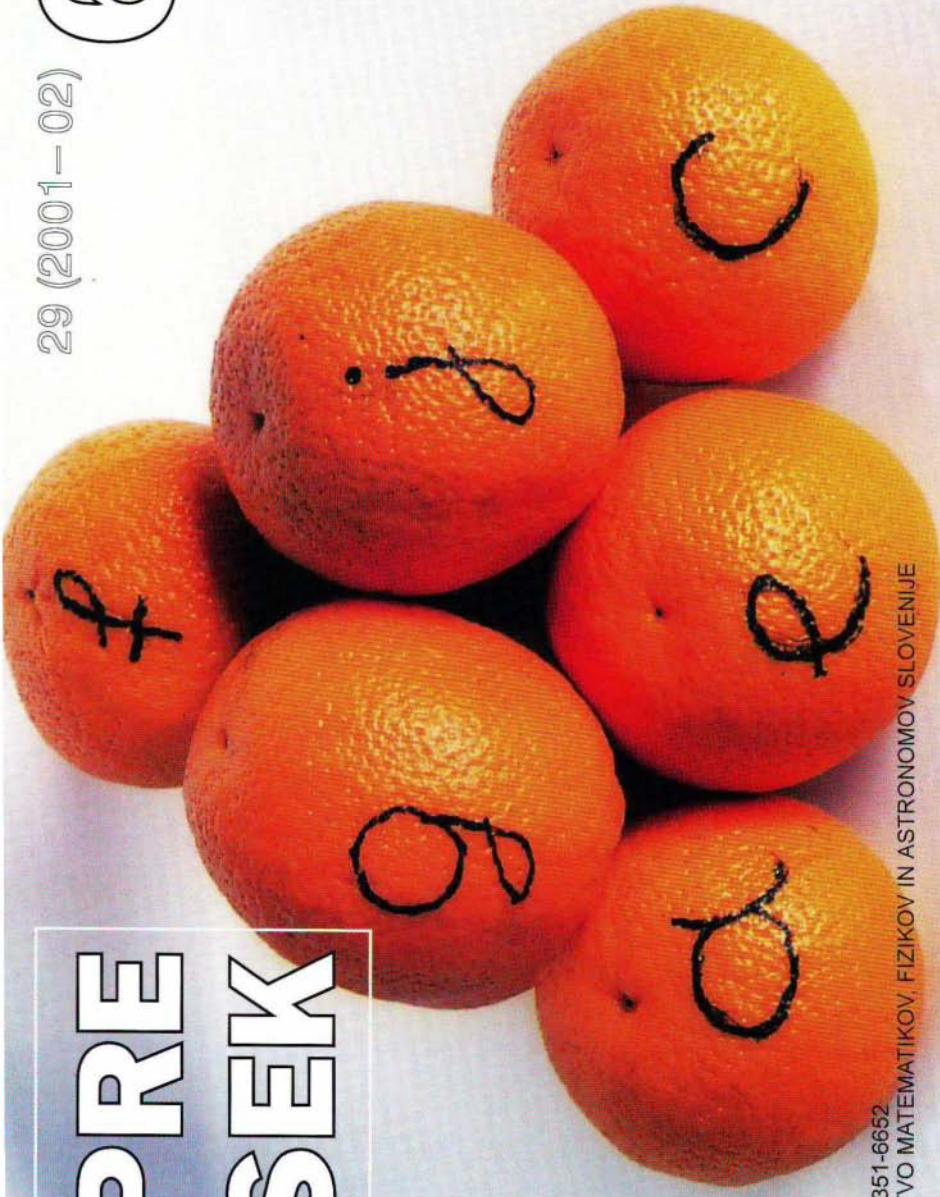


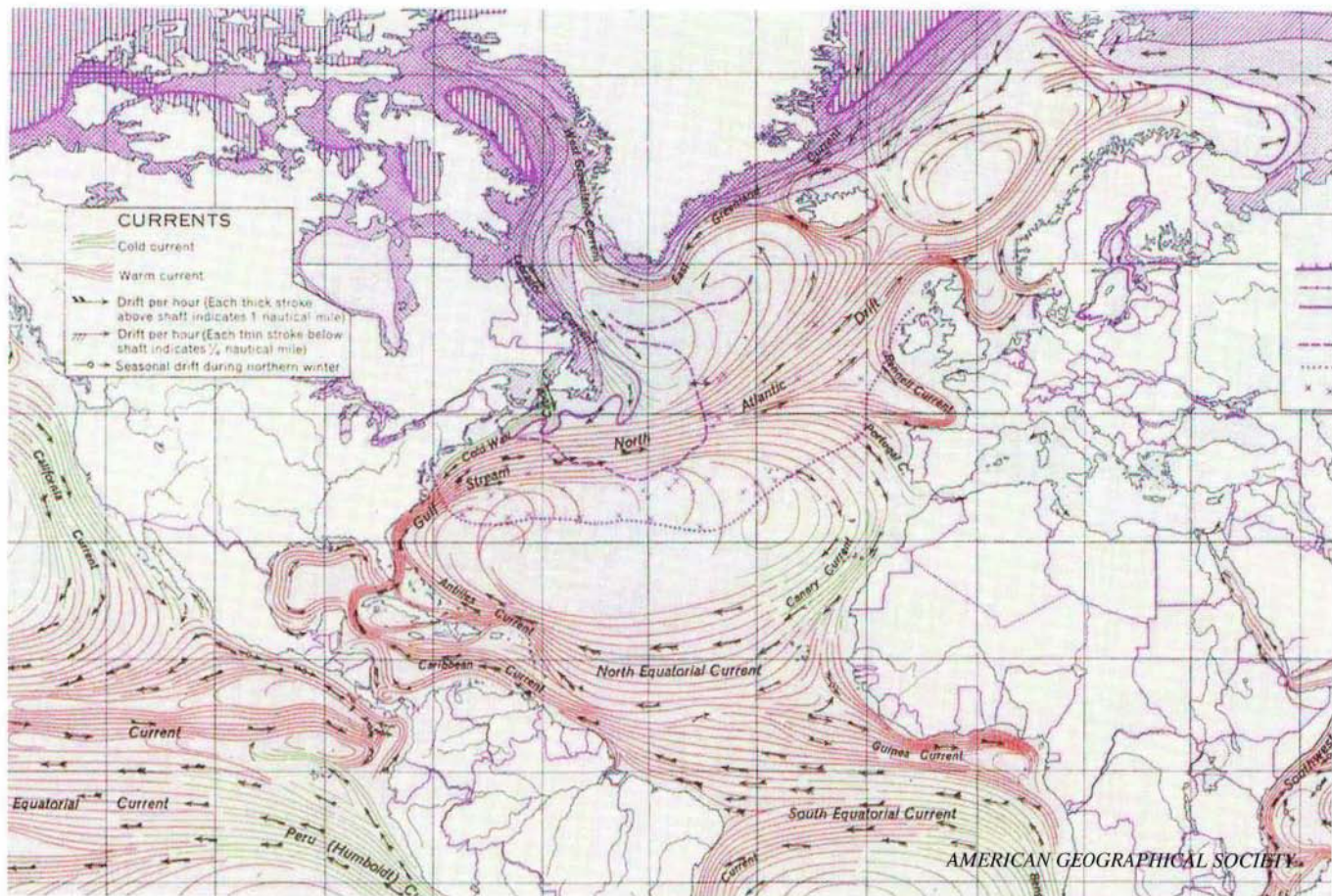
6

29 (2001-02)

PRE SEK



ISSN 0351-6652
DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE



Gulf Stream - Zalivski tok, North Atlantic Drift - Severno-atlantski tok, North Equatorial Current - Severni ekvatorialni tok, Caribbean Current - Karibski tok, Antilles Current - Antilski tok.

PRESEK

list za mlade matematike, fizike, astronome in računalnikarje
29. letnik, leto 2001/02, številka 6, strani 321–384

VSEBINA

MATEMATIKA	Kristalne mreže, 2. del – Zlaganje krogel (Peter Legiša).... 328-332 Evariste Galois (1811–1832) (Marija Vencelj) 346-349
FIZIKA	Atomi so sestavljeni (Janez Strnad) 340-345 Zalivski tok slabi (Ivan Meško)..... 354-356
ASTRONOMIJA	Zakritje (Marijan Prosen)..... 334-337 Zvezde, ki se dotaknejo obzorja – reš. na str. 366 (Marijan Prosen)..... 350-351 Odprtina (Marijan Prosen)..... 374-375
RAČUNALNIŠTVO	Rešitev pozabljenе naloge – s str. 290 (Marko Petkovšek) .. 338-339 Kako deliti skrivnosti? (Aleksandar Jurišić) 358-364
NOVE KNJIGE	J. Cofman: Kaj naj rešujemo? (Martin Juvan) 332-333 J. Strnad: Sto let fizike (Anton Ramšak) III M. in S. Prosen: Spoznavajmo Zemljo in vesolje (Marija Vencelj)..... IV
ZANIMIVOSTI, RAZVEDRILO	Križanka "Ob 200-letnici rojstva velikega matematika" – reš. na str. 379 (Marko Bokalič) 352-353 Bine in mleko (Jože Pahor) 367-372
NALOGE	Štiri muhe – Nagradna naloga (Marija Vencelj) 322 Nogometna kombinatorika – reš. na str. 365 (Boštjan Kuzman, Martin Juvan)..... 327 Povezana kriptaritma – reš. na str. 364 (Marija Vencelj)..... 349 Rojstne letnice petih matematikov – reš. na str. 364 (Marija Vencelj) 349 Ulamova spirala – reš. na str. 372 (Martin Juvan)..... 357
REŠITVE NALOG	Rešitve nagradnih nalog iz 3., 4. in 5. številke Preseka (Marija Vencelj)..... 322-323 Tri enice in enajst fizolčkov – Rešitev nagradne naloge s str. P-4/II (Peter Petek)..... 323 Produkt = vsota – Rešitev nagradne naloge s str. 258 (Martin Juvan)..... 323-324 Produkt = vsota – 2. rešitev (Matija Pretnar)..... 324-326 O vrtnarjevi nalogi (Martin Juvan)..... 326
TEKMOVANJA	22. mednarodno matematično tekmovanje mest – Naloge jesenskega kroga (Gregor Cigler) 376-379
LETNO KAZALO	 380-384
NA OVITKU	Pomaranče, zložene v kubično najgostejši sklad (foto Peter Legiša). Preberite tudi članek Kristalne mreže, 2. del, na str. 328 I Morski tokovi v severnem Atlantiku. Preberite tudi članek na str. 354..... II

ŠTIRI MUHE – Nagradna naloga

Z vrha 3 m visokega droga, ki stoji na kmečkem dvorišču, odlete točno opoldne v zrak štiri muhe. Vsaka leti premočrtno in s konstantno hitrostjo: prva 36 m/min, druga 49 m/min, tretja 64 m/min in četrta 81 m/min. Ob 12⁰⁵ se izkaže, da so vse štiri muhe v isti ravnini. Ali so še ob kakšnem času vse štiri v isti ravnini, če nobena od njih med letom ne naleti na oviro? Če so, navedite vse možnosti!

**Rešitve pošljite najkasneje do 15. julija na naš naslov:
Presek, Jadranska c. 19, 1001 Ljubljana, p.p. 2964.**

Izmed reševalcev, ki nam bodo poslali pravilno rešitev naloge, bomo izžrebali nagrajenca, ki bo prejel knjižno nagrado.

Marija Vencelj

REŠITVE NAGRADNIH NALOG IZ 3., 4. IN 5. ŠTEVILKE PRESEKA

Na **Vrtnarjevo nalogo**, ki jo je v tretji številki Preseka zastavil Bojan Mohar, nismo od bralcev, kljub podaljšanemu roku za reševanje, prejeli nobenega odgovora. Pač pa je član našega uredništva, urednik za računalništvo Martin Juvan, na eno od vprašanj prispeval zanimiv odgovor, ki si ga lahko preberete v nadaljevanju pod naslovom **O vrtnarjevi nalogi**.

Na nalogo **Tri enice in enajst fižolčkov** iz četrte številke smo prejeli kar nekaj rešitev. Očitno so se z njo spopadli tudi osnovnošolci. Žal vsi odgovori niso izpolnjevali pogojev naloge. Pravilne rešitve so nam poslali: Marta Cvijič z Nomenja pri Bohinjski Bistrici, Felicita Hromc iz Kotelj, Barbara Valentinčič iz Krškega, Jošt Novak z Bleda in Alenka Terziev iz Sebenj pri Križah.

Žreb je knjižno nagrado namenil Barbari Valentinčič. Čestitamo! Knjigo smo ji že poslali po pošti.

Srednješolci, kje ste? Naloga **Produkt = vsota**, zastavljena v peti številki Preseka, je bila takorekoč pisana vam na kožo, čeprav zadošča za njeno reševanje že osnovnošolska matematika. Pa od vas nanjo nismo dobili nobenega odgovora! Je temu kriva bitka za ocene pred koncem šolskega leta?

Pravilno rešitev naloge pa nam je poslal študent 1. letnika Matija Pretnar iz Črnuč. Vprašanje je celo razširil s $k = 5$ na poljubno končno mnogo faktorjev v produktu oziroma členov v vsoti in poiskal sicer nekoliko dolg *postopek*, s katerim lahko najdemo vse rešitve enačbe

$$a_1 \cdot \dots \cdot a_k = a_1 + \dots + a_k, \quad k \in \mathbb{N},$$

v naravnih številih. Postopek je ilustriral za $k = 5$ in s tem našel tudi rešitev zastavljene naloge. Seveda tudi njemu pripada knjižna nagrada.

Ker se metoda Matije Pretnarja pri reševanju naloge razlikuje od poti do rešitve, kot jo je pripravil avtor naloge, objavljamo oba načina.

Marija Vencelj, odg. ur.

TRI ENICE IN ENAJST FIŽOLČKOV – Rešitev nagradne naloge iz 4. številke, str. II

Razkriti račun množenja je takle:

$$\begin{array}{rcccc} & 2 & 3 & \times & 7 & 9 \\ 1 & 6 & 1 & & & \\ & 2 & 0 & 7 & & \\ \hline 1 & 8 & 1 & 7 & & \end{array}$$

Peter Petek

PRODUKT = VSOTA – Rešitev nagradne naloge iz 5. številke, str. 258

V množici naravnih števil bomo poiskali vse rešitve enačbe

$$a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5 = a_1 + a_2 + a_3 + a_4 + a_5,$$

za katere velja $a_1 \geq a_2 \geq a_3 \geq a_4 \geq a_5 \geq 1$.

Poglejmo najprej, kaj se zgodi, če je $a_5 \geq 2$. Zaradi predpostavke o urejenosti a -jev je tedaj produkt na levi strani enačbe večji ali enak $16a_1$, vsota na desni pa ni večja od $5a_1$. Ker je $16a_1 > 5a_1$, mora biti $a_5 = 1$. Podobno vidimo, da je tudi $a_4 = 1$. Pri $a_4 \geq 2$ je namreč

$$a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot 1 \geq 8a_1 > 4a_1 + 1 \geq a_1 + a_2 + a_3 + a_4 + 1.$$

Naj bo sedaj $a_3 \geq 2$. Potem imamo

$$a_1 \cdot a_2 \cdot a_3 \cdot 1 \cdot 1 \geq 4a_1 \geq 3a_1 + 2 \geq a_1 + a_2 + a_3 + 1 + 1.$$

Enakost $4a_1 = 3a_1 + 2$ velja le za $a_1 = 2$. Tedaj dobimo rešitev

$$a_1 = a_2 = a_3 = 2 \quad \text{in} \quad a_4 = a_5 = 1.$$

Ostane še možnost $a_3 = 1$. Poenostavljena enačba se glasi

$$a_1 \cdot a_2 = a_1 + a_2 + 3.$$

Glede na vrednost a_2 ločimo več možnosti. Pri $a_2 = 1$ ne dobimo rešitve, saj je $a_1 \neq a_1 + 4$. Za $a_2 = 2$ dobimo $a_1 = 5$, za $a_2 = 3$ pa $a_1 = 3$. Pri $a_2 \geq 4$ ni več novih rešitev, saj je $a_1 \cdot a_2 \geq 4a_1 > 2a_1 + 3 \geq a_1 + a_2 + 3$.

Naj povzamem. Enačba ima tri rešitve. Poleg že v besedilu naloge omenjene peterke (5, 2, 1, 1, 1) sta to še peterki (2, 2, 2, 1, 1) in (3, 3, 1, 1, 1).

Martin Juvan

PRODUKT = VSOTA – 2. rešitev

Ker smo matematiki, ne bomo reševali naloge zgolj za $k = 5$, temveč bomo pogledali, kako dobimo vse rešitve za poljubno naravno število k .

Če predpostavimo, da je $a_1 \geq a_2 \geq \dots \geq a_k$, dobimo

$$a_1 \cdot \dots \cdot a_k = a_1 + \dots + a_k \leq a_1 + \dots + a_1 = ka_1$$

oziroma $a_2 \cdot \dots \cdot a_k \leq k$. Torej bodo števila $a_2, \dots, a_k$ nastopala v razcepu števila, manjšega ali enakega k , na $k - 1$ faktorjev, kjer je med faktorji lahko tudi več enic.

Najprej pogledjmo, kako bi poiskali vse take razcepe poljubnega naravnega števila n na m faktorjev $a_1, \dots, a_m$, da bo veljalo $a_1 \geq a_2 \geq \dots \geq a_m$. Velja

$$n = a_1 \cdot \dots \cdot a_m \geq a_m \cdot \dots \cdot a_m = a_m^m.$$

Torej je a_m je delitelj števila n , manjši ali enak $\sqrt[m]{n}$.

Poiščemo vsa števila a_m , ki ustrezajo pogojem. Za vsak možen a_m dobimo enačbo, iz katere razberemo pogoje za a_{m-1} :

$$\frac{n}{a_m} = a_1 \cdot \dots \cdot a_{m-1} \geq a_{m-1} \cdot \dots \cdot a_{m-1} = a_{m-1}^{m-1}.$$

Število a_{m-1} je torej delitelj števila $\frac{n}{a_m}$ (ki je naravno število, saj a_m deli n), manjši ali enak $\sqrt[m-1]{\frac{n}{a_m}}$ ter večji ali enak a_m .

Ta postopek nadaljujemo, dokler ne pridemo do enačbe

$$a_1 = \frac{n}{a_2 \cdot \dots \cdot a_m}.$$

Na ta način lahko poiščemo vse razcepe števila n na m faktorjev.¹

Sedaj pa se lotimo iskanja razcepa vseh števil, manjših ali enakih k , na $k-1$ faktorjev.

Iz vsakega razcepa preberemo števila $a_2, \dots, a_k$, iz enačbe $a_1 \cdot \dots \cdot a_k = a_1 + \dots + a_k$ pa izračunamo še a_1 . Če bi bilo $a_2 = \dots = a_k = 1$, bi dobili $a_1 = a_1 + (k-1)$, ta enačba pa pri $k \geq 2$ nima rešitve. Tako lahko predpostavimo, da $a_2 \cdot \dots \cdot a_k \neq 1$ in

$$a_1 = \frac{a_2 + \dots + a_k}{a_2 \cdot \dots \cdot a_k - 1}.$$

Rezultate, kjer a_1 ni naravno število, večje ali enako a_2 , ovržemo in ostanejo nam natanko vse iskane rešitve.

Za rešitev enačbe $a_1 \cdot \dots \cdot a_5 = a_1 + \dots + a_5$ torej najprej poiščemo vse razcepe števil 1, 2, 3, 4, 5 na 4 faktorje, potem pa izračunamo tem razcepom pripadajoče vrednosti števila a_1 . Razcepe za tako majhna naravna števila zlahka izračunamo "na pamet", brez uporabe algoritma.

a_2	a_3	a_4	a_5	a_1
5	1	1	1	$8/4 = 2$
4	1	1	1	$7/3$
2	2	1	1	$6/3 = 2$
3	1	1	1	$6/2 = 3$
2	1	1	1	$5/1 = 5$
1	1	1	1	/

Če upoštevamo, da je a_1 naravno število, večje ali enako a_2 , ustrezajo rešitvi enačbe le peterke $(2, 2, 2, 1, 1)$, $(3, 3, 1, 1, 1)$ in $(5, 2, 1, 1, 1)$. Opazimo, da je rešitev, kjer je a_1 naravno število, a manjše od a_2 , le permutacija neke druge rešitve, kjer je $a_1 \geq a_2$. To smo tudi pričakovali, kajti

¹ Postopek lahko močno skrajšamo, če določimo najprej najmanjše možno število enic, ki nastopajo v razcepu števila n na m faktorjev. Premislite, kako! Pri parametrih, ki nastopajo v dani nalogi, je enic kar precej. (Op. ur.)

množenje in seštevanje sta komutativni operaciji, pri iskanju razcepov pa smo pazili le na urejenost števil $a_2, \dots, a_k$ (nismo izključili možnosti $a_2 > a_1$).

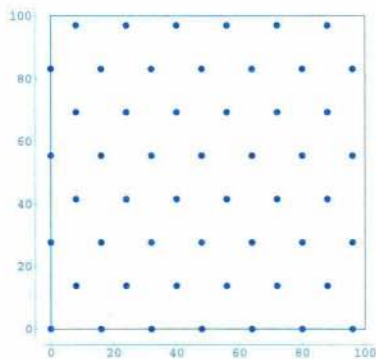
Matija Pretnar

O VRTNARJEVI NALOGI

V tretji številki tega letnika Preseka je Bojan Mohar zastavil nekaj vprašanj o Vrtnarjevi nalogi, ki jo je v prispevku Predalčno načelo v prvi številki tega letnika opisal Jože Grasselli.

Zastavljena vprašanja so težka, da pa ne bodo ostala povsem neodgovorjena, bom podal odgovor na drugi del vprašanja (B). Opisal bom tako razporeditev več kot 300 točk znotraj kvadrata s stranico 100 enot, da noben krog polmera 8 enot ne bo vseboval več kot 6 danih točk. Konstrukcija sploh ne bo zapletena, bo pa nekoliko odstopala od nasveta iz besedila naloge. Ta namreč priporoča "dokaj enakomerno" razporeditev točk po kvadratu.

Skica razporeditve je prikazana na sliki na desni. Vsaka pika pomeni gručo 6 točk, ki so zelo zelo blizu druga drugi. Vodoravne razdalje med gručami so malenkost večje od $2 \cdot 8 = 16$ enot, tako da noben krog polmera 8 ne more vsebovati točk iz dveh različnih gruč, ki sta v isti vrsti. Zaporedni piki iz iste vrste skupaj s piko nad razpoloviščem njune zveznice tvorita enakostranični trikotnik. Navpične razdalje med vrstami so tako malenkost večje od $16\sqrt{3}/2 \doteq 13.86$ enot. Noben krog polmera 8 tako ne more vsebovati točk iz gruč v dveh različnih vrstah. Krog polmera 8 lahko tako vsebuje le točke iz ene same gruč, teh pa je le 6.



Kadar začnemo na robu, lahko v vrsto zložimo 7 pik ($6 \cdot 16 = 96 < 100$), v vrsto z zamaknjenim začetkom pa jih lahko postavimo 6. V kvadrat gre 8 vrst ($7 \cdot 8\sqrt{3} \doteq 96.99 < 100$). V celoti smo torej razporedili $6 \cdot (4 \cdot 7 + 4 \cdot 6) = 312$ točk, in to v pravokotnik s stranicama, ki merita dobrih 96 in slabih 97 enot.

Martin Juvan

NOGOMETNA KOMBINATORIKA

Svetovno prvenstvo v nogometu je pred vrati. Selektor slovenske reprezentance Srečko Katanec je v Korejo pripeljal 23 igralcev: 3 vratarje, 6 branilcev, 9 veznih igralcev in 5 napadalcev. Čeprav je s tem že odpravil številne dvome in skrbi, ga še vedno muči cel kup vprašanj. Pomagaj mu poiskati odgovore.

1. Na koliko načinov lahko Srečko sestavi enajsterico, v kateri bodo vratar, trije branilci, štirje vezni igralci in trije napadalci?
2. Kaj pa enajsterico, v kateri bo poleg natanko enega vratarja vsaj en napadalec?
3. Na koliko načinov lahko Srečko razdeli drese s številkami od 1 do 11 med svojih 23 izbrancev?
4. Kaj pa, če mora številko 1 dobiti vratar, ostale pa drugi igralci?
5. Koliko različnih petmestnih števil lahko sestavimo, če se v vrsto postavi nekaj igralcev, ki imajo na hrbtu številke od 5 do 11?
6. V korejskem hotelu Mitsa-Matsa bodo slovenskim reprezentantom in selektorju na voljo 3 različne štiriposteljne sobe ter 6 različnih dvoposteljnih sob. Koliko različnih razporeditev 24 oseb po sobah je možnih?
7. Vstopnice za tekmo slovenske reprezentance menda stanejo 20 (sedeži 2. kategorije), 30 (sedeži 1. kategorije) in 70 evrov (sedeži v posebnih ložah). Skupina navijačev namerava za nakup vstopnic porabiti natanko 200 evrov. Na koliko načinov lahko kupijo vstopnice, če nas zanima samo število vstopnic posamezne vrste?
8. Cimerotič, Ačimovič in Čeh so na zadnjih treningih skupaj dosegli 7 golov, a ni nujno, da je vsak od njih res dosegel gol. Na koliko načinov se je to lahko zgodilo?
9. Zahovič, Pavlin, Osterc in Rudonja pa so na zadnjih treningih skupaj dosegli 15 golov. Na koliko načinov so to lahko storili, če je dal vsak vsaj dva gola?
- 10.* Enajsterica, primerna za tekmo, je sestavljena iz enega vratarja, vsaj dveh branilcev in vsaj enega napadalca. Med koliko primernimi enajstericami lahko izbira slovenski selektor?

Boštjan Kuzman, Martin Juvan

Rešitev je na str. 365.

KRISTALNE MREŽE – 2. del

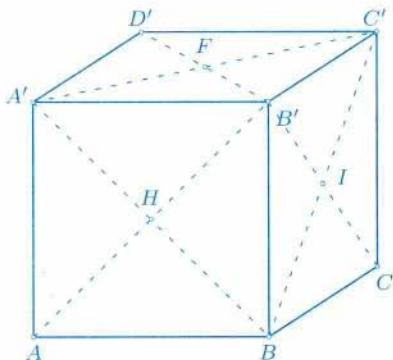
Zlaganje krogel

V prejšnji številki Preseka smo si v članku *Kristalne mreže, 1. del*, ogledali dva načina zlaganja skladnih krogel. Tu bomo predstavili še enega.

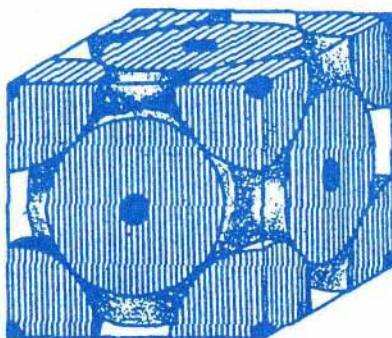
Narišimo kocko $ABCD A' B' C' D'$ z robom a . Na njej označimo vsa oglišča in vsa središča osnovnih ter stranskih ploskev (slika 1), to je skupaj $8 + 6 = 14$ točk.

Nato zlagamo skladne kopije te “osnovne celice”, ki ji pravimo “*ploskovno centrirana kocka*”, tako da imata sosednji kocki skupna štiri oglišča.

Oglišča in središča mejnih ploskev tako zloženih kock sestavljajo množico točk v prostoru. Kot je razvidno iz vprašanja 3 na koncu tega članka, je ta množica točk *trirazsežna mreža*, kakršno smo opisali v prvem delu članka o kristalnih mrežah.



Slika 1.



Slika 2.

Vsaka točka te mreže naj bo središče krogle s polmerom

$$R = \frac{1}{4} a \sqrt{2}.$$

Na sliki 1 se potem krogle s središčem v H dotika krogle s središči v točkah A, B, A' in B' .

Izračunajmo delež prostora, ki ga zavzemajo krogle. V osnovni celici imamo osemkrat po eno osmino krogle in šestkrat po polovico krogle (slika 2), skupaj štiri prostornine krogle, kar je

$$4 \cdot \frac{4}{3} \pi R^3.$$

Delež dobimo, če to delimo s prostornino kocke, torej z

$$a^3 = 16\sqrt{2}R^3.$$

Količnik je

$$\frac{\pi}{3\sqrt{2}} \doteq 74,0 \, \%.$$

To je več kot pri "telesno centrirani kocki" iz prejšnjega članka.

Veliki nemški matematik Carl Friedrich Gauss je že pred dvema stoletjema dokazal tole: Če središča krogel sestavljajo trirazsežno mrežo, ni mogoče doseči večje zapolnjenosti prostora. Zato temu načinu zlaganja krogel pravimo *kubično najgostejši sklad*.

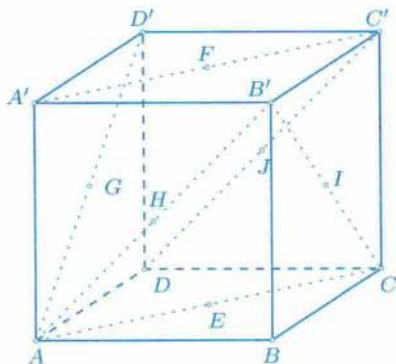
V letu 1998 je bil predstavljen izredno dolg dokaz, da tudi sicer ni mogoče zložiti krogel učinkoviteje. Dokaz je oprt na obsežna preverjanja z računalnikom.

Opozorimo pa, da obstajajo še drugi načini zlaganja krogel, ki so enako učinkoviti kot kubično najgostejši sklad.

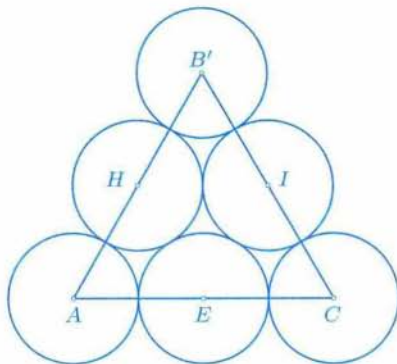
Iz osnovne celice ni takoj jasno, kako bi v praksi zložili krogle v kubično najgostejši sklad. Zato še enkrat narišimo osnovno celico (slika 3).

Točke A, E, C, I, B', H ležijo vse v isti ravnini in so središča krogel. Z malo črko označimo kroglo, ki ima središče v točki, označeni z ustrežno veliko črko. Paroma se dotikajo krogle a, h in e (saj je $|HE| = |AH| = |AE|$). Se pravi, vsak par krogel iz množice $\{a, h, e\}$ se dotika. Podobno velja za krogle iz množic $\{e, c, i\}$, $\{b', h, i\}$ in $\{e, h, i\}$.

Če krogle a, e, c, i, b', h pravokotno projiciramo na ravnino trikotnika ACB' , dobimo sliko 4.



Slika 3.



Slika 4.

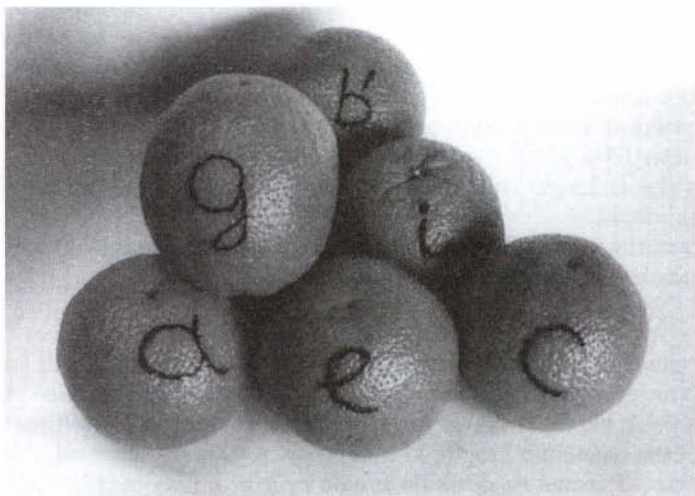
Ker je $|GH| = \frac{a}{2}\sqrt{2}$, se g in h dotikata. Enako vidimo, da se

g dotika krogel a, h, e ,

j dotika krogel i, e, c ,

f dotika krogel b', h, i .

Zdaj vemo, kam moramo položiti krogle g, j, f . Oglejte si tudi sliko 5 in fotografijo na naslovnici.



Slika 5.

Vprašanje 1. Kje na sliki 4 je projekcija točke B ? (Namig: Katerih označenih krogel se dotika kroglja b ?)

Uporabimo zdaj pridobljeno znanje za reševanje zanimivega problema.

Relativna atomska masa aluminija je 26,98, zato ima 1 mol atomov aluminija maso $m = 26,98$ g. Gostota aluminija je $2,70 \text{ kg/dm}^3$. Aluminij kristalizira v kubično najgostejšem skladu. Določi polmer atoma aluminija.

Rešitev. V 1 molu je Avogadrovo število $N_A \doteq 6,02 \cdot 10^{23}$ atomov aluminija, vsak ima torej maso $m \cdot (N_A)^{-1}$.

Če je R polmer atoma aluminija, ima osnovna celica rob $a = 2\sqrt{2}R$. Na osnovno celico odpadejo, kot smo ugotovili, 4 atomi, torej masa $\frac{4m}{N_A}$.

Gostota je

$$\rho = \frac{4m}{N_A \cdot a^3} = \frac{4m}{N_A \cdot 16\sqrt{2}R^3}.$$

Od tod je

$$R^3 = \frac{m}{4\sqrt{2}N_A\rho} = \frac{26,98}{4\sqrt{2} \cdot 6,02 \cdot 2,70} \cdot 10^{-29} \text{ m}^3 = \frac{269,8}{4\sqrt{2} \cdot 6,02 \cdot 2,70} \cdot 10^{-30} \text{ m}^3$$

in

$$R = \sqrt[3]{\frac{269,8}{4\sqrt{2} \cdot 6,02 \cdot 2,70}} \cdot 10^{-10} \text{ m} \doteq 1,43 \cdot 10^{-10} \text{ m}.$$

V nadaljevanju zahtevamo od bralca več samostojnega dela.

Vprašanje 2. Svinec ima gostoto $11,34 \text{ g/cm}^3$ in relativno atomsko maso 207,2. Kristalizira v kubično najgostejšem skladu. Določite polmer atoma svinca.

Opomba. V staljenem svincu so atomi bolj neurejeni kot v kristalu in prostora ne zapolnjujejo tako učinkovito. Zato se pri strjevanju svinec skrči.

Kovine, ki kristalizirajo v manj gostih skladih, pa pri strjevanju lahko zvečajo prostornino. Take kovine niso najbolj primerne za vlivanje.

Poseben primer je kositer, ki pri nizkih temperaturah kristalizira v manj gostem skladu kot pri sobni temperaturi. To je vzrok t.i. "kositrove kuge", ki je povzročila mnogo škode.

Vprašanje 3. Vrnimo se k sliki 3. Naj bo $\mathcal{P}$ paralelepiped z osnovno ploskvijo $B'HEI$ in s stranskim robom $B'F$.

- Določite preostala oglišča paralelepipeda.
- Če ima kocka rob a , določite robove paralelepipeda.
- Določite kota, ki ju $B'F$ oklepa z $B'H$ in $B'I$.
- Iz tršega papirja naredite nekaj modelov za $\mathcal{P}$, če rob paralelepipeda $\mathcal{P}$ meri 6 cm. Zložite modele tako, da imata sosednja modela skupna 4 oglišča. Oglišča zloženih paralelepipedov sestavljajo mrežo središč krogel kubično najgostejšega sklada. Primerjajte s sliko 3. Da je to res prava mreža, je razvidno iz naslednje točke.
- Naj bo $\overrightarrow{B'I} = \vec{a}$, $\overrightarrow{B'H} = \vec{b}$, $\overrightarrow{B'F} = \vec{c}$. Če za izhodišče vzamemo točko B' , izrazite krajevne vektorje vseh oglišč kocke in vseh središč mejnih ploskev v bazi $\{\vec{a}, \vec{b}, \vec{c}\}$.

Vprašanje 4. Na sliki 3 postavimo pravokotni koordinatni sistem tako, da bo A izhodišče O , $\vec{OB} = 2\vec{i}$, $\vec{OD} = 2\vec{j}$, $\vec{OA'} = 2\vec{k}$.

Kaj je množica vseh točk T , za katere je

$$\vec{OT} = m\vec{i} + n\vec{j} + p\vec{k},$$

kjer so $m, n, p \in \mathbb{Z}$ in je vsota $m + n + p$ sodo število?

Odgovori na vprašanja:

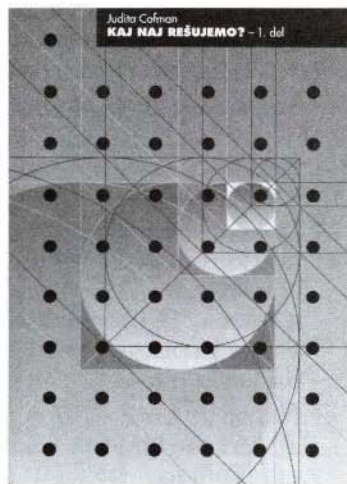
1. Projekcija točke B je v središču trikotnika ACB' .
2. $1,75 \cdot 10^{-10}$ m.
3. a) G, D, J
b) $\frac{1}{\sqrt{2}}a$
c) 60°
e) $\vec{OA} = 2\vec{b}$, $\vec{OB} = \vec{a} + \vec{b} - \vec{c}$, $\vec{OC} = 2\vec{a}$, $\vec{OD} = \vec{a} + \vec{b} + \vec{c}$,
 $\vec{OA'} = -\vec{a} + \vec{b} + \vec{c}$, $\vec{OB'} = 0$, $\vec{OC'} = \vec{a} - \vec{b} + \vec{c}$, $\vec{OD'} = 2\vec{c}$,
 $\vec{OE} = \vec{a} + \vec{b}$, $\vec{OF} = \vec{c}$, $\vec{OG} = \vec{b} + \vec{c}$, $\vec{OH} = \vec{b}$, $\vec{OI} = \vec{a}$,
 $\vec{OJ} = \vec{a} + \vec{c}$.
4. To je mreža kubično najgostejšega sklada, katerega osnovna celica je kocka $ABCD A' B' C' D'$.

Peter Legiša

Judita Cofman: KAJ NAJ REŠUJEMO? – 1. in 2. del

V zbirki Knjižnica Sigma je pred kratkim v dveh delih izšel prevod knjige *What to Solve?*, avtorice Judite Cofman. Original je v angleškem jeziku leta 1990 izdala ugledna založba Clarendon Press.

Avtorica je po rodu Madžarka iz Vojvodine, že vrsto let pa poučuje na različnih univerzah v Angliji, Nemčiji in na Madžarskem. Podnaslov knjige *Naloge in nasveti za mlade matematike* pojasnjuje, kakšna je vsebina dela. Le-to je nastalo na osnovi gradiv, ki jih je avtorica skupaj s sodelavci pripravljala za seminarje in raziskovalne taborne za mlade matematike.



Sestavljeno je iz štirih poglavij in treh dodatkov. Vsako poglavje se začne z uvodom, ki mu sledijo naloge in nato še njihove rešitve. Lažje naloge, namenjene manj izkušenim bralcem, so posebej označene.

Prvi del ima dobrih 150 strani in poleg predgovora vsebuje prevod prvega in drugega poglavja originala. V prvem poglavju, ki ima naslov *Naloge za raziskovanje*, so predstavljeni nekateri prijemi, ki jih pogosto uporabimo ob prvem srečanju z matematičnim problemom. Sem sodi uporaba analogij, iskanje vzorcev, posploševanje ipd. *Načini reševanja nalog* je naslov drugega poglavja. Tu spoznamo preverjene metode za reševanje problemov: uporabo invariant, matematično indukcijo, dokazovanje s protislovjem, pa tudi kakšen manj znan prijem, kot je npr. metoda neskončnega spusta.

Drugi del je nekoliko krajši ter poleg tretjega in četrtega poglavja originala vsebuje še vse tri dodatke. Tretje poglavje predstavi nekatere znamenite probleme iz zgodovine matematike: trditve o praštevilih in o številu π , uporabo kompleksnih števil in kvaternionov, odkritje neevklidskih geometrij in razvoj "umetnosti štetja". V zadnjem poglavju so opisani izbrani elementarni problemi, s katerimi so se ukvarjali znameniti matematiki 20. stoletja. Med njimi je tudi slavnj zadnji Fermatov izrek.

Prvi dodatek služi predvsem kot slovar, saj vsebuje definicije in pojasnila matematičnih pojmov, ki jih srečamo v besedilu. V drugem dodatku so kratki biografski podatki o matematikih, omenjenih v besedilu, tretji dodatek pa je obširen seznam knjig, priporočenih za nadaljnje branje.

Knjigi nista težko branje, moč pa ju je prebirati tudi po delih. Dejstva iz zgodovine matematike, ki so vpletena v besedilo, le-to lepo poživijo in naredijo zanimivo tudi samo za listanje. Med nalogami je kar nekaj takih, ki jih še nisem srečal. Tudi rešitve so večkrat napisane bolj "na dolgo", ne tako izpiljeno, kot jih običajno srečamo v zbirkah tekmovalnih nalog. Tak način podajanja bo verjetno bližji matematično manj izkušenim bralcem, saj je iz njega običajno lažje razbrati, kako je nastala ideja za rešitev naloge. Seveda pa so predstavljene rešitve še vedno povsem pravilne in matematično korektne.

Če vas torej zanimajo matematične naloge, popestrene s ščepcem zgodovine, vas vabim, da knjižici vzamete v roke in ju prelistate.

Knjigi lahko kupite pri DMFA – založništvo, Jadranska 19, Ljubljana, ali ju naročite po telefonu (01) 4766–553.

Martin Juvan

ZAKRITJE

Zakritje ali *okultacija* (occultatio, lat. skrivanje, tajenje) v astronomiji na splošno pomeni pojav, da prvo vesoljsko telo zakrije ali okultira drugo. V tem primeru leži drugo, to je zakrito telo, bolj daleč kot prvo telo. Zakritje večkrat uporabljamo kot pomoč pri ugotavljanju, katero od dveh vesoljskih teles, ki sta udeleženi pri zakritju, je od nas bolj oddaljeno.

Z roko zakrijmo (zastrimo) luč na steni. Kaj je od nas bolj oddaljeno, roka ali luč?

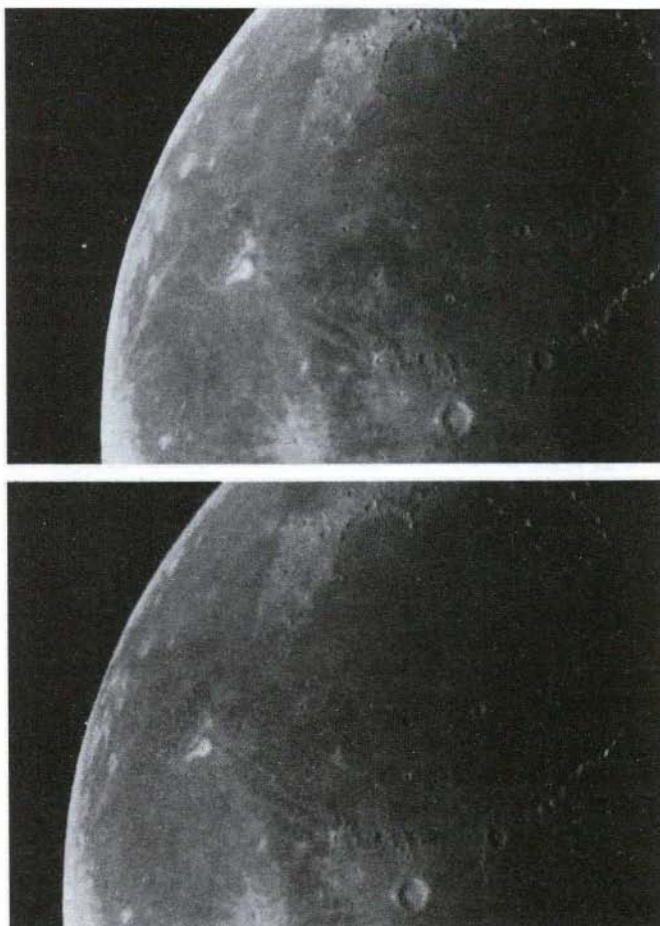
Tako lahko Luna pri svojem navideznem mesečnem gibanju na nebu zakrije zvezde, planete, glave kometov, radijske vire, kar vse pomeni, da so zvezde, planeti, kometi, radijski viri od nas bolj oddaljeni, kot je oddaljena Luna.

Planet lahko zakrije zvezdo (leta 1679 je Saturn zakril zvezdo Omi-kron Bika, 1976 je Mars zakril zvezdo Epsilon Dvojčka, 1981 pa Venera zvezdo Sigma Strelca). Znani so primeri, da planet zakrije planet (leta 1590 je Venera zakrila Mars) ali da planet zakrije satelit, ki kroži okrog njega (npr. da Jupiter zakrije kako svojo luno; o tem najdete podatke v astronomskih efemeridah *Naše nebo*).

Najbolj znana, številna, raziskana in tudi pomembna so Lunina zakritja zvezd. Zato tu predstavimo predvsem ta pojav (slika 1). Pri Luninem zakritju zvezda v hipu zaide za Luno, včasih pa prav tako tudi vzide izza nje. Ker se Luna premika glede na zvezde od zahoda proti vzhodu, zvezda (planet ali kako drugo vesoljsko telo) izgine za Luninim vzhodnim robom (pojav imenujemo tudi imersija), pojavi pa se izza njenega zahodnega roba (emersija). Od mlaja mimo prvega krajca do polne lune se izginotje zvezde torej dogaja na temnem vzhodnem robu Lune, od ščipa mimo zadnjega krajca do mlaja pa se ponovni pojav zvezde kaže na temnem zahodnem robu.

Lunina zakritja zvezd uporabljajo za določitev natančne lege Lune, za katero vemo (glej *Presek* 28, 2000–2001, 206), da ima zelo zamotano gibanje, njeno natančno lego pa pogosto potrebujemo v raznih izračunih.

Lege zvezd na nebu so določene zelo natančno, ker gre za točkasta telesa z gibanji, katerih lastnosti dobro poznamo. Luna pa ni točkasta, pravzaprav je navidezno zelo razsežno telo, pa še njeno gibanje je zelo težko natančno predvideti. Lege Lune torej ni možno napovedati z enako natančnostjo kot lege zvezd. Če pa na primer izmerimo čas (trenutek), ko Luna zakrije zvezdo, je lega točke na Luninem robu (to je zvezde, ki se ravno dotika Luninega diska, kjer se odigra pojav) v tem času tudi znana.

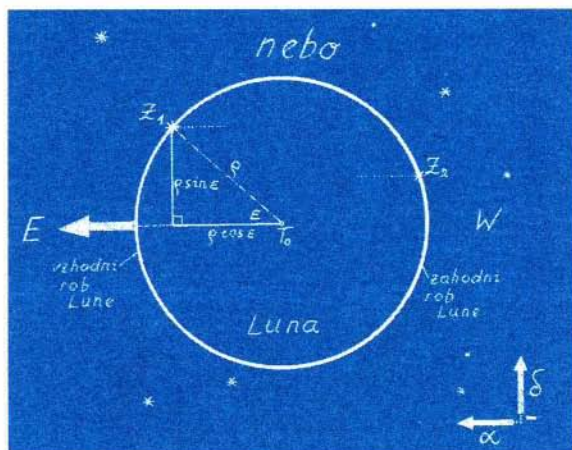


Slika 1. Ko Luna prečka nebo, občasno pride pred kakšno zvezdo v ozadju tako, da jo začasno zastre in prepreči, da bi jo opazovali – rečemo, da Luna zakrije zvezdo. Razmeroma pogosto zakrije dovolj svetlo zvezdo, ki jo lahko opazujemo že z daljnogledom manjše povečave.

Slika prikazuje, da bo Luna kmalu zakrila zvezdo – zgodilo se bo Lunino zakritje zvezde. Pojav se odigra v nekaj stotinkah sekunde. Zakritje je mogoče posneti na filmski trak, s TV kamero, fototelico, fotometrom, videom. Kot zanimivost naj povemo, da natančni pregledi posnetkov kažejo, da Luno obkroža skrajno redka atmosfera (tako redka, da bi lahko rekli, da je nima). Pri izredno natančnem opazovanju sij zvezde nekako dve do tri sekunde preden zvezda izgine za Lunin rob zelo rahlo pade, svetloba zvezde nekako šibko “zamigota” oziroma zvezda “obledi”.

Na zgornji sliki je zvezda še nekoliko navidezno oddaljena od Luninega robu; Luna se ji navidezno približuje od zahoda proti vzhodu (giblje se v levo). Spodaj je zvezda tik pred zakritjem.

Iz teh podatkov lahko nato določimo natančno lego Lune, pravzaprav središča njenega diska ob zakritju (slika 2). Zato Lunina zakritja zvezd pazljivo opazujejo. V preteklosti so opazovanja teh zakritij pomagala tudi pri odkrivanju sprememb v vrtenju Zemlje.



Slika 2. K določitvi natančne lege Lune s pomočjo Luninega zakritja zvezde.

Zaradi Luninega gibanja glede na zvezde proti vzhodu zvezda Z_1 izgine (zaide) za Luno – zakritje (imersija), zvezda Z_2 pa se pojavi (vzide) – odkritje (emersija). Zvezde imajo kot točkasta telesa natančno določeni nebesni koordinati (rektascenzijo α in deklinacijo δ), Luna kot razsežno in zelo “muhasta” telo pa ne. Natančnejši koordinati Lune (pravzaprav središča Luninega diska) ob zakritju dobimo, da upoštevamo smer Luninega gibanja na nebu, podanega npr. s kotom ε , in znanim navideznim polmerom ρ Lune.

Naj ima zvezda Z_1 znani koordinati α_1 in δ_1 . Tedaj sta koordinati središča $T_0(\alpha_0, \delta_0)$ Luninega diska enaki: $\alpha_0 = \alpha_1 - \rho \cos \varepsilon$ in $\delta_0 = \delta_1 - \rho \sin \varepsilon$ (α se veča v levo, δ pa navzgor). Pa še vedno je tako določena lega središča Luninega diska približna, kajti Luna se giblje zelo nepravilno. To povemo zato, da začutite vso zamotanost Luninega gibanja.

Nastop pojava in okoliščine Luninega zakritja zvezde, kar nekako spominja na mrk zvezde, lahko predvidimo (izračunamo) po posebno zapletenih formulah (zaradi prezahtevnosti jih seveda ne navajamo).

Trenutke zakritja svetlih zvezd, vidnih z lovskim daljnogledom, prinašajo številne astronomske efemeride. Opazovanje teh pojavov, ki jih spremljajo na številnih observatorijih, in njihova teoretična analiza se uporablja za natančno določitev osnovnih elementov tira Luninega gibanja okrog Zemlje.

Slika 3. Če zvezda zaide (vzide) skoraj v hipu, pa planet, ki je z daljnogledom viden kot majčken disk-plošček, kar nekaj časa zahaja (leze) za Lunin rob (vzhaja izza robu). Iz časa zahajanja vesoljskega telesa za Lunin rob je mogoče izmeriti zorni kot vesoljskega telesa in pri znani oddaljenosti še njegovo velikost – premer.

Slika prikazuje vzhajanje Saturna izza Luninega robu. Mimogrede, leta 1983 smo lahko opazovali, kako je Luna zakrila planet Jupiter.

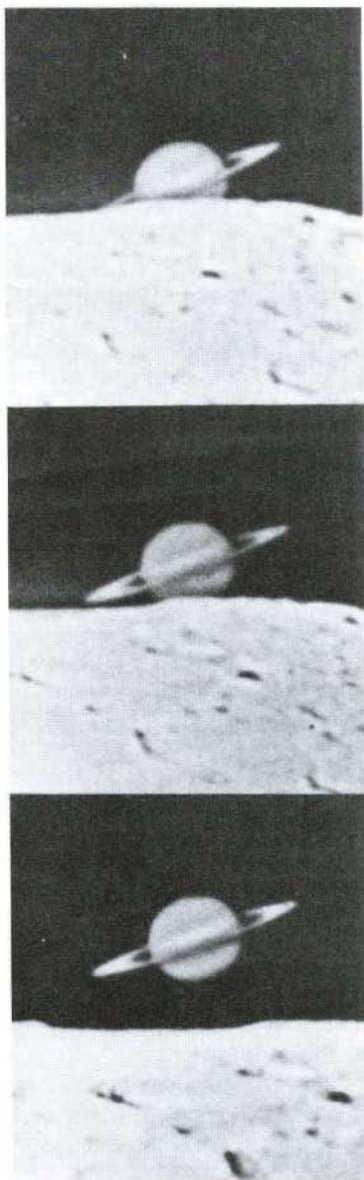
Prav pred kratkim je Luna tudi zakrila neki svetel planet. Poskusite ugotoviti, kateri.

Tudi zemljepisno dolžino je zelo prikladno določiti po trenutku, ko Luna zakrije zvezdo, saj so v nekaterih efemeridah navedeni potrebni podatki za skoraj vse svetlejše zvezde in sicer točni čas zakritja kot tudi mesta vstopa in izstopa zvezde za poljuben kraj na Zemlji, kjer lahko pojav (zakritje ali odkritje) opazujemo.

V sredini preteklega stoletja so Lunina zakritja zvezd začeli uporabljati tudi za določevanje polmerov (velikosti) zvezd. Metoda se je izkazala za uspešno in jo uporabljajo še danes.

Govoriti oziroma pisati o vsem tem pa so že druge, kar zahtevne zgodbe. Morda o njih kdaj drugič.

Marijan Prosen



REŠITEV POZABLJENE NALOGE – s str. 290

Kolega Martin ima odlično urejen arhiv. Sam sem medtem na “pozabljeno nalogo” zares že čisto pozabil. Najprej je vpraševala po praštevilu z najdaljšim desetiškim zapisom, ki ob črtanju števk z desne ves čas ostaja praštevilo. Izkaže se, da imajo takšna praštevila osem števk in da jih je pet, namreč 23399339, 29399999, 37337999, 59393339 in 73939133. Vsa števila v zaporedju 23399339, 2339933, 233993, 23399, 2339, 233, 23, 2 so praštevila, podobno velja za ostala štiri števila.

Če namesto na desni črtamo številke na levi, pridemo do dolžine 24 (ne 23, kot sem leta 1995 napačno napisal v pismu Martinu!) in do enega samega praštevila, namreč 357686312646216567629137. Vsi členi zaporedja 357686312646216567629137, 57686312646216567629137, ..., 137, 37, 7 so praštevila.

Če lahko črtamo številke na levi in desni, dobimo tri “najdaljša” praštevila (dolžine 31), in sicer

6279821572756282163864793777199 ,
 8833367216294578819534799139337 ,
 8939662423123592347173339993799 .

Zdaj je treba na vsakem koraku povedati, ali črtamo številko na levi ali na desni. Za srednje od gornjih treh števil dobimo npr. naslednje zaporedje praštevil:

8833367216294578819534799139337	457881953479913
833367216294578819534799139337	57881953479913
83336721629457881953479913933	7881953479913
3336721629457881953479913933	788195347991
336721629457881953479913933	88195347991
36721629457881953479913933	8195347991
6721629457881953479913933	819534799
721629457881953479913933	19534799
21629457881953479913933	9534799
2162945788195347991393	534799
216294578819534799139	53479
16294578819534799139	5347
6294578819534799139	347
294578819534799139	47
94578819534799139	7
9457881953479913	

Zanimivo: Zaporedje odločitev, katero števko odvreči (prvo ali zadnjo), je skoraj enolično določeno. Edino možno variacijo gornjega zaporedja dobimo, če predzadnje število v levem stolpcu (94578819534799139) nadomestimo s številom 29457881953479913.

Daljših praštevil z naštetimi lastnostmi ni. Kako sem vse to ugotovil? Seveda ne "ročno", ampak s programom *Mathematica*. Števk nisem črtal, temveč dodajal. Začel sem z enomestnimi praštevili 2, 3, 5, 7, na desni dodajal števke 1, 3, 7, 9 (zakaj ne tudi drugih?), na levi pa vse razen 0. Iz množice tako dobljenih števil sem na vsakem koraku izbral praštevila. Največjo "vmesno množico" praštevil sem dobil, ko sem dopuščal dodajanje na levi in desni, in sicer 15923 praštevil dolžine 13. Iz vsakega od njih lahko s črtanjem števk na levi oz. desni (vendar v pravilnem vrstnem redu) dobimo zaporedje trinajstih praštevil. Ali je število praštevilo, sem preverjal s funkcijo *PrimeQ+*, ki je hitra, a uporabljaja verjetnostni algoritem. Če reče "ne", je število gotovo sestavljeno, če pa reče "da", število ni nujno praštevilo. Znano je, da pri številih do 10^{16} program ne napravi napake, vendar v tem primeru to ne zadošča, saj imamo opraviti z 31-mestnimi praštevili. *Mathematica* pozna tudi funkcijo *ProvablePrimeQ+*, ki ne dela napak, je pa precej počasnejša. Zgoraj omenjena praštevila sem poiskal s funkcijo *PrimeQ+*, nato pa jih preveril še s *ProvablePrimeQ+*, a napake ni bilo. Za preverjanje 31-mestnega praštevila je funkcija *PrimeQ+* potrebovala med 0.01s in 0.02s, funkcija *ProvablePrimeQ+* pa med 6s in 7s.

Kolega Martin me je opozoril tudi na internetno stran z naslovom mathworld.wolfram.com/TruncatablePrime.html, kjer dobimo še več podatkov o teh praštevilih. Tako se npr. praštevila, ki pri črtanju števk z leve ves čas ostajajo praštevila, ne moremo pa jih na levi z od nič različno števko podaljšati v praštevilo, imenujejo *praštevila Henrika VIII*.

Vprašanja:

1. Kako dolga praštevila z zgoraj opisanimi lastnostmi dobimo v drugih številskih sestavih (npr. trojiškem, štiriškem, ..., šestnajstiškem)?
2. Kako dolga praštevila dobimo, če dovolimo črtanje katerekoli števke, ne nujno prve ali zadnje?
3. Kako dolga praštevila lahko dobimo, če dopuščamo tudi zapise, ki imajo na začetku eno ali več ničel? Primer: Število $10^{2607} + 3$ je praštevilo, število 3 pa tudi, torej je (če črtamo števke z leve) odgovor vsaj 2608.

Marko Petkovšek

ATOMI SO SESTAVLJENI

Ne bi bilo prav, če v vrsti prispevkov o atomih ne bi nazadnje omenili, da so atomi sestavljeni. Atomi so veljali za nedeljive in nesestavljene pred poltretjim tisočletjem, ko so le razmišljali o deljivosti snovi, in v 19. stoletju, ko so z njimi pojasnili osnovne kemijske zakone. Po tej lastnosti so dobili ime. Danes bi rekli, da so atome imeli za *osnovne delce*.

Vendar so se razmeroma zgodaj pojavila osamljena nasprotna mnenja. André Marie Ampère je že leta 1814 mislil, da atome sestavljajo manjši delci. Sledili so mu nekateri drugi francoski fiziki, ki so menili, da atoma osrednji del z maso obdajajo številni "etrski delci" brez mase. Po letu 1826 je nemški fizik in psiholog Gustav Theodor Fechner atome primerjal z vesoljskimi telesi in trdil, da oboje povezujejo enake sile. Wilhelm Eduard Weber¹ je leta 1871 opozoril na to, da med telesi v vesolju deluje gravitacija, med deli atomov pa električna sila.

Taka in podobna razmišljanja sprva niso imela opore v opazovanjih in so jih nekateri fiziki kot izmišljotine s poudarkom odklonili. Zaradi njih je Ernst Mach nasprotoval atomom in je prišlo do spora, ki smo ga omenili v članku Atomi in Perrinova merjenja v prejšnji številki Preseka. Pozneje pa so izidi poskusov omenjene zamisli postopno podprli. Od leta 1858 so Julius Plücker in drugi fiziki raziskovali električni tok v razredčenih plinih. Opazovali so *katodne žarke*, svetel pramen, ki je izhajal iz katode, to je negativne elektrode v stekleni cevi z razredčenim plinom. Nanj je bilo mogoče vplivati z magnetom. Večina nemških fizikov je mislila, da gre za nekakšno valovanje, večina angleških pa stavila na naelektrene delce. Leta 1897 se je Joseph John Thomson z odklanjanjem v električnem in magnetnem polju prepričal, da so katodni žarki negativno naelektreni delci s skoraj dvatisočkrat manjšo maso od vodikovega atoma. Pozneje so jih imenovali *elektroni*. K temu spoznanju, ki se je le počasi uveljavilo, je prispevalo veliko fizikov.²

Iz leta 1897 izvirajo tudi poskusi, ki so nakazali, da so elektroni sestavni del atomov. Pieter Zeeman je raziskoval sevanje natrijeve pare v magnetnem polju. Z močnim magnetom in odbojno uklonsko mrežico je ugotovil, da se rumena natrijeva spektralna črta v magnetnem polju

¹ Po njem ima ime enota za magnetni pretok. Bil je starejši brat fiziologa Ernsta Heinricha Webra, ki si je zamislil Weber-Fechnerjev zakon, da je odziv, npr. v očesu ali ušesu, sorazmeren z logaritmom dražljaja.

² Curek elektronov, ki ga pospeši napetost 10 tisoč voltov in več, ustvari sliko na zaslonu televizijskega sprejemnika ali računalnika.

razširi. Kadmijeva spektralna črta pa se je v močnem magnetnem polju razcepila na dve bližnji črti, če je opazoval svetlobo v smeri magnetnega polja, in na tri, če je opazoval svetlobo pravokotno na to smer. Antoon Hendrik Lorentz, kateremu je poročal o svojih opazovanjih, je pojav teoretično pojasnil.

Lorentzov račun. Elektron z negativnim osnovnim nabojem $-e_0$, ki so ga poznali od merjenj pri elektrolizi, in maso m naj v določeni smeri niha s frekvenco ν in s to frekvenco kroži po krogu s polmerom r v ravnini, pravokotni na to smer. Elektron veže na atom centripetalna električna sila $Ze_0^2/4\pi\epsilon_0 r^2 = m(2\pi\nu)^2 r$. Pri tem je Z število pozitivnih osnovnih nabojev v atomu in ϵ_0 influenčna konstanta. Magnetno polje z gostoto B ne vpliva na elektron, ki niha v smeri polja. Z majhno dodatno silo $e_0\nu B$ pa deluje na elektron, ki kroži v pravokotni ravnini s hitrostjo $v = 2\pi\nu r$. Smer sile je odvisna od smisla kroženja. Magnetna sila malo poveča centripetalno silo ali jo malo zmanjša in zaradi tega kroži elektron malo hitreje ali malo počasneje. Frekvenca nihajočega elektrona se v magnetnem polju ne spremeni, frekvenca krožečega elektrona pa se spremeni za $\pm\delta\nu$:

$$\frac{Ze_0^2}{4\pi\epsilon_0 r^2} \pm 2\pi\nu e_0 r B = m(2\pi)^2 (\nu \pm \delta\nu)^2 r = m(2\pi\nu)^2 r \pm 4\pi^2 m r \cdot 2\nu\delta\nu$$

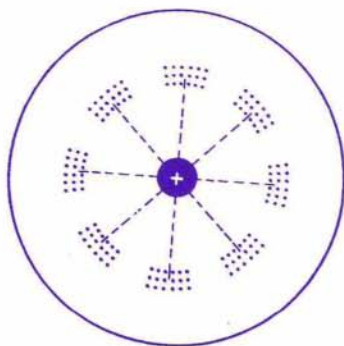
in

$$\delta\nu = \frac{B}{4\pi} \cdot \frac{e_0}{m}.$$

Člen s $(\delta\nu)^2$ smo zanemarili. Izid računa je dobro opisal izide pri merjenju in *specifični naboj* e_0/m pri tem *Zeemanovem pojavu* se je v okviru natančnosti pri merjenju ujemal s specifičnim nabojem katodnih žarkov.

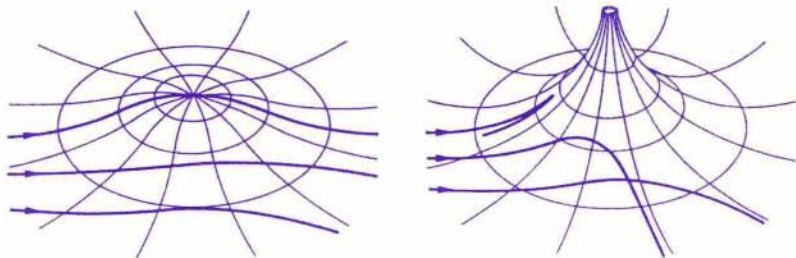
V tistem času so uspela še druga odkritja. Leta 1895 je Conrad Wilhelm Röntgen odkril rentgensko svetlobo in leto zatem Henri Becquerel radioaktivnost. Prva leta naslednjega stoletja so dala spoznanje, da so delci β , ki jih oddajajo radioaktivne snovi, elektroni in delci α helijeji ioni. Začela se je uveljavljati misel, da so atomi sestavljeni in da jih sestavljajo elektroni. Atomi so navzven električno nevtralni, zato jih poleg negativnih elektronov sestavlja tudi pozitivni električni naboj. Ker imajo elektroni zelo majhno maso, odpade domala vsa masa atoma na pozitivni naboj. O tem tedaj ni bilo eksperimentalnih podatkov, zato so si zamislili veliko različnih *atomskih modelov*.

V letih 1903 in 1904 si je J. J. Thomson predstavljal, da je pozitivni naboj enakomerno porazdeljen po vsem atomu in elektroni v njem mirujejo "kot češplje v pudingu". V tem času je japonski fizik Hantaro Nagaoka predlagal drugačen model (slika 1). V njem se okoli majhnega osrednjega pozitivnega naboja giblje več skupin elektronov. Sevanje atomov je pojasnil z dodatnim nihanjem teh skupin s frekvenco izsevane svetlobe. Nekateri drugi fiziki so vztrajali pri pozitivnem naboju, porazdeljenem po vsem atomu, in so poskusili pojasniti sevanje atomov z motnjami v gibanju elektronov.

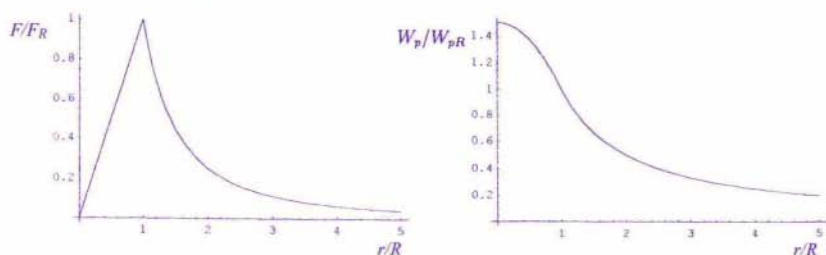


Slika 1. Model atoma, ki ga je v letih 1903 in 1904 opisal Hantaro Nagaoka. Izhajal je iz mladostne razprave James Clerka Maxwella o Saturnovih obročih, zato so ga imenovali *saturnovski model*.

Na inštitutu Ernesta Rutherforda v Manchesteru sta Hans Geiger in Ernest Marsden v letih 1908 in 1909 opazovala prehod delcev α skozi zelo tanke kovinske lističe. Maloštevilni delci α so se na lističih odklonili za velik kot (slika 2). Nekateri so se celo odbili. Iz tega je izhajalo, da pozitivni naboj atoma deluje na delec α z veliko silo. Zato mora biti pozitivni naboj v atomu zbran v zelo majhnem prostoru (slika 3).



Slika 2. Prispodoba za gibanje delca α v atomu, v katerem bi pozitivni naboj izpolnil ves atom (levo), in v atomu z jedrom (desno). Električni potencialni energiji delca α priredimo težno potencialno energijo in si mislimo, da zakotalimo kroglico proti hribu. (Na desni je hrib tako visok, da ves ne pride na ribso in smo ga zato odrezali.) V prvem primeru bi se delci α le neznatno odklonili o prvotne smeri, v drugem pa se nekateri močno odklonijo. Le z drugim je mogoče opisati opazovano vedenje delcev α pri prehodu skozi tanek kovinski listič. Polmera atoma in jedra nista narisani v pravem razmerju.



Slika 3. Električna sila (levo) in potencialna energija (desno) naelektrenega delca v enakomernem oblaku pozitivnega naboja v odvisnosti od oddaljenosti od središča. Količini smo izračunali za točkast delec, medtem ko je delec α jedro helija s polmerom $1,7 \cdot 10^{-15}$ m. Na navpično os smo nanegli razmerji F/F_R in W_p/W_{pR} , če sta F_R sila in W_{pR} potencialna energija na robu oblaka pri $r = R$, na vodoravno os pa r/R .

Rutherford je leta 1911 zapisal: "Da bi pojasnili te in druge izide, moramo privzeti, da gre naelektreni delec v atomu skozi močno električno polje. Gibanje tega delca obravnavamo za vrsto atoma, ki ga sestavlja osrednji električni naboj, zbran v točki in ki ga obdaja enakomeren krogelni naboj drugega znaka enake velikosti." Tako je v fiziko stopilo *atomsko jedro*.

Sila med naelektrenima delcema in potencialna energija. Na točkast delec z nabojem $Z_1 e_0$ deluje delec z nabojem $Z_2 e_0$ in polmerom R z odbojno silo

$$F = \frac{r}{R} F_R \quad \text{pri } 0 < r < R \quad \text{in} \quad F = \frac{R^2}{r^2} F_R \quad \text{pri } r > R.$$

$F_R = Z_1 Z_2 e_0^2 / 4\pi\epsilon_0 R^2$ je sila na robu naboja pri $r = R$.

Električna potencialna energija je

$$W_p = \left(\frac{3}{2} - \frac{r^2}{2R^2} \right) W_{pR} \quad \text{pri } 0 < r < R \quad \text{in} \quad W_p = \frac{R}{r} W_{pR} \quad \text{pri } r > R.$$

$W_{pR} = Z_1 Z_2 e_0^2 / 4\pi\epsilon_0 R$ je potencialna energija na robu naboja pri $r = R$. Za delec α je $Z_1 = 2$ in za atom zlata $Z_2 = 79$. Atom zlata ima polmer $1,44 \cdot 10^{-10}$ m, jedro zlata z relativno atomsko maso 197 pa $6,40 \cdot 10^{-15}$ m. Poenostavljeno smo vzeli, da je delec α točkast, medtem ko ima jedro helija polmer $1,7 \cdot 10^{-15}$ m.

Odbojna električna sila na robu jedra je $(1,44 \cdot 10^{-10}/6,4 \cdot 10^{-15})^2 = 5 \cdot 10^8$ -krat večja od sile na robu atoma, ki bi ga enakomerno izpolnjeval enak pozitivni električni naboj. Električna sila na robu atoma, ki bi enakomerno izpolnjeval pozitivni električni naboj, ne more znatno odkloniti hitrega delca α . Velik odklon delca pri prehodu skozi kovinski listič lahko pojasni le velika sila na veliko manjšem jedru. Potencialna energija na robu jedra je $1,44 \cdot 10^{-10}/6,4 \cdot 10^{-15} = 2,3 \cdot 10^4$ -krat večja od potencialne energije na robu atoma, ki bi ga enakomerno izpolnjeval pozitivni naboj. Negativnih elektronov ni treba upoštevati, ker imajo zelo majhno maso in jih delec α z veliko kinetično energijo brez težave odrine iz atoma. Pri tem se samo malo zmanjša njegova kinetična energija.

Delec α , za katerega je Rutherford ugotovil, da se giblje s hitrostjo $v_0 = 2,09 \cdot 10^7$ m/s in ima maso $M = 4 \cdot 1,6 \cdot 10^{-27}$ kg, se odbije od jedra zlata, ko se mu približa do najmanjše razdalje središč r_0 . V tej razdalji je potencialna energija enaka kinetični energiji: $Z_1 Z_2 e_0^2 / 4\pi\epsilon_0 r_0 = W_k = \frac{1}{2} M v_0^2$. Pri tem vzamemo, da ostane jedro pri miru. Dobimo

$$r_0 = \frac{Z_1 Z_2 e_0^2}{4\pi\epsilon_0 W_k} = 2,5 \cdot 10^{-15} \text{ m}.$$

Izid je pokazal, da je jedro veliko manjše od atoma. Z današnjim podatkom za jedro zlata bi se delec α zapičil v jedro.

Spočetka niso poznali števila elektronov v atomu in so ga precenjevali. Rutherford je po prehodu delcev α skozi tanek listič zlata sklepal, da je v atomu zlata sto (namesto 79) elektronov in ima jedro zlata sto (namesto 79) pozitivnih osnovnih nabojev. Nekateri so trdili, da je število elektronov v atomu enako polovici relativne atomske mase. Pozneje so uvideli, da število elektronov v atomu in število pozitivnih osnovnih nabojev v jedru določa *vrstno* ali *atomsko število*, to je zaporedno številko elementa v periodni preglednici.

Rutherford je spočetka dopustil možnost, da so elektroni razporejeni po vsem atomu in mirujejo. Z Osončjem so atom začeli primerjati pozneje. Tedaj so se zavedali pomanjkljivosti modela. Elektroni v atomu z jedrom ne morejo mirovati in njihovo gibanje je pospešeno, saj je tudi enakomerno kroženje pospešeno gibanje. Pospešeno se gibajoči naelektreni delec pa seva in s tem izgublja energijo. Zaradi sevanja bi se zmanjševala energija atoma, elektroni bi se približali jedru in nazadnje padli vanj.

Na to, da so atomi sestavljeni, bi lahko sklepali že po periodni preglednici elementov, ki jo je sestavil Dimitrij I. Mendelejev leta 1869. Če obstaja veliko različnih delcev, ki veljajo za osnovne, in jih je mogoče razvrstiti v urejeno preglednico, ti delci niso osnovni, ampak sestavljeni. Spoznanja ne moremo imeti za zakon narave, a se je doslej obneslo. Uporabili so ga pri atomskih jedrih, ki jih sestavljajo *protoni* in *nevtroni*, in pri protonih, nevtronih in sorodnih delcih, ki jih sestavljajo *kvarki*. Po izkušnjah z atomi nas ne preseneti, če nekateri fiziki že domnevajo, da so tudi kvarki sestavljeni, čeprav za to nimajo trdne eksperimentalne opore.

Fiziki so se znašli v zagati, saj so atomi obstojni. Rešitev je ponudil nov način razmišljanja. Max Planck je leta 1900 sevanje črnega telesa, to je telesa, ki absorbira vse vpadno sevanje in ki od vseh teles pri dani temperaturi najmočneje seva, pojasnil z nenavadno zamisljo. Sevanje izmenjuje energijo s steno telesa le v obrokih, *energijskih kvantih*, ki so jih pozneje imenovali *fotoni*. Arthur Erich Haas z Dunaja leta 1910 in John William Nicholson iz Londona in Oxforda leto zatem sta med prvimi poskusila po novem pojasniti gibanje elektronov v atomu. To je uspelo leta 1913 Nielsu Bohru, ki je bil od vsega začetka prepričan, da gibanja elektronov v atomih ne bo mogoče pojasniti po starem, *klasično*. V klasični elektrodinamiki naelektreni delci sevajo elektromagnetno valovanje s frekvenco, ki se ujema s frekvenco njihovega kroženja ali nihanja. Bohr se je naslonil na Planckovo *kvantno* zamisel in privzel, da v vodikovem atomu elektron lahko kroži okoli jedra samo po krogih z določenim polmerom, ko ima določeno energijo. Seva le, ko z enega od krogov preide na manjši krog in pri tem razliko energij prevzame foton. S tem je dosegel, da se je frekvenca izsevane svetlobe razlikovala od frekvence kroženja elektronov. Bohrov podvig bi morda kazalo opisati posebej drugo leto ob devetdesetletnici. Za zdaj se zadovoljimo s spoznanjem, da atome sestavljajo elektroni, jedra in močno električno polje med njimi.

Okvirni razvoj spoznanj o zgradbi atomov je opozoril na to, da se je zamisel o osrednjem delu atoma pojavila, ko še ni imela eksperimentalne opore. V fiziki danes ne zavržemo takih zamisli, kakor je zahteval Mach, zavedamo pa se, da jih merjenja ne podpirajo. Dokončno sprejememo samo tisto, kar podpirajo merjenja. K spoznanju, da sestavljajo atome elektroni in jedra je prispevalo veliko več fizikov, kot smo jih omenili. Njihovi koraki so šli v različne smeri in pogosto se je šele po daljšem času pokazalo, kateri so uspešni.

Janez Strnad

EVARISTE GALOIS (1811–1832) – Svetli komet na matematičnem nebu 19. stoletja

Tragično zgodbo norveškega matematika Nielsa Henrika Abela, opisano v prejšnji številki Preseka, malodane vsi pisci zgodovine matematike 19. stoletja primerjajo s temno usodo drugega matematičnega genija tistega časa, Francoza Evarista Galoisa. Njuni kratki življenji sta se časovno deloma pokrivali, delovala sta v veliki meri na istih matematičnih področjih, oba sta umrla zelo mlada. Toda Abela je ubila revščina, Galois pa je umrl po neumnem. Padel je v dvoboju, star komaj enaindvajset let in pol. Te dni (31. maja) mineva 170 let od njegove smrti.



Evariste Galois se je rodil na obrobju Pariza, v kraju Bourg-la-Reine, kjer je bil njegov oče Nicolas-Gabriel Galois župan. Evaristova izobražena starša sta bila brez matematičnega talenta, je pa sin po njiju podedoval nespravljlivo mržnjo do tiranije. Kaže, da je imel srečno otroštvo.

Dvanajstleten se je Galois vpisal na licej Louis-le-Grand v Parizu. Dotlej ga je, v nekoliko ekscentričnem filozofskem duhu, poučevala mama Adelaïde-Marie Demante. Ker se na liceju ni hotel podvreči trdi disciplini, ki sta jo v času restavracije šolam vsilili oblast in Cerkev, je kljub bistrosti veljal za problematičnega učenca.

V šoli se je pravzaprav prvič srečal z matematiko. Toda ni ga zanimala algebra, kakršno so tedaj poučevali v šolah, prevzela ga je Legendrova Géométrie. Petnajstletnik jo je na dušek preštudiral in nadaljeval z branjem Lagrangejevih del, s čimer si je pridobil solidne matematične osnove. Ob vzpodbudi odličnega učitelja matematike Louis-Paul-Emila Richarda je odkril svoj matematični talent. Ko je bil star 17 let, je začel študirati najnovejša dela iz teorije enačb, teorije števil in teorije eliptičnih funkcij. Redno šolsko delo je puščal ob strani. V ta čas sodi tudi njegov prvi objavljeni članek, v katerem je dopolnil neki Lagrangeov rezultat o verižnih ulomkih.

Ne da bi poznal Abelove rezultate, je leta 1828, podobno kot Abel osem let pred njim, najprej napak verjel, da je za splošno algebrsko enačbo pete stopnje našel rešitev z radikali. Hitro je uvidel svojo zmoto, nadaljeval s teorijo algebrskih enačb na povsem novih osnovah, dokler ni

uspešno pojasnil splošnega problema z uporabo teorije grup. Dobljene rezultate je maja 1829 predložil francoski akademiji znanosti. Ocenil naj bi jih zanje najprimernejši razsodnik, Augustin Cauchy.

Sledili so dogodki, ki so izničili blesteči začetek in pustili globoke sledi v osebnosti mladega matematika. Najprej je njegov oče, preganjan in zintrigiran zaradi svojega liberalnega delovanja, v začetku julija 1829 napravil samomor. Mesec kasneje je Galois padel na sprejemnem izpitu za École polytechnique, ker je pri matematičnem delu izpita odklonil, da bi odgovarjal na način, ki so ga zahtevali izpraševalci. Ko je tako izgubil upanje, da bi nadaljeval šolanje na šoli z visokim znanstvenim ugledom in liberalno tradicijo, materi velikih francoskih matematikov, se je prijavil na École préparatoires, današnjo École normale supérieure, ki je vzgajala bodoče srednješolske učitelje. Novembra 1829 je bil na šolo sprejet predvsem zaradi odlične ocene iz matematike pri sprejemnem izpitu.

Približno tedaj je Galois iz Bulletin des sciences mathématiques izvedel za nedavno Abelovo smrt in, kar je pomenilo nov udarec, da Abelov zadnji objavljeni članek vsebuje precej rezultatov, ki jih je on sam, kot originalne, predložil akademiji v oceno. Cauchy je Galoisu svetoval, naj svoje delo popravi, tako da bo upošteval Abelove raziskave nasploh in tudi njegove najnovejše rezultate. Tako je nastal nov tekst, ki ga je Galois predložil akademiji februarja 1930, upajoč, da bo zanj prejel veliko nagrado akademije za tisto leto. Toda delo se je nesrečno izgubilo, ko je njegov ocenjevalec, to pot Joseph Fourier, nenadoma umrl. Nepričakovano odstranjen iz natečaja za nagrado je bil Galois prepričan, da gre za načrtno preganjanje, tako s strani uradne znanosti kot družbe nasploh. Nekaj rezultatov iz izgubljenega dela, ki so se mu ohranili v zapiskih, je aprila 1830 objavil v Bulletin des sciences mathématiques in nato do junija še dva članka. To dokazuje, da je kljub smoli, ki ga je spremljala, kot matematik že stopal iz anonimnosti.

Buržoazna revolucija julija 1830, ki je pometla z Bourboni in ustoličila Louisa Philippa, je ostro vplivala tudi na Galoisovo življensko pot. Evariste se je strastno zagrizel v politiko, seveda na strani republikancev. Čedalje teže je prenašal strogo disciplino na École préparatoires, ki je dijakom prepovedovala udeležbo na demonstracijah, objavil v opozicijskem časopisu divji članek proti direktorju šole – in bil decembra 1830 iz šole izključen.

Prepuščen sam sebi je Galois večino svojega časa posvetil politični propagandi ter sodeloval v demonstracijah in neredih, ki so tedaj pretresali Pariz. Do neke mere je nadaljeval tudi matematično delo. Objavil je

krajši članek iz analize in daljši članek o pouku naravoslovja. Na Poissonovo pobudo je v naglici napisal novo verzijo svoje razprave o reševanju algebrskih enačb in jo januarja 1831 predložil akademiji. Poisson je o tem najpomembnejšem Galoisovem delu poročal v začetku julija. Menil je, da del prikazanih rezultatov lahko najdemo v nedavno posmrtno objavljenih Abelovih člankih, ostanek pa je nerazumljiv. Globoko nepravilna ocena, kot se je izkazalo kasneje, je lahko samo še zakrknila mladega Galoisa v njegovi upornosti.

9. maj 1831 je pomenil začetek konca. Galoisa so aretirali, ker je v zdravici na banketu republikancev zaželel smrt kralju, a ga je dober odvetnik izvelkel iz zapor. Med republikanskimi demonstracijami ob obletnici francoske revolucije 14. julija istega leta je bil Galois ponovno aretiran in pridržan v zaporu Sainte-Pélagie, kjer je v neprimernih razmerah nadaljeval z matematičnimi raziskavami. Popravil je svojo razpravo o reševanju algebrskih enačb in se ukvarjal z uporabo svoje teorije ter z eliptičnimi funkcijami. Marca 1832 so ga zaradi grozeče nevarnosti epidemije kolere preselili v bolnišnico. Tam je v svobodnejšem ozračju, tudi z možnostjo izhoda, urejeval svoja matematična dognanja, napisal nekaj esejev o filozofiji znanosti in se zapletel v ljubezensko afero, katere nesrečni razplet je njega in njegov ponos hudo prizadel. V nerazjasnjenih okoliščinah, ki so sledile tej zgodbi, je bil izzvan na dvobojo.

V slutnji bližnje smrti je Galois 29. maja, na predvečer dvoboja, napisal nekaj obupanih pisem svojim republikanskim prijateljem, hlastno uredil svoje matematične zapiske, namenjene akademiji, in prijatelju Augustu Chevalierju napisal oporočno pismo, tragični dokument, v katerem je poskušal skicirati glavne rezultate svojih najnovejših matematičnih dognanj. Zavedajoč se pomembnosti svojih zadnjih odkritij, je prosil Chevalierja, naj pismo izroči ali Gaussu ali Jacobiju. Ne v potrditev pravilnosti rezultatov, ampak v oceno njihove vrednosti za razvoj matematike. Ob zori, 30. maja, je bil v dvoboju smrtno ranjen. Prepeljali so ga v bolnišnico, kjer je naslednjega dne umrl. Njegov pogreb 2. junija je bil priložnost za republikanske demonstracije, predhodnico krvavih nemirov naslednje dni v Parizu.

Kaže, da se noben od Galoisovih sodobnikov ni zares zavedal vrednosti dela mladega matematika. Cauchy, ki je bil sposoben dojeti njegov pomen, je videl le prve orise, saj je kot vnet pristaš Bourbonov že septembra 1830 zapustil Francijo. Nekaj člankov, ki jih je Galois še za življenja objavil, ni nudilo dovolj vpogleda v njegovo delo, še posebej ne v teorijo algebrskih enačb, ki jo je zavrnil Poisson. Tudi objava slovitega oporočnega pisma septembra 1832 ni pritegnila zaslužene pozornosti. Kolikor je znano, pismo nikoli ni prišlo niti do Gaussa niti do Jacobija.

Šele septembra 1843 je Joseph Liouville, ki je pripravljaj Galoisove rokopise za objavo, uradno obvestil francosko akademijo, da je Galois v oporočnem pismu dejansko rešil problem o določitvi vseh enačb, ki jih lahko rešimo z radikali.¹ Kljub temu sta delo, ki je bilo 1931. leta predloženo Poissonu, in članek o rešljivosti primitivnih enačb z radikali izšla šele jeseni leta 1846 v *Journal mathématiques pures et appliquées*.

Tako je šele štirinajst let po Galoisovi smrti matematični svet izvedel za najpomembnejša odkritja mladega matematika, ki so nato bistveno vplivala na razvoj moderne matematike. Teorija grup, ki jo je Galois razvil za reševanje problema algebrskih enačb, je bila ključ do moderne algebre in moderne geometrije. Danes velja Galoisova teorija in njen povezujoči princip za enega najvidnejših dosežkov v matematiki 19. stoletja. Seveda se njene razlage v Preseku še zdaleč ne moremo dotakniti.

Marija Vencelj

POVEZANA KRIPTARITMA

Rešite kriptaritma

$$\begin{array}{rcccccc} & G & A & U & S & S & \\ + & E & U & L & E & R & \\ \hline & 6 & 8 & 0 & 0 & 3 & \end{array}$$

$$\begin{array}{rcccccc} & E & U & L & E & R & \\ + & H & E & R & O & N & \\ \hline & 7 & 1 & 6 & 7 & 7 & \end{array}$$

tako, da v obeh nadomestite enake črke z enakimi desetišskimi števki, različne z različnimi. (Odgovor je na str. 364)

Marija Vencelj

ROJSTNE LETNICE PETIH MATEMATIKOV

Pred 180 leti so hkrati živeli: norveški matematik Abel, nemška matematika Gauss in Jacobi ter francoska matematika Cauchy in Galois.

Tistega leta so bili vsi skupaj stari 127 let. Skupna starost prvih treh je bila tedaj 83 let, zadnji trije so bili skupaj stari 62 let. Poiščite njihove rojstne letnice. (Odgovor je na str. 364)

Marija Vencelj

¹ V zapisu o Abelu v prejšnji številki Preseka smo izvedeli, da se je s tem problemom ukvarjal že Abel, a je delo na njem prekinil zaradi slovitega matematičnega dvoboja z Jacobijem.

KRIŽANKA “OB 200-LETNICI ROJSTVA VELIKEGA M

				OBARVANI OPISI SE NANAŠAJO NANJU	KOLIČINA TEKOČINE, KI SE NAENKRAT POGOLTNE	ZASUK OBRAT	SMETARSKI REKVIZIT	GIBANJE PO RITMU GLASSE	ČLANEK O NJEM JE BIL OBJAV- LJEN V PRESEKU 5	LJUDSKA PRITR- DILNICA	RASTL KI DA O
				RAZBUR- LJIVO DOGAJANJE OKOLI ČESA					REVIJA		
				PODALJŠAN SLONOV SEKALEC					NJEGOVA VEJA MATE- MATIKE PROSTOR ZA VSTOP		
				PADLI BOREC						PEVEC BONJOVI	
				OČAK IZ BIBLIJE						DRŽAVA NA SV AFRIKE	
NOVA MED- NARODNA NAGRADA ZA MATE- MATIKO	PESNIK GRADNIK	GLAVNA ARTERIJA							ŠVICARSKI POLITIK (ADOLF)		
		GORE Z LISTIČI NA KLOBUKU							OPRAVI- ČENJE		
AMERIŠKI DRAVATIK, SATRIK (EDWARD)						IZBOR SLOV. POPEVKE	TRNEK (KNJIŽNO)				
				PRIMEK NJEGOVE ZAROČENKE			KONEC ŠAHOVSKE IGRE				
PRVI POBUDNIK NAGRADE, IMENOVANE PO NJEM				BODEČA RASTLINA					POKLIC OČETA		
PRESTOL- NICA NJEGOVE DOMOVINE					TENISAČ SAFIN				UREDNIKA NA POP TV (ALENKA)		
					KRILNI DEL ZGRADBE						NA OBEI PLO NOR FOS
JOŽE TOPORIŠIČ		NASPROTJE ROTORJA								SOL DUŠKA- STE KISLINE	
		IGRALNA PLOŠČICA S PIKAMI								MAMILO IZ MAKI	
GRADBENI POKLIC						RAZVALINA RUŠEVINA	CERKVENI DOSTOJAN- STVENIK				
STAREJŠA SLOVENSKA ROKOMETNA REPREZENTANTKA SONJA							SLOV. VESLAČ (IZTOK)				TOPE SKI V
UMETNO USNJE							IGRALEC NEWMAN				GOŠ DUŠE
BRIT. REŽISER MENDES				LOČEN PROSTOR V VAGONU					MEHKO KOSMATENO USNJE		
				PRITOK VISLE					PLAVALČ THORPE		
IME NORV. PRESTOL- NICE V NJEGOVEM ČASU											
NADLEŽEN IZPUŠČAJ, MOZOLJ					POTREBA, SILA					ČE JE KOMUTA- TIVNA, SE IMENUJE PO NJEM	
IGRALEC MARAIS					HRAŠKI PEVEC VITASOVIČ					UMRLJ SLOV. JAZZOVSKI TROBENTAC (PETAR)	

¹ Preberite članek v prejšnji številki Preseka.

MATEMATIKA”¹

INA JE	JEGULJI PODOBNA RIBA GRUJ	ITAL RELIGIOZNI SLIKAR (GUIDO)	NIELS BOHR	IME LADJARJA ONASSISA	MODEL AVTA ZNAMKE HYUNDAI	AVTOR MARKO BOKALIČ	IZMIŠLJENO IME	ROKOME- TAŠICA ČEČKOVA	KRAJ MED POREČEM IN NOVI- GRADOM	POKOJNI SLOV. IGRALEC (DARE)	NJEGOV PRVI UČITELJ MATEMATIKE	STAR CITROENOV MODEL
						PREVELIKA POPUST- LJIVOST KOMU PRI NAPAKAH						
						TEHNIČNA SMUČAR. PANOGA						
						ČEBELJI SAMEC						
			OBRVNA- VAL JE ELIPTIČNE									
			OSEBA IZ KEKCA									
				SLOVAŠKA REKA					GENEARL MOTORS			NEMŠKI SKLADATELJ (WERNER)
				MESTO, KJER JE DELOVAL								
	PO PENINI POZNANO IT. MESTO JV OD RIMA	PRIDELEK, LETINA										
		ZVEZA DRŽAV JV AZIJE										
		SLOVAŠKO GOROVJE										
					SLIKARSKA DELA/NICA	ZVON, KI OZNANJA SMRT						
						OBOŽEVAN VZORNIK MLADIH						
ZID JENA SCA												
MAN TER						VELIKI TRAVEN				KONSTANTIN FEDIN		
						PRČJA OČESNA GUBA				NJEGOV NEMŠKI TEKMEC		
	BULDOŽER											
	ŠOSEDI CRKE G						PLANŠAR (NAREČNO)					
L ALP- ETER					LIZA MINNELI			MORSKA RIBA Z ZELO SPLOŠČENIM TELESOM	RDEČA BARVA KART			
TEJŠA NA JED								POHOD V GORE				
		OGNJEK LASNEGA MEŠIČKA TVOR	NEW- YORSKA TISKOVNA AGENCIJA	REDKO MOSKO IME					KRAJ NAD VIRPAVKO DOLINO			
				SLOV. IGRA- LEC (IVO)					PEVSKI ZLOG			
	BOLEZEN, KI GA JE POKOPALA											
	RAJKO GERIC											
					KOVINSKA VPONKA							
					OČE				VELETOK NA INDIJSKI PODCELINI			

ZALIVSKI TOK SLABI

Morski tokovi nastanejo predvsem zaradi razlike v gostoti morske vode, ki nastane zaradi razlik v temperaturi in slanosti. Poleg tega nastajajo morski tokovi zaradi vetrov in nekaterih manj pomembnih vplivov.

Od južne obale Floride teče iz Mehiškega zaliva v smeri proti severovzhodu zelo močan morski tok, imenovan Zalivski tok. Pri rtu Hateras, to je pri 35° severne širine, ima hitrost $2,5 \text{ m/s}$, pretok pa je $80 \text{ milijonov m}^3/\text{s}$. Jugovzhodno od Nove Funlandije se razcepi tako, da del teče proti vzhodu, del pa nadaljuje pot proti severovzhodu in ogreva severni del Atlantika, zlasti severno obalo Skandinavskega polotoka. Voda, ki se ob dotiku s polarnim ledom ohladi, se zaradi povečane gostote potopi in se z globinskimi morskimi tokovi vrača nazaj proti jugozahodu, kjer se segreje in dviga ter krepi Zalivski tok. Vzhodna veja se pred špansko obalo obrne proti jugu, nato pa v loku zavije proti zahodu in ponovno prečka Atlantski ocean. Pred Velikimi Antili se tok razcepi. Južna veja teče skozi Karibsko morje v Mehiški zaliv, kjer zavije proti severovzhodu, severna pa teče ob Zahodni Indiji proti jugu Floride, kjer se obe veji združita in napajata glavno vejo Zalivskega toka. (Zemljevid morskih tokov v severnem Atlantiku najdete na II. strani ovitka; op. ur.)

Na smer morskih tokov odločilno vpliva Coriolisova sila, ki nastaja zaradi vrtenja Zemlje in deluje na telo, ki se po površini Zemlje giblje premočrtno. Ta sila, ki je usmerjena pravokotno na smer hitrosti, je enaka

$$F = 2m\omega v \sin \varphi, \quad (1)$$

kjer je m masa telesa, ω kotna hitrost vrtenja Zemlje, v vodoravna relativna hitrost telesa glede na površino Zemlje in φ geografska širina. Na severni polobli je usmerjena proti vzhodu, če se telo giblje proti severu, če se telo giblje proti vzhodu, je usmerjena proti jugu. Zato Zalivski tok teče proti severovzhodu in ne proti severu, kot ga poganja razlika v gostoti vode. Globinski morski tok hladne vode pa iz podobnega razloga teče proti jugozahodu in ne proti jugu.

Zaradi Coriolisove sile ne more nastati morski tok, ampak le sprememba smeri gibajoče se točke. Ker je Coriolisova sila usmerjena pravokotno na smer hitrosti, se zaradi nje prosto gibajoča točka navidezno giblje približno po krožnici. Od krožnice odstopa na eni strani zaradi morebitne spremembe velikosti relativne hitrosti, na drugi strani pa zato, ker se jakost Coriolisove sile spreminja z geografsko širino. Ta odstopanja so posebno velika v bližini ekvatorja. Zaradi Coriolisove sile je v vsakem od treh oceanov severno od ekvatorja velik morski vrtnec v smeri urinega kazalca, južno od ekvatorja pa v nasprotni smeri.

Vzemimo primer Zalivskega toka ob jugovzhodni obali Floride, kjer otok Grand Bahama preprečuje, da bi se tok usmeril proti vzhodu. Pri 26° severne širine ima tok smer proti severu in pretok 30 milijonov m^3/s , kar da masni pretok $M = 30$ milijonov t/s . Zanima nas, kolikšna bočna Coriolisova sila odpade na meter toka.

Maso vode, ki se pretaka na razdalji enega metra, dobimo tako, da sekundni pretok M delimo s hitrostjo v . Torej je

$$m = \frac{M}{v}.$$

Zaradi kroženja Zemlje okrog Sonca se Zemlja v enem dnevu zavrti okrog svoje osi nekaj manj kot za en obrat. Če upoštevamo, da je na 100 let 24 prestopnih let, uvidimo, da v 365,24 dneva Zemlja obkroži Sonce. V tem času se zavrti 366,24-krat, zato za en obrat potrebuje 86 164 sekund. Kotna hitrost ω je enaka

$$\omega = \frac{2\pi}{86\,164\,\text{s}} = 0,000072921\,\text{s}^{-1}.$$

Pri naši oceni seveda ne potrebujemo tako natančne vrednosti za kotno hitrost. Iz (1) izhaja, da je iskana sila enaka

$$F = 2M\omega \sin \varphi = 1918\,\text{kN/m}.$$

Če bi vedeli, kolikšen tok odpade na meter globine, bi lahko ocenili bočni tlak. Grobo oceno dobimo, če vzamemo, da tok sega do globine 400 m in da je v vseh globinah do 400 m enako močan. Potem sila 1918 kN odpade na $400\,\text{m}^2$, kar da tlak približno $4800\,\text{N/m}^2$.

Poglejmo še, za koliko bi se v našem primeru masna točka, ki se premika s hitrostjo $2\,\text{m/s}$ proti severu, zaradi Coriolisove sile v eni minuti pomaknila proti vzhodu, če nanjo ne bi delovale druge sile. Pri majhnih premikih smemo vzeti, da imamo enakomerno pospešeno gibanje, zato je premik p približno enak

$$p = \frac{at^2}{2} = \omega v t^2 \sin 26^\circ = 0,23\,\text{m},$$

kjer je a Coriolisov pospešek, ki je enak $2\omega v \sin \varphi$. V 60 sekundah se točka premakne 120 m proti severu in 0,23 m proti vzhodu. Smer gibanja se spreminja, s tem se tudi smer pospeška spreminja, kar smo pri naši oceni zanemarili.

Med Ferskimi otoki in severno Škotsko je razmeroma blizu gladine hrbet, ki ima 840 m globoko zarezo. Skozi to odprtino teče manjši del

hladnega globinskega morskega toka iz Norveškega morja v Atlantski ocean. Tok skozi to zarezo ima jakost okrog 2 milijona m^3/s . V primerjavi z rekami je to ogromen tok, saj vse reke odvedejo v morja le okrog 1,5 milijona m^3 vode v sekundi. Bogi Hansen in sodelavci ribiškega inštituta v Torshavnu na Ferskih otokih od novembra 1995 na osnovi meritev ugotavljajo količino vode, ki teče skozi omenjeno zarezo. Ocenjujejo, da se ta pretok letno zmanjša za 2 do 4%, in da se je v zadnjih 50 letih jakost severnoatlantske veje Zalivskega toka zmanjšala za 20%.

Zmanjševanje jakosti morskega toka je povezano s splošnim segrevanjem. Količina padavin se večja, izhlapevanje pa se večja predvsem v tropskem in zmernem pasu, v arktičnih predelih se bistveno ne večja. Zaradi povečane količine padavin se tudi rečni dotok sladke vode v arktična morja večja. Tam, kjer je morje stalno pokrito z ledom, so padavine v obliki snega. Če so temperature skozi vse leto pod 0°C , se ta sneg spreminja v led, ki se tali v dotiku z morsko vodo. V zadnjih letih se stali več tako nastalega sladkovodnega ledu, kot ga nastane, saj se z ledom pokrite površine manjšajo, hkrati pa se manjša debelina ledu. Povečana količina padavin in taljenje plavajočega sladkovodnega ledu povzročata zniževanje koncentracije soli in s tem gostote vode v arktičnih morjih. Zato se manjša razlika v gostoti vode v arktičnih morjih in tople vode v ekvatorialnih morjih. Ta razlika pa poganja Zalivski tok.

Ob upoštevanju Coriolisovih sil so z modeli ugotovili, da šibak tok skozi severni Atlantik ne more obstajati. Če bi se jakost toka zmanjšala na 30% prvotne jakosti, bi se po teh ugotovitvah Zalivski tok pri Novi Funlandiji v celoti usmeril proti vzhodu.

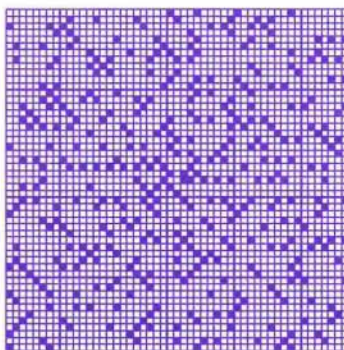
V pleistocenu, ki se je začel pred 1,7 milijona leti in končal pred deset tisoč leti, se je severnoatlantska veja Zalivskega toka nekajkrat nenadoma ustavila, zaradi česar se je del severne Evrope prekril z ledom. Ker z ledom pokrite površine odbijajo več sončne svetlobe, se je poprečna temperatura na Zemlji znižala. Zadnja taka ledena doba se je končala pred približno deset tisoč leti. Tudi v holocenu, ki sledi pleistocenu, se je Zalivski tok nekajkrat upočasnili, kar je povzročilo majhne ledene dobe. V 17. stoletju je na primer Temza v Londonu vsako zimo zamrznila, kar se je v 20. stoletju zgodilo samo enkrat. Sedanje slabitve severnoatlantskega morskega toka zaradi splošnega segrevanja ne občutimo kot ohladiitev, popolna ustavitve pa bi imela hude posledice za severno Evropo, ker bi se kljub splošnemu segrevanju nenadoma močno ohladilo.

Ivan Meško

ULAMOVA SPIRALA

Razporeditvi naravnih števil na (neskončno) kvadratno mrežo, katere osrednji del je prikazan na levem delu spodnje slike, pravimo *Ulamova spirala*.

	37	36	35	34	33	32	31	56
38	17	16	15	14	13	30	55	
39	18	5	4	3	12	29	54	
40	19	6	1	2	11	28	53	
41	20	7	8	9	10	27	52	
42	21	22	23	24	25	26	51	
43	44	45	46	47	48	49	50	



Ime je dobila po matematiku Stanislawu Ulamu (1909–1984), znana pa je predvsem po zanimivem vzorcu, ki ga dobimo, če na njej označimo polja, ki vsebujejo praštevila (ta so na sliki osenčena; glej tudi desni del slike). Pred skoraj tridesetimi leti je bil ta vzorec tudi na naslovnici druge številke prvega letnika Preseka. Več o Stanislawu Ulamu in o, po njem poimenovani, spirali lahko izveste na naslovih

- www-groups.dcs.st-andrews.ac.uk/~history/Mathematicians/Ulam.html
- www.maths.ex.ac.uk/~mwatkins/zeta/ulam.htm
- www.alpertron.com.ar/ulam.htm

Zdaj pa k nalogi. Na kvadratno mrežo vpeljimo koordinatni sistem tako, da se število 1 nahaja na polju $(0, 0)$, število 2 na polju $(1, 0)$, število 4 pa na polju $(0, 1)$. Sprašujem vas,

- (a) katero število se nahaja na polju $(2002, 2002)$ in
- (b) na katerem polju se nahaja število 2002.

Če se vam vprašanji ne zdita dovolj zahtevni, lahko poskusite izpeljati še splošna pravila, s katerimi ugotovimo, katero število je na izbranem polju oz. na katerem polju je dano število.

Martin Juvan

Odgovore najdete na str. 372.

KAKO DELITI SKRIVNOSTI?

Danes že vsi vemo, da imajo informacije enako, včasih celo večjo vrednost kot denar. Zato moramo biti pri dodeljevanju dostopa do informacij samih skrajno previdni. Iz izkušenj vemo, da ni dobro povsem zaupati nobenemu posamezniku, še posebej, če je v njegovih rokah usoda mnogih. Vedno se tudi lahko zgodi, da je uporabnik neupravičeno izključen iz sistema (npr. če izgubi ključ) ali da nepooblaščen uporabnik uspe vdreti v sistem.

V prispevku bomo predstavili nekaj splošnih postopkov za deljenje skrivnosti. Le-ti sodijo med osnovne prijeme za povečanje zaupanja v delovanje informacijskih sistemov. To področje predstavlja enega izmed stebrov moderne kriptografije in je tesno povezano s skrbjo za varno in odgovorno ravnanje s ključi.

Za začetek si ogledjmo nekaj zanimivih primerov deljenja skrivnosti.

Na tajnem projektu dela n oseb, materiali o projektu pa so spravljani v trezorju z več ključavnicami. Dostop do materialov je dovoljen le tedaj, kadar se zbere večina, t.j. več kot polovica oseb. Vsak sodelavec dobi enako število ključev. Koliko najmanj ključavnic je potrebno in koliko ključev mora dobiti vsak?

Predno si pogledate rešitev, poskusite rešiti nalogo za $n = 2, 3, 4, \dots$, nato pa tvegajte z napovedjo, kaj bi utegnila biti dobra spodnja meja za število ključavnic.

Rešitev. Predpostavimo najprej, da nam je ključ uspelo razdeliti tako, kot zahteva naloga, in pogledjmo, kaj znamo ugotoviti o številu ključev. Naj bo $k = \lfloor (n+1)/2 \rfloor$ in $s = \binom{n}{k}$. Potem obstaja natanko s različnih k -elementnih podmnožic $G_1, G_2, \dots, G_s$ oseb, ki delajo na tajnem projektu. Vsaka skupina G_i vsebuje vsaj $n/2$ oseb, zato osebe zunaj te skupine nimajo vseh ključev. Naj bo K_i množica ključev, ki jim manjkajo. Potem nobena izmed množic K_i , $i \in \{1, \dots, s\}$, ni prazna. Skupaj s katerikoli članom skupine G_i pa imajo vse ključ, torej ima vsaka oseba iz G_i vse ključ iz K_i . Naj bo $i \neq j$. V množici G_i obstaja oseba, ki ni v G_j . Ta oseba nima nobenega izmed ključev iz K_j , torej je $K_i \cap K_j = \emptyset$. Ker sta bila i in j poljubna, od tod sledi, da je različnih ključev vsaj s .

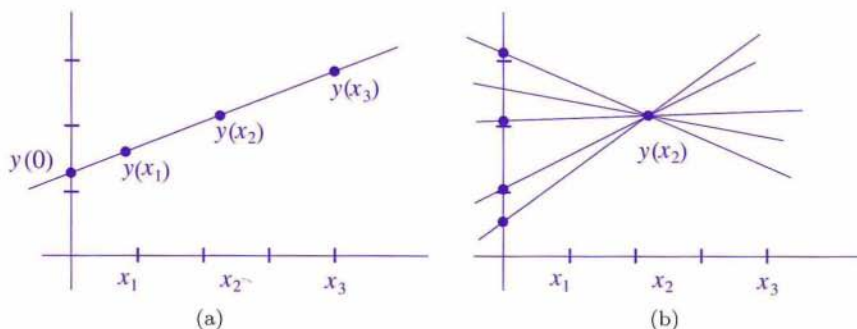
Sedaj pa pokažimo, da je s ključev $k_1, \dots, k_s$ vedno tudi dovolj za rešitev zastavljene naloge. Ključ razdelimo tako, da dobijo ključ k_i natanko vse osebe iz skupine G_i . Tako dobi vsaka oseba $\binom{n-1}{k-1}$ ključev. Le večinska skupina ima neprazen presek z vsemi podmnožicami G_i , tako da lahko le taka skupina odpre trezor.

Najprej smo ugotovili, da mora biti ključavnic vsaj s , nato pa smo našli način, kako dodeliti vsaki osebi $\binom{n-1}{k-1}$ ključev, tako da bodo lahko le večinske skupine odklenile vse ključavnice.

V banki morajo trije direktorji vsak dan odpreti trezor, vendar pa kombinacije ne želijo zaupati nobenemu posamezniku. Zato bi radi imeli sistem, po katerem lahko odpreta trezor poljubna dva med njimi.

Zgornja rešitev nam svetuje ($n = 3$, $k = 2$, $s = \binom{3}{2} = 3$), da nastavimo na trezor tri ključavnice in damo vsakemu direktorju dva ključa (seveda pa nobenemu istega para). Vendar pa lahko v tem primeru vsak direktor odklene dve ključavnici in že s tem bistveno oslabi varnost, npr. za trikrat skrajša čas, potreben za odstranitev ključavnic.

Želimo najti rešitev, pri kateri ne bo imel nihče večjih možnosti kot zunanji vlomilec. Ta problem lahko rešimo z $(2, 3)$ -stopenjsko shemo za deljenje skrivnosti (glej sliko 1). Takšne sheme sta leta 1979 neodvisno odkrila **Blakley** in **Shamir**.



Slika 1. $(2, n)$ -stopenjska shema za deljenje skrivnosti, $n \in \mathbb{N}$. Delivec si v ravnini izbere premico ℓ , ki ni navpična, in za vsako osebo na tej premici izbere svojo točko, ki ne leži na osi y . Za zgornji sliko si izberemo $n = 3$.

(a) Vsaka oseba dobi le koordinato y svoje točke, ki jo shrani, npr. na pametni kartici. Program v trezorju pozna še ustrezne od 0 različne koordinate x , zato lahko izračuna ključ $y(0)$, ki je enak odseku, kjer premica ℓ seka os y . Vsaki dve točki natanko določata premico in s tem ključ.

(b) Če imamo eno samo točko, ne moremo ugotoviti, kateri ključ je pravi, saj so vsi videti enako dobri.

V Rusiji so v 90-ih letih prejšnjega stoletja uporabljali $(2, 3)$ -stopenjsko shemo za kontrolo jedrskega orožja (predsednik, obrambni minister, vrhovni vojaški poveljnik).

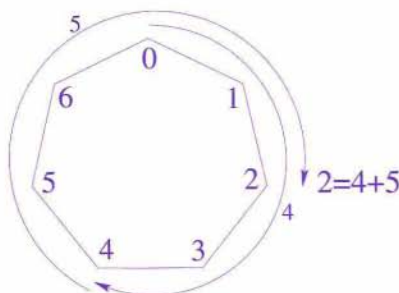
V splošnem je (t, n) -stopenjska shema za deljenje skrivnosti K med n oseb, $2 \leq t \leq n$, metoda, za katero velja:

- poljubnih t oseb lahko izračuna skrivnost K ,
- nobena skupina s $t - 1$ (ali manj) osebami ne more izračunati prav nobene informacije o skrivnosti K .

Sheme za deljenje skrivnosti so vsestransko uporabne. Lahko jih uporabimo povsod, kjer do podatkov dostopamo hierarhično. Tak način dostopa je pogost v velikih podjetjih, bankah in vojski.

Če računamo z običajnimi tipi števil, ki so na voljo v standardnih programskih jezikih, moramo rezultate izračunov zaradi omejene velikosti teh tipov nenehno zaokrožati (posebno ko postajajo števila vse večja in večja ali pa jih delimo). V kriptografiji pa približki ne zadoščajo, zato si za računanje raje omislimo končne množice kot pri številčnici na uri. Tak zgled so kolobarji $\mathbb{Z}_n$, $n \in \mathbb{N}$, v katerih računamo po modulu števila n . Za elemente vzamemo $\{0, 1, \dots, n-1\}$, računamo pa tako, da seštejemo ali zmnožimo dve števili tako, da pravi rezultat nadomestimo z njegovim ostankom pri deljenju z modulum n . Za $n = 7$ npr. velja $4 + 5 \pmod{7} = 2$ in $5 \cdot 4 \pmod{7} = 6$, saj ima vsota 9 ostanek 2 pri deljenju s 7, produkt 20 pa ostanek 6 (glej sliko 2).

Videli smo že, kako z geometrijskim argumentom zasnujemo $(2, n)$ -stopenjsko shemo za deljenje skrivnosti. Poglejmo sedaj, kako konstruiramo (t, t) -stopenjsko shemo za deljenje skrivnosti.



Slika 2. Računanje po modulu 7.

- (1) Naj bo m dovolj veliko naravno število ($m \geq t + 1$), $K \in \mathbb{Z}_m$ (skrivnost) in $\mathcal{P} = \{P_1, \dots, P_t\}$ množica oseb, ki jim želimo razdeliti skrivnost.
- (2) Delivec $D \notin \mathcal{P}$ neodvisno izbere naključna števila $y_1, y_2, \dots, y_{t-1} \in \mathbb{Z}_m$ in izračuna

$$y_t = K - (y_1 + \dots + y_{t-1}) \pmod{m}.$$

- (3) Oseba P_i dobi del y_i , $1 \leq i \leq t$.

Osebe $P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_t$ lahko izračunajo samo $K - y_i$, kar pa jim nič ne pomaga, saj je bilo število y_i naključno izbrano, medtem ko vsi skupaj samo seštejejo svoje dele in razkrijejo skrivnost K .

Shamir je skonstruiral splošno (t, n) -stopenjsko shemo za deljenje skrivnosti za poljubni naravni števili t in n , $2 \leq t \leq n$. Za tako shemo je dovolj, da v $(2, n)$ -stopenjski shemi za deljenje skrivnosti nadomestimo premico s polinomom stopnje $t - 1$, saj je tak polinom določen s t točkami.

Spomnimo se, da je **polinom** spremenljivke x definiran s predpisom

$$f(x) = a_0 + a_1x + \dots + a_nx^n, \quad a_i \in \mathcal{O}$$

kjer je $\mathcal{O}$ neki obseg (npr. $\mathbb{R}$ ali pa $\mathbb{Z}_p$, p praštevilo). **Ničla** polinoma f je taka vrednost $a \in \mathcal{O}$, za katero je $f(a) = 0$.

V praštevilskih kolobarjih $\mathbb{Z}_p$, kjer je p praštevilo, je možno tudi deljenje z vsakim od 0 različnim elementom $a \in \mathbb{Z}_p$. Zato ti kolobarji tudi sodijo med obsege, deljenje je namreč kar množenje z recipročnim elementom. Če le-tega označimo z x , potem velja $a \cdot x \pmod{p} = 1$, zato ga lahko poiščemo kot rešitev diofantske enačbe $ax + py = 1$ z razširjenim Evklidovim algoritmom (glej članek M. Juvana, O Evklidovem algoritmu, *Presek* **21** (1993-94), str. 116-121). Ta enačba je vedno rešljiva, saj sta si a in p tuja.

Izrek 1. Od nič različen polinom stopnje n ima v obsegu največ n ničel.

Zgornji izrek ne velja vedno, če koeficienti polinoma niso iz obsega. V kolobarju $\mathbb{Z}_6$ npr. zgornja trditev ne drži, saj ima kvadratni polinom $f(x) = (x - 1)x$ kar štiri ničle: 0, 1, 3, 4. Za prvi dve ničli potrebujemo prisotnost le po enega faktorja, za zadnji dve pa potrebujemo hkrati oba faktorja. V obsegih je produkt lahko nič le tedaj, ko je vsaj en izmed faktorjev enak nič. Če je a ničla polinoma f , potem nam razcep $x^i - a^i = (x - a)(x^{i-1} + \dots + a^{i-1})$ zagotavlja, da lahko zapišemo $f(x) = (x - a)q(x)$, kjer je q polinom stopnje $n - 1$. Torej se nam za vsako ničlo, ki jo izpostavimo, zmanjša stopnja preostanka za 1 in zato število ničel res ne more preseči stopnje polinoma.

- (1) Naj bo p dovolj veliko praštevilo ($p \geq n + 1$), $K \in \mathbb{Z}_p$ (**skrivnost**) in $\mathcal{P} = \{P_1, \dots, P_n\}$ množica oseb, ki jim želimo razdeliti skrivnost.
- (2) Delivec $D \notin \mathcal{P}$ izbere n različnih elementov $x_1, x_2, \dots, x_n \in \mathbb{Z}_p \setminus \{0\}$ in dodeli del x_i osebi $P_i \in \mathcal{P}$ (vrednosti x_i so lahko javne).
- (3) Za delitev ključa K delivec D naključno in neodvisno izbere $t - 1$ elementov $a_1, \dots, a_{t-1} \in \mathbb{Z}_p$ ter za $i = 1, \dots, n$ izračuna $y_i = a(x_i)$, kjer je

$$a(x) = K + a_1x + \dots + a_{t-1}x^{t-1} \pmod{p},$$

in da del y_i osebi P_i .

Primer. Naj bo $p = 17$, $t = 3$ in $n = 5$. Za javne koordinate x izberimo $x_i = i$, $1 \leq i \leq 5$. Predpostavimo, da osebe P_1, P_3 in P_5 združijo svoje dele, ki so zaporedoma enaki 8, 10 in 11. Če vzamemo $a(x) = a_0 + a_1x + a_2x^2$ in izračunamo $a(1)$, $a(3)$ ter $a(5)$, dobimo sistem treh linearnih enačb v $\mathbb{Z}_{17}$:

$$\begin{aligned} a_0 + a_1 + a_2 &= 8, \\ a_0 + 3a_1 + 9a_2 &= 10, \\ a_0 + 5a_1 + 8a_2 &= 11, \end{aligned}$$

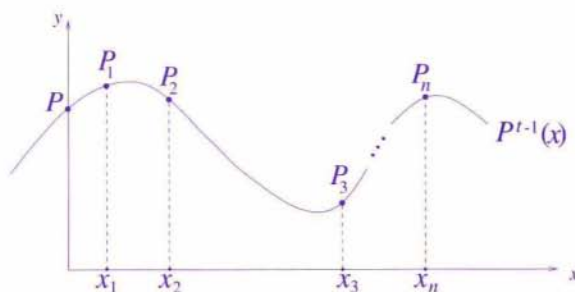
ki ima v $\mathbb{Z}_{17}$ enolično rešitev $a_0 = 13$, $a_1 = 10$ in $a_2 = 2$. Ključ je torej enak $K = a_0 = 13$.

V primeru splošne Shamirjeve sheme osebe $P_1, P_2, \dots, P_t$ določijo ključ K iz enačb

$$y_i = a(x_i) = a_0 + a_1x_i + \dots + a_{t-1}x_i^{t-1} \quad \text{za } 1 \leq i \leq t.$$

S pomočjo metod, ki močno presegajo srednješolsko matematiko, lahko z matrikami in determinantami pokažemo, da ima ta sistem enolično rešitev v $\mathbb{Z}_p$. Drugi način pa je, da si pomagamo s polinomom $p(x)$ stopnje največ $t - 1$, ki ga zna izračunati vsaka skupina t oseb iz svojih delov. Poznamo ga pod imenom **interpolacijski polinom** (glej sliko 3) in ga vpeljemo preko polinomov $p_i(x) = (x - x_1)(x - x_2) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_t)$, t.j. produktov faktorjev $(x - x_j)$ za $j \neq i$:

$$p(x) = y_1 \frac{p_1(x)}{p_1(x_1)} + \dots + y_t \frac{p_t(x)}{p_t(x_t)}.$$



Slika 3. Interpolacijski polinom.

Faktor v i -tem sumandu ob y_i zavzame vrednost 1 za $x = x_i$ in 0 za vsak drug x_j . Z neposrednim računom ugotovimo, da velja $p(x_i) = a(x_i)$, $i = 1, \dots, t$. Od tod sledi, da ima polinom $p(x) - a(x)$, ki je stopnje kvečjemu $t - 1$, vsaj t ničel. Izrek 1 nam potem zagotovi, da je to možno le, kadar sta polinoma $a(x)$ in $p(x)$ enaka. Zato je $K = p(0)$.

Da se prepričamo, da je to res (t, n) -stopenjska shema za deljenje skrivnosti, moramo utemeljiti še, da $t - 1$ oseb ne more izključiti nobenega ključa. Če k $t - 1$ osebam (te poznajo $t - 1$ delov skrivnosti) dodamo za poljubni $a_0 \in \mathbb{Z}_p$ še del $y_0 = a_0$, ki predstavlja vrednost polinoma $a(x)$ v točki $x_0 = 0$, potem z zgornjo formulo zopet dobimo polinom $a(x)$, ki ustreza vsem podatkom, ki so trenutno na voljo.

Ko želi skupina t oseb izračunati ključ K iz svojih delov, pravzaprav ne potrebuje celotnega polinoma $p(x)$, pač pa samo vrednost

$$K = y_1 \frac{p_1(0)}{p_1(x_1)} + \dots + y_t \frac{p_t(0)}{p_t(x_t)}.$$

Od tod se lepo vidi, da je iskani ključ linearna kombinacija delov y_i . $K = b_1 y_1 + b_2 y_2 + \dots + b_t y_t$, kjer je

$$b_i = \frac{p_i(0)}{p_i(x_i)} = \frac{x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_t}{(x_1 - x_i)(x_2 - x_i) \dots (x_{i-1} - x_i)(x_{i+1} - x_i) \dots (x_t - x_i)},$$

torej je bila (t, t) -stopenjska shema za deljenje skrivnosti le poseben primer splošne sheme. Še več, za samo uporabo splošne sheme za deljenje skrivnosti v resnici ne potrebujemo ne računanja interpolacijskih polinomov ne reševanja sistemov enačb, temveč le seštevanje, množenje in deljenje v končnem obsegu.

Nadaljevanje primera. Osebe P_1 , P_3 in P_5 lahko izračunajo b_1 , b_3 , b_5 po zgornji formuli. Če izračunamo recipročne elemente z razširjenim Evklidovim algoritmom, dobimo

$$b_1 = \frac{x_3 x_5}{(x_3 - x_1)(x_5 - x_1)} \pmod{17} = 3 \cdot 5 \cdot 2^{-1} \cdot 4^{-1} \pmod{17} = 4.$$

Podobno izračunamo tudi $b_3 = 3$ in $b_5 = 11$ ter za dele 8, 10 in 11 dobimo

$$K = 4 \cdot 8 + 3 \cdot 10 + 11 \cdot 11 \pmod{17} = 13.$$

Za konec poudarimo, da je varnost Shamirjeve sheme za deljenje skrivnosti *brezpogojna*, t.j. noben ključ ni na podlagi informacij, ki jih imajo nepooblaščen množice, bolj verjeten od drugega. Možne so seveda še razne posplošitve, kot je dodelitev različnih prioritet različnim osebam (npr. za dostop do vojaške skrivnosti sta potrebna dva generala ali pet majorjev), a to je že druga zgodba. Prav tako spadajo v posebno zgodbo tudi kriptosistemi, ki so odvisni od računsko zahtevnih problemov, kot je na primer faktorizacija števil (šifrirne sheme RSA) ali pa diskretni logaritem (ElGamalovi kriptosistemi in digitalni podpis DSA). Več o deljenju skrivnosti si radovedni bralec lahko poišče v učbeniku D.R. Stinsona, *Cryptography – Theory and Practice*, CRC Press, 1995 ali pa na moji domači strani (<http://valjhun.fmf.uni-lj.si/~ajurisic/>).

Aleksandar Jurišić

POVEZANA KRIPTARITMA – Rešitev s str. 349

$$38977 + 29026 = 68003 \text{ in } 29026 + 42651 = 71677.$$

Marija Vencelj

ROJSTNE LETNICE PETIH MATEMATIKOV – Rešitev s str. 349

Abel 1802, Gauss 1777, Jacobi 1804, Cauchy 1789 in Galois 1811. (Za Abela in Galoisa razberemo rojstni letnici in starost iz člankov v tej in prejšnji številki Preseka, nato jih za preostale izračunamo iz podatkov v nalogi.)

Marija Vencelj

NOGOMETNA KOMBINATORIKA –

Rešitev s str. 327

1. $\binom{3}{1}\binom{6}{3}\binom{9}{4}\binom{5}{3} = 75600$.
2. Od vseh možnosti odštejemo tiste brez napadalca (vratarja obravnavamo ločeno): $\binom{3}{1}\binom{6+9+5}{10} - \binom{3}{1}\binom{6+9}{10} = 545259$.
3. $\binom{23}{11} \cdot 11! = 53970627110400$.
4. $\binom{3}{1}\binom{20}{10} \cdot 10! = 2011327713400$.
5. Ločimo glede na število enomestnih in dvomestnih števil na dresu: $\binom{5}{1}\binom{2}{2}3! + \binom{5}{3}\binom{2}{1}4! + \binom{5}{5}\binom{2}{0}5! = 630$.
6. $\binom{24}{4}\binom{20}{4}\binom{16}{4}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2} = \frac{24!}{(4!)^3(2!)^6} \doteq 7.0 \cdot 10^{17}$.
7. $200 = 2 \cdot 70 + 2 \cdot 30 = 2 \cdot 70 + 3 \cdot 20 = 1 \cdot 70 + 3 \cdot 30 + 2 \cdot 20 = \dots = 10 \cdot 20$, skupaj 8 načinov.
8. Kombinacije s ponavljanjem: $\binom{7+3-1}{3-1} = 36$.
9. $\binom{15-2 \cdot 4+4-1}{4-1} = 120$.
10. Naj bo $\mathcal{E}$ množica vseh enajsteric z enim vratarjem, $\mathcal{B} \subseteq \mathcal{E}$ tiste enajsterice, ki vsebujejo vsaj 2 branilca, in $\mathcal{N} \subseteq \mathcal{E}$ tiste, ki vsebujejo vsaj 1 napadalca. Iščemo $|\mathcal{B} \cap \mathcal{N}|$. Z $\mathcal{B}_i \subseteq \mathcal{B}$ označimo enajsterice z natanko i branilci. Naj bo še $\mathcal{X}^c = \mathcal{E} \setminus \mathcal{X}$. Potem je $\mathcal{B}^c = \mathcal{B}_0 \cup \mathcal{B}_1$, $|\mathcal{B}_0| = \binom{3}{1}\binom{14}{10} = 3003$, $|\mathcal{B}_1| = \binom{3}{1}\binom{6}{1}\binom{14}{9} = 36036$ in $|\mathcal{B}| = |\mathcal{E}| - |\mathcal{B}_0| - |\mathcal{B}_1|$. Iz $\mathcal{B}_0 \cap \mathcal{N}^c = \emptyset$ (imamo samo 9 veznih igralcev) sledi

$$\mathcal{B} \cup \mathcal{N} = (\mathcal{B}^c \cap \mathcal{N}^c)^c = ((\mathcal{B}_0 \cup \mathcal{B}_1) \cap \mathcal{N}^c)^c = (\mathcal{B}_1 \cap \mathcal{N}^c)^c.$$

Ker je $|\mathcal{B}_1 \cap \mathcal{N}^c| = 3 \cdot 6 = 18$ (1 vratar, 1 branilec, vsi vezni igralci), je

$$|\mathcal{B} \cup \mathcal{N}| = |\mathcal{E}| - 18.$$

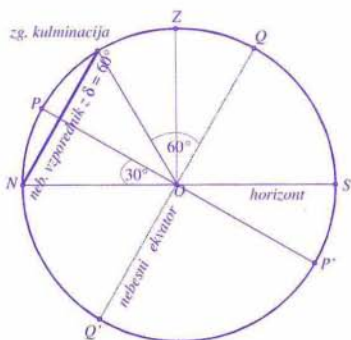
Nazadnje ob upoštevanju $|\mathcal{N}| = 3\left(\binom{20}{10} - \binom{15}{10}\right) = 545259$ dobimo

$$\begin{aligned} |\mathcal{B} \cap \mathcal{N}| &= |\mathcal{B}| + |\mathcal{N}| - |\mathcal{B} \cup \mathcal{N}| \\ &= (|\mathcal{E}| - |\mathcal{B}_0| - |\mathcal{B}_1|) + |\mathcal{N}| - (|\mathcal{E}| - 18) \\ &= |\mathcal{N}| - |\mathcal{B}_0| - |\mathcal{B}_1| + 18 \\ &= 545259 - 3003 - 36036 + 18 = 506238. \end{aligned}$$

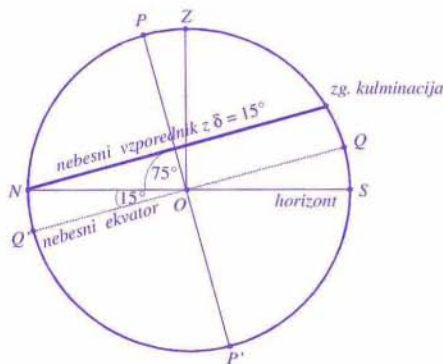
Boštjan Kuzman, Martin Juvan

ZVEZDE, KI SE DOTAKNEJO OBZORJA – Rešitve s str. 350

- 1.a) V krajih na zemeljskem ekvatorju ($\varphi = 0^\circ$) take zvezde ni. Vse zvezde so namreč vzhajalke.
- 1.b) Na severnem zemeljskem polu ($\varphi = 90^\circ$) take zvezde ni. Zvezde namreč navidezno krožijo okrog severnega nebesnega pola (= zenita) vzporedno z obzorjem.
2. Deklinacija take nadobzornice meri 60° (slika 1). Po sliki poskusi opisati navidezno kroženje zvezde.



Slika 1.



Slika 2.

3. Deklinacija take nadobzornice meri 15° (slika 2). S pomočjo slike poskusi opisati navidezno kroženje zvezde.

Marijan Prosen

BINE IN MLEKO

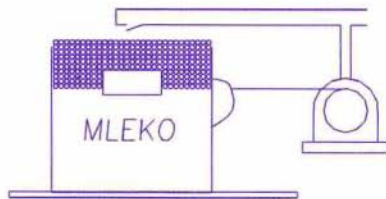
“Slovensko mleko vsebuje dvakrat več mikroorganizmov kot pa mleko v Evropski skupnosti,” je na glas brala Urša in ugotovila. “Dobro bi bilo, da ga prevreva. Bine, praviš, da si izumitelj. Potuhtaj način za čim varnejše vretje!”

Bineta je toplo prešinilo, saj ga potrebuje domovina. Mogoče ne vsa, pač pa le njen del. Tokrat se bo lotil izumljanja s poskusom in ne več z razmišljanjem kot doslej.

Bine torej sedi pred električnim štedilnikom in opazuje lonec z mlekom na ogreti plošči. Ker nima termometra, vtika občasno prst v mleko, da bi nadzoroval rast temperature. Toda mleko je, kot je splošno znano, zahrbtno. Dokler ga opazuješ, se za vretje ne spremeni. Ko pogledaš vstran, izkoristi priložnost, prekipi in se ti porogljivo hihita, ko veselo cvrči po plošči in ti napolni vso kuhinjo ter celo ob odprtem oknu noče ven.

Bine je moder in dobro pozna mlečne ukane. Mleko ga tokrat ne bo prevaralo. Zdaj je že prevroče za prst, torej je nekje na pol poti do vretja. Minute teko. Slednjič se začne gladina dvigati. Bine zasuče gumb grelne plošče na nič. Gladina se dviga še naprej. Bine zgrabi ročaj lonca, zavpije “ajsa” in potegne lonec vstran. Ajsa je bil že preveč in mleko se je prelilo prek roba na vročo ploščo. Vendar pa je iz smradu v kuhinji že vznikal patent številka 1.

Takole bo šlo: Ugotovi, kdaj se mlečne pene približujejo robu! Potegni lonec vstran in lepo v miru ugasni ogrevanje plošče! Morda bi pene dvignile plavač? Plavač bi pritisnil na tipko, sklenil električni krog in pognal elektromotor, ki bi odvedel lonec. Vendar ... pene že ne bodo dvignile ničesar. Zrak v njih nima nosilnosti.



Slika 1. Pene ne dvignejo plavača.

Morda bi si pomagal z električnim očesom? Fotocelica gleda prek lonca lučko. Ko se razpenjeno mleko dvigne med lučko in fotocelico, ta ne vidi več lučke in zavpije motorju, naj vendar odmakne lonec. Pa bo drobna lučka dovolj? Fotocelica še vedno vidi svetlobo, ki prihaja iz okolice, in

izgube drobne lučke niti ne zazna. Morda bi moral vreti mleko po tej metodi v temi? Tedaj bo izguba edine lučke dovolj zaznavna. Spomnil se je, da je bral o infrardeči svetlobi. Televizorju ukazujemo z daljinskim upravljalcem preko infrardečih poblekov. Morda bi porabil infrardečo lučko in čutilo za infrardečo svetlobo? Vendar ... infrardeča svetloba je toplotno sevanje. Vrelo mleko bi bilo najbrž izdatnejši vir infrardeče svetlobe kot drobcena nevidna lučka. Iščimo torej drugačen način, da ugotovimo, kdaj se pene bližajo robu.

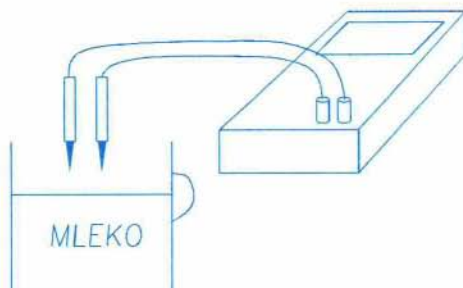


Slika 2. Ko se mleko dviga, električno oko ne vidi več lučke.

Če ne vidim, bom morda slišal? Voda močno brbota, tik preden zavre. Ko vre, je dosti tišja. Bine je spet poskušal zavreti mleko, ki se je medtem že nekoliko ohladilo. Mleko ga je razočaralo. Brez predhodnega protesta mu je hotelo ulti prek roba in Bine ga je komaj spametoval tako, da mu je pridal četrt kozarca hladne vode. Močno je podvomil, da bi Urša odobraval tak varnostni ukrep.

Treba bo najti kaj bolj izvirnega! Smo v dobi elektrike. Čista voda slabo prevaja električni tok. Razne snovi, ki so v vodi raztopljene, ji povečujejo prevodnost. Morda prevaja tudi mleko? Mleko, ki bi se dvignilo in obliko dve elektrodi, bi prepuščalo električni tok. Prepuščeni tok bi pognal elektromotorček, ki bi odmaknil lonec z grelne plošče.

Velja poskusiti. Bine Umnik je poiskal univerzalni inštrument, ga prižgal, naravnal na merjenje upornosti in vtaknil obe priključni elektrodi v mleko. Inštrument je trmasto trdil, da je upornost med elektrodama večja od 200 ohmov, večja tudi od 2 kiloohmov, tudi večja od 20 kiloohmov in celo večja od 200 kiloohmov. Na območju do dveh megaohmov se je inštrument končno odločil in pokazal upornost kak megaohm in pol. Šele napetost 1500 voltov bi potemtakem pognala skozi mleko tok 1 miliampera, ki pa gotovo ne bi zasukal elektromotorčka.

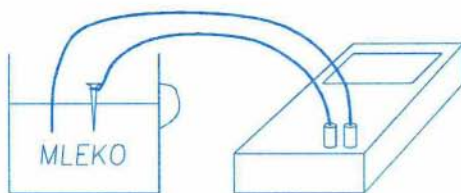


Slika 3. Preverimo, ali mleko prevaja električni tok.

Poskusimo drugače! Bi bilo mleko lahko del galvanskega člena? Zanj potrebujemo dve različni kovini in prevodno tekočino. Tak galvanski člen je že limona, kamor vtaknemo dve žici iz različnih kovin. Pri vretju bi prišlo mleko žicam samo naproti. Porojena električna napetost bi preko primerne sistema odmaknila posodo in ugasnila ploščo. Poskusimo!

Bine je izbral merilno področje 200 milivoltov in vtaknil tipalki v mleko. Številke so poplesovale po zaslonu, vendar se niso mogle zediniti za končno odločitev. Seveda, obe tipalki sta enaki. V galvanskih členih uporabljamo dve različni kovini.

Bine je brskal po škatlah. Na mizi so se znašli žebelj, bakrena žica, kovanec, pocinkan vijak in nož iz nerjavnega jekla. Zdaj so rezultati boljši. Kateri par bo najboljši? Kaže, da sta bakrena žica in pocinkan vijak rekorderja. Skupaj zmoreta napetost malenkost več od 1 volta.



Slika 4. Mleko, žica in vijak so galvanski člen.

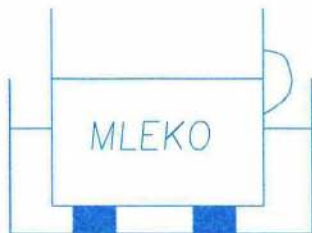
V galvanskih členih uporabljamo kislino in ne mleka. Morda bi bilo kislo mleko boljše. Bine hitro ugotovi, da to ne drži. Tudi če bi, komu pa je do zavretega kislega mleka?

Celo vodovodna voda zagotavlja bakreni žici in pocinkanemu vijaku enako napetost. Bine je poskusil vodi doliti nekoliko kisa, pa se napetost ni povečala. Očitno obe kovini vladata.

Bine je poiskal svinčnik in risal patent številka 1. Namesto ene od obeh žic uporabi lahko kar kovinski lonec. V lonec s hladnim mlekom sega bakrena žica, vendar ne doseže gladine. Ko se tik pred zavretjem gladina dvigne in omoči žico, se med žico in loncem pojavi električna napetost. Bi lahko ta napetost prižgala vsaj drobno lučko? Lučka ni gorela. Bine je ponovno meril napetost. Vsakokrat, ko je vključil lučko, je napetost izginila neznano kam. Končno se mu je posvetilo! Njegov napetostni vir ima veliko upornost, takole, kakšnih milijon ohmov. Lučka z upornostjo nekaj deset ohmov je skoraj kratek stik in napetost se sesede.

Zdaj ve, zakaj je treba vodo okisati. Taka voda bolje prevaja! Tudi sama bakrena žička ima le majhno površino, potopljeno v tekočino. Zato njegov napetostni vir sicer daje napetost, ne zmore pa skoro nikakršnega toka.

Bine zna premalo elektronike, da bi lahko nadaljeval. Rojeva se patent številka 2. Plošča bo grela vodo, voda bo grela mleko. Ko voda zavre, njena temperatura ne raste več, ampak se zaradi izparevanja ustavi pri vrelišču. Uporabil bo dvojni lonec, kakršne so nekdanje uporabljali mizarji, da ne bi zasmodili kleja.

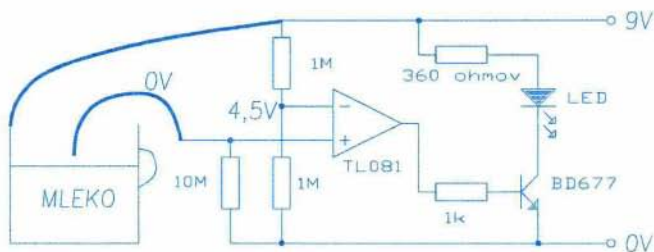


Slika 5. Mleko dobi telesno stražo v obliki lonca z vodo.

Hitro sta na grelni plošči dva lonca. V večjem je voda, pa tudi drugi lonec z mlekom. Ura teče, temperatura raste, raste pa tudi Binetova nestrpnost. Slednjič voda brbota, gladina mleka pa le rahlo valovi. Tudi po petih minutah ostaja slika enaka. Bine je srečen, pa ne dolgo.

“Ugotovil si, kar ve vsaka dobra kuharica,” oceni patent številka 2 Urša. Bine se vnovič posveti razmišljanju. Mikroorganizmi te lahko okužijo. Rane zavarujemo pred okužbo tako, da jih speremo z alkoholom. Zakaj bi torej mleko sploh vrel, če ga lahko razkuži. Alkohol je v slivovki. Če zalije mleko s slivovko, ga s tem razkuži in ga lahko varno pije. Juhu, patent številka 3! Urši pa novega dognanja ni razkril, ker ga gotovo ne bi odobraval.

Bine je spet zavozil. Prav bi bilo, da mu pomagamo pri elektroniki. Vrnimo s k prvemu patentu. Primerno vezje kaže slika 6. Najprej potrebujemo vezje, ki bo ugotovilo, kdaj je treba lonec odstaviti. Uporabimo komparator, nekakšno tehtnico, ki zna primerjati dve električni napetosti. Med obema zaporedno povezanimi uporoma po 1 Mohm, ki sta priključena na napetost 9 V, je napetost 4,5 V. To napetost opazuje zgornji vhod komparatorja. Spodnji vhod komparatorja je preko upora 10 Mohmov povezan s spodnjo žico, kjer je napetost 0 V. Tak odnos vhodnih napetosti zagotavlja komparatorju izhodno napetost 0 V.



Slika 6. Ko se mleko dvigne, preseže napetost na spodnjem vhodu napetost na zgornjem vhodu. Izhodna napetost komparatorja odpre tranzistor. Lučka posveti. Lučko lahko nadomesti elektromotorček.

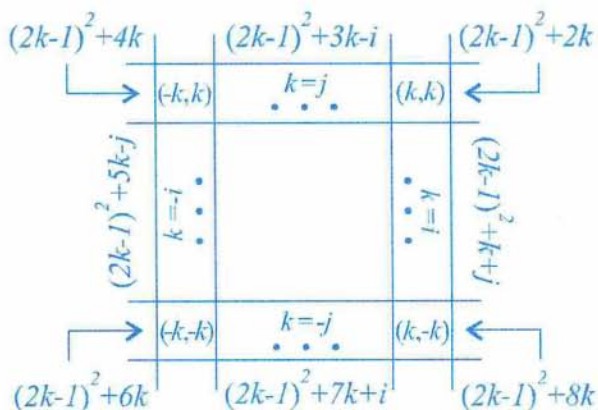
Kipeče mleko, ki doseže konico žice, pomeni povezavo komparatorjevega vhoda z napetostnim virom 9 V preko upora 1 do 2 Mohma. Zato zraste napetost na tem vhodu vsaj do 7,5 V. To je več kot napetost 4,5 V na zgornjem vhodu. Izhod komparatorja se dvigne proti vrednosti napetostnega vira, ki je v našem primeru 9-voltna baterija. Komparator pa je le pametno vezje in nima dovolj moči, da bi poganjalo elektromotor. Zato njegovo odločitev povemo močnostnemu tranzistorju preko upora za 1 kohm. Majhen tok, ki steče na račun komparatorjeve izhodne napetosti 9 V skozi tranzistorjevo bazo v emitor, lahko povzroči do nekaj stokrat večji tok na progi preko tranzistorjeve gornje elektrode, ki ji pravimo kolektor. Na sliki vidimo svetlečo diodo, ki lepo sveti že pri toku 10 mA. Namesto nje bi lahko vključili elektromotorček. Zanimivo bi bilo izračunati, kako močan naj bo, da spravi lonc stran dovolj hitro, recimo v 10 sekundah. Do podatka, kako veliko silo potrebujemo, bi morali priti s poskusom. Uporabimo lahko silomer. Ne smemo pa pozabiti, da je treba motorček tudi ustaviti. Ni pričakovati, da bo stik med mlekom in žico prekinjen ravno tedaj, ko bo lonc zapustil grelno ploščo. Elektronskemu vezju bi bilo treba torej še marsikaj dodati.

Binetova zamisel pa sploh ni dobra. Vleči lonec z vroče plošče je prav nerodno. Raje bi spremljali rast temperature v mleku z električnim termometrom. Ko temperatura doseže vrelišče, je prepozno, da bi reševali mleko. Toplota, nakopičena v grelni plošči, ga bo pogнала preko roba, čeprav gretje izključimo. Bolje bo, če grejemo s polno močjo do, denimo, 90°C , nato grelno moč zmanjšujemo. Moč v plošči je sorazmerna razliki med izmerjeno temperaturo in temperaturo, ki jo želimo doseči. Bliže smo želeni temperaturi, manjša je torej moč gretja. Tako se vse počasneje bližamo vrelišču in ni nevarnosti, da mleko prekipi. Celotno vezje bo celo bolj preprosto kot pri Binetovem premikanju lonca. Žal naši električni štedilniki ne dopuščajo električnega nastavljanja moči. Vrtimo lahko le gumbe s številkami od 0 do 12 (ali še manj, odvisno od štedilnika).

Jože Pahor

ULAMOVA SPIRALA – Rešitev s str. 357

Kvadrat s središčem na polju $(0, 0)$ in z vogali na poljih $(\pm k, \pm k)$ vsebuje števila od 1 do $(2k+1)^2$. Število $(2k+1)^2$ je v desnem spodnjem vogalu, nad njim pa je število $(2k-1)^2 + 1$ (prvo število, ki ni več v "manjšem" kvadratu). Stranice kvadrata vsebujejo po $2k+1$ števil. V desnem zgornjem vogalu je tako število $(2k-1)^2 + 2k$, v levem zgornjem število $(2k-1)^2 + 4k$, v levem spodnjem število $(2k-1)^2 + 6k$, desno spodaj pa že omenjeno število $(2k-1)^2 + 8k = (2k+1)^2$.



Število, ki se nahaja na polju (i, j) , poiščemo tako, da vzamemo kvadrat, na robu katerega leži polje (i, j) ($k = \max\{|i|, |j|\}$), določimo stranico kvadrata, ki vsebuje to polje (npr. možnosti pri $j \leq i$ sta desna in spodnja: desna nastopi pri $j > -i$, spodnja pa pri $j \leq -i$), nato pa upoštevamo še odmik polja od začetka oz. konca stranice. Tako pridemo do naslednjih formul za število, ki je v Ulamovi spirali zapisano na polju (i, j) :

pogoj	k	pravilo	stranica
$-i < j \leq i$	i	$(2k-1)^2 + k + j$	desna
$j \geq i $	j	$(2k-1)^2 + 3k - i$	zgornja
$i \leq j \leq -i$	$-i$	$(2k-1)^2 + 5k - j$	leva
$j \leq - i $	$-j$	$(2k-1)^2 + 7k + i$	spodnja

Za polje (2002, 2002) lahko uporabimo prvi ali drugi predpis (polje leži na stiku desne in zgornje stranice). Z obema predpisoma seveda dobimo enako vrednost, in sicer

$$(2 \cdot 2002 - 1)^2 + 2 \cdot 2002 = 16\,028\,013.$$

Podobno poteka tudi določanje polja, na katerem je napisano dano število n . Najprej določimo tako število k , da velja $(2k-1)^2 < n \leq (2k+1)^2$. Torej $k = \lceil (\sqrt{n} - 1)/2 \rceil$. Nato pogledamo razliko $r := (2k+1)^2 - n$ in glede na količnik med r in $2k$ določimo stranico, nato pa še lego števila na tej stranici. Tako dobimo naslednja pravila:

pogoj	polje	stranica
$0 \leq r \leq 2k$	$(k-r, -k)$	spodnja
$2k \leq r \leq 4k$	$(-k, -3k+r)$	leva
$4k \leq r \leq 6k$	$(-5k+r, k)$	zgornja
$6k \leq r < 8k$	$(k, 7k-r)$	desna

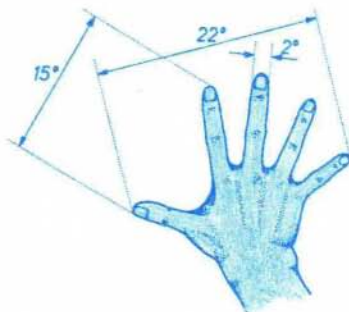
Poglejmo, kaj dobimo pri $n = 2002$. Ker je $43^2 = 1849 < 2002 < 2025 = 45^2$, imamo $k = 22$. Razlika r je enaka $2025 - 2002 = 23$. Iz prvega pravila tako razberemo, da je število 2002 zapisano na polju $(-1, -22)$.

Martin Juvan

ODPRTINA

To, da naša roka lahko služi kot dobra naprava za ocenjevanje kotov (navideznih razdalj) med predmeti na zemljišču ali pa med vesoljskimi telesi na nebu, je dobro znano (slika 1).

Roko (desno ali levo) pa lahko uporabimo še drugače. S palcem in kazalcem naredimo (približno) krožno odprtino, podlahtnico postavimo pravokotno na nadlahtnico in v pravokotni smeri pogledamo skozi odprtino (slika 2). Skozi njo vidimo določen kos pokrajine ali pa neba.



Slika 1. Ocenjevanje kotov z iztegnjeno in razprto roko.

Glej še *Presek* 26 (1998–99), str. 163.

Recimo, da nas zanima, kolikšen kos neba (nebesne polkrogle nad nami) zajamemo s to odprtino. Izmerimo razdaljo r od očesa do odprtine (kar je približno enako dolžini nadlahtnice) in polmer R odprtine. Kvocienent $\frac{\pi R^2}{2\pi r^2} = \frac{R^2}{2r^2}$ pove, kolikšen del polkrogle s polmerom r na njej zajame krožna ploskva s polmerom R oz. kolikšen del neba zajame omenjena odprtina.

Pri sebi sem izmeril $r = 30$ cm in $R = 1,5$ cm. Tako je številčna vrednost kvocienenta $\frac{1,5^2}{2 \cdot 30^2} = \frac{1}{800}$ (za drugo osebo velja drugačen kvocienent).



Slika 2. Pogled skozi odprtino, s katero lahko ocenimo število zvezd na nebu.

Sedaj pa vzemimo, da želimo oceniti število zvezd, ki jih v času našega opazovanja ponoči vidimo na nebu. Skozi odprtino pogledamo na nekaj mestih (na najmanj desetih od obzorja do nadglavišča) jasno zvezdno nebo in vsakič preštejemo število zvezd, ki jih vidimo skozi odprtino. Nato izračunamo povprečno število zvezd, ki jih vidimo skozi odprtino. Končno to število pomnožimo z recipročno vrednostjo kvocienta.

Seveda sem sam naredil to oceno. (No, v bistvu je šlo bolj za igro, ali je to mogoče narediti ali ne.) Skozi odprtino sem pogledal na desetih delih neba. Skozi

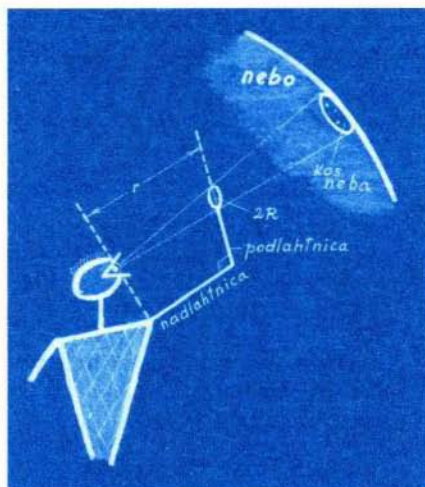
njo sem videl povprečno k zvezd (k je bilo na dve decimalni mesti izračunano decimalno število). Ocenjeno število zvezd na nebu v času mojega opazovanja je torej bilo $k \cdot 800$.

Po mojih ocenah je danes s prostim očesom možno videti na jasnem nočnem nebu le okoli 2000 in ne 3000 zvezd, kot pripovedujejo učbeniki (razlogi: nižinski smog, svetlobna onesnaženost, kerozinska onesnaženost zaradi preletavanja velikega števila letal). Ob obzorju sem naštel zares malo zvezd, raje ne izdam številke. Zgrožen sem, kaj je človek v razmeroma kratkem času (50 let) naredil z ozračjem. Vendar pa se onesnaževanje nadaljuje.

Opazovalna naloga za čas letnih počitnic

Poskusite tudi vi po gornjem načinu (ali pa si izmislite drugačnega) oceniti število zvezd na nebu. Nalogo vzemite bolj za sprostitev v naravi kot resno meritev. Inštrument (roko in oko) imate namreč stalno pri sebi, ustrezni kvocient izračunate doma, za opazovanje pa izberite kristalno jasno noč (če jo najdete) brez mesečine, najbolje nekje v gorah ali pri morju. Pa ne naprezajte se preveč, čeprav boste najbrž kmalu opazili, da celo tako preprosto opazovanje zahteva celega človeka, oz. vzame kar precej časa.

Marijan Prosen



Slika 3. K izračunu kvocienta $\frac{R^2}{2r^2}$.

23. MEDNARODNO MATEMATIČNO TEKMOVANJE MEST – Naloge jesenskega kroga

Prva skupina (prvi del)

1. Dan je štirikotnik $ABCD$ z vzporednima stranicama AD in BC . Naj bo K točka na stranici AB . Skozi oglišče A potegnemo premico p , vzporedno z daljico KC , skozi oglišče B pa premico q , vzporedno z daljico KD . Dokaži, da se premici p in q sekata v skupni točki, ki leži na stranici DC . (4 točke)
2. Klara je izračunala produkt prvih n naravnih števil, Valerija pa produkt prvih m sodih naravnih števil, pri čemer je $n, m \geq 2$. Dobili sta enak rezultat. Dokaži, da se je vsaj ena od njiju zmotila. (4 točke)
3. Klemen sumi, da sta dva od štirih kovancev v njegovi roki ponarejena. Ve, da so mase pravih kovancev enake in mase ponarejenih kovancev enake, pri čemer je masa ponarejenega kovanca manjša od mase pravega kovanca. Ali se lahko Klemen z dvema tehtanjema na primerjalni tehtnici prepriča, da je njegov sum utemeljen? (4 točke)
4. Dve skupini petih enakih kroglic, ki se ne stikajo, se gibljeta po skupni premici, pri čemer imajo vse kroglice enako hitrost. Kroglice leve skupine se gibljejo desno, kroglice desne skupine pa levo. Ko se dve kroglici zaletita, se odbijeta po odbojnem zakonu (vsaka se začne gibati v nasprotno smer z enako hitrostjo). Koliko trkov nastopi? (4 točke)
5. V ravnini so dane vsaj štiri točke. Če odstranimo katerokoli izmed teh točk, je preostala množica točk zrcalno simetrična preko neke premice. Ali je nujno, da je že prvotna množica točk zrcalno simetrična preko kake premice? (4 točke)

Druga skupina (prvi del)

1. Naj bo T oglišče petkotnika. Stranico, katere krajišči nista sosednji oglišču T , imenujmo nasprotna stranica oglišča T . Višina petkotnika je daljica, ki povezuje neko oglišče s pravokotno projekcijo tega oglišča na nosilko njemu nasprotne stranice. Srednjica petkotnika je daljica, ki povezuje oglišče z razpoloviščem njemu nasprotne stranice. Dokaži: Če so vse višine in vse srednjice petkotnika enako dolge, je ta petkotnik pravilen. (4 točke)

2. Znano je, da obstaja 1000 zaporednih naravnih števil, med katerimi ni nobenega praštevila (primer: $1001! + 2, 1001! + 3, \dots, 1001! + 1001$). Ali obstaja 1000 zaporednih naravnih števil, med katerimi je natanko pet praštevil? (4 točke)
3. Dve skupini petih enakih kroglic, ki se ne stikajo, se gibljeta po skupni premici, pri čemer imajo vse kroglice enako hitrost. Kroglice leve skupine se gibljejo desno, kroglice desne skupine pa levo. Ko se dve kroglici zaletita, se odbijeta po odbojnem zakonu (vsaka se začne gibati v nasprotno smer z enako hitrostjo). Koliko trkov nastopi? (4 točke)
4. Po tanki kvadratni piti so posuti trikotni koščki čokolade, ki se ne prekrivajo. Ali je možno pito razrezati na konveksne večkotnike tako, da je na vsakem izmed njih natanko en košček čokolade? (4 točke)
5. Na običajni šahovski deski stojijo tri trdnjave. Bela stoji v spodnjem levem vogalu, rdeča na sosednjem polju na desni in črna na sosednjem polju nad tem vogalom. S trdnjavami lahko vlečemo običajne šahovske poteze, zahtevamo pa, da je v vsakem trenutku za poljubno izbrano trdnjavo v 'njeni' vrstici ali v 'njenem' stolpcu vsaj še ena trdnjava. Ali lahko na ta način trdnjave prestavimo v položaj, kjer bela trdnjava stoji v gornjem desnem vogalu, rdeča na sosednjem polju pod njo in črna na sosednjem polju levo od tega vogala? (4 točke)

Prva skupina (drugi del)

1. Ali obstaja tako zaporedje naravnih števil $a_1 < a_2 < \dots < a_{100}$, da je največji skupni delitelj števil a_{k-1} in a_k večji od največjega skupnega delitelja števil a_k in a_{k+1} , za vsak k , $2 \leq k \leq 99$? (4 točke)
2. Naj bo $n \geq 3$ naravno število. Krožnico razdelimo z $2n$ točkami na $2n$ lokov. Vsak izmed lokov ima eno od treh možnih dolžin, pri čemer sta dolžini poljubnih dveh sosednjih lokov različni. Točke na krožnici izmenično pobarvamo z rdečo in modro barvo. Dokaži, da ima večkotnik, katerega oglišča so rdeča, enak obseg in enako ploščino kot večkotnik, katerega oglišča so modre barve. (5 točk)
3. Naj bo $n \geq 3$ naravno število. V vsako vrstico tabele velikosti $(n-2) \times n$ so vpisana vsa števila $1, 2, \dots, n$ v nekem vrstnem redu. Vemo, da so števila v poljubnem stolpcu tabele paroma različna. Dokaži, da lahko dano tabelo dopolnimo do tabele velikosti $n \times n$, ki ima v vsakem stolpcu vsa števila $1, 2, \dots, n$. (5 točk)

4. Naj bo n naravno število. Pravilni $(2n+1)$ -kotnik z diagonalami, ki se ne sekajo (razen morda v krajiščih), razdelimo na $(2n-1)$ trikotnikov. Dokaži, da so vsaj trije od teh trikotnikov enakokraki. (5 točk)
5. Aleš na prazno šahovnico velikosti 8×8 postavi trdnjavo. Potem zapored dodaja po eno trdnjavo tako, da ta napada liho število trdnjav, ki so že na šahovnici. Največ koliko trdnjav lahko Aleš tako postavi na šahovnico? (6 točk)
6. Nekaj števil je zapisanih v vrsto. Robert izbriše tak par sosednjih števil v vrsti, da je levo število večje od desnega. Nato števili podvoji, ju zamenja in vpiše na prvotni mesti. Dokaži, da lahko Robert opisani postopek ponovi le končno mnogokrat. (8 točk)
7. Vemo, da je 2^{333} 101-mestno število, katerega prva številka je enaka 1. Koliko izmed števil oblike 2^k , kjer je $1 \leq k \leq 332$, ima prvo številko enako 4? (8 točk)

Druga skupina (drugi del)

1. V ravnini ležita trikotnik z rdeče obarvanimi oglišči in trikotnik z modro obarvanimi oglišči. Oba trikotnika imata skupno notranjo točko O , ki je od poljubnega rdečega oglišča oddaljena manj kot od poljubnega modrega oglišča. Ali je možno, da oglišča obeh trikotnikov ležijo na skupni krožnici? (4 točke)
2. Ali obstaja tako zaporedje naravnih števil $a_1 < a_2 < \dots < a_{100}$, da je najmanjši skupni večkratnik števil a_{k-1} in a_k večji od najmanjšega skupnega večkratnika števil a_k in a_{k+1} , za vsak k , $2 \leq k \leq 99$? (5 točk)
3. V polja 8×8 tabele so vpisana števila $1, 2, 3, \dots, 64$ tako, da poljubni zaporedni števili ležita v sosednjih poljih iste vrstice oz. stolpca. Kolikšna je največja možna vsota števil vzdolž diagonale tabele? (6 točk)
4. Naj bo F_1 poljuben štirikotnik. Za $k \geq 1$ naj bo F_{k+1} štirikotnik, ki ga dobimo, če prerežemo F_k vzdolž ene izmed njegovih diagonal, obrnemo enega izmed dobljenih dveh kosov in ga znova prilepimo na preostali kos vzdolž prereza. Največ koliko neskladnih štirikotnikov lahko dobimo na ta način? (6 točk)
5. Naj bosta a in d taki naravni števili, da za vsako naravno število n v desetiškem zapisu števila $a + nd$ najdemo blok zaporednih števk, ki je enak desetiškemu zapisu števila n . Dokaži, da je število d potenca števila 10. (7 točk)

PRESEK — list za mlade matematike, fizike, astronome in računalnikarje — 29. letnik, leto 2001/2002, številke 1–6, strani 1–384

MATEMATIKA

Predalčno načelo (Jože Grasselli).....	4-11
Risanje kock in kvadrov (Peter Legiša).....	134-139
O približkih za število π (Martin Juvan).....	152-153
Modularna redukcija in Mersennova števila (Štefko Miklavič).....	168-170
Število 1 kot vsota in produkt ulomkov (Jože Grasselli).....	198-201
Rezanje in sestavljanje pravilnega četrverca (Nada Razpet).....	233-237
Kristalne mreže – 1. del (Peter Legiša).....	264-269
Ime rože, labirint in pregled grafa (Štefko Miklavič, Martin Juvan)...	292-297
Kristalne mreže, 2. del – Zlaganje krogel (Peter Legiša).....	328-332
Evariste Galois (1811–1832) (Marija Vencelj).....	346-349

FIZIKA

Na sejmu v Otavalu (Jože Pahor).....	12-15
Včasih se s ceste promet močno sliši (Jože Rakovec).....	40-46
Ali steklo teče? (Janez Strnad).....	140-142
Pobliskujoča morska gladina (Andrej Likar).....	154-157
Tlak pojema z višino (Janez Strnad).....	162-167
Brownovo gibanje (Janez Strnad).....	204-209
Merjenje temperature z roko (Andrej Likar).....	220-222
Monokristali (B. Čabrić, A. Janićijević, prev. M. Vencelj).....	226-230
Atomi in Perrinova merjenja (Janez Strnad).....	274-279
Avogadrov zakon (Janez Strnad).....	285-287
Atomi so sestavljeni (Janez Strnad).....	340-345
Zalivski tok slabi (Ivan Meško).....	354-356

ASTRONOMIJA

Astronomske osnove našega koledarja (Marijan Prosen).....	16-22
Kako do enačbe sence? – Rešitve vaj na str. 173 (Marijan Prosen)...	144-148
Bližnji (NEO) asteroid 2001 YB ₅ je v začetku januarja letel mimo Zemlje (Herman Mikuž).....	202
Vsi rekordi Alvana Clarka (Marijan Prosen).....	214-218
Zenitne zvezde – reš. na str. 291 (Marijan Prosen).....	280-284
Zakritje (Marijan Prosen).....	334-337
Zvezde, ki se dotaknejo obzorja – reš. na str. 366 (Marijan Prosen) ..	350-351
Odprtina (Marijan Prosen).....	374-375

RAČUNALNIŠTVO

Zlaganje kovancev – reš. str. 150 (Martin Juvan).....	23
Programski jezik Pascal (Matija Lokar)	24-27
Polkraljice – reš. str. 231 (Martin Juvan).....	158-159
$\sqrt{6} + \sqrt{15}$ je najboljši približek za π (Žiga Ramšak, Janez Brank) ...	171-173
Računanje z velikimi števili – Ubasic (Martin Juvan).....	210-213
Pozabljena naloga (Martin Juvan)	290-291
Rešitev pozabljene naloge – s str. 290 (Marko Petkovšek)	338-339
Kako deliti skrivnosti? (Aleksandar Jurišić).....	358-364

NOVICE

Uvodnik (Marija Vencelj)	II
Čestitka slovenskim mladim fizikom (Iz uredništva).....	15
Quantum prenehal izhajati (Janez Strnad)	30-31
32. mednarodna fizikalna olimpiada (Ciril Dominko)	143
42. mednarodna matematična olimpiada (Matjaž Željko)	149
Norveška ustanavlja Abelovo nagrado za matematiko (Marija Vencelj) .	XVIII
Niels Henrik Abel (1802–1829) – Ob dvestoletnici rojstva (Marija Vencelj).....	259-263

ZANIMIVOSTI – RAZVEDRILO

Ali je miš požrešnejša od slona? (Vida Kariž Merhar)	27-28
Križanka "Lastnosti računskih operacij" – reš. str. 53 (Marko Bokalič) .	32-33
Varnostna žlica (Jože Pahor)	34-37
Igra z dvema "L" (Marija Vencelj).....	III
Povratni rebus – reš. na str. 143 (Marko Bokalič)	133
Kvadriranje dvomestnih števil, ki se začenjajo s 5 – reš. str. 219 (Marija Vencelj)	157
Križanka "Členi računskih operacij" – reš. na str. 177 (Marko Bokalič)	160-161
Zlaganje zemljevida (Marija Vencelj).....	174
Bine izboljšuje avto (Jože Pahor)	175-177
Križanka "Prestizna nagrada" – reš. na str. 237 (Marko Bokalič).....	224
Rebus – reš. na str. 230 (Marko Bokalič).....	XV
Skoraj gotov dogodek – Utrinek (Dušan Murovec).....	258
Binetu je vroče (Jože Pahor)	270-273
Križanka "Matematiki antike" – reš. na str. 299 (Marko Bokalič)	288
Križanka "Ob 200-letnici rojstva velikega matematika" – reš. na str. 379 (Marko Bokalič)	352-353
Bine in mleko (Jože Pahor).....	367-372

NALOGE

Približek števila π – Nagradna naloga (Peter Petek)	2
Geometrijska križanka – reš. na str. 23 (D. M. Milošević)	3
Naloga o luninem letu – reš. na str. 51 (Marijan Prosen)	22
Trikratna ploščina – reš. na str. 31 (Marija Vencelj)	29
Poišči osnovo – reš. na str. 52 (Marija Vencelj)	29
Naloga iz zadnje številke Quantuma – reš. na str. 37 (Janez Strnad)	31
Geometrijski drobiž – odg. na str. 53 (Marija Vencelj)	38-39
Razkrijte vse tajne agente OO7 Njenega Velikanstva –	
Nagradna naloga (Marija Vencelj)	130
Vrtnarjeva naloga – Nagradna naloga (Bojan Mohar)	131-132
Skok na Luno – reš. na str. 223 (Goran Sabolič)	133
Tri škatle – reš. na str. 202 (Marija Vencelj)	151
Prerazporedi števila – reš. na str. 174 (Marija Vencelj)	159
Črke in številke – reš. na str. 209 (Boštjan Jaklič)	170
Tri enice in enajst fizolčkov – Nagradna naloga (Peter Petek)	XIV
Nekaj (ne)resnih o letu 2002 – reš. na str. 218 (Martin Juvan)	196-197
Naloga za maturante – reš. na str. 222 (Dušan Murovec)	197
Ni deljivo – reš. na str. 232 (Dragoljub M. Milošević)	197
Poveži točke – reš. na str. 230 (Marija Vencelj)	197
Tim, Fermat in količniki – reš. na str. 298 (Marija Vencelj)	203
Produkt = vsota – Nagradna naloga (Martin Juvan)	258
Črke in števila 2 - reš. na str. 299 (Boštjan Jaklič)	284
Štiri muhe – Nagradna naloga (Marija Vencelj)	322
Nogometna kombinatorika – reš. na str. 365	
(Boštjan Kuzman, Martin Juvan)	327
Povezana kriptaritma – reš. na str. 364 (Marija Vencelj)	349
Rojstne letnice petih matematikov – reš. na str. 364 (Marija Vencelj)	349
Ulamova spirala – reš. na str. 372 (Martin Juvan)	357

REŠITVE NALOG

Rešitvi nagradnih nalog iz XXVIII, P-5 in P-6 (Iz uredništva)	2
Bine bo žalosten – s str. 34 (Jože Pahor)	50-51
Desetiška – Rešitev iz XXVIII, P-6, str. 324 (Marko Razpet)	52
Rešitev nagradne naloge iz 1. številke (Marija Vencelj)	130
Razkrijte vse tajne agente Njenega Velikanstva – Rešitev nagradne	
naloge s str. 130 (Marija Vencelj)	194-195
Rešitve nagradnih nalog iz 3., 4. in 5. številke Preseka (Marija Vencelj)	322-323
Tri enice in enajst fizolčkov – Rešitev nagradne naloge s str. P-4/II	
(Peter Petek)	323
Produkt = vsota – Rešitev nagradne naloge s str. 258 (Martin Juvan)	323-324
Produkt = vsota – 2. rešitev (Matija Pretnar)	324-326
O vrtnarjevi nalogi (Martin Juvan)	326

NOVE KNJIGE

Tekmujemo v razvedrilni matematiki in logiki (Vladimir Bensa)	47-50
Evropski matematični kenguru 1996 – 2001 (Darjo Felda)	139
J. Cofman: Kaj naj rešujemo? (Martin Juvan)	332-333
J. Strnad: Sto let fizike (Anton Ramšak)	XXIII
M. in S. Prosen: Spoznavajmo Zemljo in vesolje (Marija Vencelj)	XXIV

TEKMOVANJA

37. tekmovanje za Zlato Vegovo priznanje (Aleksander Potočnik)	54-55
21. državno tekmovanje iz fizike za osnovnošolce in osnovnošolke za Zlata Stefanova priznanja (Zlatko Bradač, Mirko Cvahte)	55-57
45. matematično tekmovanje srednješolcev Slovenije (Matjaž Željko)	58-59
39. fizikalno tekmovanje srednješolcev in srednješolk Slovenije (Ciril Dominko)	59-62
1. tekmovanje dijakov srednjih poklicnih šol v znanju matematike (Dušanka Vrenčur)	62-63
1. tekmovanje dijakov srednjih tehniških in strokovnih šol v znanju matematike (Sonja Perko)	63-64
<i>Evropski matematični kenguru (pripravila Gregor Dolinar in Matjaž Željko)</i>	
Naloge za 2. razred osnovne šole	65-66
Naloge za 3. in 4. razred osnovne šole	67-68
Naloge za 5. in 6. razred osnovne šole	69-73
Naloge za 7. in 8. razred osnovne šole ter 1. in 2. letnik srednje šole, kategoriji A in B	73-78
Naloge za 3. in 4. letnik srednje šole, kategoriji A in B	78-82
Naloge za vse letnike srednje šole, kategorija C	83
Rešitve nalog	83
<i>Tekmovanje za Vegovo priznanje (pripravil Aleksander Potočnik)</i>	
36. področno tekmovanje za srebrno Vegovo priznanje – Naloge	84-88
Rešitve nalog s področnega tekmovanja	88-89
36. državno tekmovanje za zlato Vegovo priznanje – Naloge	90-91
Rešitve nalog z državnega tekmovanja	91-92
<i>Tekmovanje dijakov srednjih poklicnih šol (pripravili Anja Jesenek in Dušanka Vrenčur)</i>	
Regijsko tekmovanje – reš. str. 95	93-95
Državno tekmovanje – reš. str. 98	96-98
<i>Tekmovanje dijakov srednjih strokovnih in tehniških šol (pripravili Andreja Leskovar, Iztok Leskovar, Sonja Perko, Irena Pivko)</i>	
Regijsko tekmovanje – reš. str. 104	99-104
Državno tekmovanje – reš. str. 108	106-108
<i>Matematično tekmovanje srednješolcev Slovenije (pripravil Matjaž Željko)</i>	
Izbirno tekmovanje – reš. str. 113	112-113
Državno tekmovanje – reš. str. 119	117-119
Izbirna testa za mednarodno matematično olimpiado	125-126

Rešitve nalog z izbirnih testov za mednarodno matematično olimpiado 126-VII Urnik tekmovanj v letu 2002 (Darjo Felda).....	178-180
21. področno tekmovanje iz fizike za osnovnošolce – reš. str. 185 (Mirko Cvahte, Zlatko Bradač)	181-184
Naloge z regijskega fizikalnega tekmovanja srednješolcev Slovenije v šolskem letu 2000/01 (Ciril Dominko).....	188-192
21. državno tekmovanje iz fizike za osnovnošolce – reš. str. 243 (Zlatko Bradač, Mirko Cvahte)	238-242
Rešitve nalog s predtekmovanja iz srednješolske fizike v šolskem letu 2000/2001 – s str. 188 (Bojan Golli)	247-251
Naloge z državnega fizikalnega tekmovanja srednješolcev Slovenije v šolskem letu 2000/2001 (Ciril Dominko).....	251-256
Rešitve nalog z državnega tekmovanja iz srednješolske fizike v šolskem letu 2000/2001 – s str. 251 (Bojan Golli).....	300-307
22. mednarodno matematično tekmovanje mest – Naloge pomladanskega kroga (Gregor Cigler).....	307-311
22. mednarodno matematično tekmovanje mest – Rešitve nalog pomladanskega kroga s str. 307 (Gregor Cigler).....	311-318
42. mednarodna matematična olimpiada – rešitvi izbranih nalog s str. 149 (Matjaž Željko)	318-320
22. mednarodno matematično tekmovanje mest – Naloge jesenskega kroga (Gregor Cigler).....	376-379

PRESEK

list za mlade matematike, fizike, astronome in računalnikarje
29. letnik, šolsko leto 2001/02, številka 6, strani 321–384

UREDNIŠKI ODBOR: Vladimir Batagelj, Tanja Bečan (jezikovni pregled), Mirko Dobovišek (glavni urednik), Vilko Domajnko, Darjo Felda (tekmovanja), Bojan Golli, Marjan Hribar, Boštjan Jaklič (tehnični urednik), Martin Juvan (računalništvo), Sandi Klavžar, Boris Lavrič, Andrej Likar (fizika), Matija Lokar, Franci Oblak, Peter Petek, Primož Potočnik (novice), Marijan Prosén (astronomija), Marija Vencelj (matematika, odgovorna urednica).

Dopisi in naročnine: DMFA – založništvo, Presek, Jadranska ulica 19, 1001 Ljubljana, p.p. 2964, tel. (01) 4766-553, telefaks (01) 2517-281, št. ŽR 50106-678-47233. Naročnina za šolsko leto 2001/02 je za posamezne naročnike **3.000 SIT** (posamezno naročilo velja do preklica), za skupinska naročila šol **2.500 SIT**, posamezna številka **750 SIT**, tematska številka **1.500 SIT**, stara številka **650 SIT**, letna naročnina za tujino 25 EUR, devizna nakazila SKB banka d.d. Ljubljana, Ajdovščina 4, Ljubljana, SWIFT: SKBAS12X, številka računa 042961.

List sofinancira MŠZŠ
Založilo DMFA – založništvo
Tisk: DELO Tiskarna, Ljubljana

© 2002 Društvo matematikov, fizikov in astronomov Slovenije – 1495

Poština plačana pri pošti 1102 Ljubljana

Janez Strnad: STO LET FIZIKE

Zgodovina fizike sega v antiko in še dlje. Po velikem uspehu v Newtonovem času je veliko zanimanje za znanost in tehniko v viktorijanskem času napovedovalo njun triumfalni razcvet v 20. stoletju. S tem obdobjem se seznanimo ob branju nove knjige profesorja Strnada *Sto let fizike*.

Knjiga obravnava vsa področja fizike 20. stoletja. Tako najprej pokaže ozadje in nastanek splošne teorije relativnosti ter nakaže probleme, ki so odprli pot kvantni mehaniki. Nato preko posplošitve na relativistično kvantno mehaniko bralca privede v svet radioaktivnosti, ki je bila v vzponu v tridesetih letih, in nato na kratko oriše tehnične in moralne težave fizikov pri izdelavi atomske bombe. Po drugi svetovni vojni je bil pomemben razcvet pospeševalniške fizike ter lov za novimi delci, kar je v knjigi lepo prikazano hkrati s prikazom osnov kvantne elektrodinamike.

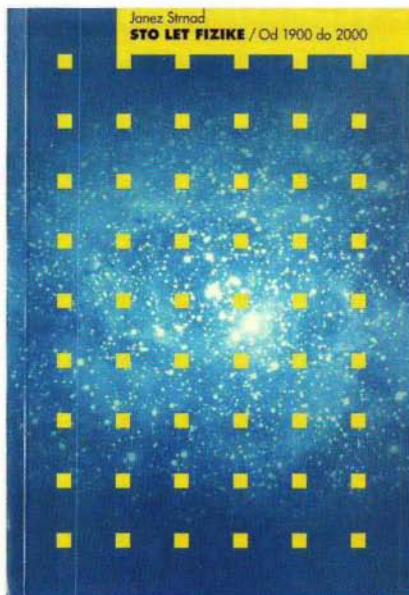
Poleg prikaza osnovnih novih idej fizike nameni avtor tudi nekaj prostora aplikativnim dosežkom, ki so neposredna posledica bazičnih odkritij. Tako na hitro opiše razvoj radia, polprevodnikov, tranzistorja in računalnikov ter laserjev. S področja fizike trdne snovi omeni pojav superprevodnosti in superfluidnosti ter Bose-Einsteinovo kondenzacijo. V zvezi s slednjo tudi napove podelitev Nobelove nagrade za fiziko.

Naslednji razdelki v knjigi so posvečeni astronomiji in astrofiziki, ki sta še posebej v zadnjem delu stoletja z razvojem nove opreme doživeli pospešen napredek. Omenjena so tudi vprašanja kozmologije, ki so prav v zadnjih letih na prvih straneh fizikalnih publikacij. Poleg opisanih standardnih tem omeni avtor še nanotehnologijo, kaotične sisteme, vpliv na biologijo, kratek razvoj fizike mehke snovi in molekularno biologijo. Knjigo zaključijo z ugibanji o prihodnosti fizike in z mnenji nekaterih uglednih fizikov na to temo.

Nova knjiga profesorja Strnada *Sto let fizike* je namenjena širšemu krogu bralcev. Napisana je zanimivo in premišljeno ter v Hawkingovem stilu brez enačb. Zato je dostopna tudi nefizikom, ki jih zanima razvoj moderne znanosti.

Knjigo lahko kupite pri DMFA – založništvo, Jadranska 19, Ljubljana, ali jo naročite po telefonu (01) 4766-553.

Anton Ramšak



Marijan in Stana Prosen: SPOZNAVAJMO ZEMLJO IN VESOLJE

Pri založbi DZS je izšel priročnik za učitelje in vzgojitelje *Spoznavajmo Zemljo in vesolje* avtorjev Marijana in Stane Prosen, ki se že dalj časa ukvarjata s posredovanjem astronomskih vsebin za otroke. Priročnik je bil napisan kot dopolnilo h knjižici *Prvi pogled* (DZS, 1998), pomožnemu učbenišskemu gradivu pri pouku spoznavanja okolja v prvem in drugem triletju osnovne šole, vendar ga bodo lahko koristno uporabili tudi učitelji naravoslovnih predmetov v višjih razredih osnovne šole.

Zvezek velikega formata z 72 bogato ilustriranimi stranmi je razdeljen na šest poglavij, ki prinašajo številne podatke in razlage o nebu, Soncu, Zemlji, Luni, planetih in zvezdah.

Priročnik je zasnovan tako, da se iz njega lahko pouče bralci, ki o Zemlji in vesolju nič ne vedo, pa tudi taki, ki niso povsem nepoučeni, a so jim nekateri podatki ali razlage že ušli iz glave. Čeprav gre za učbeniško gradivo, bi ga zato toplo priporočila tudi staršem ali kar v družinsko branje. Skupni izleti in poletni večeri bodo zanimivejši, z odgovori ne bomo v zadregi.

Delo zaključuje slovarček, pravi mali astronomski leksikon z več kot sto gesli, ki jih srečamo pri pouku naravoslovja, geografije, fizike, izbranih vsebin iz astronomije in ki so, ne nazadnje, del splošne izobrazbe.

Marija Vencelj

