8 znakov,
- vsebovalo naj bi vsaj eno veliko in eno malo črko ter
- vsebovalo naj bi vsaj eno številko itd.

Razlogi zanje so očitni iz tabele 1.

Dobro geslo si je

- enostavno zapomniti in
- težko uganiti.

Ta dva kriterija si seveda pogosto nasprotujeta.

Napadalec utegne imeti na voljo tudi večjo računsko moč, kot je naš telefon ali računalnik, zato kaže še malo premisliti o možnostih (glej tabeli 2 in 3).

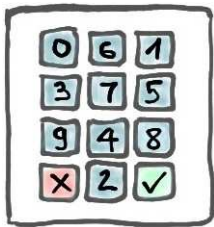
Ena od možnih obramb je, da po treh napačnih vnosih gesla sistem zamrzne za kratek čas.

primer	število	zahtevnost	dolžina gesla	čas za razbijanje
urpro	5	25 (majhne črke)	24 bitov	manj kot 2 sekundi
ke1a7Az	7	62 (črke in številke)	42 bitov	5 dni
GK,X1 b@V+	10	95 (znaki na tipkovnici)	66 bitov	233977 let

TABELA 1.
 Uganjevanje gesel, pri čemer smo upoštevali, da naš računalnik (npr. pametni telefon) preveri 10 milijonov gesel na sekundo.



SLIKA 2.
Vohunova dilema. Bilo je temno kot v rogu, ko se je vohun vračal v grad po opravljeni diverziji v sovražnem taboru. Blizu obzidja je iz teme zaslišal glas. Kako vohun prepriča »stražarja«, da pozna geslo, ne da bi ga izdal morebitnemu skritemu vsiljivcu?



SLIKA 3.
 Premešana številčnica.

Statistika gesel

Zgoraj omenjene zahteve sistemov pri izbiri gesel so bile precej pogoste, vendar bomo spoznali, da niso bistveno prispevale k varnosti (posebej, če si je uporabnik geslo res napisal na listič in ga pozabil ob računalniku).

Vseeno si oglejmo, kaj se dogaja, kadar ni nobenih omejitev (takšnih naj bi bilo skoraj 80% oblačnih storitev), glej npr. [5]. Pogosto se namreč zgodi, da je v javnost prišla kakšna večja baza gesel, ki nam omogoči vpogled v naše navade.

Pri LinkIn je imelo npr. preko 80 % uporabnikov dolžino gesel 6–10 znakov, od tega več kot 30 % dolžino 8. Statistika gesel pri Rockyou.com, kjer smo

lahko proučili 32M nezaščitenih gesel, je odkrila, da je bilo eno najbolj pogostih gesel 123456 (0,11 %). Sledila sta 12345 (0,04 %), 123456789 (0,04 %) in nato še 1234567 (0,02 %), 1234568 (0,02 %). Med prvimi desetimi so bili še password (0,03 %), i loveyou (0,03 %), princess (0,02 %), rockyou (0,02 %), abc123 (0,02 %). 40 % gesel je vsebovalo samo male črke, 15 % samo številke, 35 % samo male črke in številke, medtem ko jih je le 4 % vsebovalo tudi posebne znake. Znana je tudi uporaba variacij na temo enostavnih gesel, npr. razne kombinacije besede »geslo«, števila 123 in trojice »abc«. Pogosta so tudi imena mesecev in dni v tednu. Na koncu gesla znamo najti ločila – npr. pike, številke ali celo letnice.

Geslo za izstrelitev nuklearne rakete je bilo 20 let »00000000«. Facebook je za glavno geslo dostopa do vseh profilov uporabljal »Chuck Norris«.

Pri PIN-ih zaznamo podobne, a vseeno še hujše težave. Skoraj polovica od vseh v neki kompromitirani bazi je bilo štirimestnih (glej www.datagenetics.com/blog/september32012/). V tem primeru so bili najbolj popularni naslednji: 1234 (11 %), 1111 (6 %), 0000 (2 %), 1212 (1,2 %), 7777 (0,7 %), 1004, 2000 (vsak po 0,6 %), 4444, 2222, 6969, 9999 (vsak po 0,5 %), 3333, 5555, 6666, 1122 (vsak po 0,4 %), 1313, 8888, 4321, 2001, 1010 (vsak po 0,3 %). Torej pravkar omenjenih 20 PIN-ov pokrije več kot četrtnino vseh. Sledile so dolžine PIN-ov 6 (18 %), 8 (11 %), 5 (9 %), 7 (7 %), 9 (3 %), 10 (1,5 %) itd, vse s podobnimi težavami.

Da je stanje še slabše, skoraj 30 % uporabnikov uporablja ista gesla oz. PIN-e na številnih napravah ali računih. Slednje ni nič čudnega, saj 70 % uporabnikov vsaj 10 računov ščiti le z gesli. To število bo samo še rastle, zato prihaja do uporabe aplikacij



<i>posameznik, 1 računalnik</i>	$2^{27} - 2^{33}$ ključev/sek.
<i>akademsko omrežje, 256 računalnikov</i>	$2^{35} - 2^{41}$ ključev/sek.
<i>velika spletna skupina, 10M računalnikov</i>	$2^{50} - 2^{55}$ ključev/sek.
<i>zelo velika spletna skupina (npr. Bitcoin omrežje)</i>	$2^{58} - 2^{68}$ ključev/sek.
<i>vojaška obveščevalna organizacija</i>	$2^{50} - 2^{70}$ ključev/sek.

TABELA 2.
Napadi z grobo silo – koliko ključev lahko pregledamo v eni sekundi (za šifro AES-128).

dolžina ključa (v bitih)	posameznik	akademsko omrežje	velika spletna skupina	zelo velika spletna skupina	vojaška obveščevalna organizacija
40	minute	sekunde*	sekunde*	sekunde*	sekunde*
56	leta	dnevi	sekunde*	sekunde*	sekunde*
64	stoletja	leta	ure*	minute*	sekunde*
80	∞	stotisočletja	leta	ure*	ure*
128	∞	∞	∞	∞	∞

TABELA 3.
Napadi z grobo silo – koliko časa potrebujemo za različne dolžine ključev.
* zaradi organizacije in komunikacije med računiškimi sistemi oz. ljudmi bodo napadi običajno trajali dlje.

za upravljanje gesel. Vendar, če v ta namen uporabljate kar vaš priljubljeni brskalnik, morate imeti obvezno nastavljeno tudi **glavno geslo** (angl. master password). Če pa govorimo o podobnih geslih na različnih napravah, se delež poveča na 50 %. 66 % ljudi pa uporablja 1 ali 2 gesli za vse svoje račune. Oseba običajno zamenja geslo na vsake 2,5–3 leta.

Kako si zapomnimo varnejša gesla?

Geslom, ki vsebujejo več kot eno pomenljivo besedo, pravimo **skrivna fraza** (angl. passphrase). Ni treba, da ta fraza nekaj pomeni (slika 4).

Predstavljanje in overjanje

Če poenostavimo, je **identifikacija** dokaz uporabnikove identitete, **overjanje** pa je postopek (za nas bo pogosto kriptografski protokol), pri katerem uporab-

nik želi potrditi, da je res tisti, za kogar se predstavlja.

Za potrjevanje uporabnikove identitete se uporablja podmnožico naslednjih treh lastnosti:

- nekaj, kar uporabnik **ve** – npr. gesla, številke (PIN),
- nekaj, kar uporabnik **je** – to so biometrični podatki, ki temeljijo na fizičnih lastnostih uporabnika, kot so prstni odtis, šarenica, obraz, ali način hoje, glej sliko 7,
- nekaj, kar uporabnik **ima** – t. i. varnostni žetoni, kot so fizični ključi, osebna izkaznica, vozniško dovoljenje, bančna kartica, mobilni telefon itd.

V primeru plačila z bančno kartico ali telefonom se npr. običajno uporabljata dve lastnosti: bančna kartica ali telefon (nekaj, kar uporabnik ima) ter PIN številka (nekaj kar, uporabnik ve). V zadnjem času pa se pri plačevanju s telefonom vse bolj pogosto uporablja biometrika.



SLIKA 4.

Več kot 20 let so se sistemski administratorji trudili, da bi natrenirali uporabnike k uporabi gesel, ki si jih težko zapomnijo, računalniki pa so jih kljub temu hitro uganili (idejo iz XKCD [3] sta v slovenščino prenesli Neja Cirar in Ajda Markič).

Anita in Bojan delita tajni (skriven) ključ K , ki ga uporabljata za šifriranje.

1. Bojan izbere 64-bitni izziv X in ga pošlje Aniti.
2. Anita izračuna $Y = K \oplus X$ in ga pošlje Bojanu.
3. Bojan izračuna $Y' = K \oplus X$ in preveri, če je $Y = Y'$.

Primer. (4 biti)

$K = 10$, $X = 6$,

$Y = K \oplus X = 10 \oplus 6$

$= 1010_2 \oplus 0110_2$

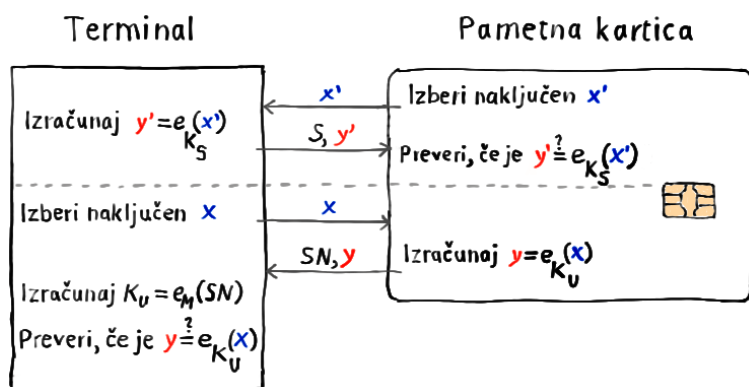
$= 1100_2 = 12$.

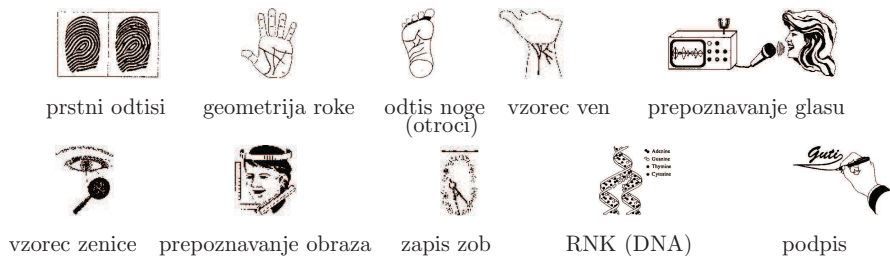
SLIKA 5.

Identifikacijski protokol z izzivom in odgovorom. Operacijo $\oplus$ (ekskluzivni ali nad istoležnimi biti) bi lahko zamenjali s kakšno drugo funkcijo, tj. $y' = e_K(x)$ ter $y' = e_K(x)$ in še vedno preverjali $y = y'$. Skoraj vse sheme uporabljajo protokole z izzivom in odgovorom, vendar pa najbolj koristne ne uporabljajo skupnih ključev. Ker presegajo ta sestavek in jih pustimo za kdaj drugič.

SLIKA 6.

Primer konkretne uporabe protokola izziv in odgovor. Kako zdravstvena kartica nekega uporabnika in terminal zdravstvenega sistema preverita pristnost drug drugega? Najprej morata imeti tako terminal kot kartica možnost generiranja naključnih števil. Kako pa je s ključi? Terminali imajo glavni ključ M , in skupinski ključ K_S , nimajo pa prostora, da bi hranili ključe vseh uporabnikov. Zato je vsakemu uporabniku U s serijsko številko SN dodeljen ključ $K_U := e_M(SN)$ (K_U določimo s pomočjo glavnega ključa M in uporabnikove serijske številke SN), ter vsi skupinski ključi, ki so potrebni za prepoznavanje različnih skupin (poleg skupine terminalov so tu še zdravniške kartice, pa kartice različnih lekarn itd).





SLIKA 7.

Biometrični testi. Poudariti je treba, da ni idealnega testa. Prstne odtise npr. puščamo na raznih predmetih, ki se jih dotaknemo. Če smo dolgo v vodi ali na mrazu, se prstni odtis malce spremeni. Še večji problem nastane, če si prst poškodujemo. Si predstavljate, da bi morali na bankomatu oddati ugriz? Se kdo spomni dejanskega preverjanja podpisa, le-to bi moral itak opraviti izurjen grafolog.

Upravljanje ključev

Postavimo si nekaj osnovnih vprašanj:

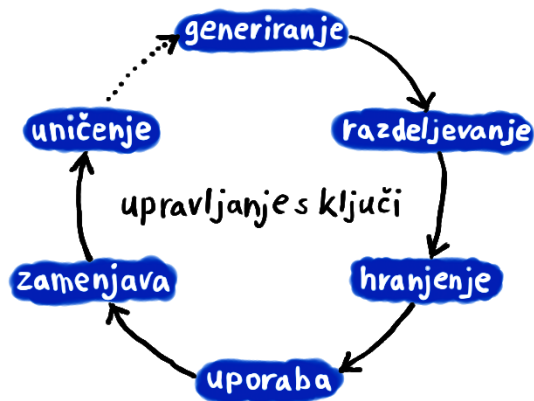
- Od kod dobimo ključ?
- Zakaj zaupamo ključem?
- Kako vemo, čigav ključ imamo?
- Kako omejiti uporabo ključev?
- Kaj se zgodi, če je izgubljen/ukraden zasebni ali tajni ključ? Kdo je odgovoren?
- Kako preklicati ključ?
- Kako omogočimo servis preprečitve zanikanja (ko nekdo ne prizna določenega dejanja)?

Za bolj izkušene naj omenimo, da ta vprašanja veljajo tako za simetrične (tajne) ključke kot tudi za javne in zasebne ključke, glej Presekov članek [1].

Osnovni cilj je vzdrževanje **zasebnosti** in **celovitosti** ključev. Prvo pomeni, da ostanejo ključki tajni, drugo pa, da jih nihče ne more zamenjati ali pokvariti. Ti dve lastnosti morata biti zagotovljeni skozi ves življenjski cikel ključa, se pravi od začetka generiranja ključa, pa vse do takrat, ko ključ ni več v uporabi in je bil uničen, glej sliko 8.

Tako rekoč vedno je ključ zamenjan z novim ključem, kar pomeni, da gre za ciklični proces, v katerem uničenju sledi namestitev/vključitev novega ključa. Vendar pa je novi ključ zgeneriran, dodeljen in shranjen, še preden je stari ključ uničen. V nekaterih sistemih imamo še dodatno zahtevo, da ključke arhiviramo.

Vzvodi za nadzor so potrebni skozi celoten življenjski cikel ključa. To vsebuje od neke vrste revizijskih postopkov (angl. audit trail) do dnevnikov



SLIKA 8.

Glavne stopnje življenjskega kroga prikazuje naslednji diagram.

uporabe ključev, ki seveda niso smiselni brez nadzora ter pooblastil za ustrezen odgovor/ukrep v primeru, da je bil ključ ukraden/izgubljen. Zato je pogosto (posebno v večjih sistemih) zaželeno, da imajo ključki ustrezne lastnike, ki so odgovorni za njihovo hranjenje/zaščito.

Pri algoritmičnih za kriptosisteme lahko uporabimo poljubno zaporedje bitov (občasno tudi drugih znakov), kar pomeni, da lahko večina uporabnikov sama generira svoje ključke. Biti morajo nepredvidljivi: pogosto uporabimo

- ročne metode (npr. metanje kovanca/kocke, ali bolj realistično, premik miške),
- izpeljavo iz osebnih podatkov (npr. PIN) ali
- (psevdo) generatorje naključnih števil (RNG).

Generiranje velikih praštevil zahteva »napredno«

1. Ne izbiraj pogostih (generičnih) gesel ali ključev posebne oblike.
2. Ne hrani gesel ali ključev na manj varnih (preveč očitnih/izpostavljenih) mestih.
3. Ne uporablaj istih ali podobnih gesel in ključev
v različnih programih oz. računih (ne recikliraj gesel in ključev).
4. Ne kopiraj gesel in ključev (kopiraj/prilepi prek odložišča – angl. clipboard).
5. Ne pošiljaj ali deli z nikomer gesel in ključev.



TABELA 4.

Popravi 5 slabih navad, ki vplivajo na varnost gesel oz. bolj splošno ključev.

1. Gesla in ključi naj bodo dovolj dolgi.
2. Pogosto posodablaj/obnavljaj/zamenjaj svoja gesla in ključe
(in stori to takoj, če/ko izveš, da je bil tvoj račun ukraden/izgubljen).
3. Skrivne fraze so dobra strategija za pomnjenje gesel (vsaj tistih glavnih).
4. Uporablaj večstopenjsko (faktorsko/dejavniško) overjanje identitete
(avtentikacijo) za pomembne/kritične račune (če je le možno).
5. Uporablaj dober program za upravljanje ključev in gesel.

TABELA 5.

Pet dobrih navad za varnost gesel oz. bolj splošno ključev.

matematično obdelavo in lahko zahteva precejšno moč/prostor/čas. Uporabniki so včasih prisiljeni zapati zunaj generiranim ključem oziroma programski opremi. Za ilustracijo: v primeru kriptosistema RSA je njegova varnost povezana z napadalčevo zmožnostjo razcepa velikega števila. Če bi proces generiranja ključev dal le omejeno število praštevil, bi napadalec lahko generiral ista praštevila in nato za vsakega izmed njih preveril, ali delijo dano število.

Razdeljevanje ključev in varno **hranjenje** sta osrednjega pomena. Problemi, na katere naletimo in njihove rešitve, so večinoma podobni, zato jih obravnavamo skupaj. Razlogi za uporabo močnih kriptografskih algoritmov je preprečiti napadalcu, da izračuna ključ. Seveda vse to nima smisla, če jih napadalec lahko najde nezaščitene nekje na sistemu.

Kako veliko je VELIKO?

Živimo le 2–3 milijarde sekund. Za kilo K (10^3), mega M (10^6), giga G (10^9) in tera T (10^{12}), ki smo se jih že kar navadili, sledijo enote peta P (10^{15}), exa E (10^{18}), zeta Z (10^{21}), jota Y (10^{24}), ronna R (10^{27}) in quetta Q (10^{30}). Slednja je v rangi števila 2^{100} (zakaj?), kar je velikost prostora, iz katerega radi v kriptografiji naključno izberemo varen ključ ali kak drug skrit parameter. Varnostni strokovnjaki so dolžni slediti priporočilom za izbiro velikosti ključev za posamezno skupino kriptosistemov, ki se s časom seveda nenehno spreminjajo, glej npr. Wikipedijo [6].





Naloge

1. Koliko je različnih znakov na tvoji tipkovnici (ne pozabi na male in velike črke)? Bi znal vse naštetih?
2. Koliko zrn riža je povprečno v enem kilogramu riža (gotovo ga imate kaj doma)? (*Namiga*: Zakaj je v vprašanju beseda povprečno? Ali to pomeni, da boš moral šteti večkrat?)
3. Koliko bi bilo možnih gesel, če bi izbirali za geslo besedo v slovenskem jeziku? Kaj pa, če bi si izbral dve ali tri besede? In kaj, če se ne bi omejili s slovenščino? Koliko je različnih jezikov?
4. Kakšna je verjetnost, da uganemo štirimestni PIN neke bančne kartice, če bi imeli možnost poskusiti 20-krat (upoštevaj, da je bil PIN izbran naključno)? Kaj pa, če bi imeli opravka s 6-ali 8- mestnim PIN-om. Ali bi bilo smiselno dati možnost večjega vnosa napačnih PIN-ov pri daljših PIN-ih?
5. Pri štirimestnih PIN-ih so izredno popularne letnice (rojstev), s katerima števčkama bi torej začel ugibanje? (Tudi sicer se največ PIN-ov začne z 1, sledijo pa tisti z 0 in 2, glej sliko na naslovnici.)
6. Ali imaš načrt B za primer, ko pozabiš geslo/ključ? Lahko predlagaš kakšnega?
7. Koliko različnih računov in gesel uporabljaš (oz. ocenjuješ, da jih boš v naslednjih 10 letih)? Zelo verjetno je, da napadalec pozna nekaj tvojih gesel. Če obstaja skupno jedro teh gesel, oceni število potrebnih ugibanj za odkritje drugih gesel.
8. Naštej nekaj dobrih in slabih lastnosti obnavljanja gesel preko e-pošte.
9. Predlagaj še kakšno rešitev za vohunovo dilemo (glej sliko 2).
10. Kako točno poteka preverjanje gesla? Ali se lahko izognemo, da bi gesla nekje hranili (kajti kot smo omenili, zna takšna baza uiti izpod nadzora, pa če se še tako trudimo)? Nekatera podjetja imajo sezname gesel za svoje zaposlene. Kje naj jih hranijo?
11. Predlagaj še kakšno funkcijo $e_K(x)$ (glej sliko 5) in premisli, kaj so njene dobre in slabe lastnosti.

12. Poišči kakšen odgovor na osnovna vprašanja glede upravljanja ključev, ki smo jih zastavili na začetku razdelka Upravljanje ključev.
13. Naštej nekaj dobrih in slabih lastnosti posameznih biometričnih testov (glej sliko 7).
14. Naštej nekaj prednosti in pomanjkljivosti zgornjih slabih in dobrih navad za izbiro gesel/ključev (tabeli 4 in 5). Bi znal dopolnit oba seznama še s tremi priporočili?
15. Na koga bi se obrnil, če bi moral implementirati varno preverjanje gesel v svoji aplikaciji? Kako bi se lahko izognil implementaciji gesel?
16. V razdelku Kako si zapomnimo varnejša gesla? smo omenili, da si za skrivno frazo izberemo npr. 4 naključne besede. Predlagaj kakšen enostaven postopek, kako priti do teh besed z uporabo igralne kocke.
17. Oceni dolžino povprečno dolžino skrivnih fraz, ki si jih uporabljal ti ali tvoji prijatelj doslej. Kako velika je množica, iz katere izbiraš besede za tvorjenje fraz?

Doslej se nam je uspelo izogniti zgoščevalnim funkcijam, kar pomeni, da se bomo morali pomeniti o geslih še enkrat.

Literatura

- [1] A. Jurišić, *Poštni nabiralnik in kriptografski protokoli*, 3. del, *Presek* 36 (2008–2009), 22–26.
- [2] A. Jurišić in J. Veselinović, *Zaupati ali ne zaupati: digitalni podpis v kriptografiji*, 4. del. *Presek* 38 (2010–2011), 25–29.
- [3] R. Munroe, *Spletni strip XKCD*, <https://xkcd.com/936/>
- [4] Y. S. Ryu, D. H. Koh, B. L. Aday, X. A. Gutierrez, J. D. Platt, *J. of usability studies* 5/2, February 2010, 65–75, dostopno na <https://uxpajournal.org/usability-evaluation-of-randomized-keypad/>, ogled 1. 4. 2023.
- [5] J. H. Simmons, *Passwords - 25 Fun Facts and Statistics!*, dostopno na <https://www.vpncrew.com/passwords-facts-and-statistics/>, ogled 1. 4. 2023.
- [6] *Security level*, dostopno na https://en.wikipedia.org/wiki/Security_level, ogled 1. 4. 2023.

× × ×

Izbrane slike in fotografije v petdesetih letih Preseka – nadaljevanje

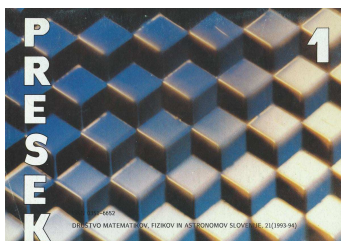
↓↓↓

NADA RAZPET, MARKO RAZPET IN ANDREJ LIKAR

→ Nadaljujemo z izborom slik in fotografij, tokrat do 31. letnika. Z njim se zaključuje obdobje izhajanja Preseka v malem formatu 14 cm × 20 cm.

Naj še enkrat spomnimo, da se nekateri Presekovi članki dobijo na spletnem naslovu www.dlib.si/ v rubriki *Periodika*. Veliko starejših prispevkov pa hitro najdemo na spletnem naslovu www.presek.si/ v *Arhivu revij*.

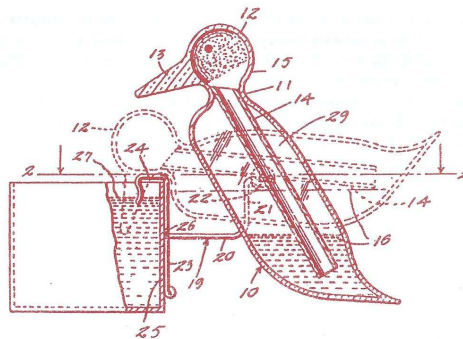
V prvi številki 21. letnika je Andrej Likar objavil članek, ki s fizikalnega stališča obravnava odsev. Vsi poznamo odsevnike, ki služijo za večjo varnost v cestnem prometu. Spomnimo se samo na kresničke, ki dobro odbijajo svetlobo avtomobilskih žarometov, ki pade nanje. Povečan del kresničke vidimo na sliki 1.



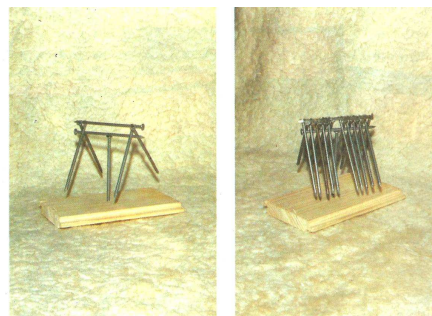
SLIKA 1.

V tretji številki naslednjega letnika je Janez Strnad natančno opisal, kako deluje priljubljena fizikalna igračka, pravzaprav toplotni strojček, ki mu popularno rečemo *žejna račka* (slika 2).

Za isto številko Preseka je Dušan Repovš prispeval spretnostno nalogo s sedmimi ravnimi, enakimi žebli. En žebelj je treba zabiti v desko, nato pa preostalih šest brez uporabe lepila, vrvce ali drugih pripomočkov postaviti na glavico zabitega žeblja tako, da se ne dotikajo deske, se medsebojno podpirajo in na njem počivajo. Rešitev naloge je bila objavljena na zadnji strani ovitka naslednje številke Preseka (slika 3).



SLIKA 2.



Sedem žeblijev ...

...lahko pa tudi več!

SLIKA 3.

Na zadnji strani ovitka pete številke istega letnika je Andrej Likar objavil opis in fotografijo (slika 4) zanimivega dogajanja v okroglem otroškem bazenu, ki je ob plimi povezan z morjem.

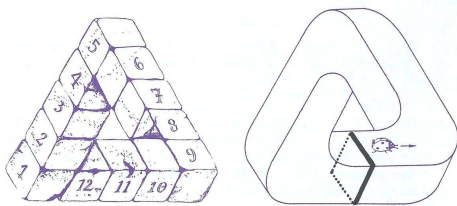
V prvi številki 23. letnika je Vilko Domajnko predstavil več slik objektov, ki jih v trirazsežnem prostoru ne moremo realizirati. Preprost primer je prikazan na sliki 5.

V isti številki je Matija Lokar pokazal, kako s štirimislinimi preslikavami ravnine pridemo do množice točk, ki spominjajo na praproto (slika 6). Vsak njen list je kopija celotne praproti. To lastnost uporabljajo v računalništvu za stiskanje podatkov. Na





SLIKA 4.



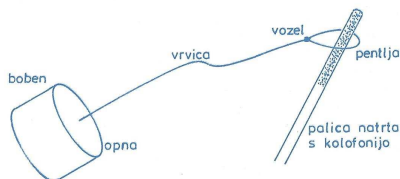
SLIKA 5.

ovitku naslednje številke Preseka je objavljenih še nekaj slik tako dobljenih praproti.



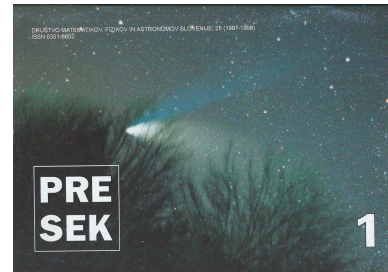
SLIKA 6.

V tretji številki prav tako 23. letnika je Andrej Likar opisal, kako lahko sami izdelamo igračo (slika 7), ki se bo ob pravilni uporabi oglašala tako kot škržat ob morju v poletnem času. Pa ne samo to, avtor je tudi fizikalno razložil njeno delovanje.



SLIKA 7.

Zanimiva je prva številka 25. letnika Preseka. Na prvih dveh straneh ovitka so objavljene fotografije kometa Hale-Bopp, ki sta jih posnela Gregor Bavdek in Janko Merše aprila 1997. Ena od teh je na sliki 8. V isti številki je Marijan Prosén opisal opazovanje sence gnomona. Vrh sence navpične palice se čez dan pomika po hiperboli, ki se ob enakonočju izrodi v premico (slika 9).



SLIKA 8.



SLIKA 9.

V zadnji številki istega letnika je Gregor Bavdek obravnaval nevihto, zlasti razelektritve v ozračju. Te pogosto spremljajo veličastne strele, ki so nevarne za ljudi in njihovo premoženje. Avtor je posnel več slik strel, ki so objavljene na ovitku. Ena od teh je na sliki 10.



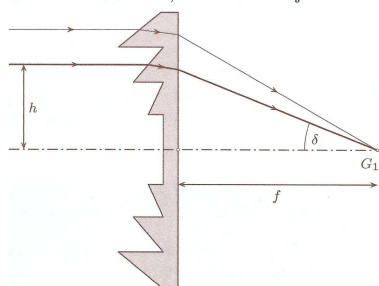
SLIKA 10.

Andrej Likar je v drugi številki 26. letnika objavil članek *Skrivljena zrcala*. Velika steklena okna modernih zgradb namreč delujejo kot zrcala, v katerih se vidijo objekti bolj ali manj popačeno, ker šipe niso idealno ravne. Avtor je besedilo opremil z nekaj fotografijami. Tista na zadnji strani ovitka je na sliki 11.



SLIKA 11.

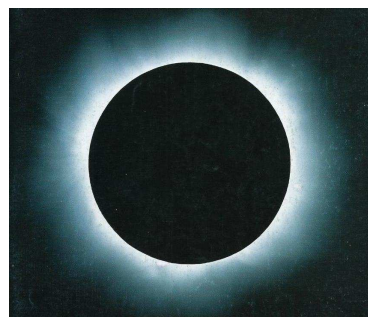
V prvi številki 27. letnika je Peter Legiša opisal Fresnelovo lečo in njeno uporabo. Take leče v manjši izvedbi so pripravne za branje drobnega tiska. Osni presek Fresnelove leče kaže slika 12.



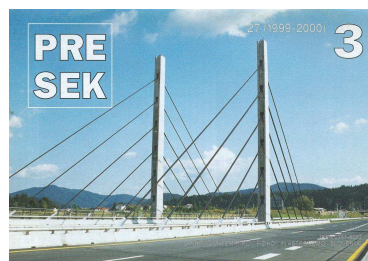
SLIKA 12.

Dne 11. avgusta 1999 je bil v naši sosesčini viden popolni Sončev mrk. Veliko ljudi se je odpravilo na opazovanje tega redkega nebesnega pojava na avstrijsko Gradiščansko ali Madžarsko ali pa vsaj v Prekmurje. Nastale so lepe fotografije. Eno od njih (slika 13) je posnel Gregor Bavdek in je bila objavljena na naslovni strani druge številke Preseka istega letnika.

Za tretjo številko 27. letnika je Andrej Likar prispeval krajši članek o brveh in mostovih. V njem obravnava sile in navore na tovrstnih objektih. Zanimiv je most čez Ljubljano na vzhodni ljubljanski obvoznici (slika 14). Fotografiral ga je avtor in je objavljen na naslovnici te številke.



SLIKA 13.



SLIKA 14.

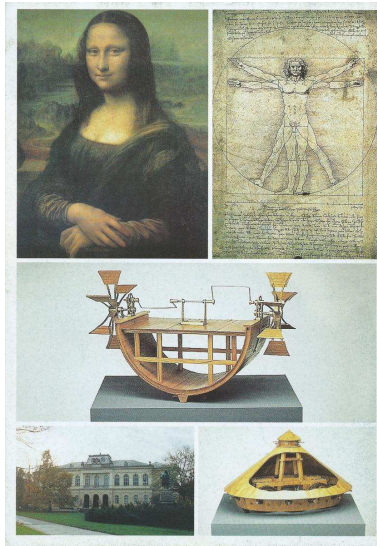
Isti avtor je na naslovni strani naslednje številke Preseka objavil fotografijo Tartinijevega trga v Piranu (slika 15). Del tega trga ima obliko elipse. Bralci pa so morali ugotoviti, ali je središče Tartinijevega spomenika v gorišču te elipse. Enako vprašanje zastavljamo bralcem pričujoče številke.



SLIKA 15.

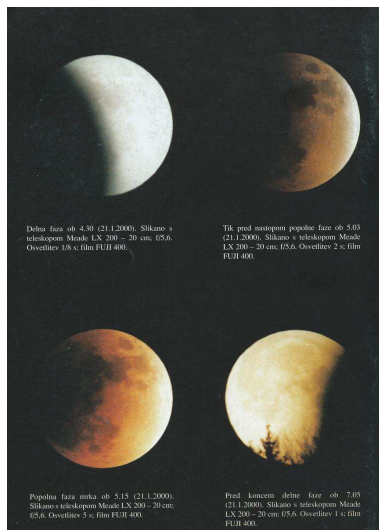
Janez Strnad je v isti številki objavil dva članka o Leonardu da Vinciju. Da Vinci je zapustil, razen svojih umetniških del, tudi mnogo skic vsakovrstnih naprav. Nekatere imajo v svojih sestavih zrcala, škripce, vzvode, vitle, kroglične ležaje, zobnike in polže (slika 16).





SLIKA 16.

V peti številki je Mitja Rosina spraševal, kako bi izračunali svetlost Lune ob popolnem Luninem mrku 21. januarja 2000. Nekaj faz mrka je posnel Lojze Vrankar (slika 17).



SLIKA 17.

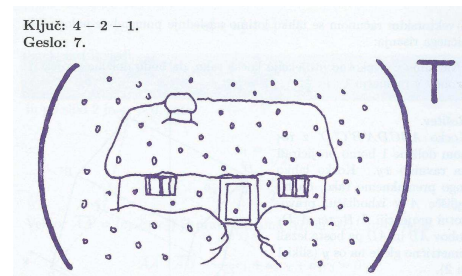
Leto 2000 je bilo razglašeno za svetovno leto matematike. Ob tej priložnosti je bilo organizirano tekmovalstvo v izdelavi matematičnih plakatov. Dragica in Gregorij Kurillo iz Kranja sta si prislužila nagrado

za plakat, ki ilustrira toge premike z idrijsko čipko (slika 18). Nekoliko večjega si lahko ogledate na zadnji strani ovitka tretje številke 28. letnika.



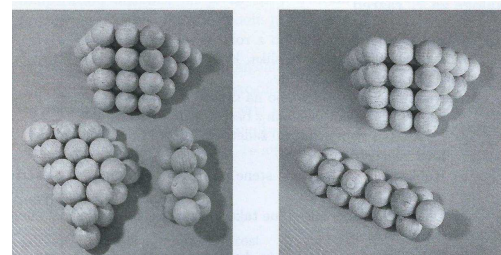
SLIKA 18.

Marko Bokalič si je izmislil povratni rebus (slika 19), ki je povezan z matematiko. Z rešitvijo vred je objavljen v tretji številki 29. letnika.



SLIKA 19.

V četrti številki istega letnika je Nada Razpet pokazala, kako lahko pravilni četrček razrežemo na manjša telesa in kako iz teh nazaj sestavimo pravilni četrček. Lahko pa postopek izvedemo tudi z enakimi kroglicami, ki jih primerno zlepimo (slika 20).



SLIKA 20.

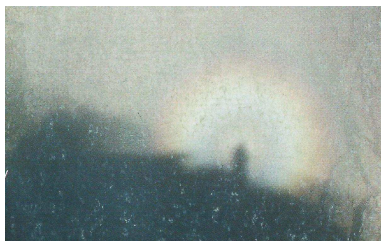
Pobočje Nanosa, ki ga vidimo pri vožnji po primorski avtocesti v smeri Kopra, ima zanimivo obliko (slika 21). V 4. številki 30. letnika je Andrej Likar, ki je tudi avtor fotografije na naslovni strani, pokazal, kako z računom pridemo do krivulje, ki se zelo dobro ujema z dejanskim obrisom pobočja Nanosa.



SLIKA 21.

Na naslovnici naslednje številke je fotografija glorijske (slika 22), ki jo je posnel Matjaž Vencelj z Miza-ste gore pri Cape Townu. Avtor v posebnem članku podrobno razloži, kako nastane naravni pojav, ki mu pravimo glorijska, in zakaj ima tako ime.

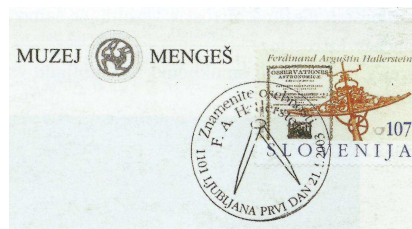
Na zadnji strani ovitka je predstavljena poštna znamka o Hallersteinu (slika 23). Na kratko je opisano tudi njegovo življenje in delo.



SLIKA 22.

Prva številka 31. letnika ima na naslovnici fotografijo (slika 24), ki kaže, kako se začne kaditi, če dovolj vztrajno z vrtenjem drgnemo leseno palico na dovolj suhem lesu. Posnel jo je Andrej Likar, ki je napisal tudi članek, ki s fizikalnimi argumenti pojasni, zakaj lahko na tak način zakurimo ogenj.

Četrta številka istega letnika je v celoti posvečena 250. obletnici rojstva barona Jurija Vege. Ob tej priložnosti je Banka Slovenije izdala priložnostne ko-



SLIKA 23.



SLIKA 24.



SLIKA 25.

vance, katerih fotografija je objavljena na zadnji strani ovitka (slika 25).

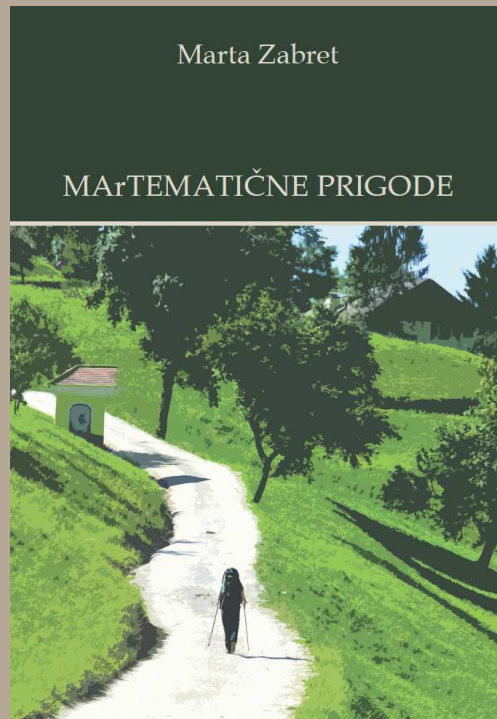
(Se nadaljuje.)

× × ×

MaRtematične prigode

Izšel je že tretji natis knjige MARTEMATIČNE PRIGODE

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



12,50 EUR

Poleg omenjene ponujamo tudi druga matematična, fizikalna in astronomska dela. Podrobnejše predstavitve so na spodnjem naslovu, kjer lahko vse publikacije tudi naročite:

<http://www.dmfa-zaloznistvo.si/>

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