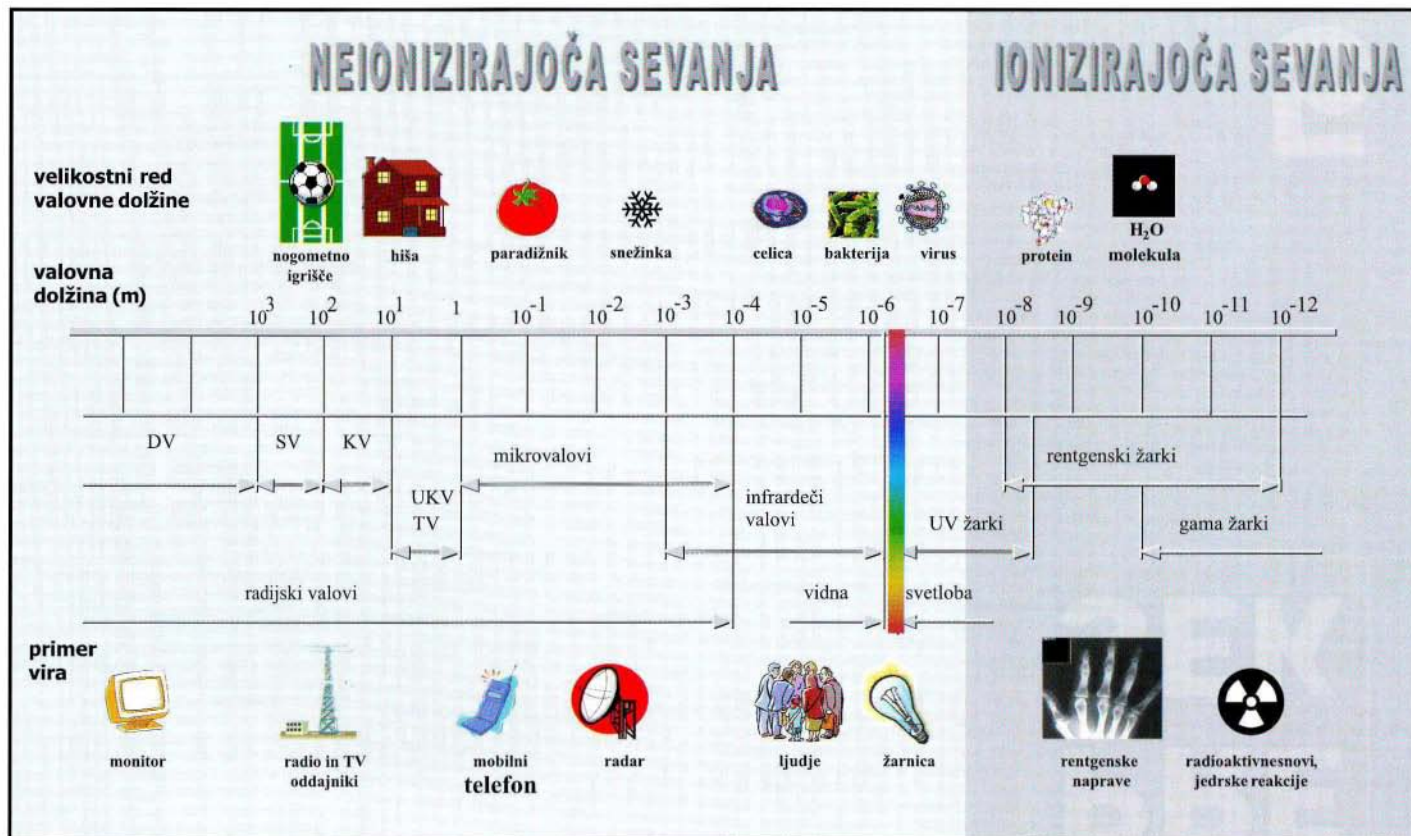


PRE SEK

30 (2002 – 03)

5

ISSN 0351-6652
DRUŠTVO MATEMATIKOV, FIZIKOV
IN ASTRONOMOV SLOVENIJE



Slika 2. Spekter elektromagnetnega valovanja s prikazom posameznih skupin valov, valovnimi dolžinami, primeri virov in predmeti, ki ponazarjajo velikostni red valovnih dolžin posameznih skupin valov.

list za mlade matematike, fizike, astronome in računalnikarje
30. letnik, leto 2002/03, številka 5, strani 257–320

	VSEBINA
MATEMATIKA	Glasba in matematika – 1. del, Tonski sistemi (Marija Vencelj) 267-272 Računala nove dobe, 2. del (Aleksandar Jurišić) ... 290-296
FIZIKA	Oh, to sevanje! (Irena Mele, Metka Kralj, Nadja Železnik) 261-266 Bine dobi pismo (Jože Pahor) 283-287 Še več vodikovih antiatomov (Janez Strnad) 297-298
ASTRONOMIJA	Koliko nebesne krogle – odgovori na str. 300 (Marian Prosen) 281-282
RAČUNALNIŠTVO	Vizualna kriptografija – šum skrivnosti (Martin Pečar) 274-280
ZANIMIVOSTI, RAZVEDRILO	Glorija z Mizaste gore (Matjaž Vencelj) 259-260 Križanka "Mehanika" – reš. na str. 300 (Marko Bokalič) 288-289 S kolikošno hitrostjo? (Marian Prosen) III Poštna znamka o Hallersteinu (Marian Prosen) IV
NALOGE	Z ognjem in smodnikom – Nagradna naloga (Tim Vidmar) 258 Periodični decimalni zapis – reš. na str. 298 (Anton Cedilnik) 260
REŠITVE NALOG	Najkrajši čas potovanja – Rešitev s str. 195 (Karel Šmigoc) 272-273 Krivični tenis – Rešitev s str. 199 (Marija Vencelj) 280
TEKMOVANJA	Rešitve nalog z državnega tekmovanja iz srednješolske fizike v šolskem letu 2001/2002 (Bojan Golli) ... 301-308 23. mednarodno matematično tekmovanje mest – Naloge pomladanskega kroga (Gregor Cigler) ... 308-310 23. mednarodno matematično tekmovanje mest – Rešitve nalog pomladanskega kroga s str. 308 (Gregor Cigler) 311-320
NA OVITKU	Glorija, fotografski motiv, ki te mora najti sam. Preberi tudi zapis na str. 259 (foto Matjaž Vencelj) I Tabela k članku Oh, to sevanje! na str. 261 II

NAGRADNA NALOGA

Urejanje pričujoče številke Preseka smo zaradi urnika tekmovanj morali zaključiti pred potekom razpisanega roka za rešitev nagradne naloge Kriptaritem v različnih številskih sestavih. Zato bomo njeno rešitev in rezultate nagradnega razpisa objavili v 6. številki.

Pred vami pa je že nova nagradna naloga Z ognjem in smodnikom, ki jo je zastavil Tim Vidmar. Izmed reševalcev, ki nam bodo poslali njeno pravilno rešitev, bomo izžrebali nagrajenca, ki bo prejel knjižno nagrado.

Rešitve naloge pošljite najkasneje do 18. aprila na naš naslov:

Presek, Jadranska c. 19, 1001 Ljubljana, p.p. 2964.

Marija Vencelj, odg. ur.

Z OGNJEM IN SMODNIKOM – Nagradna naloga



Pan Michal Wołodyjowski, Mali vitez, nenadkriljivi sabljač in ljubljenelec dam s poljskega dvora, se je znašel v brezizhodnem položaju v gradu, ki ga oblegajo Turki. Pisatelj Sienkiewicz mu je v tradicionalno tragičnem evropskem slogu namenil junaško smrt, v katero bo z razstrelitvijo gradu potegnil tudi sovraga. A Wołodyjowski se ne da. Njegov delodajalec, strašni vojvoda Wisniowiecki, mu je dobavil dovolj smodnika, a le dve vžigalni vrvici. Vrvici sta različni. Skupno jima je le to, da vsaka od njiju gori natanko eno uro, a s povsem neenakomerno hitrostjo. Wołodyjowski je s svojim poznavanjem navad sovraga in

njegove oblegovalne tehnike ocenil, da bodo Turki vdrli v grad natanko čez tričetrt ure. Tedaj naj bi trdnjavo razstrelil. Stavbo lahko požene v zrak le s svojima vžigalnima vrvicama, saj bi se rad s posadko pred eksplozijo pravočasno umaknil na varno. Pomagaj Wołodyjowskemu domisliti, kako naj z vrvicama odmeri tri četrtine ure, da bi maščeval padle tovariše, si zagotovil mesto med nesmrtnimi junaki poljskega literarnega panteona in ostal živ.

Pomni, da vrvici ne gorita s stalno hitrostjo.

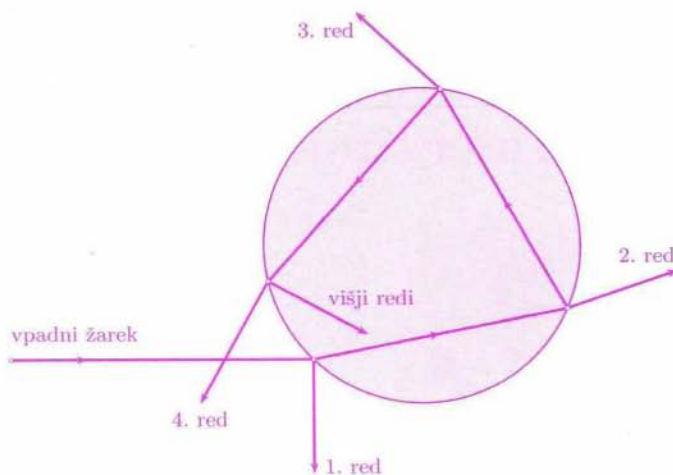
Tim Vidmar

GLORIJA Z MIZASTE GORE

Nenadoma se je pojavila spodaj v megli. Glorija, prelepi naravni pojav, o katerem sem pred trinajstimi leti bral v Preseku, a ga nikoli nisem videl v živo... Tokrat pa se mi je ponudila celo v fotografiranje in zato dobila mesto na Presekovi naslovnici!

Ko smo letos februarja opravljali jedrski poskus na pospeševalniku iThemba Labs pri Cape Townu, smo si privoščili popoldanski izlet na znamenito Mizasto goro sredi mesta. Pot po planoti vrh gore prečka sotesko, ki se zajeda v pobočje. Pogled v vrtoglavo razpoko nas je več kot presenetil. V megli, ki se na tej gori imenuje Namizni prt, ker pogosto kar teče z vrha v dolino, smo zagledali svoje sence, obrobljene z mavričnim krogom.

Podoba nastane na podoben način kot navadna mavrica. Če boste pobrskali po šolskih knjižnicah, boste matematično-fizikalno razlago mavrice našli v prvih dveh številkah sedemnajstega letnika Preseka. Prav na kratko jo pa le ponovimo ob naslednji sliki:



Sončni žarki, ki vstopijo v kapljico vode, se pri vstopu vanjo prvič lomijo, nato se enkrat odbijejo na notranji strani od stene kapljice, nazadnje se lomijo iz kapljice ven. Glede na to, kje vstopijo v kapljico, se lomijo ven pod vsemi koti med 0° in 42° , glede na smer od kapljice proti soncu. Vendar pa se največji del sončnih žarkov, ki padejo na kapljico, lomi ven v smeri med 40° in 42° . Na od sonca obsijanem mokrem nebu zato vidimo svetel lok dobrih 40° od osi skozi sonce in naše oči. Ker pa

ima voda za svetlobo različnih barv različne lomne količnike, se žarki teh barv lomijo pod nekoliko različnimi koti in namesto brezbarvnega svetlega loka nastane mavrica.

Podobno velja za sončne žarke, ki se v kapljici med obema lomoma večkrat odbijejo. Tisti, ki se odbijejo dvakrat, pričarajo drugi mavrični lok, ki ga včasih blede vidimo pri približno 50° na zunanji strani glavne mavrice. Glorijo pa pripravijo žarki še višjega reda, torej taki, ki se še večkrat odbijejo znotraj meglene kapljice, preden se lomijo nazaj ven. Očitno je kot tega mavričnega loka zelo majhen, le nekaj stopinj, saj je velik približno toliko kot človeška senca na nekaj deset metrov oddaljeni megljeni tančici. Če bi bil mavrični kot glorijske večji, bi jo še težje opazili, saj bi se šibki žarki iz odbojev višjega reda povsem izgubili na svetlem nebu.

Ime je glorijska dobila po tem, da jo vedno vidimo okoli svoje sence in zato spominja na svetniški sij. V šali bi lahko rekli, da je to dodaten argument k zgornji razlagi, da je njen pojav tako redek.

Glorijska je vidna tudi pri nas; po tem je znan hrib Kurešček nad Igomo pri Ljubljani. Večkrat jo vidijo tudi potniki iz letala. V tem primeru dobi mavrično obrobo senca letala na oblakih pod njim.

Matjaž Vencelj

PERIODIČNI DECIMALNI ZAPIS



Pozorno pogledjmo

$$\frac{1}{3} = 0.3333 \dots = 0.\overline{3}$$

$$\frac{1}{6} = 0.16666 \dots = 0.1\overline{6}$$

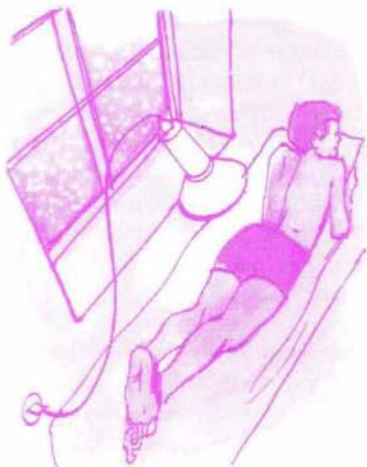
$$\frac{1}{347} = 0.0028818443804\overline{0347}$$

in se vprašajmo: Ali ima še kakšno pozitivno celo število x lastnost, da se njegova obratna vrednost zapiše s periodičnim decimalnim zapisom, v katerem se ponavlja prav x ?

Anton Cedilnik

Rešitev je na str. 298.

OH, TO SEVANJE!



Kaj vse je sevanje?

Sevanje, žarki, radiacija so besede, ki jih v našem vsakdanjem življenju pogosto srečujemo. Včasih nam te besede ponazarjajo nekaj svetlega in zaželenega, nekaj, zaradi česar je življenje lepše. Drugič, predvsem tedaj, ko jih povezujemo s tehnologijo, nam vzbujajo neprijetne občutke. Nekateri te besede povezujejo tudi z idejami, ki so povezane s področjem mejnih znanosti ali celo praznoverja, vendar bomo to pojmovanje sevanja tu pustili ob strani.

Sevanje obstaja, odkar obstaja vesolje. Je normalen del narave in življenja. Svetloba, toplota, radijski valovi, sevanje radioaktivnih snovi, celo zvok so primeri sevanj, s katerimi se srečujemo vsakodnevno. Naše telo je vsak trenutek izpostavljeno različnim virom sevanja. Sevanje prihaja tudi iz vesolja. Sevanje Sonca vsi dobro poznamo in tudi vemo, da je močnejše, čim više gremo. Manj vemo o kozmičnem sevanju, to je toku delcev, ki z veliko energijo priletijo iz globin vesolja v našo atmosfero. Tudi to sevanje z višino narašča. Čim višje v gore se vzpnemo, tem več ga prejmemo; še več, če letimo z letalom.

Sevanje prihaja tudi iz zemeljske skorje. Minerali vsebujejo radioaktivne elemente, ki oddajajo sevanje ob svojem razpadu, zato je sevanje vsakdanji spremljevalec dejavnosti, s katerimi posegamo v globlje geološke plasti. Z njim se srečujemo v rudnikih, v podzemnih jamah, pa tudi mineralne vode in topli vrelci, ki prihajajo iz globin, nosijo s seboj radioaktivne snovi, ki oddajajo sevanje.

Ne nazadnje je vir sevanja tudi človek sam. Oddajamo toploto, sevamo pa tudi zaradi radioaktivnih snovi, ki so prisotne v telesu vsakogar: v kosteh se kopičita radioaktivni polonij in radij, v mišicah se nabirata radioaktivni ogljik in kalij, v naših pljučih se zadržujejo radioaktivni žlahtni plini.

Velika večina teh sevanj je naravnega izvora in je torej del našega naravnega okolja, le zelo majhen del je plod človekove dejavnosti in razvoja tehnologije.

O večini teh pojavov niti ne razmišljamo kot o sevanju. Če govorimo o sevanju, danes večina ljudi pomisli na sevanje radioaktivnih snovi, včasih še na sevanje mobilnih telefonov, računalniških in televizijskih zaslonov ali sevanje v mikrovalovnih pečicah. Na splošno je razširjeno prepričanje, da so sevanja nevarna in zdravju škodljiva. Kaj je res in kaj ni res? Zakaj so nekatera sevanja na tako slabem glasu, za druga pa se niti ne zmenimo? Je strah pred sevanji upravičen ali je plod pretiravanja? Je to posledica dejstva, da za veliko večino sevanj človek nima ustreznih čutil (oči, ušesa, nos, jezik in koža se nanje ne odzovejo)? Zaznamo jih le z instrumenti, brez njih pa ne moremo vedeti, kakšno je sevanje v naši okolici. Ali je razlog za strah morda dejstvo, da o sevanju ne vemo dovolj?

Definicija sevanja ni enolična

Fiziki sevanje opisujejo kot **pojav, pri katerem se energija iz vira širi v obliki delcev ali valovanja**. Sevanje je torej oddajanje in razširjanje valovanja ali delcev in s tem energije v prostor. Vendar uporaba pojma sevanje ni enolična; poleg pojava oddajanja in širjenja valovanja in delcev v prostor se lahko pojem sevanja uporablja tudi za energijo, ki se širi pri tem pojavu.

Od energije valovanja ali delcev, ki jih vir oddaja, je odvisno, kakšen učinek bo sevanje imelo na snov, skozi katero gre ali jo na svoji poti zadene. Če je ta energija dovolj velika, bo sevanje pri prehodu skozi snov iz atomov izbilo elektrone. V snovi se pojavijo ioni in zato taka sevanja imenujemo ionizirajoča sevanja. Sevanja, ki nimajo dovolj velike energije, da bi povzročila nastanek ionov, pa so neionizirajoča sevanja. Kadar govorimo o valovanju, namesto o energiji, raje razmišljamo o valovni dolžini ali pa frekvenci. Obe sta neposredno povezani s količino energije, ki se prenaša z valovanjem. Daljša valovna dolžina in hkrati nižja frekvenca sta značilni za neionizirajoče sevanje. Krajša valovna dolžina in hkrati večja frekvenca pa sta značilnosti ionizirajočega sevanja.



Slika 1. Valovna dolžina λ je razdalja med dvema sosednjima valovnima vrhovoma ali valovnima dolinama. Frekvenca ν je povezana z valovno dolžino z enačbo $c = \lambda\nu$. Enota za valovno dolžino je m, za frekvenco pa s^{-1} ali Hz.

Če je živo bitje izpostavljeno ionizirajočemu sevanju, se tudi v njegovih celicah in v medceličnini pojavijo ioni in prosti radikali, kar ima lahko škodljive učinke. Življenje v okolju, kjer so viri ionizirajočega sevanja, je torej lahko tvegano. Zato so ti viri pod nadzorom.

Vrste sevanj

V grobem lahko sevanja razdelimo na:

- sevanja, pri katerem vir oddaja mehansko valovanje,
- sevanja, pri katerem vir oddaja elektromagnetno (EM) valovanje in
- sevanja, pri katerem vir oddaja delce.

Iz praktičnih razlogov za ta sevanja velikokrat uporabljamo krajše izraze kot elektromagnetno sevanje ali sevanje delcev. Po analogiji lahko tudi oddajanje mehanskega valovanja poimenujemo mehansko sevanje, vendar ta izraz pri nas ni pogost.

Mehansko sevanje

Mehansko valovanje se lahko širi samo skozi snov, zato je mehansko sevanje možno le v mediju, ki je plin, tekočina ali trdna snov. Najznačilnejši in najbolj znan predstavnik mehanskega valovanja je zvok, ki se od vira širi v obliki zgoščin in razredčin. Kot mehansko valovanje zvok za razširjanje nujno potrebuje medij. Brez snovi, po kateri se širi, tudi zvoka ni.

Elektromagnetno sevanje

Elektromagnetno sevanje zajema valovanja zelo različnih valovnih dolžin. Ker med elektromagnetnimi valovi različnih območij valovnih dolžin obstajajo precejšnje razlike, so se za posamezna območja valovnih dolžin uveljavila različna imena, vse skupaj pa imenujemo elektromagnetni spekter (slika na II. strani ovitka):

- radijski valovi (vključno s televizijskimi in mikrovalovi),
- infrardeči ali toplotni valovi (tudi infrardeči žarki ali infrardeča svetloba),
- svetloba (tudi vidna svetloba),
- ultravijolični (UV) žarki (tudi ultravijolično sevanje ali ultravijolična svetloba),
- rentgenski žarki (tudi rentgensko sevanje) in
- žarki gama (tudi gama sevanje).

Poimenovanje območij v spektru ni enolično, ampak se za posamezna območja v pogovornem in strokovnem jeziku uporablja več različnih besednih zvez kot npr. žarki, valovi, sevanje, svetloba (zgoraj že nakazano v oklepajih).

Ultravijolični žarki s krajšimi valovnimi dolžinami, rentgenski žarki in žarki gama se uvrščajo med ionizirajoča sevanja, neionizirajoča sevanja pa so radijski valovi vključno z mikrovalovi, infrardeča svetloba, vidna svetloba in ultravijolična svetloba z daljšimi valovnimi dolžinami.

Razpon valovnih dolžin **radijskih valov** je izredno velik – od več 1000 km do nekaj desetlin mm (dolgi valovi, srednji valovi, kratki valovi, ultrakratki valovi in televizijski valovi, mikrovalovi). **Televizijski valovi** imajo valovno dolžino od 1 do 3 m, **mikrovalovi** pa od desetine mm do 1 m.

Radijske valove oddajajo različne kombinacije in izvedbe anten. Energija, ki jo oddajajo, ni zelo velika, zato zdravju niso posebej nevarni. Zanje človek nima posebnih čutil. Radijski in televizijski valovi so pomembni prenosniki informacij, mikrovalove pa uporabljajo radarji.

Infrardeči valovi imajo valovno dolžino od 1 mm do 0,8 tisočin mm. Oddajajo jih segreta telesa in jih imenujemo tudi toplotni valovi. Z njimi lahko snov segrejemo. Čutilo za toploto imamo v koži, ker pa čutnice niso enakomerno razporejene, so nekateri deli telesne površine za toploto bolj občutljivi, drugi pa manj.

Elektromagnetno valovanje z valovnimi dolžinami od 0,8 do 0,4 tisočin mm človeško oko lahko zazna. Ta del spektra imenujemo **vidna svetloba**. Različne valovne dolžine zaznavamo kot različne barve. Tudi vidno svetlobo sevajo močno segreta telesa. Čim višja je temperatura telesa, tem krajša je valovna dolžina svetlobe, ki jo telo seva. Svetloba z najmanjšimi valovnimi dolžinami je modre in vijoličaste barve. Tudi ta vrsta sevanja za živa bitja ni nevarna.

Elektromagnetno valovanje s še manjšimi valovnimi dolžinami – od 0,4 tisočin do 5 milijonin mm – je **ultravijolično sevanje**. Oddajajo ga telesa pri zelo visokih temperaturah ali nastane ob razelektritvah v plinih. Človeško oko tega sevanja ne zaznava, ker zanj nima ustreznih vidnih pigmentov, nekatere žuželke pa vidijo tudi v ultravijolični svetlobi. Človek nekaj ultravijoličnega sevanja potrebuje, saj pod njegovim vplivom v koži nastaja vitamin D, ki je potreben za vgrajevanje kalcija v kosti. Večje količine takega sevanja so lahko za kožo nevarne, povzročajo opekline, zdravniki pa opozarjajo, da dolgotrajno izpostavljanje temu sevanju lahko povzroči tudi kožnega raka.

Rentgensko sevanje ima zelo majhno valovno dolžino – od 10 milijonin do 1 milijardine mm. To sevanje oddajajo pospešeni elektroni, ki jih zavira polje atomskega jedra težke kovine. Pri tem se del energije izseva v obliki elektromagnetnega valovanja. Tega sevanja živa bitja ne zaznavajo. Ker pa je rentgensko sevanje zelo prodorno in lahko prodre skozi telesno površino do notranjih organov, ga uporabljamo v medicini za slikanje notranjih organov. Mesta v tkivu, ki so gostejša, sevanje bolj zadržijo in na filmu se tam zato pojavi senca.

Sevanje, katerega valovna dolžina je krajša od 1 milijardine mm, imenujemo **sevanje gama**. Nastane tedaj, ko nestabilno atomsko jedro razpade in s tem preide v bolj stabilno obliko. Pri tem se del energije sprosti v obliki elektromagnetnega sevanja gama. Hkrati se spremeni tudi jedro. Pojav imenujemo radioaktivni razpad in je značilen za radioaktivne snovi, ki vsebujejo velika atomska jedra, v katerih število protonov in nevtronov ni uravnovešeno. Sevanje gama nastaja tudi pri jedrskih reakcijah, pri katerih jedra obstreljujemo z delci ali fotoni, ki povzročijo spremembe v jedru. Pri tem jedro lahko izseva tudi enega ali več žarkov gama.

Sevanje delcev

Ob radioaktivnem razpadu nekaterih jeder se poleg elektromagnetnega sevanja gama sproščajo oziroma izsevajo tudi delci – elektroni in helijeve jedra – skupki dveh protonov in dveh nevtronov. Prvo imenujemo **sevanje beta**, drugo pa **sevanje alfa**. Tudi ti dve vrsti sevanja sta ionizirajoči sevanji. Snovi, za katere je značilen radioaktiven razpad, imenujemo **radioaktivne snovi**. Mnoge so prisotne v naravi, lahko pa jih naredijo tudi umetno z obsevanjem v reaktorju ali obstreljevanjem v pospeševalnikih.

Omenimo še **kozmično sevanje**. Kozmični žarki, ki prihajajo do nas iz globin vesolja, so mešanica atomskih jeder (90% protonov – vodikovih jeder, 9,5% helijevih jeder in 0,5% drugih težjih jeder) z zelo veliko energijo. Ob vstopu v našo atmosfero zadevajo ob jedra atomov, ki ozračje sestavljajo in sprožajo različne jedrske pretvorbe. Pri tem nastajajo novi delci, ki kot nekakšni plazovi padajo v spodnje plasti zemeljskega ozračja do zemeljskega površja, nekateri pa prodrejo celo v zemeljsko notranjost.

Koristi in tveganja pri uporabi sevanj

Ker so sevanja že od nekdaj običajen pojav v okolju vseh živih bitij na Zemlji, ni presenetljivo, da se je v razvoju pojavilo mnogo različnih načinov izkoriščanja energije, ki jo sevanje nosi s seboj. Najpomembnejši je gotovo fotosinteza, v kateri rastline lahko izkoristijo svetlobno energijo za izdelovanje organske snovi – sladkorja. Tako rastline zagotovijo hrano

sebi, hkrati pa je fotosinteza neposredno ali pa posredno tudi vir hrane za vsa druga živa bitja na Zemlji.

Dve vrsti sevanja – svetloba in zvok – služita mnogim živalim za medsebojno sporazumevanje in spoznavanje okolice. Mnoge živali svetlobo in zvok zaznavajo in ju tudi oddajajo. Imajo zelo različno občutljive oči; nekaterim zadostuje že zelo malo svetlobe, druge vidijo tudi ultravijolično svetlobo, nekatere ločijo barve, druge ne. Imajo tudi različno občutljiva ušesa; pes na primer sliši bistveno višje frekvence kot človek. Vendar ne človek ne žival ne moreta s čutili zaznati vseh vrst sevanj, ki so prisotna v naravi. Človek je z razvojem znanosti in tehnologije izdelal posebne merilne instrumente, s katerimi je mogoče zaznavati tudi drugovrstna sevanja (sevanje gama ali pa radijske valove).

Razvoj tehnologije ni le razširil spektra sevanja, ki ga lahko zaznavamo, omogočil je tudi koristno uporabo dolgovalovnih in kratkovalovnih elektromagnetnih sevanj, izkoriščamo pa tudi ultrazvok. Z njim je na primer mogoče zelo dobro očistiti kovinske površine, v medicini pa z ultrazvokom tudi preiskujejo notranjost človeškega telesa. Radijski/televizijski oddajnik in radijska/televizijska antena omogočata spremljanje programa, z radarjem je mogoče zaznati predmete, ki so daleč ali v megli, pa tudi mobilni telefoni za prenos informacij izrabljajo radijske valove.

Neionizirajoča sevanja nas v običajnem okolju ne ogrožajo. Pri uporabi ionizirajočih sevanj moramo biti previdni, saj v celicah povzročijo nastanek prostih radikalov, zelo reaktivnih snovi, ki spremenijo delovanje celice. Lahko celo poškodujejo molekulo DNK v celičnem jedru, torej dedno informacijo, ki določa, kaj se bo v celici dogajalo. Prav lastnost, da sevanje poškoduje celico, izrabljamo za uničevanje bakterij in tumorjev. Lastnost, da ionizirajoče sevanje prodira skozi goste in trdne snovi, pa izrabljamo v zdravstvu za preiskave notranjih organov ter v industriji za preiskavo materialov. Če vire ionizirajočega sevanja uporabljamo premišljeno in upoštevamo načela varnega ravnanja z njimi, se nam jih ni potrebno bati.

Svet brez sevanja – mrzel, tih in temen – gotovo ni okolje, kjer bi kdorkoli želel živeti. Pravzaprav to sploh ne bi bilo mogoče. Neionizirajoče in ionizirajoče sevanje nas spremlja od začetka, živa bitja so se razvila ob prisotnosti sevanja. Res je, da sevanja lahko predstavljajo tudi vir tveganja v našem okolju, vendar so dovolj očitne tudi njihove koristi. Proti velikokrat pretiranemu in neupravičenemu strahu pred sevanjem pa se najbolje borimo z znanjem in razumevanjem.

Irena Mele, Metka Kralj, Nadja Železnik

GLASBA IN MATEMATIKA – 1. del

Tonski sistemi



Pred dobrimi štirinajstimi leti sta v Preseku že izšla dva prispevka o izgradnji glasbenih lestvic (Presek XVI, št. 1, str. 12 in št. 2, str. 66). Na številne pobude, naj članka ponatisnemo, sta nastala dva nova zapisa: prispevek o tonskih sistemih in članek o kitari, ki bo izšel v naslednji številki Preseka. Vseeno pa tiste mlade bralce, ki jih tema zanima, vabim, da si ogledajo tudi oba stara članka. Tam boste našli razložen marsikateri osnovni pojem, ki ga bomo tu kar uporabili. Ustrezna Preseka gotovo hrani vaša šolska knjižnica.

Glasba sega v večino področij človekovega udejstvovanja, je del znanosti, umetnosti, kulture, zgodovine, ... Dejansko je to ena najstarejših ved. Tako je npr., bolj kot karkoli drugega, potrjevala Pitagorejce v prepričanju, da je kozmos harmonični prostor, ki mu vladajo števila. Tudi mi bomo nanjo pogledali predvsem z matematičnega vidika.

Vsako nihajoče telo je izvor prostorskega valovanja, ki se širi na vse strani in v vseh snoveh. Človeško uho je sposobno zaznati valovanje zraka v širokem slušnem območju in ga pretvoriti v slušni dražljaj. Prostorsko valovanje v tem frekvenčnem območju imenujemo zvok. Zvočne pojave lahko razdelimo na tone, zvene in šume. Vsi zvoki lahko postanejo glasbeno gradivo, vendar so njeni najosnovnejši zidaki glasbeni toni. *Ton* (čisti ali sinusni ton) je s fizikalnega stališča zvok z natančno določeno frekvenco. Ustvarimo ga lahko le umetno s tonskimi generatorji. Glasbila oddajajo *glasbene tone*, ki so posebna kombinacija čistih tonov. Poleg osnovnega tona s frekvenco f nastopajo v njih še *aliquotni toni*, to so toni, katerih frekvence so večkratniki frekvence osnovnega tona $2f$, $3f$, $4f$ itd. Ton z dvojno frekvenco, pa tudi interval med osnovnim tonom in tonom z dvojno frekvenco, imenujemo *oktava*, interval med tonoma s frekvenco f in $3f$ je *kvinta* v oktavi višje, $4f$ je dvojna oktava itd. *Višina glasbenega*

tona je določena s frekvenco osnovnega tona. Pojav alikvotnih tonov je pomemben faktor, ki odloča o zvočni barvi, to je razliki v zvoku enako visokega tona, ki ga izvajajo različni instrumenti ali glasovi. Teoretično bi sicer lahko zveneli vsi alikvotni toni dane osnovne frekvence. Toda to bi zagotovo povzročilo neznosno disonanco. Dejansko pa intenziteta višjih alikvotov naglo in pri različnih instrumentih različno hitro pada. Res. Na nekaterih instrumentih je težko zaznati več kot tretji alikvot (npr. pri kitari), violine in oboe pa imajo nasprotno močne visoke alikvotne tone, ki jim dajejo svetel ton. Flavte in frule imajo šibke višje alikvote. Nadalje ima klarinet močne lihe alikvote, zaradi česar ima votel zvok.

Kako neizmerno je zvočno gradivo, ki ga ponujajo glasbeni toni, pove podatek, da sega naše slušno območje od 16 Hz (ali s^{-1} , to je nihajev v sekundi) do 20 000 Hz. Pri tem smo v občutljivejšem delu tega območja sposobni med seboj ločiti tona, ki se razlikujeta za vsega 1 Hz. Zato se je že davno pokazala potreba uvesti v glasbo določeno enotnost in red, med drugim izbrati omejeno množico tonov, s katerimi bi gradili melodije. Nastali so razni *tonski sistemi* s svojimi *glasbenimi lestvicami*, ki predstavljajo izbor možnih tonov v okviru ene oktave.

Poznamo različne tonske sestave, ki so bili v različnih zgodovinskih obdobjih in različnih kulturah različno pomembni. Tako v religiozni kot zabavni **indijski glasbi** je oktava neenakorazmerno razdeljena na 22 intervalov - šrutov, lestvice pa so pet ali sedemtonske z dodatno četrtonsko delitvijo.

V **kitajski glasbi** je izrazita pentatonika brez poltonov (glasba na petih tonih) obvladovala melodije tako nekoč kot danes. Sam pojav pentatonike in vztrajanje pri njej sta odraz kitajskega odnosa do sveta. Kitajska glasba je zadržana, zgoščena in hladna, kar v znatni meri izhaja iz pentatonike; izražati hoče splošna čustva, ne individualnih. Njeno sistematiko je utemeljil že filozof Fohi pred 5000 leti. Tako kot Pitagorejci je bil tudi on prepričan, da je glasba odmev harmonije vesolja in zato, tako kot vesolje, temelji na sistemu števil. Zanj je bilo najpopolnejše število pet, ki se ujema s številom t.i. starih planetov (Merkur, Venera, Mars, Jupiter, Saturn) kakor tudi s številom glavnih elementov, iz katerih je sestavljen svet.

Zahodna glasba zadnjih treh stoletij uporablja tone kromatične tonske lestvice, ki ima oktavo razdeljeno na 12 *poltonskih intervalov*. Če začnemo s C, so njeni toni poimenovani takole:

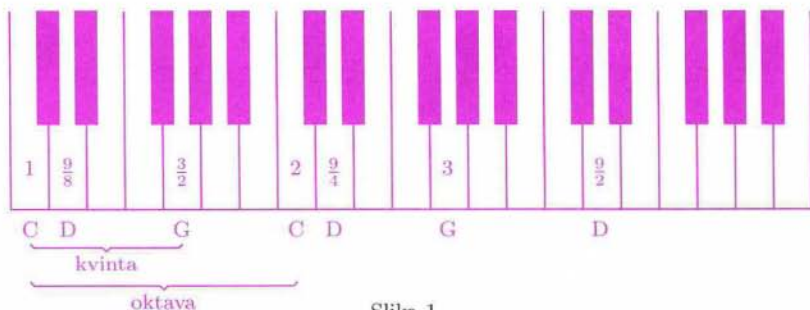
C, Cis(Des), D, Dis(Es), E, F, Fis(Ges), G, Gis(As), A, Ais(Hes), H

Nato se ponovi C, toda oktavo višje, in z njim vsa lestevica. To se nadaljuje navzgor in navzdol vse do mej slušnega območja. Srednji C, to je c^1 , osnovni ton prve oktave, ima frekvenco 262 Hz. Frekvence zaporednih tonov tvorijo geometrijsko zaporedje, kar pomeni, da je *razmerje njihovih frekvenc konstantno*. To je zelo pomembna lastnost, ki je dejansko nujna zaradi nelinearnega odziva človeškega bobniča na višino zvoka. Če zanemarimo ritem, sliši naše uho isto melodijo ne glede na višino, če je razmerje frekvenc tonov, ki jo sestavljajo, vsakokrat isto. To pa pomeni, da lahko melodije prenašamo višje ali nižje le, če tonski sestav sestoji iz zaporednih tonov, katerih frekvence tvorijo geometrijsko zaporedje.

Na klavirju pripadajo bele tipke tonom

C, D, E, F, G, A, H.

Zapored zaigrane dajo melodijo C-durove lestvice (poznamo 12 durovih in 12 molovih lestvic). Oktavnemu intervalu ustreza torej vrzel osmih belih tipk. Črne tipke dajejo zvišane (ali znižane) tone (slika 1).



Slika 1.

Današnji sistem se je razvil v dolgi časovni periodi in je kompromis med protislovnimi zahtevami, ki jim lahko sledimo vse do Pitagorejcev v antični Grčiji. Zaradi enostavnosti bomo pri razlagi razvoja uporabljali moderne oznake, čeprav s tem tvegamo očitke, da smo pomešali rahlo različne pojme.

Legenda pripoveduje, da je Pitagora poslušal klavira štirih kovačev, katerih melodija se mu je zdela zelo prijetna. Ko je klavir stehal, so tehtali 12, 9, 8 in 6 utežnih enot. Iz teh tež je Pitagora dobil razmerja

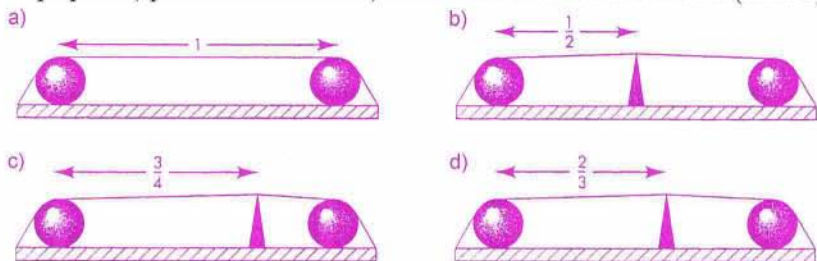
$$12:6 = 2:1, \quad 12:8 = 3:2, \quad 12:9 = 4:3 \quad \text{in} \quad 9:8.$$

Od tod je prišel na idejo, da posebej sozvočno zvene toni, katerih frekvence so v navedenih razmerjih.

Težko je reči, kaj se je zares zgodilo pred 2600 leti. Vsekakor je imel starodavni učenjak z idejo precej sreče. Vidimo namreč, da gre v

prvem primeru za oktavni interval med tonoma, naslednja razmerja pa pomenijo današnje čisto kvinto, čisto kvarto in cel ton, to je interval iz dveh poltonov. Mogoče pa je Pitagora tedaj sedel v isti banji kot Arhimed 400 let kasneje.

Klavdij Ptolemej, ki je živel okrog leta 150 našega štetja, je predvsem znan po svojih astronomskih in geografskih delih, napisal pa je tudi knjigo o teoriji glasbe *Harmonics*. V njej poroča o zgornji Pitagorovi trditvi, da lahko sozvočne intervale med glasbenimi toni predstavimo s kvocienti celih števil. To je prikazal eksperimentalno, pri čemer je uporabil precej nerodno pripravo, poznano kot kánon, neke vrste enostrunsko kitaro (slika 2).



Slika 2.

Če premikamo premični most, prečko, vzdolž kánona, je videti, da dobimo pri določenih legah tone, ki skupaj s tonom, s katerim zveni vsa struna, zvane bolj harmonično od drugih. Najosnovnejši tak interval je oktava. Na kánonu je to interval med tonom, ki ga dobimo pri igranju na celi struni (slika 2a), in tonom, zaigranim na (natančno) polovični struni (slika 2b). Torej je razmerje med dolžino strune, ki odda dani ton, in dolžino strune, ki odda njegovo oktavo, enako $\frac{2}{1}$. To velja neodvisno od višine originalnega tona. Druga celoštevilaska razmerja dolžin strun dajejo prav tako lepo zveneče (harmonične) intervale. Najpomembnejša intervala sta kvarta z razmerjem $\frac{4}{3}$ (slika 2c) in kvinta z razmerjem $\frac{3}{2}$ (slika 2d). Če začnemo z osnovnim tonom C, je drugi ton pri kvarti F, pri kvinti G in pri oktavi naslednji višji C. V C-durovi lestvici C, D, E, F, G, A, H, C so to četrty, peti in osmi ton. Od tod slede njihova latinska imena.

Druge intervale dobimo iz teh zidakov.

Domnevajo, da so Pitagorejci, da bi oblikovali harmonično tonsko lestvico, začeli z osnovnim tonom in napredovali navzgor s kvintami. Na ta način dobimo tone, ki jih zaigramo na strunah, katerih dolžine so z osnovno dolžino v razmerjih

$$1, \frac{3}{2}, \left(\frac{3}{2}\right)^2, \left(\frac{3}{2}\right)^3, \left(\frac{3}{2}\right)^4, \left(\frac{3}{2}\right)^5$$

ali

$$1, \frac{3}{2}, \frac{9}{4}, \frac{27}{8}, \frac{81}{16}, \frac{243}{32}.$$

Večina teh tonov leži zunaj ene oktave, saj je večina razmerij večja kot $\frac{2}{1}$. Toda s teh tonov se lahko spuščamo po oktavni intervalih (tako, da razmerja delimo z 2), dokler ne dobimo rezultatov med $\frac{1}{1}$ in $\frac{2}{1}$. Če dobljena razmerja uredimo po velikosti, dobimo

$$1, \frac{9}{8}, \frac{81}{64}, \frac{3}{2}, \frac{27}{16}, \frac{243}{128}.$$

Če za osnovni ton izberemo C, zaporedje približno ustreza tonom C, D, E, G, A, H.

Oznake namigujejo, da nekaj manjka. Tudi slišati je, da je vrzel med $\frac{81}{64}$ in $\frac{3}{2}$ širša kot ostale. Vrzel lahko spodobno zamašimo tako, da dodamo kvarto, razmerje $\frac{4}{3}$, oziroma ton F. Pravzaprav bi kvarto lahko vgradili že na samem začetku, če bi se od osnovnega tona spustili za kvinto in se nato dvignili za oktavo, saj je

$$2 \times \left(\frac{3}{2}\right)^{-1} = 2 \times \frac{2}{3} = \frac{4}{3}.$$

Zaporedje

$$1, \frac{9}{8}, \frac{81}{64}, \frac{4}{3}, \frac{3}{2}, \frac{27}{16}, \frac{243}{128}, 2, \quad (1)$$

ki ga dobimo na ta način (dodali smo še oktavo), ustreza približno tonom, ki jih dobimo z belimi tipkami na klavirju. Kaj pa črne tipke? Kar se same barve tipk tiče, bi najbrž glasba lahko shajala brez njih. Zakaj dobljeno zaporedje tonov ne zadošča? Če iz zaporedja (1) izračunamo razmerja frekvenc zaporednih tonov, dobimo

$$\frac{9}{8}, \frac{9}{8}, \frac{256}{243}, \frac{9}{8}, \frac{9}{8}, \frac{9}{8}, \frac{256}{243}.$$

Vidimo, da imamo natanko dve razmerji, večje, $\frac{9}{8}$, nastopa petkrat, manjše, $\frac{256}{243}$, pa dvakrat. Ker je

$$\frac{9}{8} = 1.125 \quad \text{in} \quad \left(\frac{256}{243}\right)^2 \approx 1.11,$$

lahko vzamemo, da je $\frac{9}{8} \approx (\frac{256}{243})^2$. Dva manjša intervala sta torej velika približno za en večji interval. To pomeni, da so v skali še vedno vrzeli. Vsak večji interval (cel ton) moramo razdeliti na dva manjša, od katerih bo vsak tako blizu manjšemu (poltonu), kot je le možno. Torej moramo dodati še pet tonov, ki jih bomo na klavirju zaigrali s črnimi tipkami.

Obstaja več načinov, kako se to naredi. Tako imenovana kromatična lestvica začne z ulomki $(\frac{3}{2})^n$ za $n = 0, 1, 2, \dots, 10, 11$. Dobljene vrednosti nato reducira na isto oktavo, tako da jih ponavlja se deli z dve in jih potem še uredi po velikosti (sistem: po kvintah navzgor, po oktavah navzdol, slika 1).

Rezultat prikazuje naslednja tabela za C-durovo lestvico, v kateri navajamo vrednosti razmerij harmoničnih intervalov in vrednosti, dobljene na opisan način.

ton	C	D	E	F	G	A	H	C
harmonični interval	1	$\frac{9}{8}$	$\frac{5}{4}$	$\frac{4}{3}$	$\frac{3}{2}$	$\frac{5}{3}$	$\frac{15}{8}$	2
kromatični interval	1	$\frac{9}{8}$	$\frac{81}{64}$	$\frac{177147}{131072}$	$\frac{3}{2}$	$\frac{27}{16}$	$\frac{243}{128}$	$\frac{531441}{262144}$

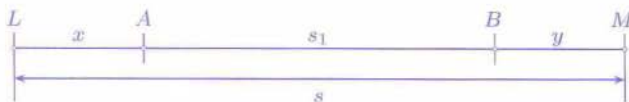
Vidimo, da se pri nekaterih tonih ulomki ne ujemajo. Tako je tudi pri oktavi, kjer dobimo namesto faktorja 2 ulomek s šestmestnim imenovalcem. Njegova vrednost je približno 2.0273. Če to število delimo z dve, da se vrnemo k osnovnemu tonu, dobimo namesto 1 približno vrednost 1.0136. To odstopanje je poznano pod imenom *pitagorejska* ali *ditonična koma*.

O razlogu zanjo in o kitari pa v naslednji številki Preseka.

Marija Vencelj

NAJKRAJŠI ČAS POTOVANJA – Rešitev s str. 195

Na začetku potovanja (točka L na sliki 1) se dva študenta odpeljeta z motorjem, tretji pa se odpravi na pot peš. V točki B na oddaljenosti y od Maribora začne eden od potnikov z motorja pešačiti, drugi pa se z motorjem vrne po prvega pešca, ki ga sreča na razdalji x (v točki A) od Ljubljane. S prvim pešcem se motorist ponovno odpelje proti Mariboru, kjer na koncu poti (M) dohiti drugega pešca.



Slika 1.

Celotna pot s od Ljubljane do Maribora je enaka vsoti poti pešcev $x + y$ in razdalje s_1 med krajema A in B . Čas, ki ga porabi prvi pešec, da prehodi razdaljo x , je enak času, ki ga potrebuje motorist za razdaljo $x + 2s_1$. Prav tako sta enaka časa drugega pešca in motorista na ustreznih razdaljah y in $y + 2s_1$.

Če označimo z v_1 hitrost pešcev in z v_2 hitrost motorista, lahko zapišemo enačbi

$$\frac{x}{v_1} = \frac{x + 2s_1}{v_2}, \quad \frac{y}{v_1} = \frac{y + 2s_1}{v_2},$$

iz katerih sledi, da sta poti prvega in drugega pešca enaki ($x = y$).

Pot prvega pešca do srečanja z motoristom v kraju A je $x = v_1 t_1$, motorista pa $x + 2s_1 = v_2 t_1$.

Če upoštevamo, da je $t_1 = \frac{x}{v_1}$ in $s_1 = s - 2x$, spremenimo drugo enačbo v obliko

$$x + 2(s - 2x) = x \frac{v_2}{v_1},$$

iz katere izračunamo neznano razdaljo x :

$$x = \frac{2sv_1}{3v_1 + v_2}.$$

Celotni najkrajši čas potovanja t od L do M je enak vsoti časov hoje prvega pešca in vožnje motorista na razdalji $s - x$:

$$t = \frac{x}{v_1} + \frac{s - x}{v_2}.$$

Razdaljo x smo že izračunali, zato lahko zapišemo

$$t = \frac{s}{v_2} \cdot \frac{3v_2 + v_1}{3v_1 + v_2}.$$

Pri danih številčnih vrednostih za $v_1 = 5$ km/h, $v_2 = 60$ km/h in $s = 144$ km je ta čas 5,92 ure.

Karel Šmigoc

VIZUALNA KRIPTOGRAFIJA – ŠUM SKRIVNOSTI



Zagotovo ste že kdaj brali zgodbo o zakopanem zakladu. Ta zaklad je običajno gusarski, kapitan, kriptograf samouk, pa dovolj premeten, da je zemljevid, ki vodi do zaklada, raztrgal na več kosov. Predstavljajte si, da ravno vi izhajate iz neupogljive rodbine kapitanov Sinjebradcev, katerim so legende pripisovale bajna bogastva. To bogastvo vas žal ni doseglo, saj ga je eden od Sinjebradcev kot zgleden gusarski kapitan namesto v sef švicarske banke zaklad zakopal v nedrja zemlje enega od otokov. Na srečo pa na podstrešju najdete del zemljevida!

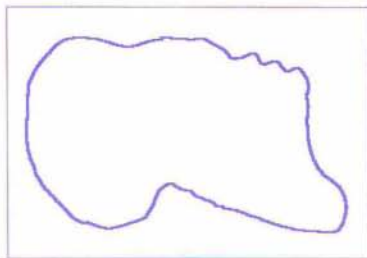
Najprej si oglejmo, s čim se sploh ukvarja kriptografija. Pošiljatelj ima sporočilo, polno skrivnih informacij, zato ga po izbranem šifrnem sistemu zašifrira (raztrga zemljevid) in dobi tajnopis. Ta tajnopis potem nekako pošlje naslovniku, ki ga odšifrira (zloži kose zemljevida) in prebere sporočilo. Med pošiljanjem na tajnopis običajno prežijo napadalci, ki bi se radi dokopali do skrivnih informacij ali pa naslovniku podtaknili lažne informacije. Kriptografi ves čas seveda tekmujejo v sestavljanju in izboljševanju šifrnih sistemov ter iskanju napadov na te sisteme.

Vsi šifrirni sistemi, ki se zanašajo na *računsko varnost*, temeljijo na tem, da po določenem sistemu "premešajo" informacijo oziroma sporočilo. Ključ imenujemo podatke (parametre), ki v okviru danega šifrnega sistema (algoritma) natančno določajo, kako iz sporočila narediti tajnopis in kako potem vrniti premešano informacijo oziroma tajnopis v prvotno obliko. Ključ je običajno precej krajši od sporočila, sistem pa tem boljši, čim več možnih ključev mora napadalec preizkusiti na poti do rešitve. Ob tem je smiselno upoštevati *Kerckhoffov princip*, ki predpostavlja, da napadalec pozna uporabljeni šifrirni sistem, ne pa tudi ključa. Napadalec ve, kdaj je prišel na cilj: ko dobi tajnopis, razvozlan po določenem sistemu, smiselni pomen, je to zelo verjetno izvirno sporočilo. Verjetnost, da bi dobil smiselno, a napačno sporočilo, je neznatna, če je le tajnopis dovolj dolg. Lahko pokažemo, da je pri sistemu, kjer vsako črko nadomestimo z neko drugo oziroma zamenjamo abecedo, za verodostojnost smiselnega angleškega sporočila potrebna dolžina približno 25 črk.

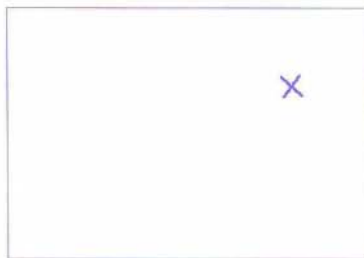
Vrnimo se k zakopanemu zakladu. Če je najdeni del zemljevida dovolj velik, boste lahko prepoznali otok. Na najdenem delu pa žal ni označenega mesta, kje točno je zaklad zakopan. Gotovo bi vam skrito bogastvo prišlo zelo prav, zato lahko vzamete kramp in lopato, se odpravite na pravi otok ter vsega prekopljete. Kriptografi bi to imenovali napad z grobo silo, saj morate v okviru informacije, ki jo imate (uporabljeni šifrirni sistem oziroma ime otoka), preizkusiti vse možnosti (uporabiti vse mogoče ključe, oziroma prekopati vsak kvadratni meter). Če boste problemu namenili dovolj najlepših let svojega življenja, boste zaklad prej ali slej našli.

Vsi, ki želite zakopati zaklad na skrivnem mestu, pa lahko iskalcem še bolj otežite delo, če boste le prebrali nadaljevanje članka. Seveda ga lahko preberete tudi iz gole radovednosti.

Ker nismo gusarji stare šole, bomo zemljevide namesto na pergament risali na prosojnici. Neuki Sinjebradec bi zemljevid na prosojnici verjetno narisal takole (glej sliki 1 in 2): na eno prosojnico sliko otoka, na drugo pa križec, ki označuje zakopani zaklad.



Slika 1. Zemljevid otoka.



Slika 2. Križec označuje skriti zaklad.

Ko prosojnici poravnamo in prekrijemo, je skrivnost razkrita. Tudi vsaka prosojnica zase razkrije nekaj informacije. Tako nam prva razkrije, na katerem otoku nas čaka zaklad. V nadaljevanju se bomo naučili, kako prosojnici porisati tako, da z vsake posebej nihče ne bo mogel pridobiti nikakršne informacije, obe skupaj pa bosta razkrili skrivnost (takorekoč $0 + 0 = 1$).

V prejšnjem stoletju so se kriptografi domislili, kako informacijo zakriti tako, da je brez ključa nihče ne bo mogel razkriti. V kriptografiji temu pravimo *popolna varnost*. Dosežemo jo tako, da informacijo "zlijemo" s povsem naključnimi podatki. Tako onemogočimo napadalce, saj morajo le-ti odstraniti naključne podatke, s čimer pa lahko dobijo povsem drugačno sporočilo (glej primer 1). Ob danem tajnopisu so vsa sporočila enake dolžine enako verjetna. V tajnopisu lahko najdeš, karkoli iščeš, zato ni več samo ene smiselne rešitve. Tajnopis pa odšifriramo tako, da odstranimo prej dodane naključne podatke.

Primer 1. Pravi ključ je ključnega pomena, četudi je naključen.

$k r u h = P$ (1. sporočilo)	$v i n o = P'$ (2. sporočilo)
$a s k f = K$ (1. ključ)	$n b s \check{z} = K' = K + P - P'$ (2. ključ)
$l k h o = C = P + K$ (tajnopis)	$l k h o = C = P' + K'$ (tajnopis)

V primeru 1 se zlivanje istoležnih črk (navpično) izvede kot seštevanje zaporednih števil črk v abecedi ('k' + 'a' = 'l', saj je $12 + 1 = 13$), kjer se ta ciklično ponavlja (za 'z' pride spet 'a'). Če napadalec prestreže tajnopis C , ne more določiti sporočila, saj sta oba ključa K in K' (s tem pa tudi sporočila P in P') enako verjetna, saj sta naključna. Kdor pa pozna ključ, lahko odkrije sporočilo tako, da od tajnopisa odšteje ključ.

Največji problem pri tem šifrnem sistemu je dolžina ključa – ključ je enako dolg kot sporočilo samo. Pri drugih sistemih je ključ običajno bistveno krajši, npr. pri enoabecedni zamenjavi je potrebno poznati le zamenjavo za vsako črko, pa lahko s temi manj kot 30 podatki zašifriramo in odšifriramo celotno knjigo.

Opisana shema za doseglo popolne varnosti se imenuje *enkratni ščit* (angl. one-time-pad), saj ključ kakor ščit prekrije podatke, uporabimo pa ga lahko samo enkrat (tudi vitezi so morali polomljene ščite zamenjati). Če bi ga uporabljali večkrat, bi napadalec lahko podtaknil njemu poznano sporočilo P , potem pa iz prestreženega tajnopisa C izračunal ključ $K = C - P$. Če je ključ razkrit, sistem ne ponuja nobene varnosti več.

Vemo, da vsako sporočilo lahko zapišemo v dvojiškem zapisu, torej kot zaporedje ničel in enic. Prekrivanje z enkratnim ščitom se v dvojiškem zapisu na istoležnih bitih izvede kot dvojiški *izključni (ekskluzivni) ali* (XOR – glej tabelo 1).

Izvorno sporočilo razkrijemo tako, da tajnopis še enkrat prekrijemo s ključem, saj je pri dvojiškem zapisu seštevanje enako odštevanju.

Leta 1994 sta se znana kriptografa Adi Shamir, soiznajditelj sistema javne kriptografije RSA, in Moni Naor domislila *vizualne kriptografije*. Ideja je podobna enkratnemu ščitu, le da namesto zaporedja bitov uporabimo ravnino, tlakovano s črnimi in belimi ploščicami, ki predstavljajo vrednosti bitov. Poleg tega pa namesto operacije 'izključni ali' (XOR) uporabimo operacijo navadni *ali* (OR – glej tabelo 2).

XOR	0	1
0	0	1
1	1	0

Tabela 1. Izključni ali.

OR	0	1
0	0	1
1	1	1

Tabela 2. Ali.

Na ta način slike zašifriramo, ko pa jih odšifriramo, so malce spremenjene, a še vedno prepoznavne. Najpomembneje pa je, da je vizualna kriptografija po sistemu enkratnega ščita podedovala popolno varnost. To pomeni, da napadalec ne more prepoznati zašifrirane slike, četudi ima še tako veliko časa in računske moči. Slaba stran popolne varnosti pa je, da je ključ prav tako dolg (obsežen) kot samo sporočilo; zaradi tega ni bistvene razlike med ključem in zašifriranim sporočilom (primerjaj sliki 3 in 4).

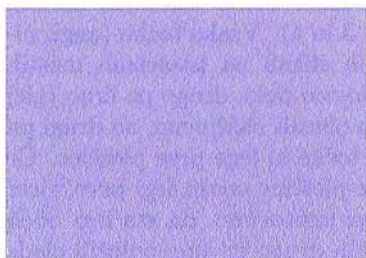
Poglejmo si idejo malce podrobneje: sliko bomo razstavili na dve različni, a enako veliki delni sliki (glej sliki 3 in 4). Vsako točko (angl. pixel) originalne slike bomo na obeh delnih slikah na istoležnih mestih nadomestili s ploščicama, ki imata eno polovico belo, drugo pa črno (glej tabelo 3). Na prvi delni sliki bomo ploščico obrnili naključno, na drugi pa bo njena lega odvisna ob barve originalne točke in lege prve ploščice. Če je bila originalna točka bela, bo lega druge ploščice enaka legi prve, sicer pa jo položimo zrcalno. Z malo razmisleka ugotovimo, da sta legi obeh ploščic naključni, saj smo za prvo to privzeli, drugo pa smo položili glede na prvo, ki leži naključno.

verjetnost	$p = 0.5$		$p = 0.5$	
na prvi delni sliki				
originalna slika	črno	belo	črno	belo
na drugi delni sliki				

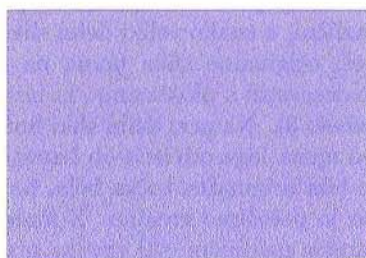
Tabela 3. Po shemi točko za točko postopno gradimo delni sliki.

Dešifriranje poteka nekoliko drugače. Predstavljajmo si, da mrežo ploščic narišemo na prosojnico, nato pa, če je ploščica (oz. njen del) črna, ustrezajoči del na prosojnici pobarvamo s črno barvo. Potem obe prosojnici prekrijemo. Kjer je bila vsaj ena od prosojnic pobarvana, vidimo črno, drugje pa je prosojno. Kjer se prekrijeta enako obrnjeni ploščici (npr. prva v zgornji vrstici in druga v spodnji vrstici tabele 3), tam oko majhno črno-belo polje vidi kot sivo. Kjer pa se prekrijeta različno obrnjeni ploščici (npr. prva v zgornji vrstici in prva v spodnji vrstici tabele 3), vidimo črno polje.

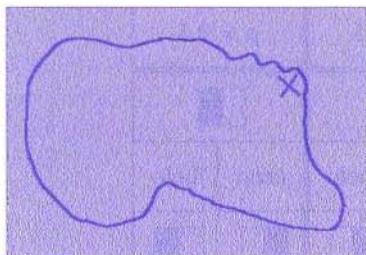
Originalno sliko torej razbijemo na dve enako veliki delni sliki, na katerih je vsaka točka naključno bela ali črna (to imenujemo šum). Ko obe delni sliki prekrijemo, zagledamo skrito podobo. Ta podoba je malce spremenjena (glej sliko 5), saj tam, kjer so bile na originalni sliki bele ploščice, dobimo napol črne. Če so ploščice dovolj majhne (oziroma, če gledamo od daleč), oko napol črne ploščice vidi kot sive. Torej iz črno-bele slike dobimo črno-sivo sliko. Kljub tej izgubi kontrasta so enostavne slike še vedno prepoznavne.



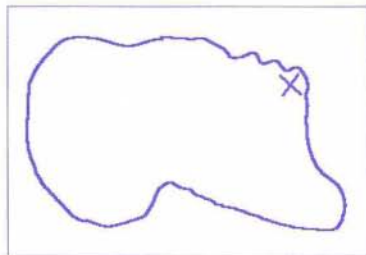
Slika 3. Prva delna slika.



Slika 4. Druga delna slika.



Slika 5. Zlita slika oziroma prekriti delni sliki razkrijeta skrivnost.



Slika 6. Originalna slika.

Opisali smo osnovno idejo vizualne kriptografije. Kmalu pa so se začele pojavljati nadgradnje te zamisli. Prvo sta podala že Naor in Shamir v svojem članku. Kako zašifrirati sliko, ki ni le črno-bela, ampak vsebuje tudi sive tone? Lahko uporabimo okrogle ploščice. Na prvi delni sliki ploščico zavrtimo za naključen kot. Na drugi delni sliki jo položimo enako, če je originalna ploščica bela (prekriti prosojnici bi pokazali napol črn krog), nasprotno, če je originalna ploščica črna (prekriti prosojnici pokažeta črn krog), in ustrezno zavrtena (prosojnici pokažeta krog, katerega več kot polovica je črna) ob ustrezno sivi ploščici (glej tabelo 4). Na ta način dobimo novo prostostno stopnjo (zvezne tone sivine)

z (zveznim) vrtenjem ploščic. Žal pa je ta način, čeprav zelo eleganten, precej neprikladen za izvedbo s pomočjo računalnika, zato so nove ideje zelo dobrodošle.

prvi del	drugi del	prekrito
		

Tabela 4. Okrogle ploščice nam omogočijo šifriranje sive slike.

Deljenje skrivnosti

Vizualna kriptografija je tesno povezana s področjem deljenja skrivnosti (glej članek [1]). Spomnimo se zopet kapitana Sinjebgradca; imel je tri sinove in namesto rentnega varčevanja jim je namenil del naropanega bogastva, ki ga je po stari gusarski šegi zakopal. Bal pa se je njihovega pretiranega pohlepa. Ker je želel ohraniti vsaj nekaj družinske sloge, naj bi pri izkopavanju zaklada sodelovala vsaj dva brata. En sam se ne bi mogel polastiti vsega bogastva. Zato je kapitan (proti koncu članka že bolj kriptografsko vešč) zemljevid razdelil na tri delne slike na prosojnicah tako, da se skrivnost razkrije, ko sta prekriji vsaj dve delni slike. To je tako imenovana *shema 2-od-3*. Možno je skonstruirati tudi bolj zapletene sheme, ki so sestavljene iz več delnih slik, med katerimi so lahko nekatere bolj, druge pa manj pomembne. Oglejmo si preprost primer konstrukcije sheme 2-od-3 (glej tabeli 5 in 6):

1	0	0
0	1	0
0	0	1

Tabela 5. Šifriranje črne točke.



Slika 7. Ploščica, ki predstavlja drugo vrstico tabele 5 (0 1 0).

1	0	0
1	0	0
1	0	0

Tabela 6. Šifriranje bele točke.

Ko gradimo tri delne slike, za vsako točko uporabimo tabelo 5, če je točka na originalni sliki črna (ima vrednost 1), oziroma tabelo 6, če je točka bela (ima vrednost 0); stolpce izbrane tabele naključno premešamo, vrstice premešane tabele pa zaporedoma predstavljajo ploščice na posameznih delnih slikah (slika 7). Enostavno povedano: če je originalna točka bela, so na delnih slikah istoležni kosi ploščic enaki, če pa je črna, se istoležni kosi razlikujejo. V vsakem primeru pa so naključno razporejeni.

Tu gre po eni strani za varnost (vsaka ploščica na delni sliki je $1/3$ črna), po drugi pa za kontrast (če prekrijemo ploščici na delnih slikah, ki predstavljata originalno belo točko, dobimo $1/3$ črno ploščico, če pa predstavljata originalno črno točko, dobimo $2/3$ črno ploščico – kontrast je $1/3$). Podrobnejše napotke je moč najti v članku [2], članki o barvni vizualni kriptografiji in drugih zanimivostih pa so dosegljivi tudi na spletu z iskanjem po ključnih besedah *visual cryptography* in *secret sharing*. Če bi kapitan Sinjebradec redno bral Presek, bi gotovo vedel, kako doseči popolno varnost za svoje skrivnosti. Morda pa bi ga branje tako prevzelo, da bi mu zmanjkalo časa za gusarske podvige.

Martin Pečar

Literatura:

- [1] A. Jurišić, *Kako deliti skrivnosti*, Presek **29** (2001–02), št. 6, str. 358–364.
- [2] D. Stinson, *Visual cryptography & threshold schemes*, Dr. Dobb's Journal, april 1998, str. 36–43.

KRIVIČNI TENIS – Rešitev s str. 199

Točkovanje je pri tenisu nekaj posebnega. Vsaka napaka prinese točko nasprotniku. Prvo štejemo 15 (npr. 15 : 0), drugo 30, tretjo 40, četrta je *igra*, razen v naslednjem primeru: Če nastopi rezultat 40 : 40, to je, če imata oba igralca po tri točke, dobi igro tisti igralec, ki po izenačenju prvi dobi dve točki zapored. Igralec, ki prvi dobi šest iger, dobi *set*, vendar ga mora dobiti z razliko dveh iger. Sicer se set podaljša, dokler ni dosežena razlika dveh iger. (Pri sistemu tie-break je ta del pravil drugačen.) Končni zmagovalec je tisti, ki prvi doseže bodisi dva bodisi tri sete, odvisno od turnirja. Ženske ponavadi igrajo na dva dobljena seta, moški na tri.

Dvoboj, ki ga je Tina, kljub objektivno boljši igri, izgubila, je potekal takole: Maja je tekmo dobila z 0 : 6, 6 : 4, 6 : 4 v setih. V vseh igrah, ki jih je dobila, je pustila Tino "na 30", kar pomeni 4 : 2 v točkah. Tina pa je vse svoje igre dobila brez izgubljene točke, z rezultatom 4 : 0. Maja je torej priigrala $12 \cdot 4 = 48$ točk, Tina pa $12 \cdot 2 + 14 \cdot 4 = 80$ točk. Razmerje Tininih in Majinih točk je 80 : 48, kar je res 5 : 3. Pri kakršnemkoli drugačnem poteku tekme dobimo razmerje točk, spremenjeno v Majino korist, kot se lahko sami priprčate.

Za $m > n > 0$ velja namreč ocena $\frac{80+n}{48+m} < \frac{80+n}{48+n} < \frac{5}{3}$.

Marija Vencelj

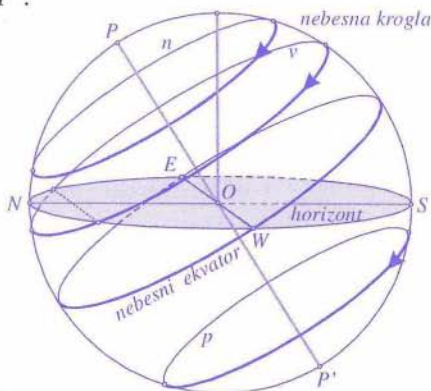
KOLIKO NEBESNE KROGLE

Pri obravnavanju nadobzornic in zvezd vzhajalk (glej Presek 29, 280) naletimo na zanimivo vprašanje: *Kolikšen del nebesne krogle vidimo s kakega kraja na Zemlji?*

Takoj se oglasi zdrava pamet, ki odgovori, da zanesljivo vidimo polovico nebesne krogle, t.j. tisto njeno polovico (polkroglo), ki se kot nebo boči nad vsakim opazovališčem. Ker pa zaradi Zemljinega vrtenja nebesna krogla skupaj z zvezdami navidezno kroži okrog nas, vidimo več kot pol nebesne krogle, in to tem več, čim več zvezd vzhaja. Če vzhajajo vse, potem s tistega kraja vidimo vso nebesno kroglo. To pa velja za kraje na zemeljskem ekvatorju.

Obravnavajmo to vprašanje nekoliko podrobneje. Vzemimo idealno obzorje in splošni primer, da opazujemo nebo iz kraja na severni zemeljski poluti (slika 1), kjer je zemljepisna širina φ kraja pozitivna ($\varphi = \angle PON > 0$). Za kraje v Sloveniji to zagotovo velja, saj je $\varphi \approx 46^\circ$. Predstavljajmo si, da smo v središču nebesne krogle, zvezde pa navidezno krožijo postrani glede na naše obzorje. Povedano še natančneje: zvezde krožijo okrog nebesne osi PP' , ki gre skozi naše opazovališče O ter severni nebesni pol P in južni nebesni pol P' .

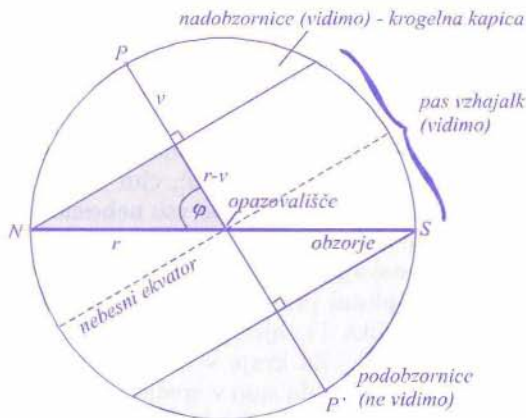
Slika 1. Navidezno kroženje zvezd okrog nebesne osi PP' v kraju na severni zemeljski poluti. Puščica kaže smer navideznega kroženja zvezd (nebesne krogle). O – opazovališče, $\varphi = \angle PON$ – zemljepisna širina kraja, n – nadobzornica in njena dnevna pot, v – vzhajalka in njena dnevna pot, p – podobzornica in njena dnevna pot (ne pride v poštev).



Nebesna os oklepa kot φ z vodoravno ravnino, saj je po definiciji višinski kot severnega nebesnega pola za kraje na severni zemeljski poluti enak vrednosti zemljepisne širine. Vzhajalke vzhajajo na vzhodu, na jugu so najvišje, zahajajo pa na zahodu, nadobzornice pa so tako in tako ves čas nad obzorjem (slika 1). Čim manjši je torej φ , več nebesne krogle vidimo.

Sedaj si oglejmo še sliko 2. Nadobzornice krožijo po kapici (nebesne krogle) z višino v , vzhajalke pa po pasu (nebesne krogle) z višino $2(r - v)$,

kjer je $r - v = r \cos \varphi$, od koder sledi $v = r(1 - \cos \varphi)$. Zaradi vrtenja Zemlje vidimo iz danega kraja O vse zvezde na kapici in na pasu, vidimo $\frac{2\pi r v + 2 \cdot 2\pi r(r-v)}{4\pi r^2} = \left(\frac{1}{2} + \frac{\cos \varphi}{2}\right)$ -ti del nebesne krogle.



Slika 2. Presek nebesne krogle z meridijsko ravnino (k izpeljavi izraza $\frac{1}{2} + \frac{\cos \varphi}{2}$, ki pove, kolikšen del nebesne krogle je viden iz kakega kraja z zemljepisno širino φ na Zemlji).

Iz kraja O z zemljepisno širino φ torej res vidimo $\frac{1}{2}$ (50%) nebesne krogle, vendar pa še del nebesne krogle, t.j. $\frac{\cos \varphi}{2}$ -ti del (kar je odvisno od φ).

Navedimo tri tipične primere:

- i) Iz naših krajev vidimo $\frac{1}{2} + \frac{\cos 46^\circ}{2} = 0,847$, t.j. približno 85% nebesne krogle.
- ii) Iz severnega ali južnega zemeljskega pola ($\varphi = \pm 90^\circ$) vidimo $\frac{1}{2} + \frac{\cos 90^\circ}{2} = 50\%$. Narišite skico in se po skici prepričajte o tem.
- iii) Iz krajev na ekvatorju ($\varphi = 0^\circ$) pa vidimo $\frac{1}{2} + \frac{\cos 0^\circ}{2} = 100\%$, t.j. vso nebesno kroglo. Narišite skico in se po skici prepričajte o tem.

Ti trije računi veljajo za idealno obzorje. Če so v okolici hribi ali visoke zgradbe, vidimo seveda manj.

Vprašanje pa lahko tudi obrnemo. Recimo, da sprašujemo za tiste kraje (φ) na Zemlji, od koder je viden določen del nebesne krogle.

Za vajo:

1. Izračunajmo zemljepisno širino kraja, od koder je vidno
 - a) $\frac{3}{4}$ nebesne krogle
 - b) 90% nebesne krogle
 - c) 30% nebesne krogle.
2. Koliko nebesne krogle vidimo? Obravnavajmo matematično.

Marijan Prosen

Odgovori so na strani 300.

BINE DOBI PISMO

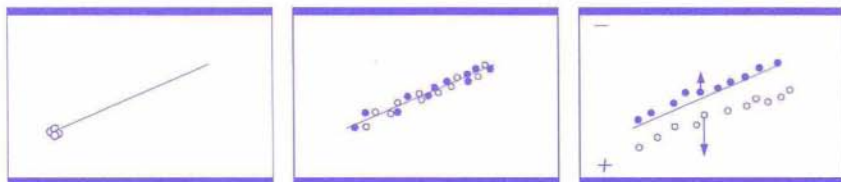
Bine Umnik je odprl pravkar prispelo pismo, ki mu ga je pisal dr. Nula, predstojnik patentnega urada:

Dragi Bine,

veseli me, da si napredoval v fiziki. Morda si zdaj že zrel za izume, ki temelje na klasični fiziki. Če pa hočeš kaj storiti v svetu atomov, ga moraš prej spoznati.

Pravilno si ugotovil, da si najbližje zaznavi delcev alfa prek njihovega električnega naboja. Z delcem alfa, ki leti skozi plin, pa lahko sprostimo še dosti več naboja. Ko leti delec, ki je nabit pozitivno, mimo plinskih molekul ali atomov, privlači njihove elektrone, saj nosijo negativni naboj. Marsikateri elektron se loči od svojega doma in skuša slediti delcu alfa, ki pa elektronu ubeži. Tako ostane vzdolž poti delca alfa množica osamljenih elektronov in prav tako atomov ali molekul, ki so izgubili po en elektron. Pravimo jim ioni in nosijo zaradi izgube elektrona presežek pozitivnega naboja. Seveda ustvarjanje množice elektronov in ionov ni zastoj. Delec alfa plačuje z izgubo energije. Vsak par ga v povprečju velja 30 eV. Ko je uporabil vseh svojih, recimo 6 MeV, naštejemo vzdolž poti 200 000 parov elektron – ion.

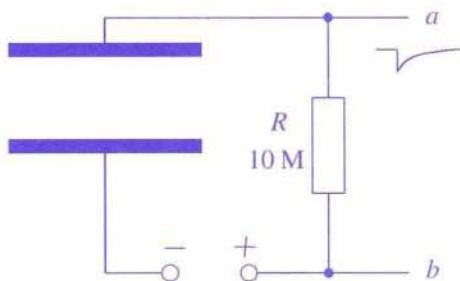
Delec alfa postopoma izgublja svojo energijo in se slednjič po nekaj centimetrih poti ustavi. Prisvoji si dva elektrona, ki mu manjkata do popolnega helijevega atoma, in se, nevtralen kot je, izgubi za vselej v zraku, ki že sam po sebi vsebuje posamezne atome helija. Vzdolž bolj ali manj ravne poti ostane množica pozitivnih ionov in elektronov, ki se naključno gibajo sem in tja. Prej ali slej se najdejo in se ponovno združijo v atome in molekule. O sevanju poslej ni več sledu.



Slika 1. Levo: Odletel je delec alfa. Sredina: Pri prehodu napravi množico elektronov in ionov. Desno: Z električnim poljem zberemo elektrone in ione vsake na svoji strani.

Z električnim poljem pa lahko ione in elektrone preusmerimo k dvema elektrodama. Slika 1 kaže tako polje med ploščama nabitega kondenzatorja in nabite delce, ki teko vsak proti svoji plošči. Z napetostjo nekaj sto voltov spravimo vitke elektrone na pozitivno ploščo v nekaj milijoninah

sekunde, medtem ko rabijo debelušasti ioni do svojega cilja tisočkrat daljši čas. Ko ioni dosežejo negativno nabito ploščo, si dopolnijo manjkajoči naboj z elektronom. Naboj negativne plošče se zmanjša. Enako zmanjšajo naboj pozitivne plošče elektroni potem, ko jo dosežejo. Če kondenzatorski plošči s kapaciteto C nista priključeni na vir napetosti, se zaradi zmanjšane naboja Δe zmanjša napetost za $\Delta U = \Delta e / C$. Ko ugotovimo tako spremembo napetosti, vemo, da jo je povzročil sprehod delca alfa med ploščama. Naših 200 000 parov, od katerih vsak nosi elementarni naboj $1,6 \cdot 10^{-19}$ As, zmanjša naboj kondenzatorja za $3,2 \cdot 10^{-14}$ As. Napetost na kondenzatorju s kapaciteto 10 pF se zmanjša za 3,2 mV. Malo, če bi merili celotno napetost, ki je bila prej 1000 V, zdaj pa je 999,998 V. Meritev napetosti na šest mest ni lahka. Meritev napetosti na šest mest, ne da bi izpraznili kondenzator, pa je sploh nemogoča. Življenje je polno trikov. Najpreprostejši je, da ne merimo celotne napetosti, ampak le spremembo. Pomagalo nam bo vezje, ki ga kaže slika 2. Pozitivna plošča je priključena na napetostni vir prek velikega upora R . Normalno prek upora ni napetosti. Pozitivna plošča je nabita na enako napetost, kot je napetost vira, zato prek upora ne teče tok. Po prehodu delca alfa sprejme pozitivna plošča množico elektronov in zgubi zato del naboja. Napetost na plošči se zmanjša. Takoj po skokoviti spremembi pa se začne vzpostavljati prvotno stanje. Pozitivna plošča se spet nabije na prvotno napetost in prek upora ne zaznamo nobene napetosti več.



Slika 2. Kadar zgubi pozitivna plošča zaradi prihoda elektronov nekaj naboja, se zmanjša njena napetost za nekaj milivoltov. Potem se plošča spet nabije prek velikega upora R . Rezultat je majhen napetostni sunkov.

Tako pridemo do majhnih napetostnih sunkov, ki jih ojačimo v velike. Pomagajo enote jedrske elektronike. Iz velikosti sunka lahko izračunamo tudi energijo delca. Sunkov, velik 4,3 mV, bi pomenil, da je med ploščama kondenzatorja delec alfa zapravil energijo 8 MeV.

Z delci beta bo več težav. Imajo manjše energije kot delci α , tja do 2 MeV, torej bo množica elektronov in ionov manj številna. Delci beta se na poti skozi snov ne dajo tako zlahka oropati. Zato bo njihova sled dosti bolj na redko posejana z elektroni in ioni in bo tudi segala dosti dlje. Doseg delcev beta z energijo 2 MeV v zraku je okoli 10 metrov. Da bi z električnim poljem polovili vse novonastale elektrone in ione, bi potrebovali ogromni nabiti plošči. Zato bomo poskušali ustavljati elektrone v bolj gosti snovi. Električni prevodniki ne bodo dobri, saj bi predstavljali kratek stik med ploščama kondenzatorja. Iz električnih izolatorjev ne bi mogli poloviti elektronov. Poznamo pa še polprevodnike. Najbolj znana sta silicij in germanij. Zelo čisti polprevodniki ne prevajajo električnega toka, če pa sevanje iz radioaktivnih jeder sprosti v njih elektrone, jih je mogoče zbrati. Silicij in germanij sta več tisočkrat gostejša od zraka, zato bodo zadoščali več tisočkrat manjši detektorji.

Z dovolj veliko električno napetostjo, ki je za polprevodniške kristale z razsežnostjo nekaj centimetrov enaka nekaj tisoč voltov, spravimo pozitivni in negativni naboj vsaksebi v času, ki ponavadi ni daljši od mikrosekunde.

Dodatna prednost novih detektorjev je, da so elektroni, kupljeni v siliciju ali germaniju, cenejši. Za elektron plačamo le nekaj eV. Tu bi nam en sam delec alfa z energijo 6 MeV sprostil okoli dva milijona elektronov in tako dal 10-krat večji naboj kot v zraku. Zato bodo tudi spremembe električne napetosti večje in s tem lažje merljive. Seveda pa pot do dobrega polprevodniškega merilnika ni lahka. Le povsem čist in ohlajen silicij ali germanij ne prevaja električnega toka že brez obsevanja. Tehnično čista snov vsebuje manj kot odstotek primesi. Kemično čistost si snov zagotovi, če vsebuje manj kot 10^{-4} primesi. Do naslova spektralne čistosti pride, če naštejemo med milijonom pravih atomov le en tujerodni atom. Hiperčisti germanij se ponaša z manj kot atomom primesi na milijardo germanijevih atomov. Za primerjavo: naš planet šteje nekaj milijard prebivalcev. Da bi bili hiperčisti, bi morali biti pošteni vsi z izjemo nekaj barab. Za nove detektorje pa morata biti silicij in germanij hiperčista.

Tudi hlajenje bo zahtevno. Primerne temperature okoli -180°C zagotovi tekoči dušik, vendar ga je treba imeti.

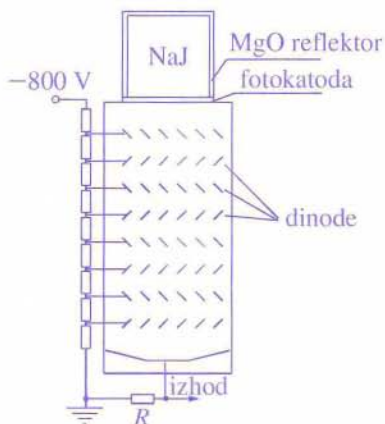
Povsem različni so scintilacijski detektorji. Že prvi raziskovalci radioaktivnosti so opazili, da se zaslon, prekrit s cinkovim sulfidom, pobjiska na mestu, kjer ga je zadel delec alfa. Iskrica svetlobe je šibka in jo je mogoče opaziti le v popolni temi. Tudi preštevanje teh iskrice ni lahko. Pri delcih beta tako štejte odpove. Delec beta prodira v globino in večina svetlobe se izgubi v neprozornem sulfidu, medtem ko je delec alfa zapravlil vso energijo že na površini.

Poleg cinkovega sulfida pa so našli še vrsto snovi, ki se pod vplivom sevanja vedejo podobno in so povrh še prozorne. Tako lahko opazujemo svetlobo, ki nastaja kjerkoli. Med najbolj prijazne scintilatorje – tako pravimo pobjiskavajočim se snovem – sodi kristaliziran natrijev jodid s primesjo talija.

Tudi večše oči raziskovalcev so zamenjala elektronska čutila. Razvoj elektronike je prinesel fotopomnoževalke. Cilindrični kristal natrijevega jodida, postavljen na fotopomnoževalko, imenujemo scintilacijski števec (slika 3). Delci svetlobe, fotoni, ki se rode znotraj kristala ob prehodu delca alfa ali beta, odletavajo v vse smeri. Kristal je obdan z magnezijevim oksidom, ki odbija fotone. Ti lahko izstopijo le v fotopomnoževalko. Fotopomnoževalka ima na vrhu fotokatodo, posebno plast, iz katere fotoni izbijejo elektrone, sami pa izginejo. Teh elektronov je precej manj, kot pa bi jih iztržili za enako sevanje v polprevodniškem detektorju. Vendar pa tu zgodbe še ni konec. Izbite

elektrone vabi naslednja elektroda, ki je priključena na pozitivno napetost. Znotraj fotopomnoževalke je vakuum, tako da imajo elektroni prosto pot. Proti prvi elektrodi lete vedno hitreje. Če prilete do te elektrode z dovolj veliko hitrostjo, v elektrodi ne obtiče, ampak se od nje odbijejo in hkrati izbijejo še nove elektrone, morda enega ali dva. Odbite in izbite elektrone pritegne naslednja elektroda, še bolj pozitivna od prve. Na tej elektrodi, kjer se igra ponovi, naštejemo lahko že štiri do devet elektronov. Takih elektrod, ki jim pravimo dinode, je do deset. Na zadnji dinodi polovimo pomnoženi plaz elektronov. Ko stečejo zbrani elektroni prek upora, se na njem pojavi napetostni sunek, ki traja nekaj deset milijonin sekunde. Velikost sunka je sorazmerna energiji, ki jo je v kristal natrijevega jodida prinesel delec, odvisna pa je tudi od napetosti med posameznimi pomnoževalnimi elektrodami. Z lahkoto dobimo sunke nekaj deset ali sto milivoltov, ki jih ni težko preštovati in sortirati po velikosti ter tako meriti tudi energije zaznanih delcev.

Preostali so nam delci gama, ki so fotoni s precej večjimi energijami, kot jih najdemo v vidni svetlobi. Foton nima električnega naboja in pri

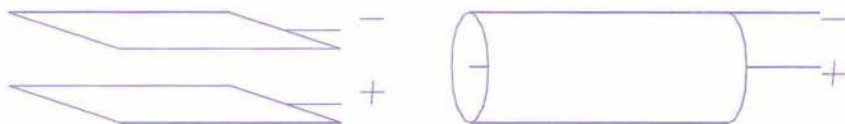


Slika 3. Scintilacijski detektor. Z uporovno verigo porazdelimo visoko napetost po posameznih dinodah.

prehodu skozi snov vzdolž poti ne sprošča elektronov. Lahko pa se mu zgodi, da trešči naravnost v kakšen elektron, ga odbije in mu preda del svoje energije, včasih pa kar vso. Tak pojav omogoča posredno zaznavo sevanja gama. Veliki kristali natrijevega jodida s premerom 5 cm in z enako višino so prav primerni za zaznavo sevanja gama.

Sicer pa, dragi Bine, vse tole bo predrago za raziskovanje tvojih radioaktivnih kumaric. Priporočam ti geigerski števec, ki je sicer neumen in ne daje podatkov o energiji zaznanega delca, zato pa jih javlja glasno in jasno s sunki, ki so lahko veliki celo 10 V ali več. Za take sunke potrebujemo milijone in milijone elektronov. Kako do njih?

V geigerskem števcu pride do podobnega pomnoževanja kot v scintilacijskem števcu. Da bomo razumeli pomnoževanje, se vrnimo k prvotnemu ploščnemu kondenzatorju, kjer smo lovili elektrone in ione, rojene med ploščama. Plošči sta vlekli nabite delce vsaksebi ves čas z enako silo, molekule zraka so gibanje zavirale, zato so se delci gibali enakomerno proti cilju. Če pa uporabimo cilindrično ogrado, priključeno na negativno napetost, s tanko žico v sredini, priključeno na pozitivno napetost, dobimo nehomogeno električno polje (slika 4). Bliže smo žici, močnejše je polje. Zato bo na poti proti žici hitrost elektronov naraščala. Elektron, ki z dovolj veliko hitrostjo trči ob molekulo plina, jo lahko ionizira. Namesto enega elektrona imamo po trku dva. Zgodba se ponavlja, elektroni se množe, do žice pride cel plaz elektronov.



Slika 4. Električno polje med nabitima ploščama je povsod enako močno. Električno polje v nabiti valjasti cevi raste proti tanki žici, napeti po osi.

Tlak plina v geigerskem števcu je precej pod atmosferskim tlakom. Ob bolj redkih trkih ima elektron večjo možnost, da si nabere dovolj energije za ionizacijo. Geigerski števec potrebuje za normalno delovanje napetost le nekaj sto voltov.

Dragi Bine, toliko za tokrat o svetu atomov.

Pozdravlja te

Dr. Nula,
predstojnik patentnega urada

Jože Pahor

KRŽANKA “MEHANIKA”

	KOLIČNIK POTI IN ČASA	PRODUKT VZTRAJN. MOMENTA IN KOTNE HITROSTI	ANDREJ HIENG	STANO- VANSKI PROSTOR	OGNOJEK NA KOŽI, TUR	SMUČAR, REŠEVALNA PRIPRAVA	DEL MESTA KVART		PRIMOŽ PETERKA	HRUP TRUŠČ	OLIVNO ZELEN MINERAL	AFRI- ZNAI DOLČ VRAT
BAHAČ, DOMŠ- LJAVEC (REDKO)								DOTIK DVEH TELES S POPOLNIM ODBOJEM				
IRHAŠTE HLAČE								UMETNA SNOV ZA IZDELAVO UMETNIH VLAKEN				
ENAKI ČRKI			NEKD. KEN. TEKAC (MIKE) NASPROTJE MLADOSTI					ZA RENOM DRUGA NAJVEČJA REKA V ŠVICI	MESTO V VZHOODNI SRBIJI MEHANIČNO UCENJE			
GRAFIK, ILUS- TRATOR						NAŠA SOPRA- NISTKA (NORINA)						
VELIK PRITOK DONAVE IZ ROMUNIJE				SPOŠTLJIV IZRAZ ZA ODRASLO ZENSKO	DEJAVNIK, POVZRO- ČITE LJ	KNIŽNI IZRAZ ZA HINAVCA, LICEMERCA						
ČISTOČA							OZNAKA MESTA REKA			VRTILNI MOMENT ISLAMSKE DUHOVNOSTI		
							IGRALEC WALLACH UGOTAVLJ. VELIKOSTI KOLIČINE				UMETNIŠKO DELO	MEH- SRBI OBU PESN NO
IGRALSKO OBLAČILO								IZUM, KI OMOGOČA PREMI- KANJE VOZILA	USEDLJINA NA REČNEM ALI JEZERSKEM DNJU			
KOLIČINA, KI OPRE- DELJUJE SPREMEM. HITROSTI								FRANC. SMUČAR (SEBASTIEN) KLESTILNI NOŽ				
ZVIŠAN DARITVENI PROSTOR						NEMŠKI GENERAL V AFRIKI MEDLA SVETLOBA						
ZNAK ZA LITU			KRAJ PRI DOMZALAH	POGONSKO SREDSTVO ZA WATTOV STROJ	KOLIČINA, KI POVZROČI PREMIK ALI DEFORMA- CIJO TELES					SENZOR PRISTANIŠČE V JEMNU		
POLNA LUNA					KDOR ŽIVI NA OTOKU NAJDAJŠA REKA NA SVETU							MIT FENI KRAJ KADI OC
SINUSNO PERIODIČ. GIBANJE								TV NOVINAR PUCER ROSVITA PESEK				OTOK ANG IN IR JUI IVANI
VELIKO JEZERO NA SEVERU FINSKE						GIBANJE TELESA OKOLI OSI, ROTACIJA						
FREKVENČ. OBMOČJE ODDANJA RADIJSKE POSTAJE						IME ROMUN-FRANC. PISATELJA ISTRATJA, AVTORJA NOVELE "KIRA KIRALINA"						

SKA Z JIM OM	ŽLAHTNI PLIN (Ne)	OTOK SZ OD ZADRA	TINA TURNER	PRED- STAVNIK REIZMA	PRVI KRŠČAN. ZAKRAMENT		MODRO ZELEN POLDRAG KAMEN	OČE	NINO ROBIČ	PRODUKT MASE TELESA IN NJEGOVE HITROSTI	VINO Z OTOKA VISA
						STANDARDNI PLES ARGENTIN. IZVORA					
						PULZ					
						SHOD. ZBORO- VANJE					
			ŽAREČ DROBEČ SNOVI						OZNAKA BOLOGNE		
									ZMEDA, NERED		
		SL. JEZIKO- SLOVEC, PREŠENOV PRIJATELJ (MATIJA)	JAVK SEDMI PLANET OSONČJA					POGANJEK IZ SEMENA			
								ŽIVO SREBRO			
	ZAZNAVNA SPOSOB- NOST BOHINJSKA PLANINA				TELO, KI SE ODKLANJA OD RAVNOVE- SNE LEGE						
				ENOTA ZA SILO PO ANG. FIZIKU	SILA NA TELESA V TEKOČINI ZNAK ZA MNOŽENJE						GIBANJE TELESA PROTI TLEM ZA- RADI TEŽE
KA SKA FEV ICA ZY							POSUŠENA TRAVA ZA KRMO	KRAJ PRI GRO- SUPLJEM			
								FINTA			
		NEMŠKI FIZIK (WALTER) NASPROTJE PORAZA							KRANJ		
			PO BITKI ZNAN KRAJ V BELGIJI PEVKA GODEC						ESTETSKA VREDNOTA		
	IGRALCA DAMON IN DILLON					FIZIK BOHR					
	UM					NAJVEČJI GRŠKI OTOK					
					PILOTSKA KABINA (PONAŠENO) PREDNIKI MADŽAROV						
OL- CAN- LJ. MOV- E											
MED- LJO SKO RE- JSIČ				DEDNA MASA ORGANIZMA UROŠ ZUPAN							
		LAHKOŽIVKA IZ VIŠJIH SLOJEV LJUDI									
		SLABŠALNI IZRAZ ZA AZUČA									
								SESTAVIL MARKO BOKALIČ	LATINSKI PREDLOG		

RAČUNALA NOVE DOBE, 2. del

Matematiko lahko definiramo kot predmet, pri katerem nikoli ne vemo, o čem govorimo, niti nikoli ne vemo, ali je tisto, kar pravimo, resnično.

Bertrand Russell

V prejšnji številki Preseka smo z analizo seštevanja in množenja naravnih, celih oziroma racionalnih števil vpeljali pojma *grupa* in *obseg*, ki imata pomembno vlogo v algebri. Ponovimo:

V grupi $(G, \circ)$ velja:

- (G1) za vsaka elementa $a, b \in G$ je $a \circ b \in G$;
- (G2) obstaja tak element $e \in G$, da za vsak element $g \in G$ velja $e \circ g = g \circ e = g$;
- (G3) za vsak element $g \in G$ obstaja tak element $f \in G$, da je $g \circ f = f \circ g = e$;
- (G4) za vse elemente $a, b, c \in G$ velja $(a \circ b) \circ c = a \circ (b \circ c)$.

V obsegu $(\mathcal{O}, +, *)$ pa velja:

- (O1) par $(\mathcal{O}, +)$ je grupa z enoto 0;
- (O2) par $(\mathcal{O} \setminus \{0\}, *)$ je grupa z enoto 1;
- (O3) za vse elemente $a, b, c \in \mathcal{O}$ je $a * (b + c) = a * b + a * c$ in $(b + c) * a = b * a + c * a$.

V tem sestavku bomo odgovorili na vprašanja o najmanjših grupah in obsegih ter na še nekatera sorodna vprašanja, naš cilj pa so končni obsegi, t.j. končne strukture, v katerih bomo znali ne samo seštevati in množiti, pač pa tudi odštevati in deliti.

Gotovo ste hitro ugotovili, da mora imeti grupa zaradi aksioma (G2) vsaj en element, enoto e namreč, obseg pa vsaj dva, enoto za operacijo “+” in enoto za operacijo “*”. Nadalje se ni težko prepričati, da en element v primeru grupe že zadošča, saj $e \circ e = e$ izpolnjuje vse aksiome (G1)–(G4). V primeru obsega z dvema elementoma enako velja za multiplikativno grupo: $1 * 1 = 1$ izpolni aksiom (O2).

Ne pozabite, da operaciji “+” in “*” ne predstavljata (nujno) običajnega seštevanja in množenja. V tem sestavku bomo spoznali kar nekaj takih obsegov. V vsakem obsegu je produkt poljubnega elementa a z aditivno enoto 0 enak 0, saj je $0 * a = (0 + 0) * a = 0 * a + 0 * a$ (upoštevati smo (G2) in (O3)). Če odštejemo $0 * a$, res dobimo $0 * a = 0$. Podobno dobimo, da je tudi $a * 0 = 0$. V primeru najmanjšega obsega zato velja $0 * 0 = 0$ in $0 * 1 = 0 = 1 * 0$, kjer je 1 multiplikativna enota.

Kako pa je z grupo, ki ima dva elementa, npr. enoto e in a ? Poleg $e \circ e = e$ in $e \circ a = a = a \circ e$ mora zaradi (G3) in $e \neq a$ veljati še $a \circ a = e$ in že so izpolnjeni vsi aksiomi (G1)-(G4). Torej velja za obseg z dvema elementoma in pravkar odkrito aditivno grupo tudi aksiom (O1). Zlahka preverimo še (O3), torej smo že našli najmanjši obseg.

Vrnimo se k vprašanju, koliko informacij potrebujemo za določitev grupe kot matematičnega objekta. Na to vprašanje je leta 1854 odgovoril *Arthur Cayley*. Po analogiji s tabelo množenja je vpeljal tabelo za poljubno binarno operacijo, ki ji bomo rekli *komponiranje*. Elemente množice G , v kateri je definirano komponiranje, razporedimo v zgornjo vrstico tabele in v enakem vrstnem redu še v levi stolpec tabele (imenovali ju bomo *koordinatna vrstica in stolpec*). V polja tabele pa vpišemo ustrezne *kompozitume* (tabeli 6a in 6b).

+	0	1
0	0	1
1	1	0

(a)

*	0	1
0	0	0
1	0	1

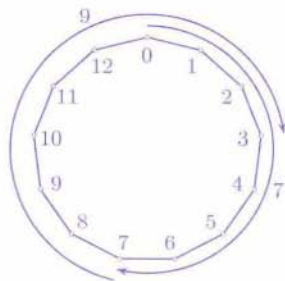
(b)

Tabela 6. Najmanjši obseg ima dva elementa, tabeli za njegovi operaciji pa sta (a) za seštevanje in (b) za množenje.

Gotovo ste opazili, da je $1+1=0$. V naslednjem razdelku bo postalo jasno, da ne gre za napako. Omeniti moramo le še, da pri iskanju grupe z enim in dvema elementoma sploh nismo imeli izbire pri določanju tabele, pri grupi s štirimi elementi pa obstajata že natanko dve različni grupi (ena ustreza grupi simetrij pravokotnika, drugo pa boste spoznali v naslednjem razdelku).

Praštevski obseg $\mathbb{Z}_p$

Namesto s celimi števili bomo tokrat računali z ostanki pri deljenju s 13, t.j. z elementi iz množice $\mathbb{Z}_{13} = \{0, 1, \dots, 12\}$. Računamo na naslednji način: števili seštejemo ali zmnožimo tako, da običajni rezultat nadomestimo z njegovim ostankom pri deljenju z *modulom* 13, npr. $7 +_{13} 9 = 7 + 9 \bmod 13 = 3$ in $5 \cdot_{13} 4 = 5 \cdot 4 \bmod 13 = 7$, saj ima pri deljenju s 13 vsota 16 ostanek 3, produkt 20 pa ostanek 7 (tabela 7 in slika 1).



Slika 1. Prikaz računanja po modulu 13.

+13	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	3	4	5	6	7	8	9	10	11	12	0	1
3	3	4	5	6	7	8	9	10	11	12	0	1	2
4	4	5	6	7	8	9	10	11	12	0	1	2	3
5	5	6	7	8	9	10	11	12	0	1	2	3	4
6	6	7	8	9	10	11	12	0	1	2	3	4	5
7	7	8	9	10	11	12	0	1	2	3	4	5	6
8	8	9	10	11	12	0	1	2	3	4	5	6	7
9	9	10	11	12	0	1	2	3	4	5	6	7	8
10	10	11	12	0	1	2	3	4	5	6	7	8	9
11	11	12	0	1	2	3	4	5	6	7	8	9	10
12	12	0	1	2	3	4	5	6	7	8	9	10	11

*13	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

(a)

(b)

Tabela 7. Seštevanje po modulu 13 (a), množenje po modulu 13 (b).

Če želimo sešteti ali zmnožiti več števil iz $\mathbb{Z}_{13}$, lahko pridemo do pravega rezultata tudi tako, da števila najprej seštejemo oziroma zmnožimo kot običajna cela števila in šele nato poiščemo ostanek pri deljenju s 13. To pomeni, da iz zakonov o združevanju celih števil za seštevanje in množenje (asociativnost) ter zakona o razčlenjevanju (distributivnost) sledi veljavnost zakonov o združevanju za seštevanje in množenje ter razčlenjevanju po modulu.

Pozoren bralec bo opazil, da se v vsakem stolpcu in v vsaki vrstici tabele za seštevanje nahajajo prav vsi elementi iz $\mathbb{Z}_{13}$. Podobno velja tudi za tabelo množenja, če odmislimo vse ničle. (Če bi 13 nadomestili s 14, bi videli, da tabela množenja po modulu 14 nima te lastnosti; le-ta je rezervirana samo za praštevila.) Torej lahko s pomočjo tabel 7(a) in 7(b) najdemo tudi razlike in kvociente. Če želimo izračunati $2 :_{13} 7$, iščemo odgovor na vprašanje, 7 krat koliko je 2. V tabeli 7(b) izberemo vrstico, ki ustreza številu 7, in ugotovimo, da se število 2 nahaja v stolpcu, ki pripada številu 4. Zato zaključimo, da je $2 :_{13} 7 = 4$. Do enakega zaključka bi prišli tudi, če bi številu 2 prišteli število 13 tolikokrat, da bi dobljena vsota postala deljiva s 7 in bi nato izračunali kvocient. Povejmo, da ne moremo izračunati $2 :_{14} 7$, torej $2 : 7$ v množici $\mathbb{Z}_{14}$. Zakaj ne?

S pomočjo tabel se ni težko prepričati, da je trojica $(\mathbb{Z}_{13}, +_{13}, *_{13})$ obseg. Prav tako hitro ugotovimo, da je $(\mathbb{Z}_n, +_n)$ grupa za poljubno naravno število n . Z razširjenim Evklidovim algoritmom (glej članka

M. Juvana, *O Evklidovem algoritmu*, Presek **21** (1993–94), str. 116–121, ter A. Jurišića, *Kako deliti skrivnost?*, Presek **29** (2001–02), str. 356–364), pa lahko enako pokažemo tudi za $(\mathbb{Z}_p \setminus \{0\}, *_p)$, kjer je p poljubno praštevilo. Tako pridemo do **praštevilskega obsega** $(\mathbb{Z}_p, +_p, *_p)$.

Tabele in grupe

Sedaj si oglejmo tabele nekoliko поблиže. Vprašali se bomo, kako lahko iz tabele ugotovimo, ali gre za grupo. Pri tem bomo opazovali naslednje lastnosti:

- (T1) V tabeli se lahko pojavijo samo tisti elementi, ki jih komponiramo.
- (T2) Ena vrstica in en stolpec morata biti element za elementom enaka koordinatni vrstici in koordinatnemu stolpcu, množica enot v tabeli pa je simetrična glede na glavno diagonalo, t.j. diagonalo, ki izhaja iz levega zgornjega kota.
- (T3) V vsaki vrstici in vsakem stolpcu se pojavi vsak element natanko enkrat.
- (T4) V tabeli si izberimo enoto e in v njeni vrstici oziroma stolpcu še element r oziroma s . Potem je element, ki leži v isti vrstici kot s in istem stolpcu kot r , enak $s \circ r$, (tabela 8(b)).

$\circ$				$\circ$	x'	y
				y'	$s \circ r$	s
		$?$	s	x	r	e
		r	e			

(a)
(b)

Tabela 8.

Lastnost (T1) je ekvivalentna zaprtosti množice za komponiranje, medtem ko je lastnost (T2) ekvivalentna obstoju enote. Tablicam, ki zadovoljujejo lastnost (T3), pravimo *latinski kvadrati*. Lastnost (T3) je ekvivalentna zahtevi, da sta za poljubna elementa a in b enačbi $a \circ x = b$ in $x \circ a = b$ rešljivi, saj v vrstici oziroma stolpcu, ki ustreza elementu a , poiščemo element b , katerega stolpec oziroma vrstica ustreza elementu x . Če si za b izberemo enoto, potem nam ta lastnost zagotavlja obstoj inverznega elementa za vsak a . Prepričajmo se še, da velja lastnost (T4) v vsaki

grupi z enoto e (tabela 8(b)). Iz $x \circ y = e$, $x \circ x' = r$ in $y' \circ y = s$ namreč sledi $y \circ x = e$ in

$$y' \circ x' = (y' \circ e) \circ x' = y' \circ e \circ x' = (y' \circ (y \circ x)) \circ x' = (y' \circ y) \circ (x \circ x') = s \circ r.$$

Velja pa tudi obratno: pogoji (T1)–(T4) nam zagotavljajo, da tabela za komponiranje ustreza neki grupi.

Izrek. Tabela za komponiranje ustreza lastnostim (T1)–(T4) natanko takrat, ko je tabela neke grupe.

Dokaz. Prepričati se moramo le še, da iz (T1)–(T4) sledi asociativnost. Najprej izpeljemo asociativnost za elemente b^{-1} , b in c , t.j. $c = (b^{-1} \circ b) \circ c = b^{-1} \circ (b \circ c)$. Seveda lahko privzamemo $e \neq b$ in $c \neq b^{-1}$, saj je tedaj pogoj (G4) očitno izpolnjen. V tabeli izberemo vrstici e in b ter stolpca c in b^{-1} . Zapišemo ustrezne produkte, uporabimo (T4) in dobimo želeno relacijo (tabela 9(a)).

$\circ$	c	b^{-1}
$e = b^{-1} \circ b$	$c = b^{-1} \circ (b \circ c)$	b^{-1}
b	$b \circ c$	e

(a)

$\circ$	$b \circ c$	b
a	$a \circ (b \circ c) = (a \circ b) \circ c$	$a \circ b$
b^{-1}	$b^{-1} \circ (b \circ c) = c$	e

(b)

Tabela 9.

Sedaj pokažimo asociativnost še za poljubne elemente, t.j. $a \circ (b \circ c) = (a \circ b) \circ c$. Privzamemo $a \neq b^{-1}$ in $c \neq e$, kajti sicer sledi želeni relacija iz pravkar obdelanega posebnega primera. Izberemo si vrstici a in b^{-1} ter stolpca $b \circ c$ in b ter uporabimo lastnost (T4) (tabela 9(b)).

Končni obseg $\text{GF}(p^n)$

Pokažimo, da tabeli 10(a) in 10(b) ustrezata grupnima operacijama in da je množica binarnih trojic $\{000, 001, 010, 011, 100, 101, 110, 111\}$ za ti operaciji obseg.

Zakon o združevanju (asociativnost) za seštevanje je pravzaprav očitni, saj seštevanje poteka tako, da seštevamo trojice po mestih (prvo, drugo in tretje) po modulu 2 (tabela 6(a)). Zato označimo to grupo z $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +_2)$. Zakona o združevanju za množenje in zakona o razčlenjevanju (distributivnost) pa ni tako lahko neposredno preveriti. Če pa v ta namen uporabimo zgornji izrek, si lahko pomagamo z zakonom o zamenjavi, saj sta tabeli simetrični glede na glavno diagonalno.

+	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

(a)

*	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	111	101	011	001	100	110
011	000	011	101	110	111	100	010	001
100	000	100	011	111	010	110	001	101
101	000	101	001	100	110	011	111	010
110	000	110	100	010	001	111	101	011
111	000	111	110	001	101	010	011	100

(b)

Tabela 10. Seštevanje (a), množenje (b).

Za konec vključimo v našo zgodbo še polinome s stopnjo, manjšo od n , $n \in \mathbb{N}$, in s koeficienti iz obsega $(\mathbb{Z}_p, +_p, *_p)$, kjer je p praštevilo. Te polinome seštevamo na enak način kot števila v tabeli 10(a), le da tokrat seštevamo enakoležne koeficiente. Množimo jih tako, da običajni produkt zmanjšamo po modulu nekega polinoma stopnje n , ki ga ne moremo razcepiti v obsegu $(\mathbb{Z}_p, +_p, *_p)$. Tako zopet dobimo končni obseg. Matematikom je celo uspelo dokazati, da mora biti vsak končni obseg take oblike in da velja za množenje zakon o zamenjavi (Wedderburnov izrek), a to že presega okvir našega razmišljanja. Omenimo le še, da jih imenujemo **Galoisovi obsegi** in jih označimo z $\text{GF}(p^n)$. Za $n = 1$ dobimo seveda prašteviliški obseg.

Primer. Naj bo $n = 3$, $p = 2$ (tabeli 6(a) in 6(b)), za nerazcepni polinom pa si izberemo $x^3 + x^2 + 1$. Potem v zgornjih binarnih trojicah prvo mesto ustreza koeficientu ob x^3 , drugo koeficientu ob x^2 , tretje pa konstantnemu koeficientu.

Opomba. Osnova za Evklidov algoritem je lastnost, da lahko za vsak par naravnih števil a in b , $a > b$, najdemo natanko določeni števili q in r , da velja $a = qb + r$, kjer je ostanek r manjši od b . Za polinoma $a(x)$ in $b(x)$ nad končnim obsegom, $\text{st}(a) > \text{st}(b)$ (st je oznaka za stopnjo polinoma) pa velja $a(x) = q(x)b(x) + r(x)$, kjer je $\text{st}(b) > \text{st}(r)$. Za zgled pokažimo, kako z razširjenim Evklidovim algoritmom poiščemo obratni element polinoma $x^4 + x + 1$ v obsegu $\text{GF}(2^5)$ z nerazcepnim polinomom $x^5 + x^2 + 1$. Leva stran ustreza Evklidovemu algoritmu, desna pa razširjenemu delu:

$$x^5 + x^2 + 1 = x(x^4 + x + 1) + x + 1$$

$$x \cdot 1 + 0 = x$$

$$x^4 + x + 1 = (x^3 + x^2 + x + 1)(x + 1) + 1 \quad (x^3 + x^2 + x + 1)x + 1 = x^4 + x^3 + x^2 + 1$$

Naloge

1. Isto grupo lahko srečamo v različnih preoblekah. Prepričaj se o tem za grupo $(\mathbb{Z}_4, +_4)$ in množico $\{1, -1, i, -i\}$, kjer je $i = \sqrt{-1}$, z običajnim množenjem. Potrebno je najti bijekcijo iz $\mathbb{Z}_4$ v $\{1, -1, i, -i\}$, ki preslika vsoto dveh elementov v produkt njihovih slik. Taki preslikavi pravimo *izomorfizem*.
2. Znano je, da je multiplikativna grupa poljubnega končnega obsega *ciklična*, kar pomeni, da v grupi obstaja tak element, da so vsi elementi grupe njegove potence. Prepričaj se, da je ciklična grupa z n elementi izomorfna grupi $(\mathbb{Z}_n, +_n)$ (element 1 *generira* s svojimi večkratniki, kakor v aditivnem primeru pravimo potencam, vse elemente). To grupo označimo na kratko s C_n . Trditev preveri najprej na primeru (tabela 7(b) in 10(b)).
3. *Diederska grupa* D_n je grupa simetrij pravih n -kotnika. Pokaži, da v grupi D_3 ne velja zakon o zamenjavi (komutativnost) (grupo D_3 lahko predstavimo tudi kot grupo permutacij treh elementov S_3).
4. Naslednja zanimiva grupa ima 8 elementov in ji pravimo *kvaterni-onka* (tabela 11). Poišči njeno tabelo množenja.

moč	ime grupe
1	C_1
2	C_2
3	C_3
4	$C_4, C_2 \times C_2$
5	C_5
6	C_6, D_3
7	C_7
8	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, D_8, Q_8$
9	$C_9, C_3 \times C_3$
10	C_{10}, D_{10}

Tabela 11. Moč grupe je število njenih elementov. Zgornja tabela vsebuje vse grupe z največ desetimi elementi.

Za nadaljnje branje priporočamo: I. Grossman in W. Magnus, *Grupe in njihovi grafovi*, Školska knjiga Zagreb, 1975 in internet, npr. <http://members.tripod.com/dogschoo1/>, za zrelejšje bralce pa Vidav, *Algebra*, Mladinska knjiga, 1972.

Aleksandar Jurišić

ŠE VEČ VODIKOVIH ANTIATOMOV

V prejšnji številki je Presek poročal o vodikovih antiatomih, ki jih je dobila mednarodna raziskovalna skupina ATHENA v Evropskem laboratoriju CERN v Ženevi. S to skupino tekmuje v istem laboratoriju druga, nekoliko manjša mednarodna raziskovalna skupina ATRAP s 15 člani z nemških, ameriških in kanadskih inštitutov ter univerz. Nekateri njeni člani so sodelovali že pri poskusih z antiatomi vodika leta 1996. Vodi jo Gerald Gabrielse, znan po poskusih, pri katerih so v pasti zadrževali več tisoč antiprotonov dlje kot dva meseca. Tudi ta skupina uporablja Penningovo past, v kateri je na skupni osi priključenih na različne napetosti več valjastih elektrod z enakim premerom. Elektrode so v močnem magnetnem polju v smeri osi.

Antiprotone iz antiprotonskega pojemalnika zavrejo in jih vložijo v past ter pozitrone iz umetnega radioaktivnega izotopa natrija zavrejo in jih vložijo v past. Oboji delci zaradi nasprotnega naboja ne morejo mirovati v istem delu pasti. Oblak pozitronov miruje na sredi, oblak antiprotonov pa niha skozenj. Pri tem se antiprotoni vežejo s pozitroni v vodikove antiatome. Do sem ni bilo omembe vrednih razlik med poskusoma obeh skupin. Le napravo druge skupine so hladili s tekočim helijem, ki pri navadnem zračnem tlaku vre pri temperaturi 4,2 stopinje nad absolutno ničlo. Oblak pozitronov v pasti se je tako ohladil do te temperature in preko njega tudi oblak antiprotonov. Pri poskusu prve skupine so oblaka ohladili le na 15 stopinj nad absolutno ničlo. Druga skupina je bila leta 2001 uspešnejša kot prva, tako da je objava prve skupine septembra lani vse nekoliko presenetila. V novembru in decembru je o svojih dosežkih poročala druga skupina – ATRAP.

Druga skupina je antiatome zaznavala drugače kot prva, na način bolj prilagojen atomski fiziki. Antiatome, ki so se oddaljili od srednjega dela pasti, so v močnem električnem polju ionizirali v antiprotone in pozitrone. Antiprotone so zbrali in jih prešteli v *ionizacijski pasti*. Posebej so se prepričali, da je pri tem šlo za antiprotone iz antiatomov in ne morda za antiprotone iz nihajočega oblaka. Ti antiprotoni so se pojavili samo, če so bili v pasti tudi pozitroni. Antiprotoni iz oblaka pa so imeli preveliko energijo, da bi jih mogla zadržati ionizacijska past. Zaznali so 657 antiatomov in po tem sklepali, da je nastalo kakih 170 tisoč antiatomov. Ne brez ponosa so zapisali: "V eni uri lahko ujamemo več antiprotonov iz ioniziranih atomov $\bar{H}$, kot je skupaj vseh antiatomov, o katerih so poročali doslej."

Nov korak so naredili s tem, da so raziskali energijo nastalih antiatomov. Antiatomi lahko nastanejo na dva načina. Pri prvem sodelujejo trije delci: pozitron se z antiprotonom spoji v antiatom, drugi pozitron pa prevzame presežno energijo. Pri drugem pa sodelujeta samo dva delca: antiproton ujame pozitron in presežno energijo prevzame izsevani foton. Antiatomi so nastali na prvi način in so imeli precejšnjo energijo. Opazovali so, kako se število antiprotonov v ionizacijski pasti spreminja v odvisnosti od električnega polja v njej. Čim više je antiatom vzbujen, tem manjšo energijo mu je treba dovesti, da se razdeli na antiproton in pozitron – tem šibkejše električno polje ga ionizira. Število zbranih antiprotonov se je manjšalo, ko so uporabili vse močnejše električno polje. Toda ko je preseglo določeno mejo, se je število nehalo manjšati. Po tem so sklepali, da so nastali antiatomi v visokih vzbujenih stanjih nad petdesetim. Atome v visokih vzbujenih stanjih imenujejo *Rydbergovi atomi*. Za odločilne poskuse, ki naj bi pokazali, ali se energije antiatomov natanko ujemajo z ustreznimi energijami atomov, pa bi potrebovali antiatome v osnovnem stanju. Ponavadi je težavni del naloge, kako dobiti Rydbergove atome. V tem primeru pa je naloga obrnjena. Kako spraviti antiatome v kratkem času brez večjih izgub v osnovno stanje? V novi vrsti poskusov, ki jih bodo začeli junija, bodo poskušali z obsevanjem z lasersko svetlobo doseči, da bi antiatomi s sevanjem iz vzbujenih stanj čim prej prešli v osnovno stanje.

Čeprav poskusi akupine ATRAP pomenijo korak naprej, je vendar ostalo več odprtih vprašanj. Med drugim opozarjajo, da je zaznavanje antiatomov z ionizacijo lahko precej nezanesljivo, posebno zaradi močnega magnetnega polja. Skupina ATHENA meni, da so pri njenih poskusih nastali večinoma antiatomi v osnovnem stanju. Tako vse kaže, da se bo tekmovanje obeh skupin še nadaljevalo.

Janez Strnad

PERIODIČNI DECIMALNI ZAPIS – Rešitev s str. 260

Samo 3 in 6 sta taki števili, tretji primer v vprašanju je namreč lažen in je tam le za boljše razumevanje problema. Dokažimo to trditev!

Za števila od 1 do 10 trditev preverimo v eni minuti z žepnim računalom. Zato naj bo odslej $x \geq 11$ in naj velja

$$\frac{1}{x} = 0.\boxed{z}\boxed{x}\boxed{x}\boxed{x}\dots,$$

kjer ima predalček $\boxed{x}$ dolžino m (v njem je m števk), predalček $\boxed{z}$ pa dolžino n . V igri imamo torej štiri naravna števila x, z, m, n , ki zadoščajo trem pogojem:

$$11 \leq x < 10^m \quad (m > 1), \quad 0 \leq z < 10^n, \\ \frac{1}{x} = z \cdot 10^{-n} + x \cdot 10^{-m-n} + x \cdot 10^{-2m-n} + x \cdot 10^{-3m-n} + \dots \quad (1)$$

Kolik je n , ni natanko določeno, saj lahko k $\boxed{z}$ pripišemo nekaj ponovitev predalčka $\boxed{x}$. Tako torej lahko zapišemo $\frac{1}{3} = 0.33\bar{3}$, pa je $z = 33$ in $n = 2$. Odslej bomo zato privzeli, da je $n > 1$.

V pogoju (1) tvorijo členi, ki vsebujejo x , geometrijsko vrsto, ki jo znamo sešteti. Velja

$$\frac{1}{x} = z \cdot 10^{-n} + \frac{x \cdot 10^{-m-n}}{1 - 10^{-m}},$$

kar preuredimo takole:

$$10^n = xz + \frac{x^2}{10^m - 1}. \quad (2)$$

Sledi, da $(10^m - 1)$ deli x^2 .

Recimo, da ima $10^m - 1$ praštevilski faktor p^a z lihim eksponentom a . Ker se $10^m - 1$ končuje s števk 9, je $p \neq 2, p \neq 5$. Seveda mora biti tudi x deljiv s p , x^2 vsebuje torej sodo potenco praštevila p , kvocient $\frac{x^2}{10^m - 1}$ pa zato liho potenco p . V (2) je potemtakem desna stran deljiva s p , kar pa je v protislovju z dejstvom, da ima leva stran praštevilski razcep $2^n \cdot 5^n$.

Vsi praštevilski faktorji v $10^m - 1$ torej nastopajo le s sodimi eksponenti, zato je $10^m - 1 = y^2$. Ta **diofantska enačba** pa za $m > 1$ nima rešitve, kar sprevidimo takole: $10^m - 1$ je liho število, zato je tak tudi y , torej $y = 2k - 1$. Potem je $2^m 5^m - 1 = 4k^2 - 4k + 1$ ali, malo drugače, $2^m 5^m - 4k^2 + 4k = 2$. Ker je $m > 1$, je v tej enačbi leva stran deljiva s 4, desna pa ne. Dokaz je s tem končan.

Opomba. Diofantske enačbe so enačbe, v katerih so koeficienti in neznanke cela števila. Od preprostega vprašanja, ki nima takega globljega pomena, razen možganskega treninga, smo prišli do diofantske enačbe $10^m - 1 = y^2$, ki pa je precej bolj resna stvar. Kdor bi rad kaj več vedel o tej vrsti diofantskih enačb, naj si ogleda članek J. H. E. Cohn: *The diophantine equation $x^2 + C = y^n$* . Acta Arith. **65** (1993), 367–381.

Anton Cedilnik

REŠITVE NALOG Z DRŽAVNEGA TEKMOVANJA IZ SREDNJEŠOLSKE FIZIKE V ŠOLSKEM LETU 2001/2002 – s str. 252

Objavljamo rešitve nalog z državnega tekmovanja srednješolcev iz fizike, ki je bilo v Mariboru 13. aprila 2002. Besedila nalog smo objavili v letošnji četrti številki Preseka.

Skupina I

1. Podatki: $h_G = 20$ m, $h_M = 40$ m, $v_0 = 7$ m/s.

a) Gibanje žoge opišemo kot navpični met. Višino Gregorjeve žoge ob času t označimo z y_G , višino Majine z y_M . Velja

$$y_G = v_0 t - \frac{1}{2} g t^2 + h_G \quad \text{in} \quad y_M = -v_0 t - \frac{1}{2} g t^2 + h_M.$$

Ob času t_1 sta obe žogi na enaki višini, $y_G = y_M$; ko izraza za višini izenačimo, dobimo

$$2v_0 t_1 = h_M - h_G, \quad t_1 = \frac{h_M - h_G}{2v_0} = 1,4 \text{ s}. \quad (1)$$

Dobljeni čas vstavimo v izraz za višino Majine (ali Gregorjeve) žoge:

$$y_G = v_0 t_1 - \frac{1}{2} g t_1^2 + h_G = h_G + \frac{1}{2} (h_M - h_G) - \frac{1}{2} g \left(\frac{h_M - h_G}{2v_0} \right)^2 = 20 \text{ m}.$$

b) Čas srečanja izrazimo z začetno hitrostjo, tako kot pri primeru a): $t_2 = (h_M - h_G)/2v_2$. (Začetno hitrost sedaj označimo z v_2 .) Iz zahteve, da se žogi srečata na višini 0, sledi

$$0 = h_G + \frac{1}{2} (h_M - h_G) - \frac{1}{2} g \left(\frac{h_M - h_G}{2v_2} \right)^2$$

in od tod

$$v_2 = \sqrt{g \frac{(h_M - h_G)^2}{4(h_M + h_G)}} = 4,0 \text{ m/s}.$$

2. Podatki: $D = 100$ cm, $d = 30$ cm, $k = 0,4$.

Listi se gibljejo hitreje od obtežilnika, zato sila trenja na obtežilnik kaže v smeri gibanja listov. Obtežilnik se giblje s pospeškom $a_o = = kmg/m = kg$. V času t , ko pride do roba, napravi pot $D = \frac{1}{2}kgt^2$, listi pa pot $D + \frac{1}{2}d = \frac{1}{2}at^2$. Za pospešek listov dobimo

$$a = kg \frac{D + \frac{1}{2}d}{D} = 4,5 \text{ m/s}^2.$$

3. Podatki: $P = 100$ W, $K = 0,80$ kg/m, $m = 350$ kg, $k = 0,010$.

a) Ker se giblje enakomerno, je sila podlage na gosenice nasprotno enaka sili upora. Moč motorja zapišemo $P = Fv = Kv^3$; od tod sledi

$$v = \sqrt[3]{\frac{P}{K}} = 5,0 \text{ m/s}.$$

b) Največja sila podlage na gosenice je kar lepenje $F_l = kmg$; iz $F_l = = F_u = Kv^2$ izračunamo

$$v = \sqrt{\frac{F_l}{K}} = 6,6 \text{ m/s} \quad \text{in} \quad P = Kv^3 = 230 \text{ W}.$$

4. Podatki: $s = 4$ m, $h = 2$ m, $\alpha = 30^\circ$, $v_0 = 15$ m/s.

Trk žogice s tlemi je neprožen, zato kot, pod katerim se žogica odbije od tal, ni enak vpadnemu kotu, prav tako nista enaki hitrosti pred odbojem in po njem. Kot β , merjen glede na vodoravnico, pod katerim se žogica odbije, in njeno hitrost tik po odboju v izračunamo iz višine stene in oddaljenosti mesta odboja od stene. Ker žogica ravno še preskoči steno, pomeni, da ima tik nad steno navpično hitrost 0. Od tod izračunamo čas, potreben da doseže višino stene $t = v \sin \beta / g$. V tem času prepotuje v vodoravni smeri razdaljo $s = = v \cos \beta t = (v^2/g) \cos \beta \sin \beta$ in v navpični smeri $h = v \sin \beta t - \frac{1}{2}gt^2 = (v^2/2g) \sin^2 \beta$. Kot najhitreje izrazimo iz razmerja

$$\frac{h}{s} = \frac{1}{2} \tan \beta, \quad \beta = 45^\circ.$$

Začetno hitrost po odboju dobimo iz izraza za višino h :

$$v = \sqrt{\frac{2gh}{\sin^2 \beta}} = \sqrt{4gh} = 8,85 \text{ m/s}.$$

Pred odbojem je hitrost žogice enaka začetni hitrosti (v_0), prav tako je vpadni kot, merjen proti vodoravnici, enak kotu (α), pod katerim jo je Miha vrgel.

Pri odboju deluje na kroglico v navpični smeri sunek navpične komponente sile podlage $F\Delta t$, v vodoravni smeri pa sunek vodoravne komponente podlage (trenja) $kF\Delta t$, kjer je k iskani koeficient trenja. Zapišimo izrek o gibalni količini za vodoravno in navpično komponento:

$$-kF\Delta t = m(v \cos \beta - v_0 \cos \alpha), \quad F\Delta t = m(v \sin \beta - (-v_0 \sin \alpha)).$$

Enačbi delimo in dobimo

$$k = \frac{v_0 \cos \alpha - v \cos \beta}{v_0 \sin \alpha + v \sin \beta} = 0,49.$$

Skupina II

- Podatki: $T_0 = 10^\circ\text{C}$, $T_2 = 65^\circ\text{C}$, $\Phi_r = 200 \text{ l/s}$, $\Phi_v = 10 \text{ l/s}$, $a = 1 \text{ m}$, $d = 2 \text{ cm}$, $\lambda = 390 \text{ W/m}\cdot\text{K}$, $c_p = 4160 \text{ J/kg}\cdot\text{K}$, $\rho = 1000 \text{ kg/m}^3$.
Količino vode, ki v času Δt priteče v rezervoar, označimo z Δm . V rezervoarju jo toplotni tok, ki ga oddaja elektrarna, segreje s temperature T_0 na temperaturo vode v rezervoarju T_1 . Toplotni tok, ki teče skozi šest sten rezervoarja, zapišemo kot $P = 6a^2\lambda(T_2 - T_1)/d$, pri čemer je T_2 temperatura zunanjega plašča rezervoarja. Zapišemo engijsko bilanco

$$\Delta mc_p(T_1 - T_0) = \frac{6a^2\lambda(T_2 - T_1)}{d} \Delta t,$$

od koder izrazimo

$$T_1 = \frac{T_2 + kT_0}{1 + k} = 51^\circ\text{C}, \quad k = \frac{c_p d \rho \Phi_v}{6a^2 \lambda}.$$

V času Δt se zmeša $\Delta m = \rho \Phi_v \Delta t$ vode s temperaturo T_1 in $\Delta m' = \rho(\Phi_r - \Phi_v)\Delta t$ s temperaturo T_0 . Velja $\Delta m(T_1 - T) = \Delta m'(T - T_0)$ oziroma $\Phi_v(T_1 - T) = (\Phi_r - \Phi_v)(T - T_0)$, pri čemer s T označimo končno temperaturo reke. Za iskano temperaturo in temperaturno razliko dobimo

$$T = \frac{\Phi_v T_1 + (\Phi_r - \Phi_v) T_0}{\Phi_r}, \quad T - T_0 = \frac{\Phi_v (T_1 - T_0)}{\Phi_r} = 2,0^\circ\text{C}.$$

2. Podatki: $d = 5 \text{ cm}$, $P = 2 \text{ kW}$, $\lambda = 0,4 \text{ W/m}\cdot\text{K}$, $T_0 = -10^\circ\text{C}$, $S = 3 \text{ m} \times 2,5 \text{ m} = 7,5 \text{ m}^2$.

Zaradi simetrije lahko vzamemo, da sta temperaturi v obeh vmesnih sobah enaki. S T_2 označimo temperaturo v sobi s pečjo in s T_1 temperaturo v zaprtih sobah brez peči. Toplotni tok skozi steni med sobo s pečjo in vmesnima sobama je enak toplotnemu toku med vmesnima sobama in sobo z odprtimi okni ter enak toplotnemu toku, ki ga oddaja peč:

$$2S \lambda \frac{T_2 - T_1}{d} = 2S \lambda \frac{T_1 - T_0}{d} = P.$$

Iz druge enakosti izračunamo $T_1 = 7^\circ\text{C}$ in nato še $T_2 = 23^\circ\text{C}$.

3. Podatki: $I = 0,1 \text{ A}$, $R = 100 \Omega$, $C = 100 \text{ nF}$.

a) Če na kondenzatorjih ni prišlo do preboja, v stacionarnem stanju skozi njih ne teče tok. Tok I tedaj teče le skozi upornik AD in zaporedno vezane upornike AB, BC in CD. Za nadomestni upor vezja R_v velja

$$\frac{1}{R_v} = \frac{1}{R} + \frac{1}{3R}, \quad R_v = \frac{3}{4} R,$$

kar pomeni, da je napetost med A in D enaka $U_{AD} = R_v I = 7,5 \text{ V}$.

- b) Zaradi simetrije je napetost U_{ED} polovica tiste med A in D, torej $U_{ED} = 3,75 \text{ V}$, med C in D pa tretjina, $U_{CD} = 2,5 \text{ V}$. Napetost na kondenzatorju EC je torej $U_{EC} = U_{ED} - U_{CD} = 1,25 \text{ V}$ in naboj $e = C U_{EC} = 1,25 \cdot 10^{-7} \text{ As}$.

Vse izračunane napetosti so manjše od maksimalne napetosti izvira.

4. Podatki: $\gamma = -5,0 \cdot 10^{-8} \text{ As/m}$, $e = -1,6 \cdot 10^{-19} \text{ As}$, $m = 9,1 \cdot 10^{-31} \text{ kg}$, $\mu_0 = 4\pi \cdot 10^{-7} \text{ Vs/Am}$.

a) Kroženje elektronov povzroča sila $\vec{F} = -e_0 \vec{v} \times \vec{B}$, ki kaže proti središču kroženja. Če ima magnetno polje smer iztegnjenega palca desne roke, ima hitrost elektronov smer prstov, tok pa zaradi negativnega naboja nasprotno smer. Takšen tok ustvarja magnetno polje, ki ima nasprotno smer kot prvotno polje.

b) Hitrost elektronov vzdolž magnetnega polja je $v_{\parallel} = v \cos \varphi$, hitrost elektronov v smeri, pravokotni na polje, pa $v_{\perp} = v \sin \varphi$. Gibajoči elektroni predstavljajo električni tok $I = \gamma v$ (glej besedilo naloge) in ustvarjajo dodatno magnetno polje, ki je v osi po velikosti enako $B' = \mu_0 N I / l = \mu_0 \gamma v / s$. Pri tem je $s = l / N$ hod vijačnice, ki ga lahko zapišemo kot $s = v_{\parallel} t_0$, kjer je t_0 čas, ki ga elektroni

potrebujejo za prelet enega hoda. To je hkrati tudi obhodni čas, s katerim elektroni krožijo v ravnini, pravokotni na smer magnetnega polja. Obhodni čas izračunamo iz drugega Newtonovega zakona za kroženje:

$$ev_{\perp}B = \frac{mv_{\perp}^2}{r}, \quad \omega = \frac{v_{\perp}}{r} = \frac{eB}{M}, \quad t_0 = \frac{2\pi}{\omega} = \frac{2\pi m}{eB}.$$

Tedaj je

$$s = \frac{2\pi m}{eB} v_{\parallel}, \quad B' = \frac{\mu_0 \gamma v}{s} = \frac{\mu_0 \gamma e}{2\pi m} B \frac{v}{v_{\parallel}} = \frac{\mu_0 \gamma e}{2\pi m} B \frac{1}{\cos \varphi}.$$

Od tod lahko izrazimo iskani kot

$$\cos \varphi = \frac{\mu_0 \gamma e}{2\pi m} \frac{B}{B'}.$$

Za $B' = B/100$ dobimo $\varphi = 80^\circ$.

Skupina III

- Podatki: $R = 20$ m, $v_0 = 80$ km/h, $k_{t2} = 0,1$.
Zapišimo Newtonov zakon za kroženje boba po ovinku z radijem R . Centripetalni pospešek kaže proti središču kroženja, torej v smeri $-\vec{R}$, in Newtonov zakon v vektorski obliki zapišemo kot

$$-m\omega^2 \vec{R} = \vec{F}_g + \vec{N} + \vec{F}_{tr},$$

pri čemer so na desni teža, pravokotna sila podlage in trenje, ki ima smer tangente na polkrog. Vektorje razstavimo na komponente v tangentialni smeri

$$-mg \sin \varphi = -m\omega^2 R \cos \varphi + k_{t2} N$$

in komponente v pravokotni smeri

$$m\omega^2 R \sin \varphi = -mg \cos \varphi + N.$$

Iz druge enačbe izrazimo N in vstavimo v prvo. Sledi

$$\operatorname{tg} \varphi = \frac{v_0^2 - k_{t2} g R}{g R + k_{t2} v_0^2}, \quad \varphi = 63^\circ.$$

2. Podatki: $m_p = 4$ kg, $L = 0,5$ m, $m = 0,3$ kg, $h_2 = 10$ m, $h_1 = 2$ m, $D = 750$ Nm.

Žoga ob stropu obmiruje, potem pa pade za $h = h_2 - h_1 = 8$ m, tako da ima pred odbojem od palice (roke) hitrost $v = \sqrt{2gh}$. Pri odboju dobi palica kotno hitrost ω , potem pa se zaradi torzijske vzmeti ustavi pri kotu ϕ oziroma odklonu H .

Pri trku deluje na sistem palice in žoge le teža. Trk je kratkotrajen, zato lahko sunek navora teže zanemarimo, vrtilna količina se ohranja glede na komolec:

$$mLv = J\omega - mLv'.$$

Z v' označimo hitrost žoge po odboju, za katero predpostavimo, da ima smer navpično navzgor. Ker pa je trk popolnoma prožen, se ohrani tudi kinetična energija

$$\frac{1}{2}mv^2 = \frac{1}{2}J\omega^2 + \frac{1}{2}mv'^2.$$

Enačbi prepisemo v obliko:

$$\begin{aligned} mL(v + v') &= J\omega, \\ \frac{1}{2}m(v^2 - v'^2) &= \frac{1}{2}J\omega^2. \end{aligned}$$

Drugo enačbo delimo s prvo:

$$v - v' = L\omega.$$

Iz zadnje in predpredzadnje enačbe izrazimo ω z v , upoštevamo izraz za vztrajnostni moment palice $J = \frac{m_p L^2}{3}$ in dobimo

$$\omega = \frac{2v}{L(1 + \frac{1}{3}\frac{m_p}{m})}.$$

Kinetična energija palice $\frac{1}{2}J\omega^2$ se spremeni v potencialno prožnostno energijo vzmeti $\frac{1}{2}D\phi^2$:

$$\frac{1}{2}J\omega^2 = \frac{1}{2}D\phi^2.$$

Prosti konec palice se poda za $H = L \sin \phi$; kot ϕ izrazimo iz zadnje enačbe, ω iz predzadnje in dobimo

$$H = L \sin \left(\sqrt{\frac{J}{D}} \cdot \frac{\sqrt{8gh}}{L \left(1 + \frac{1}{3} \frac{m_p}{m}\right)} \right) = 0,097 \text{ m}.$$

3. Podatki: $k = 0,2 \text{ N/m}$, $l = 10 \text{ cm}$, $m = 10 \text{ g}$, $I = 0,8 \text{ A}$, $B = 0,05 \text{ T}$, $s_0 = 2,5 \text{ cm}$.

V prostoru nad magnetnim poljem niha žička s frekvenco $\omega = \sqrt{k/m}$, nihajnim časom $t_0 = 2\pi/\omega = 2\pi\sqrt{m/k}$ in amplitudo s_0 . Ker v magnetnem polju deluje na žičko konstantna sila $F = IlB$, se frekvenca ne spremeni; spremeni se le mirovna lega. Sila kaže navzdol, zato se mirovna lega premakne navzdol za $h = F/k = IlB/k = 2 \text{ cm}$. Celotni nihajni čas je sestavljen iz časa, ki ga porabi za nihanje zunaj magnetnega polja, to je pol nihajnega časa $\frac{1}{2}t_0$, in časa znotraj polja, $\frac{1}{2}t_0 + 2t_1$, kjer je t_1 čas, ki ga porabi nihalo od mirovne lege do izhoda iz polja (ali od vstopa v polje do mirovne lege v polju).

Čas t_1 določimo iz zahteve, da ima na izstopu iz polja (vstopu v polje) žička tolikšno hitrost, kot jo ima v mirovni legi pri nihanju zunaj magnetnega polja, torej $v = \omega s_0$. Enačbi, ki opisujeta odmik in hitrost žičke pri nihanju v polju, sta $x = A \sin \omega t$ in $v = \omega A \cos \omega t$, pri čemer x merimo od mirovne lege v polju in je A amplituda nihanja v polju. Ob času t_1 doseže odmik vrednost h , hitrost pa ωs_0 :

$$h = A \sin \omega t_1, \quad \omega s_0 = \omega A \cos \omega t_1.$$

Od tod sledi

$$t_1 = \frac{1}{\omega} \arctg \left(\frac{h}{s_0} \right), \quad A = \sqrt{h^2 + s_0^2}.$$

Za nihanji čas velja

$$T_0 = \frac{1}{2}t_0 + \frac{1}{2}t_0 + 2t_1 = t_0 \left(1 + \frac{1}{\pi} \arctg \left(\frac{h}{s_0} \right) \right) = 1,70 \text{ s}.$$

Pri tem doseže žička globino, merjeno glede na zgornjo mejo magnetnega polja,

$$y = h + A = h + \sqrt{h^2 + s_0^2} = 5,2 \text{ cm}.$$

4. Podatki: $l = 20$ cm, $L = 400$ cm, $\Delta x_1 = 9,4$ cm, $x'_1 = 37,2$ cm.
- a) Ko opna niha v nihajnem načinu, tako da ima N hrbtnih črt, velja $l = Na = N\lambda/2$, kjer je $a = \lambda/2$ razdalja med sosednjima vozelnima črtama in je kar enaka mrežni razdalji uklonske mrežice za mikrovalove. Pogoj za N' -to ojačenje v uklonski sliki mikrovalov po prehodu skozi opno lahko zaradi majhnih kotov (velja $x'_1 \ll L$) zapišemo kot

$$a \sin \beta_{N'} = N' \lambda', \quad a \sin \beta_{N'} \approx \operatorname{atg} \beta_{N'} = a \frac{x_{N'}}{L},$$

kjer je λ' valovna dolžina mikrovalov. Ker nas zanima le prvi pas ojačenja, postavimo $N' = 1$. Za prvotno lego upoštevamo $a = L/N$ in dobimo

$$x_1 = \frac{L}{l} \lambda' N.$$

Za lego po spremembi frekvence generatorja tresljajev velja $a = L/(N+1)$ in

$$x'_1 = \frac{L}{l} \lambda' (N+1).$$

Ko prvo enačbo odštejemo od druge, sledi

$$\Delta x_1 = x'_1 - x_1 = \frac{L}{l} \lambda', \quad \lambda' = \frac{l}{L} \Delta x_1 = 4,7 \text{ mm}.$$

- b) Iz znane λ' lahko sedaj iz druge enačbe izrazimo $N+1 = x'_1/\Delta x_1 \approx 4$, torej opna na koncu poskusa niha tako, da ima štiri hrbte in je razdalja med sosednjima vozelnima črtama enaka $a' = l/(N+1) = 5,0$ cm.

Bojan Golli

23. MEDNARODNO MATEMATIČNO

TEKMOVANJE MEST – Naloge pomladanskega kroga

Prva skupina (prvi del)

1. Na razpolago imamo zadostno število pravokotnih kosov lepenke velikosti $a \times b$, kjer sta a in b naravni števili ter $a < b$. Vemo, da lahko s takimi kosi prekrijemo (brez prekrivanja kosov) pravokotnik, velikosti 49×51 , in pravokotnik, velikosti 99×101 . Ali sta števili a in b s temi podatki natančno določeni? (4 točke)

2. Ali je mogoče vsak trikotnik razrezati na štiri konveksne kose: trikotnik, štirikotnik, petkotnik in šestkotnik? (5 točk)
3. Za naravni števili m in n vemo, da je zadnja števka števila $k = m^2 + mn + n^2$ enaka 0. Dokaži, da sta vsaj dve zadnji števki števila k enaki 0. (5 točk)
4. Štirikotniku $ABCD$ je včrtana krožnica, ki se stranic AB , BC , CD in DA dotika zapored v točkah K , L , M in N . Naj bo S presečišče daljic KM in LN . Vemo, da je $SKBL$ tetivni štirikotnik. Dokaži, da je tedaj tudi $SNDM$ tetivni štirikotnik. (5 točk)
5. (a) Imamo 128 kovancev dveh različnih tež, pri čemer ima polovica kovancev eno, polovica pa drugo težo. Kako lahko s pomočjo največ sedmih tehtanj na primerjalni tehtnici poiščemo par različno težkih kovancev? (3 točke)
(b) Imamo osem kovancev dveh različnih tež, pri čemer ima polovica kovancev eno, polovica pa drugo težo. Kako lahko s pomočjo največ dveh tehtanj na primerjalni tehtnici poiščemo par različno težkih kovancev? (3 točke)

Druga skupina (prvi del)

1. Za naravni števili m in n vemo, da je zadnja števka števila $k = m^2 + mn + n^2$ enaka 0. Dokaži, da sta vsaj dve zadnji števki števila k enaki 0. (4 točke)
2. Iz papirja izrežemo skladna trikotnika ABC in $A'B'C'$, enega izmed njiju obrnemo in ju položimo na mizo. Dokaži, da so razpolovišča daljic AA' , BB' in CC' kolinearna. (5 točk)
3. Imamo šest različno težkih kosov sira, med katerimi obstajajo trije, katerih skupna masa je enaka skupni masi preostalih treh. Denimo, da lahko iz primerjave velikosti za poljubna dva kosa sira ugotovimo, kateri izmed njiju je težji. Ugotovi, kako lahko le z dvema tehtanjema na primerjalni tehtnici določimo dve enako težki trojici kosov sira. (5 točk)
4. Na koliko načinov lahko v tabelo velikosti 2×50 zapišemo naravna števila od 1 do 100 tako, da sta vsaki dve zaporedni števili zapisani v polji s skupnim robom? (5 točk)
5. Ali obstaja pokončna pravilna tristrana prizma, ki jo lahko pokrijemo s paroma različnimi enakostraničnimi trikotniki, ki se medsebojno ne prekrivajo? (Pri tem lahko trikotnike 'zapognemo' preko robov prizme.) (6 točk)

Prva skupina (drugi del – izbrane naloge)

5. Ostrokotni trikotnik z ravnim rezom prerežemo na dva (ne nujno trikotna) dela. Zatem izberemo enega od dobljenih kosov in ga z ravnim rezom ponovno razdelimo na dva dela. Postopek ponavljamo in v nekem trenutku ugotovimo, da so vsi dobljeni koščki trikotni. Ali je možno, da so vsi dobljeni koščki topokotni trikotniki? (7 točk)
6. Dano je tako naraščajoče zaporedje naravnih števil $a_1 < a_2 < \dots < a_{2002} < a_{2003} < \dots$, da za vsak $n \geq 2002$ število a_n deli vsoto $\sum_{j=1}^{n-1} a_j$. Dokaži, da obstaja tak indeks m , da za vsak $n \geq m$ velja

$$a_n = \sum_{j=1}^{n-1} a_j. \quad (7 \text{ točk})$$

7. Domine so zložene v vrsto na običajen način (sosednji domini imata ob stiku enako število pik). Če v vrsti najdemo verigo domin, ki se začne in konča z enakim številom pik, lahko to verigo dvignemo in obrnjemo (zasukano za 180°) vrnemo na prvotno mesto. Naj bosta V_1 in V_2 verigi, ki sta sestavljeni iz enakega nabora domin in se začneta z enakim številom pik ter končata z enakim številom pik. Dokaži, da lahko s primerno izbranim zaporedjem zgoraj opisanih potez verigo V_1 pretvorimo v verigo V_2 . (8 točk)

Druga skupina (drugi del – izbrane naloge)

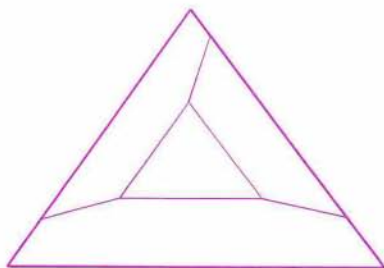
5. Naj bodo AA_1 , BB_1 in CC_1 višine ostrokotnega trikotnika ABC . Z O_A , O_B in O_C označimo zapored središča trikotnikom AB_1C_1 , BC_1A_1 in CA_1B_1 vrtanih krožnic. Trikotniku ABC včrtana krožnica naj se stranic BC , CA in AB dotika zapored v točkah T_A , T_B in T_C . Dokaži, da imajo vse stranice šestkotnika $T_AO_CT_BO_AT_CO_B$ enako dolžino. (6 točk)
6. Na mizi leži 52 igralnih kart, razporejenih v obliko pravokotnika s 4 vrsticami in 13 stolpci. Dve sosednji karti istega stolpca ali vrstice imata bodisi enako vrednost bodisi enako barvo. Dokaži, da so vse karte poljubno izbrane vrstice enake barve. (7 točk)
7. Ali obstajata taki iracionalni števili $a, b > 1$, da za poljubni naravni števili m, n velja $[a^m] \neq [b^n]$? (Za realno število x označimo z $[x]$ največje celo število, ki ni večje od x .) (8 točk)

Gregor Cigler

23. MEDNARODNO MATEMATIČNO TEKMOVANJE MEST – Rešitve nalog pomladanskega kroga s str. 308

Prva skupina (prvi del)

1. Edina skupna delitelja števil $49 \cdot 51 = 3 \cdot 7^2 \cdot 17$ in $99 \cdot 101 = 3^2 \cdot 11 \cdot 101$ sta 3 in 1. Ker je $a < b$, je $ab > 1$, od koder sledi, da je $ab = 3$ in $a = 1$ ter $b = 3$.
2. Slika kaže, kako lahko to naredimo.



3. Če bi bilo eno od števil m ali n liho, bi bilo tudi število k liho, zato sta m in n sodi števili. Če je eno od števil m ali n deljivo z 10, drugo pa ne, število k ni deljivo z 10. Denimo, da nobeno izmed števil m in n ni deljivo z 10. Tedaj se števili m^2 in n^2 končata s 4 ali 6, produkt mn pa se ne more končati z 0, kar pomeni, da se m^2 in n^2 končata z enako števko. Ni se težko prepričati, da se tedaj tudi produkt mn konča s števko 4 ali 6, kar pomeni, da število k ne more biti deljivo z 10. S tem smo dokazali, da sta m in n deljivi z 10.
4. Ker sta premici BK in BL tangenti na krožnico, na kateri leži točka M , velja

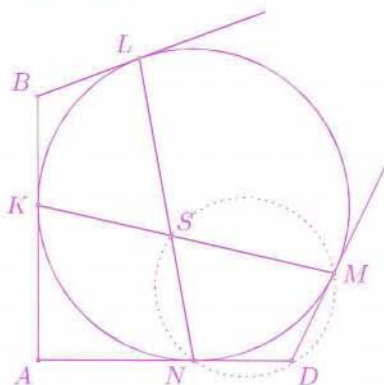
$$\sphericalangle BKL = \sphericalangle KML = \sphericalangle BLK = \theta.$$

Podobno ugotovimo, da je

$$\sphericalangle DMN = \sphericalangle MLN = \sphericalangle DNM = \phi.$$

Tedaj je $\sphericalangle LBK = 180^\circ - 2\theta$ in $\sphericalangle MDN = 180^\circ - 2\phi$, zato je $\sphericalangle KSL = \sphericalangle MLS + \sphericalangle SML = \theta + \phi$ in zaradi sovršnosti $\sphericalangle MSN = \theta + \phi$. Ker je

$SKBL$ tetivni štirikotnik, velja $\sphericalangle LBK + \sphericalangle KSL = 180^\circ$, od koder sledi, da je $\theta = \phi$. Od tod dobimo $\sphericalangle MDN + \sphericalangle MSN = 180^\circ$, kar pomeni, da je $SNDM$ tetivni štirikotnik.

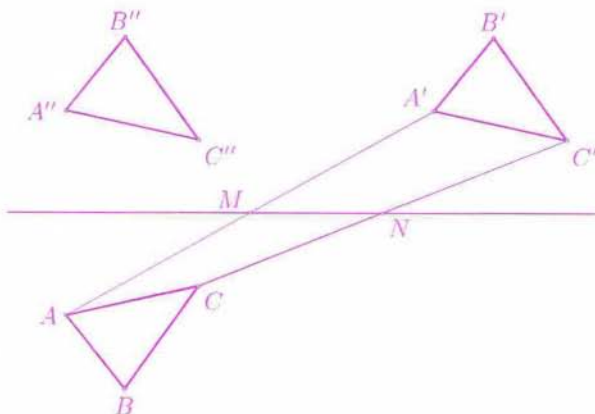


5. (a) Najprej na vsako stran tehtnice položimo 64 kovancev. Če je tehtnica v ravnesju, enega od kupov odstranimo in iz preostalega kupa na vsako stran tehtnice položimo 32 kovancev. Če znova dosežemo ravnesje, postopek ponavljamo in v primeru, da se nam šestkrat pojavi ravnesje, po šestih tehtanjih pridemo do para kovancev, ki nujno vsebuje en lažji in en težji kovanec. Denimo, da se nam na nekem koraku opisanega tehtanja pojavi neravnesje. Naj bo število kovancev v vsaki od posodic enako $2m$. Tedaj m kovancev za novo tehtanje naberemo iz ene posodice, drugih m kovancev pa iz druge. Če se pojavi ravnesje, odstranimo $2m$ kovancev iz tega tehtanja, sicer pa odstranimo $2m$ kovancev iz prejšnjega tehtanja. V vsakem primeru izločimo $2m$ kovancev, ki gotovo vsebujejo par različno težkih kovancev. Na ta način po največ sedmih tehtanjih dobimo par različno težkih kovancev.
- (b) Položimo na vsako stran tehtnice štiri kovanec. Če je tehtnica uravnotežena, odstranimo štiri kovanec iz ene izmed posodic, dva kovanca iz preostale posodice pa primerjamo z drugima dvema. Če je tehtnica ponovno v ravnesju, je iskani par v katerikoli izmed posodic, v nasprotnem primeru pa sta v vsaki posodici enako težka kovanca, zato iz vsake vzamemo po en kovanec. Denimo, da je v prvem tehtanju s po štirimi kovanci na vsaki strani desna stran težja. Tedaj v drugem tehtanju razdelimo štiri kovanec iz desne posodice na dva para. Če je tehtnica v

drugem tehtanju v ravnovesju, so vsi štirje kovanci težje vrste, zato izberemo en kovanec iskanega para iz te četverice, drugi kovanec pa izmed preostalih kovancev. V nasprotnem primeru sta na težji strani dva težka kovanca, na lažji strani pa en težji in en lažji kovanec, zato se iskani par nahaja v tej posodici.

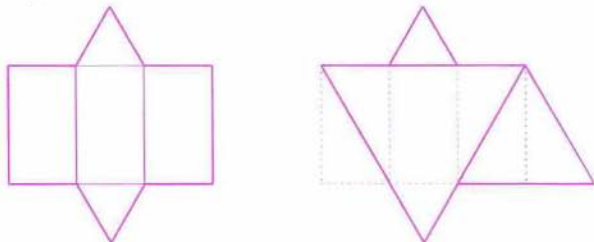
Druga skupina (prvi del)

1. Glej rešitev 3. naloge za prvo skupino.
2. Naj bo M razpolovišče daljice AA' in N razpolovišče daljice CC' . Tedaj je točka A enako oddaljena od premice $p = MN$ kot točka A' . Enako velja za par točk C in C' . Naj bo $A''B''C''$ zrcalna slika trikotnika ABC preko premice p . Tedaj trikotnik $A''B''C''$ dobimo s premikom trikotnika $A'B'C'$ v smeri premice p . Od tod sledi, da sta točki B'' in B' enako oddaljeni od premice p , torej tudi razpolovišče daljice BB' leži na premici p .



3. Razporedimo najprej kose sira po naraščajoči teži in jih označimo s števili od 1 do 6, pri čemer je najlažji kos sira označen z 1 in najtežji s 6. Tedaj so možne razvrstitve na enako težki trojici naslednje (126, 345), (136, 245), (146, 235), (156, 234) in (236, 145). Primerjajmo najprej trojici 146 in 235. Če je trojica 146 težja, je tudi trojica 156 težja od trojice 234. Nato stehamo še trojici 136 in 245. Če je trojica 136 težja, je tudi trojica 236 težja od trojice 145, zato sta trojici 125 in 345 enako težki. Če je v prvem tehtanju trojica 146 lažja, je trojica 136 lažja od trojice 245, trojica 126 lažja od trojice 345 in trojica 145 lažja od trojice 236, zato sta enako težki trojici 156 in 234.

4. Predstavimo postavitev števil v tabeli s potjo po poljih tabele, ki povezuje središča polj, v katerih so vpisana zaporedna števila. Če sta števili 1 in 100 vpisani v sosednji polji, je pot 'prekinjeni' cikel, ki poteka po vseh poljih gornje vrstice, na koncu tabele preide v spodnjo vrstico, po kateri se vrne do prvega stolpca in po tem v izhodiščno polje levo zgoraj. Ker lahko cikel prekinemo na kateremkoli od stotih mest, je postavitev, ki ustrezajo ciklu, ravno sto. Če števili 1 in 100 nista sosednji, ustreza pot ni zaključena. Razvrstimo te vrste poti glede na število skupin navpičnih povezav v teh poteh, pri čemer so navpičnice v isti skupini, če polja, po katerih potekajo te navpičnice, tvorijo povezano množico. Če si ogledamo izsek poti med zadnjim stolpcem neke skupine navpičnic in prvim stolpcem naslednje skupine navpičnic, opazimo, da je cikličen, zato so lahko navpičnice v eni, dveh ali treh skupinah. Opazimo, da razen dveh cikličnih poti vse vsebujejo navpičnici v prvem in zadnjem stolpcu. Preštejmo vse možne oblike poti! Iz cikla dobimo 100 različnih oblik poti. Med preostalimi sta dve poti taki, da so navpičnice v eni skupini (v eni je levi konec poti v spodnji, v drugi pa v zgornji vrstici). Za poti z dvema skupinama navpičnic lahko večja skupina vsebuje od 2 do 48 navpičnic, druga skupina pa ima nujno le eno navpičnico. Ker je večja skupina lahko na levi ali desni in levi konec poti v spodnji ali zgornji vrstici, dobimo $4 \cdot 47 = 188$ možnih oblik poti. Pri poteh s tremi skupinami navpičnic skupina na levi in skupina na desni vsebujeta le eno navpičnico, srednja skupina pa ima lahko od 1 do 46 navpičnic. Če srednja skupina vsebuje k navpičnic, se lahko nahaja na $47 - k$ možnih mestih. Ker se lahko levi konec poti nahaja v spodnji ali zgornji vrstici, dobimo $2 \cdot (46 + 45 + \dots + 1) = 2162$ mest. Ker lahko števila razvrstimo vzdolž vsake poti v dveh možnih smereh, dobimo $2 \cdot (100 + 2 + 188 + 2162) = 4904$ možnih razvrstitev.
5. Slika prikazuje pravilno pokončno tristrano prizmo, ki jo lahko prekrijemo z likom, sestavljenim iz treh paroma neskladnih trikotnikov (slika desno).



Prva skupina (drugi del)

5. Opazujemo konveksni n -kotnik. Če od tega večkotnika z ravnim rezom odrežemo trikotnik, se število oglišč preostalega dela, ki je znova konveksni večkotnik, zmanjša kvečjemu za eno. Lahko se zgodi, da je število oglišč preostanka celo za eno večje od n . Od tod sledi, da pri našem načinu rezanja iz konveksnega n -kotnika dobimo vsaj $n - 2$ trikotnikov. Če želimo natanko $n - 2$ trikotnikov, morajo vsi rezi potekati skozi oglišča, saj se sicer v nekem koraku rezanja število oglišč ostanka ne zmanjša. V nadaljevanju bomo rekli, da n -kotnik vsebuje $n - 2$ trikotnikov.

Opazujemo proces rezanja. Ko na nekem koraku prerežemo konveksni n -kotnik P , razpade na konveksni a -kotnik in konveksni b -kotnik, ki skupaj vsebujeta $a - 2 + b - 2$ trikotnikov. Obstajajo trije načini rezanja P : skozi dve oglišči, skozi eno oglišče in stranico in skozi dve stranici. V prvem primeru je $a + b = n + 2$, zato se število vsebovanih trikotnikov ohrani. Poleg tega ne dobimo v nobenem izmed dobljenih večkotnikov novega topega kota, saj iz kota ob oglišču večkotnika P z rezanjem ne more nastati topi kot. V drugem primeru je $a + b = n + 3$, zato se število vsebovanih trikotnikov poveča za eno. Pri takem rezanju lahko nastane kvečjemu en topi kot, in sicer ob točki, kjer rez seka stranico P . V primeru, ko rez poteka skozi dve stranici P , je $a + b = n + 4$, zato se število vsebovanih trikotnikov poveča za dva, prav tako pa se za kvečjemu dva poveča število topih kotov.

V vsakem izmed gornjih treh primerov se število topih kotov poveča kvečjemu za toliko, za kolikor se poveča število vsebovanih trikotnikov. Ker je začetni trikotnik ostrokotni, nam tudi na koncu ostane vsaj en ostrokotni trikotnik.

6. Naj bo

$$S_n = \sum_{i=1}^{n-1} a_i.$$

Tedaj za $n \geq 2002$ člen a_n deli S_n , zato obstaja tako naravno število d_n , da je $a_n = \frac{S_n}{d_n}$. Od tod dobimo

$$S_{n+1} = S_n + a_n = \frac{(d_n + 1)S_n}{d_n}.$$

Če je $d_{n+1} \geq d_n + 1$, dobimo

$$a_{n+1} = \frac{S_{n+1}}{d_{n+1}} \leq \frac{S_n}{d_n} = a_n,$$

kar je v nasprotju s predpostavko. To pomeni, da zaporedje d_n od indeksa $n = 2002$ dalje ne narašča, od koder sledi, da obstaja tak indeks m , da za $n \geq m$ velja $d_n = k > 1$, kjer je k konstantna vrednost. Za $n \geq m$ tedaj velja

$$S_n = \left(\frac{k+1}{k}\right)^{n-m} S_m.$$

Ker sta števili k in $k+1$ tuji, S_n pa je naravno število, mora za $n \geq m$ število k^{n-m} deliti S_m . Zadnje je mogoče le za $k = 1$, kar pomeni, da za $n \geq m$ velja $a_n = S_n$. S tem je dokaz končan.

7. Dokazujemo z indukcijo na število domin v verigah. Za $n = 1, 2$ ni kaj dokazovati, saj sta verigi enaki. Domine označujemo z urejenimi pari (a, b) , kjer je a število pik na levi polovici, b pa število pik na desni polovici domine. Denimo, da se verigi začneta z a pikami. Naj bo prva domina v verigi V_2 enaka (a, b) , prva domina v verigi V_1 pa (a, c) . Če je $b = c$, lahko uporabimo indukcijsko predpostavko za dela verig od druge domine naprej. Denimo, da je $b \neq c$. Tedaj v verigi V_1 najdemo domino (a, b) ali (b, a) . V drugem primeru v verigi V_1 obrnemo niz domin med prvo domino in domino (b, a) ter znova uporabimo indukcijo. V preostalem primeru je veriga V_1 videti takole

$$(a, c), \dots, (d, a), (a, b), \dots$$

Iz te verige lahko dobimo verigo $X = (a, d), \dots, (c, a), (a, b), \dots$. Ni se težko prepričati, da je problem ekvivalenten problemu, kjer lahko hkrati spreminjamo obe verigi, zato lahko predpostavimo, da je veriga V_2 oblike

$$(a, b), \dots, (a, c), \dots$$

kjer je $a \neq c$, saj v nasprotnem primeru (t.j. v primeru, da je v verigi V_1 domina (c, a)) lahko iz verige V_1 dobimo verigo, ki ima enako prvo domino kot veriga V_2 in lahko induktivno nadaljujemo. Če v verigi V_1 najdemo domino (d, a) , lahko iz nje dobimo verigo X in nato verigo V_2 . Predpostavimo torej, da je v verigi V_1 domina (a, d) in $a \neq d$.

Obravnavamo dva primera:

1. primer:

Veriga V_1 je oblike

$$(a, b), \dots, (a, d), \dots, (e, a), (a, c), \dots$$

Obrnemo verigo med dominama (a, d) in (e, a) in dobimo verigo oblike

$$(a, b), \dots, (d, a),$$

ki jo lahko pretvorimo v verigo X .

2. primer:

Veriga V_1 je oblike

$$(a, b), \dots, (a, c), \dots, (e, a), (a, d), \dots$$

Z obratom verige med dominama (a, c) in (e, a) dobimo verigo oblike

$$(a, b), \dots, (c, a), \dots,$$

ki jo lahko pretvorimo v verigo V_2 .

Druga skupina (drugi del)

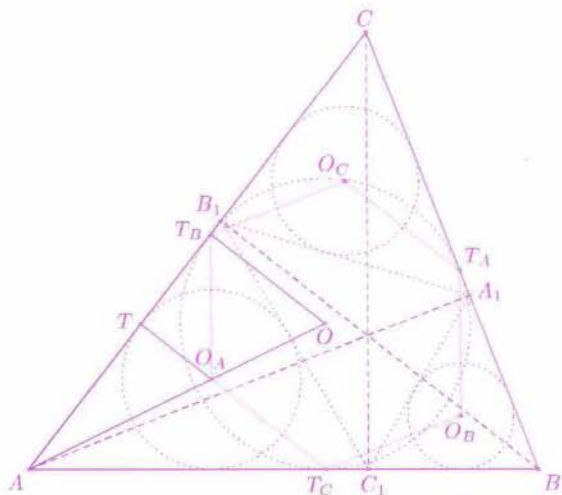
5. Ker je BCB_1C_1 tetivni štirikotnik, z opazovanjem obodnih kotov ugotovimo, da sta ABC in AB_1C_1 podobna trikotnika. Naj bo α kot ob oglišču A . Tedaj velja $\cos \alpha = \frac{|AB_1|}{|AB|}$. Naj bo O središče trikotniku ABC včrtane krožnice in r njen polmer. S T označimo dotikališče trikotniku AB_1C_1 včrtane krožnice s stranico AC . Tedaj velja $OT_B = r$, $OA_T = r \cos \alpha$, $AT = AT_B \cos \alpha$, $AT_B = r \operatorname{ctg} \frac{\alpha}{2}$ in

$$TT_B = AT_B - AT = AT_B(1 - \cos \alpha) = r \operatorname{ctg} \frac{\alpha}{2} \cdot 2 \sin^2 \frac{\alpha}{2} = r \sin \alpha.$$

Od tod sledi

$$OA_T B = \sqrt{OA_T^2 + T_B T^2} = r.$$

Analogno iz simetrije ugotovimo, da imajo vse stranice šestkotnika $T_A O_C T_B O_A T_C O_B$ enako dolžino.



6. Sosednji karti enake barve imenujmo *povezani po barvi*, sosednji karti enake vrednosti pa imenujmo *povezani po vrednosti*. Ker v naboru kart nimamo dveh enakih kart, dve karti ne morata biti hkrati povezani po barvi in vrednosti. Imamo 12 stolpcev iz vodoravnih povezav in 3 vrstice navpičnih povezav. Dokazali bomo, da so vse povezave v istem stolpcu (ali isti vrstici) enake vrste. Denimo, da obstaja stolpec, v katerem najdemo povezave obeh vrst. Tedaj najdemo sosednji vrstici tega stolpca, v katerih sta vodoravni povezavi različne vrste. Opazujemo štiri karte na koncih teh dveh povezav. Predpostavimo, da sta v gornji vrstici srčev as in srčev kralj. Potem imata karti v spodnji vrstici enako vrednost. Če je ta vrednost as, ni povezave v desnem stolpcu (med spodnjim asom in kraljem nad njim). Podobno ugotovimo, da spodnji karti nista kralja. Tedaj sta karti v spodnji vrstici nujno srčevi, kar pa je v nasprotju s predpostavko, da sta povezavi v vrsticah različnega tipa. S tem smo trditev dokazali. Opazujemo sedaj tri vrstice navpičnih povezav. Vemo, da so vse povezave v eni vrstici istega tipa. Pojavijo se možnosti:
- (1) V vseh treh vrsticah so povezave po vrednosti. To pomeni, da so vse karte nekega stolpca enake vrednosti. Tedaj sta sosednji karti neke vrstice nujno enake barve (saj ne moreta biti povezani po vrednosti), od koder sledi veljavnost postavljene trditve.
 - (2) V vseh treh vrsticah so povezave po barvi. To pomeni, da je 52 kart razdeljenih na 13 skupin s štirimi kartami, pri čemer so vse karte ene skupine enake barve. Ker obstaja 13 kart ene barve, bi od tod sledilo, da 4 deli 13. Protislovje!

(3) Le v srednji vrstici so povezave po vrednosti. Tedaj dobimo 26 disjunktnih parov kart enake barve. Tudi to ni možno, ker 2 ne deli 13.

(4) Le v srednji vrstici so povezave po barvi. Opazujemo 13 parov kart (ena karta iz druge in druga karta iz tretje vrstice), ki so povezane po barvi. Denimo, da sta v prvem paru pikovi karti. Poiščimo prvi naslednji par, ki ni pikov. Predpostavimo, da sta karti tega para srčevi in da ležita v $(m+1)$ -tem stolpcu.

Oglejmo si najprej primer, ko sta gornja karta prvega stolpca in zadnja karta prvega stolpca enake barve, ki seveda ni pikova. Recimo, da imata ti dve karti barvo srca. Tedaj bi bile karte prvih m stolpcev prve vrstice barve srca, saj so v prvih $m-1$ stolpcih vodoravnih povezav nujno le povezave po barvi. Karta na mestu $(2, m)$ je pikova in je s srčevo karto na mestu $(2, m+1)$ povezana po vrednosti. Prav tako je po vrednosti povezana s srčevo karto nad seboj. Karti na mestih $(2, m+1)$ in $(1, m)$ imata tedaj enako vrednost in barvo. Protislovje! Gornja in spodnja karta prvega stolpca tako nista srčevi. Predpostavimo lahko, da sta ti dve karti križevi. Tedaj sta karti na mestih $(1, m+1)$ in $(4, m+1)$ nujno kari. Ko par v srednjih dveh vrsticah znova zamenja barvo, mora ta barva biti nujno bodisi pikova bodisi križeva. Od tod sledi, da so vse štiri karte v poljubnem stolpcu bodisi črne bodisi rdeče. Ker obstaja 26 rdečih ter 26 črnih kart in 4 ne deli 26, to ni možno.

Denimo sedaj, da sta gornja in spodnja karta prvega stolpca različne barve. Tedaj je ena nujno karova in druga križeva. Predpostavimo lahko, da je gornja karova. Tedaj je gornja karta v $(m+1)$ -tem stolpcu nujno križeva, spodnja pa karova. Podobno kot prej lahko ugotovimo, da je barva parov iz srednjih dveh vrstic lahko le pikova ali srčeva, od koder sledi, da imamo 13 parov, ki zajamejo vse srčeve in vse pikove karte. Ker 13 ni deljivo z 2, to ni mogoče.

(5) Le v spodnji vrstici so povezave po vrednosti. Predpostavimo, da so gornje tri karte prvega stolpca pikove, spodnja pa križeva. Denimo, da so karte v prvih $m-1$ stolpcih po barvi enakovredne prvemu stolpcu, v m -tem stolpcu pa nastopi sprememba. Ni se težko prepričati, da so tedaj karte m -tega stolpca vse rdeče barve. Ker imamo 26 rdečih in 26 črnih kart, rdečih (ali črnih) kart ne moremo razdeliti po stolpcih, ki vsebujejo po 4 karte.

(6) Le v gornji vrstici so povezave po vrednosti. Ta primer je analogen primeru (5).

(7) Le v spodnji vrstici so povezave po barvi. Sledi, da v vsakem stolpcu obstaja trojica kart enake vrednosti. Ker obstajajo le 4 karte neke vrednosti, so vrednosti trojic iz 13 stolpcev različne. V vsakem

paru stolpcev najdemo v neki vrstici karti, različni po vrednosti, od koder sledi, da so vse vodoravne povezave barvne. To pomeni, da so v zadnji vrstici vse karte določene barve, od koder sledi, da med zadnjo in predzadnjo vrstico ne more biti povezav po barvi.

(8) Le v gornji vrstici so povezave po barvi. Ta primer je analogen primeru (7).

7. Naj bo $a = \sqrt{6}$ in $b = \sqrt{3}$. Predpostavimo, da velja $[a^m] = [b^n] = k$ za naravni števili m in n . Tedaj je $k^2 \leq 6^m < k^2 + 2k + 1$ in $k^2 \leq 3^n < k^2 + 2k + 1$. Če neenačbi odštejemo, ugotovimo, da velja $2k \geq |6^m - 3^n| = 3^m |2^m - 3^{n-m}|$. Očitno je $n > m$, zato je $|2^m - 3^{n-m}| \geq 1$. Od tod sledi, da je $2k \geq 3^m$ in zato

$$\frac{9^m}{4} \leq k^2 \leq 6^m,$$

od koder sledi, da je

$$\frac{1}{4} \leq \left(\frac{2}{3}\right)^m.$$

Iz zadnje neenačbe dobimo $m = 1, 2, 3$. Ker je $[a] = 2$, $[a^2] = 6$, $[a^3] = 14$ in $[b] = 1$, $[b^2] = 3$, $[b^3] = 5$, $[b^4] = 9$, $[b^5] = 15$, sledi, da za poljubni naravni števili m in n velja $[a^m] \neq [b^n]$.

Gregor Cigler

PRESEK

list za mlade matematike, fizike, astronome in računalnikarje
30. letnik, šolsko leto 2002/03, številka 5, strani 257–320

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, Marijan Prosen (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. Naročnina za šolsko leto 2002/03 je za posamezne naročnike **3.300 SIT** (posamezno naročilo velja do preklica), za skupinska naročila šol **2.700 SIT**, posamezna številka **825 SIT**, tematska številka **1.650 SIT**, stara številka **650 SIT**, letna naročnina za tujino **25 EUR**, devizna nakazila SKB banka d.d. Ljubljana, Ajdovščina 4, Ljubljana, SWIFT: SKBASIX, transakcijski račun številka 03100-1000018787.

List sofinancira MŠZŠ

Založilo DMFA – založništvo

Tisk: DELO Tiskarna, Ljubljana

© 2003 Društvo matematikov, fizikov in astronomov Slovenije – 1524

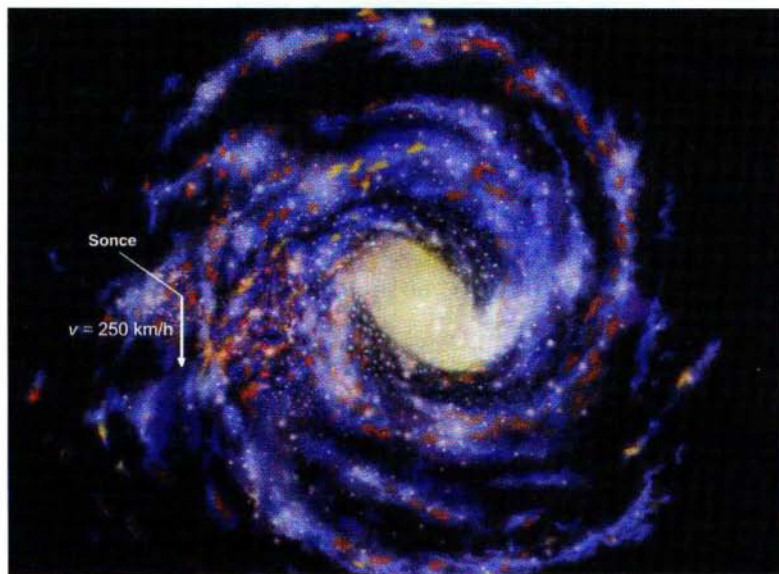
Poština plačana pri pošti 1102 Ljubljana

S KOLIKŠNO HITROSTJO?

V družbi pogosto nanese pogovor o tem, s kolikšno hitrostjo se pravzaprav gibljemo, saj imamo občutek, da Zemlja miruje. Poglejmo, kako je s to rečjo.

Samo zaradi vrtenja Zemlje se kraji na ekvatorju gibljejo s hitrostjo
$$\frac{2\pi \cdot (\text{polmer Zemlje})}{24 \text{ h}} = \frac{2 \cdot 3,14 \cdot 6400 \text{ km}}{14 \cdot 60 \cdot 60 \text{ s}} = 0,465 \text{ km/s} = 465 \text{ m/s}.$$

Kraji na Zemljinih vzporednikih se seveda gibljejo z manjšo hitrostjo. Mi v Sloveniji, z zemljepisno širino $\varphi = 46^\circ$, se gibljemo s hitrostjo $465 \text{ m/s} \cdot \cos \varphi = 465 \text{ m/s} \cdot \cos 46^\circ$, to je približno s 320 m/s , kar je hitrost reaktivnega letala. To je razmeroma majhna hitrost v vesolju, če samo pomislimo, da se Zemlja giblje okoli Sonca s hitrostjo
$$\frac{2\pi \cdot (\text{oddaljenost Zemlje od Sonca})}{1 \text{ leto}} = \frac{2 \cdot 3,14 \cdot 150\,000\,000 \text{ km}}{365 \cdot 24 \cdot 60 \cdot 60 \text{ s}} = 30 \text{ km/s},$$
 torej v eni sekundi smuknemo iz Ljubljane v Kranj. Tudi ta hitrost za vesoljske razmere ni velika.



Slika 1. Pogled na Galaksijo – shema: smer gibanja Osončja, torej Sonca skupaj s planeti, okoli središča naše Galaksije je prikazana s puščico. En obhod traja približno 200 milijonov let.

Poleg tega, da Zemlja kroži okoli Sonca in se hkrati vrti, se skupaj s Soncem in bližnjimi okoliškimi zvezdami giblje še okoli središča naše Galaksije, to je velikanske skupine zvezd, v kateri domujemo, in to s hitrostjo, ki jo ocenimo iz enačbe
$$\frac{2\pi \cdot (\text{oddaljenost Sonca od sredine Galaksije})}{200 \text{ milijonov let}} = \frac{2 \cdot 3,14 \cdot 26\,000\,365 \cdot 24 \cdot 60 \cdot 60 \cdot 300\,000 \text{ km}}{200\,000\,000 \cdot 365 \cdot 24 \cdot 60 \cdot 60 \text{ s}},$$
 kar je okoli 250 km/s . V eni sekundi preletimo Slovenijo. Kar hitro se vozimo, pa mirno in zastonj, mar ne?

Marijan Prosen

POŠTNA ZNAMKA O HALLERSTEINU

Dne 21. 1. 2003 je Pošta Slovenije na predlog Muzeja Mengeš izdala spominsko znamko ob 300-letnici rojstva jezuita in misijonarja na Kitajskem, znamenitega astronoma in matematika, naravoslovca in etnografa slovenskega rodu, patra Ferdinanda Avgušтина Hallerja, pl. Hallersteina.

F. A. Hallerstein (1703 – 1774) je bil sicer rojen v Ljubljani, vendar njegov rod izvira iz Mengša, kjer je tudi preživel svojo mladost. Matematično in astronomsko izobrazbo si je pridobil na Dunaju in v Gradcu, 1739 pa je kot misijonar odšel na Kitajsko, kjer je ostal do smrti.

Slika 1. Spominska znamka ob 300-letnici rojstva F. A. Hallersteina. Na znamki vidimo naslovnico njegovega glavnega dela **OBSERVATIONES ASTRONOMICAE** (*Astronomska opazovanja*) in del sekstanta, inštrumenta, ki so ga na pekinškem dvoru v tistem času uporabljali pri opazovanju zvezd.



Na Kitajskem je dosegel poleg pomembnih uspehov na strokovnem področju tudi visok politični položaj, in sicer na cesarskem dvoru v Peking. Med drugim je bil predsednik astronomsko-matematičnega oddelka, izdeloval je zemljevide delov kitajskega cesarstva, opazoval severni sij, komete, mrke, planete (posebno Merkur), satelite.



Slika 2. Zgornji grad v Mengšu, kjer je Hallerstein preživel svojo mladost. To lepo zgradbo si lahko, nekoliko predelano, ogledate še danes. Izdal in založil Muzej Mengeš 2003.

Hallersteina prištevamo med najpomembnejše slovenske znanstvenike preteklosti. Več o Hallersteinu je pisal Presek **18** (1990/91), 110, nekaj o starih kitajskih inštrumentih pa Presek **16** (1988/89), 210.

Marijan Prosen