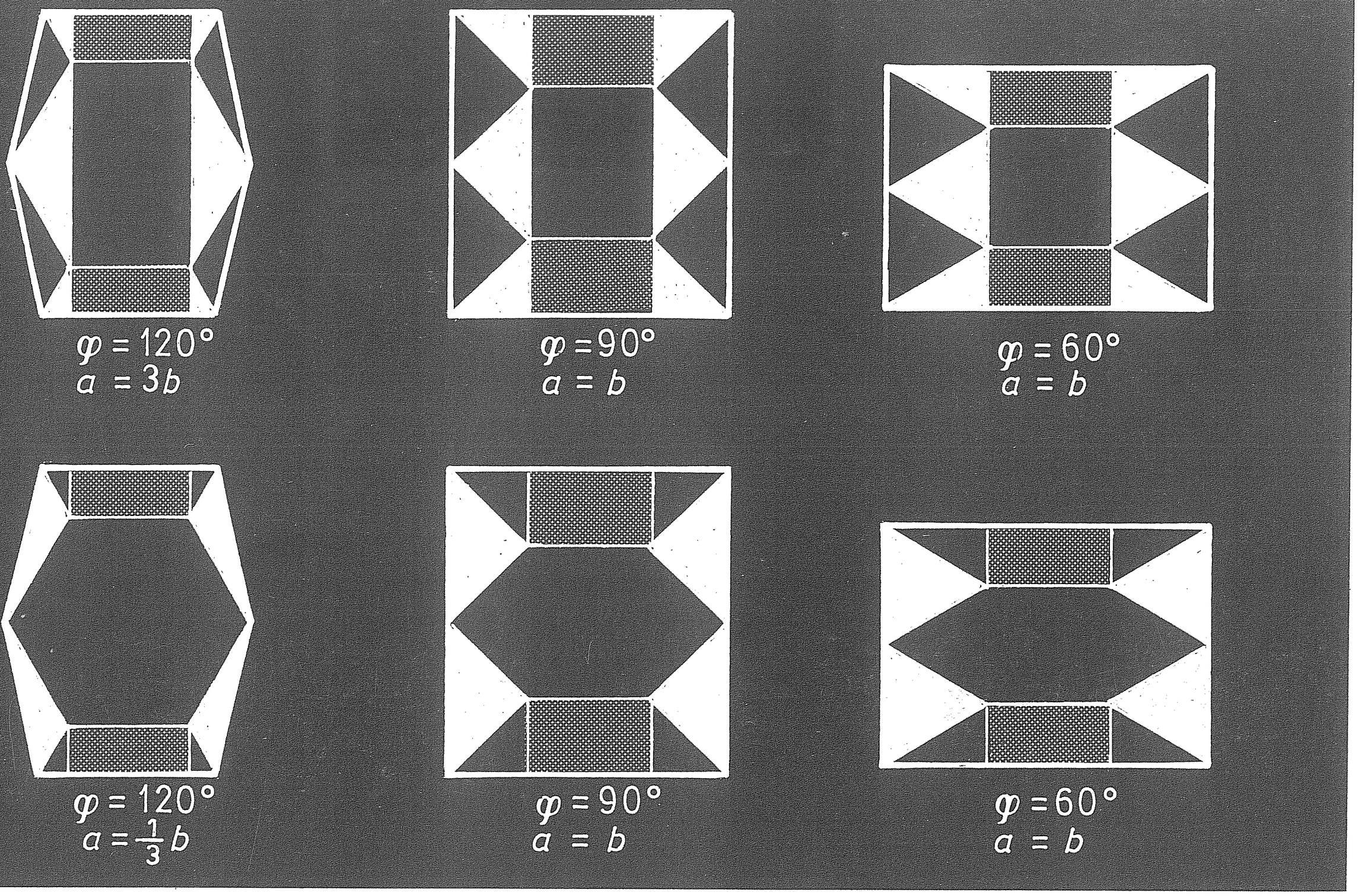
IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SR SLOVENIJE

YU ISSN 0473-7446

1991
Letnik 38
1

OBZORNIK ZA MATEMATIKO IN FIZIKO



OBZORNIK ZA MATEMATIKO IN FIZIKO

LJUBLJANA, JANUAR 1991

letnik 38, številka 1, strani 1–32

Glasilo Društva matematikov, fizikov in astronomov Slovenije, 61111 Ljubljana, Jadranska c. 19, p.p. 64, telefonska št. (061) 265-061/53, žiro račun 50101-678-47233, devizni račun pri Ljubljanski banki 50101-620-107-257300-5694/4.

Člani društva prejemajo Obzornik brezplačno. Celoletna članarina 200.– din. Naročnina v knjigarnah in za ustanove 300.– din, za tujino 40 DEM. Posamezna številka 40.– din, dvojna številka 80.– din, stare številke 20.– din.

Tisk: Tiskarna Kurir. Naklada 1500 izvodov. Izdajo revije sofinancirata Republiški komite za raziskovalno dejavnost in tehnologijo in Republiški komite za vzgojo in izobraževanje ter telesno kulturo.

Poštnina plačana na pošti 61102 Ljubljana

Članki — Articles Str.–Page

Na ovitku: Slika k članku na str. 19. Nekaj prizmatičnih magnetnih sistemov. φ je kot ob ogljišču romboida, a in b pa stranici romboida

HERONOVI TRIKOTNIKI IN DIOFANTSKE ENAČBE

IVAN VIDAV

Math. Subj. Class. (1985) 11 D 25

V članku sta opisani dve metodi, kako dobimo neskončno mnogo Heronovih trikotnikov, ki si niso podobni, njihova ploščina pa je popoln kvadrat.

HERON TRIANGLES AND DIOPHANTINE EQUATIONS

Two methods are described how to find infinitely many Heron triangles whose sides have no common factor and whose area is a perfect square.

1. Heronov obrazec nam pove, kako izračunamo ploščino trikotnika, če poznamo njegove stranice. Zapišimo ga v obliki

$$p^2 = s(s-a)(s-b)(s-c)\,. \tag{1}$$

Tu pomenijo a, b, c stranice trikotnika, s polovični obseg, tedaj $2s = a+b+c$, in p ploščino. Če so a, b, c cela števila, ploščina p ni vselej celo število, ker produkt na desni v splošnem ni popoln kvadrat. Heronov trikotnik imenujemo tak trikotnik, ki ima za stranice in ploščino cela števila. Dobro znan primer je trikotnik s stranicami $a = 13$, $b = 14$, $c = 15$ in ploščino $p = 84$. Iskanje Heronovih trikotnikov je diofantski problem: poiskati je treba naravna števila a, b, c in p tako, da je izpolnjena enačba (1).

Vsak trikotnik se da z ravnilom in šestilom pretvoriti v ploščinsko enak kvadrat. Če so njegove stranice cela števila, pa po navadi stranica kvadrata z enako ploščino ni celo število, tudi pri Heronovih trikotnikih ne. Stranica kvadrata z enako ploščino, kakor jo ima zgoraj navedeni trikotnik, je $d = 2\sqrt{21}$, torej iracionalno število. Ali Heronovi trikotniki, pri katerih je ploščina popoln kvadrat, sploh obstajajo? Videli bomo, da obstajajo in celo neskončno mnogo jih je. Pred kratkim je namreč postavil R. A. Melter v časopisu Amer. Math. Monthly [2] tale problem:

Dokaži, da obstaja neskončno Heronovih trikotnikov, ki si niso podobni in katerih ploščina je popoln kvadrat.

V tem članku bomo na dva načina reševali to nalogo. Če je d stranica ploščinsko enakega kvadrata, velja enačba

$$s(s-a)(s-b)(s-c) = d^4, \quad 2s = a+b+c\,. \tag{2}$$

Iščemo njene rešitve v naravnih številih a, b, c in d. Poskušajmo najprej takole: Če je vsak faktor na levi četrta potenca naravnega števila, je njihov produkt četrta potenca in je tedaj d naravno število. Pišimo torej $s-a = x^4$, $s-b = y^4$, $s-c = z^4$ in $s = t^4$. Iz (2) dobimo $d = xyzt$. Ker velja zveza

$(s-a)+(s-b)+(s-c)=s$, števila x, y, z in t niso poljubna, zadoščati morajo enačbi

$$x^4+y^4+z^4=t^4 \tag{3}$$

Vsaka rešitev te enačbe v naravnih številih x, y, z, t nam da Heronov trikotnik s stranicami $a=z^4+y^4$, $b=x^4+z^4$, $c=x^4+y^4$ in s ploščino $p=(xyzt)^2$. Žal pa piscu tega članka ni znana nobena rešitev enačbe (3) v naravnih številih. Euler je postavil domnevo, da take rešitve sploh ni.

Lotimo se naloge nekoliko drugače. Produkt $s(s-a)(s-b)(s-c)$ je lahko četrta potenca, ne da bi bil vsak faktor četrta potenca. Če npr. postavimo $s-a=x^4$, $s-b=8y^4$, $s-c=z^2$ in $s=2z^2$, je produkt enak $16x^4y^4z^4$, se pravi četrta potenca. Med števili x, y, z je zdaj zveza $2z^2=x^4+8y^4+z^2$ ali

$$x^4+8y^4=z^2 \tag{4}$$

Vsaka netrivialna celoštevilska rešitev x, y, z te enačbe da Heronov trikotnik s stranicami

$$a=8y^4+z^2,\ b=x^4+z^2,\ c=x^4+8y^4 \tag{4*}$$

in s ploščino $p=(2xyz)^2$, ki je popoln kvadrat. (Trivialna rešitev je taka, pri kateri je $y=0$ in je tedaj $z=\pm x^2$.) Eno netrivialno rešitev enačbe (4) takoj uganemo, namreč $x=1$, $y=1$, $z=3$. Ta nam da trikotnik $a=17$, $b=10$, $c=9$ s ploščino $p=36=6^2$. Torej smo tokrat imeli več sreče kakor pri prvem poizkusu.

Če je (x,y,z) celoštevilska rešitev enačbe (4) in m poljubno celo število, je tudi $x'=mx$, $y'=my$, $z'=m^2z$ celoštevilska rešitev. Pripadajoči trikotnik dobimo tako, da vse stranice prejšnjega trikotnika pomnožimo z m^4. Ker je novi trikotnik podoben prejšnjemu, nas tako dobljene rešitve ne zanimajo. Iskali bomo samo take rešitve enačbe (4), pri katerih sta si števili x in y tuji.

Poskusimo rešiti nalogo še na tale podoben način: Postavimo $s=9u^4$, $s-a=8w^2$, $s-b=w^2$ in $s-c=18v^4$. Produkt teh faktorjev je četrta potenca $(6uvw)^4$. Ker mora biti $9u^4=8w^2+w^2+18v^4$, dobimo v tem primeru enačbo

$$u^4-2v^4=w^2 \tag{5}$$

Vsaka celoštevilska netrivialna rešitev u, v, w nam da Heronov trikotnik

$$a=18v^4+w^2,\quad b=18v^4+8w^2,\quad c=9w^2 \tag{5*}$$

s ploščino $p=(6uvw)^2$, ki je popoln kvadrat. (Trivialna rešitev enačbe (5) je taka, pri kateri je $v=0$.) S poskušanjem hitro najdemo rešitev $u=3$, $v=2$, $w=7$. Pripadajoči trikotnik $a=337$, $b=680$, $c=441$ ima ploščino $p=252^2$.

Diofantski enačbi (4) in (5) sta med seboj povezani. Velja namreč tole:

Če zadoščajo x, y, z enačbi (4), *je trojka*

$$u=z,\ v=2xy,\ w=\pm(x^4-8y^4) \tag{6}$$

rešitev enačbe (5). *Če pa zadoščajo* u, v, w *enačbi* (5), *je trojka*

$$x = w,\ y = uv,\ z = u^4 + 2v^4 \tag{7}$$

rešitev enačbe (4).

To dokažemo s preprostim preskusom. Naj bo trojka (x, y, z) rešitev enačbe (4). Potem je

$$u^4 - 2v^4 = z^4 - 2(2xy)^4 = (x^4 + 8y^4)^2 - 32x^4y^4 = (x^4 - 8y^4)^2 = w^2$$

Torej trojka (6) zadošča enačbi (5). Podobno se prepričamo, da trojka (7) zadošča enačbi (4).

Trojka (6) sestoji očitno iz samih celih števil, če so x, y, z cela števila. Isto lahko trdimo o trojki (7). Tudi ni težko ugotoviti, da sta u in v tuji si števili, če sta si x in y tuja; prav tako sta si x in y v trojki (7) tuja, če sta taka u in v.

Iz rešitve $x = 1$, $y = 1$, $z = 3$ dobimo po formulah (6) rešitev $u = 3$, $v = 2$, $w = 7$ enačbe (5). Iz te rešitve pridemo s formulami (7) do nove rešitve enačbe (4), namreč $x = 7$, $y = 6$, $z = 113$. Tako lahko nadaljujemo. S tem postopkom dobivamo izmenoma rešitve enačbe (4) in enačbe (5). Te rešitve se večajo in so zato vse med seboj različne. Torej imata obe diofantski enačbi neskončno rešitev v tujih si številih. Formule (4*) in (5*) pa dajo neskončno zaporedje nepodobnih Heronovih trikotnikov, katerih ploščina je popoln kvadrat. S tem smo rešili nalogo, ki jo je postavil A. R. Melter.

2. Obravnavajmo problem Heronovih trikotnikov, ki imajo za ploščino popoln kvadrat, še z drugačno metodo.

Naj bodo a, b, c stranice Heronovega trikotnika s ploščino $p = d^2$, kjer je d naravno število. Potem so $a' = a/d$, $b' = b/d$ in $c' = c/d$ racionalne stranice podobnega trikotnika s ploščino 1. Obratno, imejmo trikotnik z racionalnimi stranicami a', b', c' in s ploščino 1. Pišimo $a' = a/d$, $b' = b/d$, $c' = c/d$, kjer so a, b, c naravna števila in je d najmanjši skupni imenovalec ulomkov a', b' in c'. Potem so a, b in c stranice Heronovega trikotnika s ploščino $p = d^2$. Ta razmislek pove, da lahko Melterjev problem formuliramo tudi v tej ekvivalentni obliki: Dokaži, da je neskončno trikotnikov, ki imajo racionalne stranice in ploščino 1.

Imejmo trikotnik z racionalnimi stranicami a, b, c in racionalno ploščino p, njegovi koti pa naj bodo α, β, γ. Kosinusov izrek pove, da so v takem trikotniku $\cos\alpha$, $\cos\beta$, $\cos\gamma$ racionalna števila, formula za ploščino $p = \frac{1}{2}bc\sin\alpha$ pa, da so tudi $\sin\alpha$, $\sin\beta$, $\sin\gamma$ racionalna števila. Če sta $\sin\varphi$ in $\cos\varphi$ racionalna, je prav tako $\operatorname{tg}\frac{1}{2}\varphi = \sin\varphi/(1+\cos\varphi)$ racionalno število. Torej so v našem trikotniku $\operatorname{tg}\frac{\alpha}{2}$, $\operatorname{tg}\frac{\beta}{2}$, $\operatorname{tg}\frac{\gamma}{2}$ racionalna števila.

Vzemimo zdaj trikotnik, v katerem sta

$$\operatorname{tg}\frac{\alpha}{2} = x \quad \text{in} \quad \operatorname{tg}\frac{\beta}{2} = y \tag{8}$$

racionalni števili. Ker je $\operatorname{tg}\frac{\gamma}{2} = \operatorname{ctg}\frac{\alpha+\beta}{2} = (1-xy)/(x+y)$, je tudi $\operatorname{tg}\frac{\gamma}{2}$ racionalno število. Z uporabo formule $\sin\varphi = 2\operatorname{tg}\frac{1}{2}\varphi/(1+\operatorname{tg}^2\frac{1}{2}\varphi)$ dobimo

$$\sin\alpha = \frac{2x}{1+x^2},\ \sin\beta = \frac{2y}{1+y^2},\ \sin\gamma = \frac{2(x+y)(1-xy)}{(1+x^2)(1+y^2)} \tag{9}$$

Torej so $\sin\alpha$, $\sin\beta$, $\sin\gamma$ racionalna števila. Ker je po sinusovem izreku $a:b:c = \sin\alpha:\sin\beta:\sin\gamma$, lahko pri primerno izbranem faktorju k pišemo

$$a = kx(1+y^2),\ b = ky(1+x^2),\ c = k(x+y)(1-xy). \tag{10}$$

Za vsak $k > 0$ so a, b, c stranice trikotnika, pri katerem je $\operatorname{tg}\frac{\alpha}{2} = x$ in $\operatorname{tg}\frac{\beta}{2} = y$. Ploščina tega trikotnika pa je

$$p = k^2xy(x+y)(1-xy). \tag{11}$$

Vidimo tole: Če je k racionalen, so stranice in ploščina trikotnika racionalna števila. Ker je vselej $c > 0$, mora biti produkt $xy < 1$.

Pripomba. Mimogrede smo našli metodo, s katero pridemo do vseh Heronovih trikotnikov: Izberimo si poljubni pozitivni racionalni števili x in y, ki zadoščata pogoju $xy < 1$. Vstavimo to v obrazce (10) in potem določimo racionalno število k tako, da so a, b, c naravna števlia. Pri primerno izbranem k so a, b, c brez skupnega faktorja. (Če je največji skupni faktor vseh stranic enak $m > 1$, zamenjamo k s k/m.)

Ploščina trikotnika je 1, kadar je med x, y, k zveza

$$k^2xy(x+y)(1-xy) = 1. \tag{12}$$

Naj bo x, y, k poljubna pozitivna racionalna rešitev te enačbe. Formule (10) nam dajo trikotnik z racionalnimi stranicami in ploščino 1. S tem smo problem trikotnikov z racionalnimi stranicami in ploščino 1 prevedli na iskanje pozitivnih racionalnih rešitev enačbe (12). Ena rešitev je npr. $x = 2$, $y = 1/4$, $k = 4/3$. Pripadajoči trikotnik imą stranice $a = 17/6$, $b = 10/6$, $c = 9/6$. Podoben je trikotniku s stranicami 17, 10, 9.

Poglejmo, ali obstajajo racionalne rešitve enačbe (12), pri katerih je med x in y zveza

$$x + y = 2\,. \tag{13}$$

Ker je $y = 2-x$, se zdaj enačba (12) glasi $2x(2-x)(1-x)^2k^2 = 1$. Vidimo, da je treba $x \in \mathbb{Q}$ izbrati tako, da bo produkt $2x(2-x)$ kvadrat racionalnega števila, npr. enak z^2, $z \in \mathbb{Q}$. Torej

$$2x(2-x) = z^2. \tag{14}$$

Ta enačba, ki jo lahko pišemo v obliki $2(x-1)^2 + z^2 = 2$, pomeni v ravnini (xz) elipso. Vsaka elipsa pa ima parametrični enačbi, kjer sta koordinati x

in z racionalni funkciji parametra t. Parametrični enačbi elipse (14) sta

$$x = \frac{2t^2}{t^2+2}, \quad z = \frac{4t}{t^2+2}.$$

O tem se prepričamo tako, da vstavimo ta izraza za x in y v enačbo (14). Če je t racionalen, sta taka tudi x in z. Zato je na elipsi (14) neskončno racionalnih točk. Iz (12) in (13) zdaj izračunamo

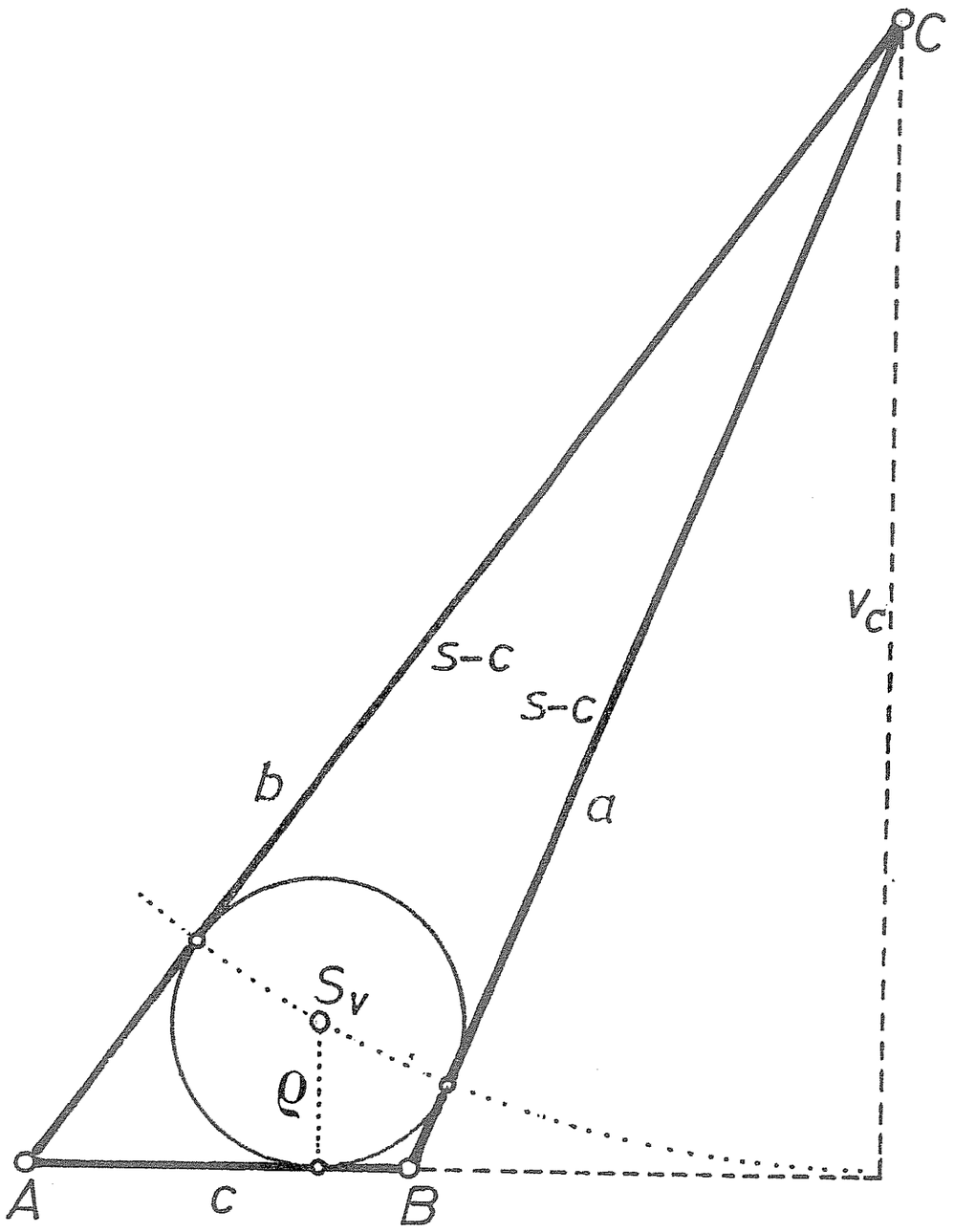
$$x = \frac{2t^2}{t^2+2}, \quad y = \frac{4}{t^2+2}, \quad k = \pm\frac{(t^2+2)^2}{4t(t^2-2)}. \tag{15}$$

Ta trojka za vsak t, $t \neq 0$, $t^2 \neq 2$, zadošča enačbi (12). Je racionalna, če je t racionalen. Torej ima enačba (12) neskončno racionalnih rešitev. Enačbe (10) pa nam dajo neskončno racionalnih trikotnikov s ploščino 1.

Vzemimo za t pozitivno racionalno število in ga pišimo v obliki $t = u/v$, kjer sta u in v naravni števili. Vstavimo to v (15), nato dobljene izraze v (10). Preprost račun nam da Heronov trikotnik s stranicami

$$\begin{gathered} a = u^6 + 4u^4v^2 + 20u^2v^4, \quad b = 10u^4v^2 + 8u^2v^4 + 8v^6 \\ c = u^6 - 2u^4v^2 - 4u^2v^4 + 8v^6 \end{gathered} \tag{16}$$

in s ploščino $p = 4u^2v^2(u^4-4v^4)^2$, ki je popoln kvadrat. Ker si lahko naravni števili u in v poljubno izberemo, določajo formule (16) dvoparametrično družino Heronovih trikotnikov. Ni težko ugotoviti, da so a, b, c brez skupnega faktorja, če je u lih in če sta si u in v tuja. Posebej za $u = 1$, $v = 1$ dobimo trikotnik $a = 25$, $b = 26$, $c = 3$ s ploščino $p = 6^2$.



Pri vseh trikotnikih (16) je $x + y = 2$, se pravi $\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\frac{\beta}{2} = 2$. Kaj je značilno za trikotnike, pri katerih velja med kotoma α in β ta zveza? Odgovor se glasi: V trikotniku je $\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\frac{\beta}{2} = 2$ natanko tedaj, ko je $s - c = v_c$, kjer pomeni v_c višino na stranico c (Glej sliko).

Dobili smo tri neskončne družine trikotnikov: družino (4*), ki pripada rešitvam enačbe (4), družino (5*), ki pripada rešitvam enačbe (5) in družino (16). Družini (4*) in (5*) ter družini (4*) in (16) nimata nobenega skupnega trikotnika. Edini skupni trikotnik družin (5*) in (16) pa je trikotnik $a = 337$, $b = 680$, $c = 441$. O tem se

prepričamo tako, da izračunamo $\operatorname{tg}\frac{\alpha}{2} = x$ in $\operatorname{tg}\frac{\beta}{2} = y$ za trikotnike navedenih družin. Izkaže se, da je za vse trikotnike družine (4*) $xy = 1/2$, za vse trikotnike družine (5*) pa $y = 8x$.

V formulah (16) se izražajo stranice s polinomi šeste stopnje parametrov u in v. Zato so vrednosti teh polinomov že pri razmeroma majhnih u in v precej velike. Vendar bi kakih dvajset trikotnikov s pomočjo žepnega računalnika kmalu izračunali. Povsem drugače je pri družinah (4*) in (5*). Če bi želeli izračunati prvih deset trikotnikov družine (4*), bi morali imeti na voljo največje računalnike, saj se stranice desetega trikotnika izražajo s števili, ki imajo stotisoče cifer.

3. Na koncu si natančneje poglejmo enačbo (12). Postavimo $k = 1/z$, pa dobimo

$$z^2 = xy(x+y)(1-xy) \tag{17}$$

Zanimajo nas racionalne rešitve te enačbe. Trivialna rešitev je tista, pri kateri je $z = 0$. Če imamo kakšno netrivialno pozitivno racionalno rešitev x, y, z in postavimo $k = 1/z$, dobimo rešitev enačbe (12), iz nje pa trikotnik z racionalnimi stranicani in ploščino 1. Preprost račun pokaže, da so hkrati z x, y, z rešitve enačbe (17) tudi $x' = -1/x$, $y' = y$, $z' = \pm z/x^2$, nadalje $x' = x$, $y' = -1/y$, $z' = \pm z/y^2$ in $x' = -1/x$, $y' = -1/y$, $z' = \pm z/(xy)^2$. Ker je ena od teh rešitev gotovo pozitivna, določa vsaka netrivialna rešitev enačbe (17) trikotnik z racionalnimi stranicami in ploščino 1.

V enačbi (17) nastopajo tri spremenljivke x, y in z. Izberimo si za y fiksno število, npr. $y = y_0 \neq 0$. Potem imamo med x in z enačbo

$$z^2 = xy_0(x+y_0)(1-xy_0) \tag{18}$$

Ker stoji na desni polinom tretje stopnje spremenljivke x, določa enačba (18) v ravnini (xz) kubično krivuljo, ki ji pravimo eliptična krivulja. Če je $y_0 \in \mathbb{Q}$, so koeficienti racionalni in je eliptična krivulja definirana v obsegu $\mathbb{Q}$. Zanimajo nas rešitve, kjer sta tudi x in z racionalni števili. Taki rešitvi pravimo racionalna točka na krivulji (18). Naj bo npr. $y_0 = 1$. Ker je $\operatorname{tg}\frac{\beta}{2} = y_0 = 1$, torej $\beta = 90°$, je naš trikotnik pravokoten. Fermat je dokazal, da ni pravokotnega trikotnika z racionalnimi stranicami in ploščino 1. Zato diofantska enačba (18) pri $y_0 = 1$, torej enačba

$$z^2 = x(1-x^2)$$

nima nobene netrivialne racionalne rešitve.

Naj bo (x_0, z_0) kakšna netrivialna racionalna točka na krivulji (18), torej taka, pri kateri je $z_0 \neq 0$. Postavimo v tej točki tangento na krivuljo in poiščimo presečišča tangente s krivuljo. Premica seče kubično krivuljo največ v treh točkah. Dotikališče (x_0, z_0) pa šteje za dve presečišči in zato seče tangenta krivuljo (18) le še v eni nadaljnji točki, ki naj ima koordinati (x_1, z_1). Ker so koeficienti v enačbi (18) racionalni, je racionalna tudi točka (x_1, z_1). V točki (x_1, z_1) spet postavimo tangento; le-ta naj seče krivuljo

še v točki (x_2, z_2), ki je prav tako racionalna. Če ta postopek nadaljujemo, dobimo na krivulji (18) neskončno zaporedje racionalnih točk (x_n, z_n). Ni rečeno, da so vse točke med seboj različne. Trikotniki, ki pripadajo temu zaporedju racionalnih rešitev, imajo isti $y = y_0 = \operatorname{tg} \frac{\beta}{2}$, torej vsi isti kot β.

Izberimo si katerikoli trikotnik družine (16) in zanj izračunajmo $\operatorname{tg} \frac{\alpha}{2} = x_0$ in $\operatorname{tg} \frac{\beta}{2} = y_0$. Pri tem y_0 ima enačba (18) racionalno rešitev (x_0, z_0). Če izhajamo iz točke (x_0, z_0), dobimo z opisano metodo tangent zaporedje racionalnih točk (x_n, z_n) na krivulji (18), temu zaporedju pa pripada zaporedje Heronovih trikotnikov, katerih ploščina je popoln kvadrat. Ker imajo vsi trikotniki tega zaporedja isti $y = y_0$, se pravi isti kot β, so različni od vseh trikotnikov družine (16), samo začetni trikotnik je skupen. Ne vemo pa, ali je v tem zaporedju neskončno ali le končno število različnih trikotnikov. Verjetno jih je neskončno.

Enačba (18) nima netrivialne racionalne rešitve pri vsakem racionalnem številu y_0. Zgoraj smo namreč ugotovili, da ni rešljiva pri $y_0 = 1$. Zato postavimo tole vprašanje:

Za katera racionalna števila y_0 premore enačba (18) *kakšno netrivialno racionalno rešitev?*

Verjetno je ta problem zelo težek. Rešili bi ga, če bi našli kak kriterij, s katerim bi se dalo za vsako dano racionalno število y_0 ugotoviti, ali ima enačba (18) pri tem y_0 netrivialno rešitev ali ne.

V zvezi s problemom, ki smo ga obravnavali v članku, lahko zgornje vprašanje formuliramo tudi takole: Za katere kote β obstaja trikotnik, ki ima en kot β, racionalne stranice in ploščino 1? Kakor vemo, je potreben pogoj, da je $\operatorname{tg} \frac{\beta}{2}$ racionalno število. Žal ta pogoj ni zadosten.

Dodatek. Prof. J. Grasselli me je opozoril, da je pred kratkim N. D. Elkies dokazal, da ima enačba (2) neskončno rešitev v naravnih številih [1]. Torej Eulerjeva domneva ni bila pravilna. Najmanjšo rešitev so našli z računalnikom. Glasi se

$$x = 95\,800, \quad y = 217\,519, \quad z = 414\,560, \quad t = 422\,481\,.$$

Stranice pripadajočega Heronovega trikotnika se izražajo s števili, ki imajo nad 20 cifer.

LITERATURA

[1] N. D. Elkies, *On* $A^4 + B^4 + C^4 = D^4$, Math. Comp. 51 (1988) 825–835.
[2] R. A. Melter, *Problem 6628,* Amer. Math. Monthly 97 (1990) 350.

NOVE KNJIGE

BATAGELJ V., Golli B., TEX. Povabilo v TEX, LATEX, BIBTEX, PICTEX, Ljubljana, Društvo matematikov, fizikov in astronomov Slovenije, 1990, 232 str. (Učbeniki in priročniki)

Knjiga je prvi domači učbenik za TEX, in bo prišla prav vsem tistim, ki bi radi TEX uporabljali, pa nimajo časa ali priložnosti prebrati The TEXbook D. E. Knutha ali Lamportovega priročnika za LATEX.

Avtorja najprej predstavita osnove TEX-a in njegove nadgradnje LATEX, potem pa nadrobno opišeta vse elemente stavljenja teksta v TEX-u in LATEX-u. Začneta s stavljenjem matematičnih izrazov, nadaljujeta pa z zahtevnejšimi ukazi za oblikovanje teksta: definiranje novih ukazov, postavljanje teksta v škatle in zlaganje škatel, kontrolne programske strukture in uporaba zahtevnejših vgrajenih ukazov, na primer za stavljenje razpredelnic. Opišeta tudi družino pisav Computer Modern in njeno uporabo v TEX-u in LATEX-u.

Drugi del knjige je posvečen orodjema za posebne namene: PICTEX-u za risanje slik in BIBTEX-u za sestavo bibliografije. Poglavje o PICTEX-u je opremljeno z velikim številom primerov in popelje bralca po najkrajši poti skozi zapleteno goščavo PICTEX-ovih ukazov.

Zadnja tri poglavja so pravzaprav dodatki; v njih so zbrani podatki, ki se ne vklapljajo logično v druge dele knjige. Poglavje 13 opiše najpogostejše napake pri delu in zdravila zanje, poglavje 14 govori o dostopnih implementacijah TEX-a na različnih računalnikih, zadnje poglavje pa natrosi množico zanimivih in včasih precej zapletenih zgledov za uporabo.

Marko Čibej

ZA VZPODBUDO

Za začetnika je iskanje in odpravljanje napak v opisu besedila zamuden posel, ki zahteva precej potrpljenja. Pomoč izkušenejšega uporabnika je pri prvih korakih nadvse koristna. Začetni napor in potrpljenje bosta poplačana, ko bomo zagledali lepo oblikovan in izpisan izdelek. Po dveh ali treh sestavkih postane delo s TEXom že bolj rutinsko in priprava opisa besedila ne vzame bistveno več časa kot tipkanje na pisalnem stroju ali delo na kateremkoli drugem urejevalniku. Pravzaprav lahko izkušen uporabnik TEXa piše članke v LATEXu celo hitreje kot z drugimi sredstvi, saj mu ni treba razmišljati o obliki in položaju naslovov poglavij, presledkih med poglavji in lomljenju strani, poleg tega pa lahko uporablja dele opisa besedila ali določene vzorce za matematične izraze, razpredelnice in slike iz prejšnjih sestavkov.

Odlomek iz priročnika V. Batagelj,
B. Golli, TEX. *Povabilo v TEX,*
LATEX, BIBTEX in PICTEX,
DMFA Slovenije, Ljubljana 1990

TAJNOPISI

BOJAN MAGAJNA

Math. Subj. Class. (1985): 11 Z 50

Razložene so osnove nekaterih kriptografskih metod, ki temeljijo na elementarni teoriji števil.

ON CRYPTOGRAPHY

Some cryptosystems based on elementary number theory are explained.

0. Uvod

Problem, kako šifrirati sporočila, da jih bodo razumeli le tisti, ki so jim namenjena, je zanimiv za diplomacijo in vojsko že od antičnih časov. V moderni dobi se je temu pridružila še potreba po varnem shranjevanju zapisanih informacij (na primer na računalniških diskih), tako da nepoklicane osebe, ki bi jim uspelo prodreti do podatkov, le-teh ne bi mogle razvozlati. Vedo, ki proučuje metode šifriranja sporočil, imenujemo kriptologija, načine šifriranja pa kriptosistemi ali tajnopisi. Tukaj si bomo ogledali nekaj vrst tajnopisov, ki temeljijo na teoriji števil.

Vsem znana je naslednja preprosta metoda šifriranja: dve osebi se dogovorita, da na primer beseda KRT pomeni NAPAD in za ta dogovor ne ve nihče drug. To je gotovo učinkovita metoda, vendar le enkrat ali nekajkrat. Pri večkratni uporabi bi namreč nasprotnik zlahka ugotovil, kaj pomeni beseda KRT, na osnovi posledic, ki so jih zapustile prejšnje uporabe te besede. Druga resna pomanjkljivost takega načina šifriranja tiči v dejstvu, da bi za pošiljanje in razvozlavanje daljših sporočil potrebovali obsežne slovarje, do njih pa bi se nasprotnik lahko dokopal. V tem sestavku nas bodo zanimali načini šifriranja, ki jih lahko uporabimo večkrat in ki dopuščajo (tistim, ki so jim sporočila namenjena) relativno enostavno dešifriranje. Pri tem se bomo omejili izključno na razlago osnovnih idej; s konkretno računalniško izvedbo algoritmov za šifriranje se tukaj ne bomo ukvarjali. Najpreprostejši taki tajnopisi temeljijo na modularni aritmetiki, to je na lastnostih kolobarjev $\mathbb{Z}_n$ ostankov po modulu n.

1. Nekaj preprostih kriptosistemov

Cezarjeva metoda. Privzemimo, da je sporočilo, ki ga želimo šifrirati, napisano v slovenščini. Prvi korak pri šifriranju je nadomestitev črk s števili. Vsaki od petindvajsetih črk slovenske abecede priredimo neko naravno število, tako da so različnim črkam prirejena različna števila. Denimo, zaradi enostavnosti, da smo črkam A, B, C,...,Ž priredili kar njihova zaporedna števila v abecedi. Vsako od teh števil predstavlja neki element kolobarja $\mathbb{Z}_{25}$. Vsaki besedi je na ta način prirejeno neko natanko določeno zaporedje elementov kolobarja $\mathbb{Z}_{25}$. Naj bo sedaj f poljubna bijektivna preslikava množice $\mathbb{Z}_{25}$ nase. Kot šifro za besedo, ki je reprezentirana z zaporedjem

$a_1, a_2, \ldots, a_n$ elementov kolobarja $\mathbb{Z}_{25}$, vzamemo sedaj zaporedje črk, ki pripadajo elementom $f(a_1), f(a_2), \ldots, f(a_n)$. Oseba, ki ji je sporočilo namenjeno, pozna funkcijo f in ga bo zato lahko dešifrirala z uporabo inverzne funkcije f^{-1}. Pri tem je lahko f poljubna bijektivna preslikava, saj le tedaj obstaja inverzna preslikava, ki jo potrebujemo za dešifriranje. V naslednjem zgledu bomo za f izbrali premik, to je preslikavo oblike $f(x) = x + a$, kjer bo a fiksen element iz $\mathbb{Z}_{25}$; inverzna preslikava je potem $f^{-1}(x) = x - a$. Preslikava f samo ciklično permutira elemente kolobarja $\mathbb{Z}_{25}$. Baje je ta način šifriranja prvi uporabil Julij Cezar in se zato imenuje *Cezarjev ključ*.

Zgled 1. Besedi UMIK ustreza v $\mathbb{Z}_{25}$ zaporedje elementov $22, 14, 10, 12$. Naj bo $f : \mathbb{Z}_{25} \to \mathbb{Z}_{25}$, $f(x) = x + 15$. Ker je $22 + 15 \equiv 12 \pmod{25}$ itd., je šifra za besedo UMIK zaporedje 12, 4, 0, 2 oziroma KČŽB. Prejemnik tega sporočila, ki pozna funkcijo f, lahko ugotovi, da je $f^{-1}(x) = x - 15$ in nato iz dobljenega zaporedja izračuna prvotno zaporedje ter s tem razvozla sporočilo.

Način šifriranja, ki smo ga videli v prejšnjem zgledu, je sicer zelo preprost, vendar ga je tudi zelo lahko "zlomiti". Kdor hoče ugotoviti, kaj šifre pomenijo (čeprav ne pozna šifrirnega ključa), potrebuje dve vrsti podatkov: splošno informacijo o načinu šifriranja in podatke o konkretnih parametrih, uporabljenih pri šifriranju danega teksta. V zgornjem zgledu je splošen podatek to, da smo uporabili Cezarjev način šifriranja, konkreten parameter pa je bil $a = 15$. Splošno informacijo o načinu šifriranja je težko obdržati tajno daljši čas. Šifrirni in dešifrirni stroji, ki se praktično uporabljajo, so namreč običajno zgrajeni le za določen kriptosistem (= način šifriranja), zato lahko nepoklicani sčasoma ugotovijo, kateri kriptosistem uporabljamo. Tukaj bomo privzeli, da je ta splošni podatek javen, torej, da je splošno znano, kakšne vrste kriptosistem uporabljamo. Podatke o konkretnih parametrih pa je (pri realno uporabnih kriptosistemih) nepoklicanim osebam veliko težje ugotoviti, še posebej, če jih pogosto spreminjamo. Pri Cezarjevem kriptosistemu pa tudi konkretnega parametra a ni težko odkriti. Dano šifrirano sporočilo lahko na primer poskusimo razvozlati tako, da jemljemo za a zaporedoma vseh 25 možnih elementov; zelo verjetno bo dešifrirano sporočilo smiselno samo pri eni vrednosti parametra a. Pri daljših sporočilih si lahko pomagamo s tem, da primerjamo zastopanost posameznih črk z njihovo povprečno zastopanostjo v tekstih. Črka, ki se v sporočilu najpogosteje pojavlja, je zelo verjetno šifra za črko, ki se v tekstih običajno najpogosteje pojavlja itd...

Izboljšana Cezarjeva metoda. Obstaja mnogo modifikacij Cezarjevega načina šifriranja, ki jih je precej težje razvozlati. Namesto premika lahko uporabimo kako bolj zapleteno preslikavo, na primer preslikavo $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = ax + b$, kjer nastopata dva parametra: a in b. Recimo, da uporabljamo abecedo z n znaki (npr. $n = 33$, če poleg petindvajsetih črk upoštevamo ločila in presledek). Da bi šifrirana sporočila lahko dešifrirali, mora obstajati za f inverzna preslikava. Lahko se je prepričati, da inverzna preslikava obstaja natanko tedaj, ko je a tuj z n in se glasi $f^{-1}(x) = \\ = a^{-1}x - ba^{-1}$, kjer je a^{-1} inverz elementa a v multiplikativni grupi $\mathbb{Z}_n^*$

vseh ostankov po modulu n, ki so tuji z n. Prisluškovalec, ki bi hotel prodreti v ta šifrirni sistem, bi moral ugotoviti a in b. V ta namen bi mu zadoščalo ugotoviti pomen dveh znakov, torej, da dva elementa y_1 in y_2 dejansko predstavljata x_1 in x_2. Potem bi namreč iz dveh enačb $ax_i + b = y_i$, $(i = 1, 2)$ lahko izračunal neznanki a in b (razen v izjemnih primerih). Ker se je do pomena dveh znakov mogoče dokopati s primerjanjem zastopanosti posameznih znakov v šifriranem tekstu z običajno zastopanostjo črk v tekstih, tudi tako modificiranega Cezarjevega ključa ni težko zlomiti.

Doslej opisana šifrirna sistema je bilo tako lahko razvozlati, ker smo elemente kolobarja $\mathbb{Z}_n$ prirejali posameznim črkam. Težje zlomljiv šifrirni sistem dobimo tako, da tekst, ki ga želimo šifrirati, najprej razdelimo v skupine po r znakov, kjer je r fiksno naravno število in nato tem r-terkam znakov priredimo elemente kolobarja $\mathbb{Z}_{n^r}$. (Če število znakov v tekstu ni deljivo z r, dodamo na koncu potrebno število presledkov.) Poljubni r-terki S znakov lahko priredimo element kolobarja $\mathbb{Z}_{n^r}$ na primer na naslednji način: naj bodo $x_1, \ldots, x_r$ naravna števila, ki ustrezajo posameznim znakom iz S (kot v prejšnjih načinih šifriranja); celotni r-terki S priredimo potem element iz $\mathbb{Z}_{n^r}$, predstavljen s številom $s = x_1 + x_2 n + x_3 n^2 + \cdots + x_r n^{r-1}$. Ker so števila $x_1, \ldots, x_r$ enolično določena z s (saj gre za cifre pri razvoju števila s z osnovo n), je celotna r-terka znakov S enolično določena z s. Ko na opisani način priredimo vsem r-terkam znakov danega sporočila elemente kolobarja $\mathbb{Z}_{n^r}$, ga lahko šifriramo z uporabo na primer afine preslikave $f : \mathbb{Z}_{n^r} \to \mathbb{Z}_{n^r}$, $f(x) = ax + b$, kjer mora biti a tuj z n. Če je r dovolj velik, je zelo težko prodreti v šifrirano sporočilo z analiziranjem frekvence zastopanosti znakov. Tokrat bi namreč morali analizirati zastopanost r-terk znakov, toda če r ni majhen, je število r-terk ogromno in je njihovo povprečno zastopanost v tekstih nemogoče ugotoviti.

Uporaba matrik nad $\mathbb{Z}_n$. Drugačno variacijo Cezarjevega kriptosistema lahko sestavimo z uporabo linearne algebre nad končnimi kolobarji $\mathbb{Z}_n$. Kot v prejšnjem odstavku bomo tudi sedaj tekst, ki ga hočemo šifrirati, najprej razdelili v skupine po r-znakov, kjer je r fiksno naravno število. (Če število vseh znakov ni deljivo z r, dodamo na koncu ustrezno število presledkov.) Vsakemu znaku naj bo prirejen neki element kolobarja $\mathbb{Z}_n$; vsaki r-terki znakov potem priredimo ustrezno r-terko elementov iz $\mathbb{Z}_n$, torej element množice $\mathbb{Z}_n^r = \mathbb{Z}_n \times \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n$ (r primerkov). Za šifriranje lahko sedaj uporabimo kako bijektivno preslikavo množice $\mathbb{Z}_n^r$ vase. Pri tem bomo izkoristili dejstvo, da je $\mathbb{Z}_n^r$ (levi) modul nad kolobarjem $\mathbb{Z}_n$. (To pomeni, da zadošča $\mathbb{Z}_n^r$ vsem aksiomom običajnega vektorskega prostora, le da je pri tem osnovni obseg nadomeščen s kolobarjem $\mathbb{Z}_n$; če je n praštevilo, je $\mathbb{Z}_n$ obseg in $\mathbb{Z}_n^r$ vektorski prostor nad njim.) Bijektivna preslikava f, ki jo bomo tukaj uporabili, bo linearna, torej podana z neko $r \times r$ matriko A z elementi v $\mathbb{Z}_n$. Če si predstavljamo elemente modula $\mathbb{Z}_n^r$ kot stolpce, potem je f definirana s predpisom

$$f(x) = Ax, \quad x \in \mathbb{Z}_n^r .$$

Kot običajno v linearni algebri je tudi tukaj zahteva, da mora biti f obrnljiva, ekvivalentna z zahtevo, da je matrika A obrnljiva v kolobarju $M_r(\mathbb{Z}_n)$ vseh $n \times n$ matrik z elementi v $\mathbb{Z}_n$. Obstajati mora torej taka matrika $A^{-1} \in M_r(\mathbb{Z}_n)$, da je $AA^{-1} = I$, kjer je I identična matrika (t.j., I ima enke po diagonali in ničle drugod). Za obrnljivost matrik nad poljubnim komutativnim kolobarjem K z enoto velja naslednji kriterij:

Matrika $A \in M_r(K)$ je obrnljiva natanko tedaj, ko je njena determinanta $\det(A)$ *obrnljiv element kolobarja K (če je K obseg, to pomeni, da je* $\det(A) \neq 0$*).*

Dokaz te trditve je podoben znanemu dokazu za realne matrike in ga zato tu ne bomo navajali.

Zgled 2. Po pravkar opisani metodi bomo šifrirali sporočilo

MIRKO–TIPKA–NA–RADIRKO.

Pri tem bomo uporabili naslednjo korespondenco med znaki abecede in elementi obsega $\mathbb{Z}_{31}$:

$$\begin{pmatrix} \text{A} & \text{B} & \text{C} & \dots & \text{V} & \text{Z} & \check{\text{Z}} & . & : & , & ! & ? & - \\ 1 & 2 & 3 & \dots & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 0 \end{pmatrix}.$$

Sporočilu ustreza torej naslednje zaporedje elementov kolobarja $\mathbb{Z}_{31}$:

$$14, 10, 18, 12, 16, 0, 21, 10, 17, 12, 1, 0, 15, 1, 0, 18, 1, 5, 10, 18, 12, 16, 26.$$

Sedaj razdelimo to zaporedje v skupine po $r = 3$ elementov; ker število znakov 23 ni deljivo s 3, dodamo na koncu še 0. Tako dobimo naslednje zaporedje vektorjev v $\mathbb{Z}_{31}$:

$$(14, 10, 18), (12, 16, 0), (21, 10, 17), (12, 1, 0), (15, 1, 0), (18, 1, 5), (10, 18, 12), (16, 26, 0). \tag{1.1}$$

Izberimo neko obrnljivo matriko v $M_3(\mathbb{Z}_{31})$, na primer matriko

$$A = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \\ 1 & 2 & 7 \end{pmatrix}.$$

Ker je $\mathbb{Z}_{31}$ obseg, lahko izračunamo inverz matrike A na običajen način; po krajšem računu dobimo

$$A^{-1} = \begin{pmatrix} 29 & 13 & 8 \\ 1 & 23 & 15 \\ 0 & 27 & 8 \end{pmatrix}.$$

Sporočilo sedaj šifriramo tako, da vse vektorje v zaporedju (1.1) napišemo kot stolpce ter jih nato pomnožimo z leve z matriko A. Dobljeni produkti,

napisani kot vektorji, se glasijo

$$(10,21,5),(29,26,13),(12,29,5),(15,28,14),(18,3,17),(15,8,24),(0,9,6),(1,12,6).$$

Temu ustreza naslednje zaporedje znakov, ki ga lahko odpošljemo kot šifrirano sporočilo:

ITD!.LK!DN,MRCPNGZ–HEAKE

Kdor bi hotel dešifrirati naše tajno sporočilo, bi moral poznati matriko A^{-1} (oziroma A). Ker ima $r \times r$ matrika A njemu r^2 neznanih elementov, bo za dovolj velike r tak šifrirni ključ precej težje zlomil kot Cezarjevega.

2. RSA kriptosistem

V vseh doslej navedenih primerih in v vseh kriptosistemih, ki so jih uporabljali do leta 1976, je bilo sporočilo lahko dešifrirati, če smo poznali šifrirni ključ (to je, način šifriranja skupaj z vrednostmi nastopajočih parametrov). Poznavanje šifrirnega ključa je namreč omogočalo na enostaven način izračunati dešifrirni ključ. Pred približno petnajstimi leti pa so odkrili kriptosisteme, pri katerih nam poznavanje šifrirnega ključa še ne omogoča dešifriranja. Pri takih kriptosistemih lahko šifrirni ključ celo objavimo, zato jih bomo imenovali *kriptosistemi z javnim ključem*. Eden najstarejših in najučinkovitejših takih sistemov je *RSA kriptosistem*, ki so ga leta 1978 odkrili Rivest, Shamir in Adleman. O tem je Obzornik že poročal [7], vendar v [7] niso razloženi številsko teoretični temelji RSA kriptosistema; tukaj se bomo omejili prav na te temelje.

Za vsako naravno število n označimo s $\varphi(n)$ moč množice vseh naravnih števil, ki so manjša od n in tuja z n. Če je na primer n praštevilo p, potem je $\varphi(n) = \varphi(p) = p - 1$. Če pa je n potenca praštevila, $n = p^e$, potem med števili, manjšimi ali enakimi n, niso tuja z n natanko števila $p, 2p, \ldots, p^{e-1}p$. Ker je teh števil p^{e-1}, je $\varphi(n) = \varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. Preslikavo φ, ki vsakemu naravnemu številu n priredi $\varphi(n)$, imenujemo *Eulerjeva funkcija* φ. Podrobnejšo razlago Eulerjeve funkcije lahko najde bralec v [2] ali [6], tukaj omenimo le še njeno zelo pomembno lastnost: če sta m in n tuji števili, potem je $\varphi(mn) = \varphi(m)\varphi(n)$. Ta lastnost, ki jo imenujemo multiplikativnost Eulerjeve funkcije, temelji na dejstvu, da predstavlja dano naravno število a obrnljiv element kolobarja $\mathbb{Z}_n$ natanko tedaj, ko sta števili a in n tuji. Torej pomeni $\varphi(n)$ ravno moč grupe vseh obrnljivih elementov kolobarja $\mathbb{Z}_n$. Od tod sledi, da je $a^{\varphi(n)} \equiv 1 \pmod{n}$ za vsak a, ki je tuj z n.

Naj bosta sedaj n in e naravni števili, pri čemer naj bo e tuje s $\varphi(n)$. Potem predstavlja e obrnljiv element kolobarja $\mathbb{Z}_{\varphi(n)}$, torej obstaja tako naravno število $\bar{e}$, da je $e\bar{e} \equiv 1 \pmod{\varphi(n)}$ oziroma $e\bar{e} = 1 + k\varphi(n)$ za primeren $k \in \mathbb{N}$. Za poljubno naravno število b, tuje z n, imamo potem $b^{e\bar{e}} = b^{1+k\varphi(n)} = b(b^{\varphi(n)})^k \equiv b \pmod{n}$. Pravkar izpeljana kongruenca

$$(b^e)^{\bar{e}} \equiv b \pmod{n} \tag{2.1}$$

je osnova RSA kriptosistema.

Kot doslej tekstu, ki ga bomo šifrirali, najprej priredimo zaporedje, recimo, kvečjemu dvomestnih naravnih števil. Ta števila lahko potem zlepimo v skupine po r števil, ki jih lahko imamo za $2r$ mestna števila. Katerokoli od teh $2r$ mestnih števil bomo imenovali *beseda* in označili z b. Naj bo n tako veliko naravno število, da je vsak njegov prafaktor večji od vseh možnih besed. Potem je vsaka beseda b tuja z n. Izberimo sedaj še število e tuje s $\varphi(n)$. Dano sporočilo potem šifriramo tako, da priredimo vsaki besedi b (enolično določeno) število s, ki zadošča pogojema $s < n$, $s \equiv b^e \pmod{n}$. Prejemnik bo sporočilo dešifriral tako, da bo izračunal število $\bar{b}$, kjer je $\bar{b} \equiv \cdot \equiv s^{\bar{e}} \pmod{n}$, $\bar{b} < n$; zaradi (2.1) bo namreč dobil rezultat $\bar{b} = b$.

Zgled 3. Zaradi lažjega računanja bomo tukaj vzeli za n majhno število, $n = 41$, in iz istega razloga naj bo $r = 1$. Sporočilo, ki ga bomo šifrirali, pa naj sestoji iz ene same besede NE. Če črkam priredimo kar njihove zaporedne številke v abecedi, potem lahko besedo NE zapišemo kot par števil 15, 6. Ker je $n = 41$ praštevilo, je $\varphi(n) = 40$. Izberimo še število $e = 3$, ki je tuje s 40. Šifriramo tako, da izračunamo $15^3 \pmod{41}$ in $6^3 \pmod{41}$. Imamo

$$15^2 \equiv 20 \Rightarrow 15^3 = 15^2 \cdot 15 \equiv 20 \cdot 15 \equiv 13 \pmod{41}$$

in podobno

$$6^2 \equiv -5 \Rightarrow 6^3 \equiv (-5) \cdot 6 = -30 \equiv 11 \pmod{41}.$$

Šifrirano sporočilo je torej 13, 11 oziroma LJ.

Za dešifriranje potrebujemo število $\bar{e}$, ki zadošča temule pogoju $e\bar{e} \equiv 1 \pmod{\varphi(n)}$, oziroma $3\bar{e} \equiv 1 \pmod{40}$. Ta pogoj je ekvivalenten enačbi

$$3\bar{e} = 1 + 40x,$$

kjer morata biti $\bar{e}$ in x celi števili. Enačbo lahko napišemo v obliki $\bar{e} = 13x + \frac{1+x}{3}$, od koder vidimo, da mora biti $\frac{1+x}{3}$ celo število, ki ga bomo imenovali y. Potem je $x = 3y - 1$ in $\bar{e} = 40y - 13$. Za $y = 1$ je $\bar{e} = 27$. Šifrirano sporočilo razvozlamo tako, da izračunamo $13^{27} \pmod{41}$ in $11^{27} \pmod{41}$. Lahko je preveriti, da res dobimo nazaj prvotni par 15, 6.

Pravkar navedeni zgled seveda ni uporaben v praksi, saj je praštevilo 41 premajhno, da bi spretnemu nasprotniku pri razvozlavanju povzročilo resne težave. V praksi je n sestavljeno število in sicer produkt dveh orjaških praštevil, $n = p_1 \cdot p_2$. Potem je $\varphi(n) = (p_1 - 1)(p_2 - 1)$. Za šifriranje potrebujemo torej še kako število e, tuje s $(p_1 - 1)(p_2 - 1)$. *Šifrirni ključ* je par (n, e). Kdor hoče dešifrirati, mora poznati število $\bar{e}$, ki zadošča pogoju $e\bar{e} \equiv 1 \pmod{\varphi(n)}$, v ta namen pa mora seveda poznati $\varphi(n)$. Privzemimo, da nasprotnik pozna n. Da bi ugotovil $\varphi(n)$, mora najprej razcepiti n na prafaktorja p_1 in p_2, kar pa je praktično neverjetno težka naloga, če sta le p_1 in p_2 dovolj veliki praštevili in tudi njuna razlika ni premajhna. Objava RSA kriptosistema je pospešila mrzlično iskanje hitrih algoritmov za razcep

števil na prafaktorje. Z najzmogljivejšimi računalniki je zato danes lahko razcepiti na prafaktorje 60-mestna števila, toda razcep 120- mestnega števila lahko traja več mesecev. Danes se zdi, da bo razcep 200 mestnih števil na prafaktorje tudi v dogledni bodočnosti praktično nerešljiv problem [4, str. 2,26]. To dejstvo omogoča, da lahko šifrirni ključ (n, e) objavimo, a nasprotnik kljub temu ne bo mogel dešifrirati sporočil.

Opomba. Za dešifriranje na prvi pogled ne potrebujemo samega razcepa števila n na prafaktorje, temveč le $\varphi(n)$. Toda problem, kako poiskati $\varphi(n)$, ni nič lažji od problema razcepitve na prafaktorje (vsaj v primeru, ko ima n le dva prafaktorja). Če namreč poznamo $\varphi(n)$, potem lahko iz enačbe $\varphi(n) = (p_1 - 1)(p_2 - 1) = p_1 p_2 - (p_1 + p_2) + 1$ izrazimo $p_1 + p_2 = n + 1 - \varphi(n)$. Iz zveze $(p_1 - p_2)^2 = (p_1 + p_2)^2 - 4p_1 p_2 = (p_1 + p_2)^2 - 4n$ izrazimo nato še $p_1 - p_2$. Ko poznamo $p_1 + p_2$ in $p_1 - p_2$, je malenkost izračunati p_1 in p_2.

Pošiljatelju sporočila je seveda razcep števila n na prafaktorje znan, saj je n dobil tako, da je zmnožil dve zelo veliki (recimo 100-mestni) praštevili. Kako pa dobimo tako velika praštevila, saj se zdi problem, pokazati, da je dano število p praštevilo, ekvivalenten problemu iskanja vseh možnih deliteljev števila p? Obstajajo zelo hitri algoritmi, ki omogočajo testiranje, ali je p praštevilo, ne da bi bilo pri tem treba preizkusiti vsa manjša števila kot možne delitelje. Ti algoritmi, ki jih tukaj ne bomo opisovali (glejte npr. [3]), temeljijo na lastnostih praštevil. Znano je na primer, da je

$$b^p \equiv b \pmod{p} \tag{2.2}$$

za vsako naravno število b, če je p praštevilo. Če torej relacija (2.2) za kak b ne velja, potem p ni praštevilo. Izkaže se, da verjetnost za to, da p ni praštevilo, zelo hitro pada s številom b-jev, za katere smo relacijo (2.2) že potrdili; če smo torej zadovoljni z verjetnostnim kriterijem, potem zadošča, da preverimo relacijo (2.2) le za nekaj vrednosti števila b. Toda tudi če velja (2.2) za vse b (kar je ekvivalentno z njeno veljavnostjo za vse $b < p$), se lahko zgodi (čeprav zelo redko), da p ni praštevilo. Naravno število $p > 1$, ki zadošča pogoju (2.2) za vsak naraven b, imenujemo *psevdopraštevilo*. Sestavljena psevdopraštevila so izredno redka: praštevil, manjših od 1000, je 168, toda edino sestavljeno psevdopraštevilo manjše od 1000, je $561 = 3 \cdot 11 \cdot 17$; manjših od 100 000 000 je 5 761 455 praštevil in le 252 sestavljenih psevdopraštevil [1]. Pokazali bomo, da so psevdopraštevila prav tako uporabna za RSA kriptosistem kot prava praštevila. V ta namen potrebujemo nekaj priprave.

Lema 1. *Psevdopraštevilo p ni deljivo s kvadratom nobenega naravnega števila, različnega od 1.*

Dokaz. Predpostavimo nasprotno, da je $p = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, kjer so $p_1, \ldots, p_r$ različna praštevila in vsaj eden od eksponentov, recimo e_1, večji od 1. Po kitajskem izreku o ostankih [2, str. 92] obstaja naravno število b, ki zadošča pogojem

$$b \equiv p_1^{e_1 - 1} \pmod{p_1^{e_1}} \tag{2.3}$$

$$b \equiv 0 \pmod{p_j^{e_j}}, \quad j = 2, \ldots, r.$$

Potem je očitno $b^p \equiv 0 \pmod{p_i^{e_i}}$ za vsak $i = 1, \ldots, r$, torej $b^p \equiv 0 \pmod{p}$. Iz (2.3) sledi tudi, da b ni deljiv s $p_1^{e_1}$, torej $b \not\equiv 0 \pmod{p}$. Iz povedanega sledi $b^p \not\equiv b \pmod{p}$, toda to nasprotuje privzetku, da je b psevdopraštevilo. ■

Lema 2. *Naj bo p psevdopraštevilo, $p = p_1 \ldots p_r$ razcep na prafaktorje in $m = [p_1 - 1, p_2 - 1, \ldots, p_r - 1]$ najmanjši skupni mnogokratnik števil $p_j - 1$. Potem m deli $p - 1$.*

Dokaz. Ker je grupa obrnljivih elementov končnega obsega $\mathbb{Z}_{p_j}$ ciklična [2, str. 109], obstaja za vsak $j = 1, \ldots, r$ v $\mathbb{Z}_{p_j}$ element b_j reda $p_j - 1$ (to pomeni, da je $b_j^{p_j - 1} \equiv 1 \pmod{p_j}$ in $p_j - 1$ deli vsako naravno število t, ki zadošča pogoju $b^t \equiv 1 \pmod{p_j}$). Ker je p psevdopraštevilo, je $b_j^p \equiv b_j \pmod{p}$, torej tembolj $b_j^p \equiv b_j \pmod{p_j}$. Ker je b_j tuj s p_j, sledi iz zadnje kongruence, da je $b_j^{p-1} \equiv 1 \pmod{p_j}$. Od tod sklepamo, da je število $p - 1$ deljivo z vsemi števili $p_j - 1, j = 1, \ldots, r$, torej tudi z njihovim najmanjšim skupnim mnogokratnikom m. ■

Trditev 1. *Če sta p_1 in p_2 tuji psevdopraštevili in $n = p_1 p_2$, potem je*

$$b^{k(p_1-1)(p_2-1)+1} \equiv b \pmod{n}$$

za poljubni naravni števili b in k.

Dokaz. Naj bo $n = q_1 q_2 \cdots q_r$ razcep števila n na prafaktorje. Ker sta si psevdopraštevili p_1 in p_2 tuji, sledi iz leme 1, da so q_j med seboj različna števila. Z uporabo leme 2 vidimo, da najmanjši skupni mnogokratnik m števil $q_1 - 1, \ldots, q_r - 1$ deli $(p_1 - 1)(p_2 - 1)$; naj bo torej $(p_1 - 1)(p_2 - 1) = tm$, kjer je $t \in \mathbb{N}$. Nadalje naj bodo t_j, $(j = 1, \ldots, r)$ taka naravna števila, da je $m = t_j(q_j - 1)$. Potem lahko zapišemo

$$b^{k(p_1-1)(p_2-1)+1} = b^{ktm+1} = b^{ktt_j(q_j-1)+1} = b(b^{q_j-1})^{ktt_j} \tag{2.4}$$

za vsak j. Če je b deljiv s q_j, potem je izraz $\sigma = b^{k(p_1-1)(p_2-1)+1} - b$ očitno deljiv s q_j. Če pa b ni deljiv s praštevilom q_j (torej, če je b tuj s q_j), potem je $b^{q_j-1} \equiv 1 \pmod{q_j}$ in iz (2.4) tedaj sledi $b^{k(p_1-1)(p_2-1)+1} \equiv b \pmod{q_j}$. Torej je izraz σ v vsakem primeru deljiv s q_j; ker so q_j različna praštevila, je deljiv tudi z njihovim produktom n. ■

Iz zadnje trditve takoj sledi, da so psevdopraštevila prav tako dobra za uporabo v RSA kriptosistemih kot prava praštevila. Kar vzemimo, da je naš šifrirni ključ par (n, e), kjer je $n = p_1 p_2$ produkt dveh tujih psevdopraštevil in e tuj s $(p_1 - 1)(p_2 - 1) = \varphi_n$ (če sta p_1 in p_2 praštevili, je $\varphi_n = \varphi(n)$). Sporočilo, predstavljeno s številom b, šifriramo tako, da izračunamo $s \equiv b^e \pmod{\varphi_n}$, $s < n$. Za dešifriranje pa je treba izračunati $s^{\bar{e}} \pmod{\varphi_n}$, kjer $\bar{e}$ zadošča pogoju $e\bar{e} \equiv 1 \pmod{\varphi_n}$, oziroma $e\bar{e} = 1 + k\varphi_n$ za primeren $k \in \mathbb{Z}$.

Ker je $b^{k\varphi_n+1} \equiv b \pmod{n}$ po trditvi 1, dobimo pri dešifriranju res prvotno sporočilo, saj velja: $s^{\bar{e}} \equiv (b^e)^{\bar{e}} = b^{k\varphi_n+1} \equiv b \pmod{n}$.

Običajno je zelo pomemben del vsakega dokumenta podpis, ki potrjuje njegovo pristnost. Pri elektronskem komuniciranju ne moremo prenašati fizičnega podpisa, zato se je treba opreti na drugačno potrjevanje pristnosti. Oglejmo si, kako RSA kriptosistem omogoča zanesljivo potrjevanje avtentičnosti. Recimo, da si Anton in Bernarda na daljavo izmenjujeta tajna sporočila z uporabo RSA kriptosistema. Pri tem naj uporabljata javna šifrirna ključa (n_A, e_A) in (n_B, e_B); ustrezni dešifrirni števili $\bar{e}_A$ in $\bar{e}_B$ pa sta znani seveda samo Antonu in Bernardi. Recimo, da želi Anton poslati Bernardi svoj podpis, ki je predstavljen s številom b. Potem šifrira b z uporabo ključa $(n_A, \bar{e}_A)$. Bernarda bo na dobljenem sporočilu uporabila ključ (n_A, e_A); če bo dobila b, bo vedela, da je sporočilo poslal Anton, kajti samo on pozna $\bar{e}_A$ in uporaba vsakega od $\bar{e}_A$ različnega števila pri šifriranju bi pri dešifriranju z e_A dala rezultat različen od b. Če hoče Anton zagotoviti, da nihče drug (razen Bernarde) ne bo prebral podpisa b, potem ga šifrira dvakrat: najprej s ključem $(n_A, \bar{e}_A)$, nato še s ključem (n_B, e_B). Bernarda lahko sporočilo prebere z zaporedno uporabo ključev $(n_B, \bar{e}_B)$ in (n_A, e_A).

3. Drugi kriptosistemi z javnim ključem

RSA kriptosistem temelji na dejstvu, da je mnogo lažje poiskati dve veliki praštevili in ju zmnožiti kot pa razcepiti zelo veliko število na prafaktorje. V teoriji števil obstajajo še drugi postopki, ki jih je v praksi zelo težko obrniti. Eden takih je *problem diskretnih logaritmov*. V realnih številih ni operacija logaritmiranja nič težja od eksponenciranja, situacija pa je povsem drugačna v končnih grupah. Vzemimo na primer grupo $\mathbb{Z}_n^*$ vseh obrnljivih elementov kolobarja $\mathbb{Z}_n$, kjer je n fiksno naravno število. Z uporabo metode zaporednega kvadriranja (kot v zgledu 3) je mogoče hitro izračunati vse potence a^x za poljuben $a \in \mathbb{Z}_n^*$, tudi če je x zelo veliko naravno število. Obratni problem, pri danem $y \in \mathbb{Z}_n^*$ poiskati tak x, da bo $a^x = y$ (če seveda tak x sploh obstaja), pa je pri velikem n praktično mnogo težje rešljiv. Ta problem imenujemo problem diskretnih logaritmov.

Na problemu diskretnih logaritmov temelji več šifrirnih sistemov z javnim ključem. Tukaj bomo na kratko opisali le *El Gamalov kriptosistem*. Naj bo n zelo veliko naravno število in a fiksen obrnljiv element kolobarja $\mathbb{Z}_n$. Izberimo število e med 1 in $n-1$ ter ga ohranimo v tajnosti. Šifrirni ključ, ki ga lahko objavimo, je a^e. Predpostavimo, da je sporočilo, ki ga hočemo šifrirati, predstavljeno z elementom b kolobarja $\mathbb{Z}_n$. Potem je šifrirano sporočilo predstavljeno kot par (a^k, ba^{ek}), kjer k fiksno naravno število. Kdor pozna tajni eksponent e, lahko sporočilo razvozla (se pravi, izračuna b) tako, da najprej izračuna $(a^k)^e = a^{ke}$ in nato z dobljenim rezultatom deli ba^{ek}. Nasprotnik, ki bi mu iz javnega ključa a^e uspelo ugotoviti e, bi prodrl v ta šifrirni sistem, vendar je za primerno izbrana a in e to lahko v praksi silno težka naloga.

Vsi kriptosistemi, ki smo jih doslej opisali, temeljijo na uporabi končnih kolobarjev $\mathbb{Z}_n$ oziroma končne grupe $\mathbb{Z}_n^*$. Ali je mogoče tudi druge končne grupe uporabiti za konstrukcijo kriptosistemov? Da bi bil tak šifrirni sistem učinkovit, mora imeti končna grupa zelo veliko elementov, njena struktura pa mora biti dovolj bogata, da dopušča relativno enostavno praktično računanje. Obsežno družino takih končnih Abelovih grup predstavljajo eliptične krivulje nad končnimi obsegi. Opis kriptosistemov, temelječih na eliptičnih krivuljah, pa presega namen tega sestavka, najti ga je mogoče npr. v [3].

LITERATURA

[1] L. Childs, *A concrete introduction to higher algebra,* UTM, Springer-Verlag, New York 1979.
[2] J. Grasselli, *Osnove teorije števil, Knjižnica Sigma* 14a, DMFA, Ljubljana 1975.
[3] N. Koblitz, *A course in number theory and cryptography,* GTM, Springer-Verlag, Berlin 1987.
[4] J. H. Loxton, *Number theory and cryptography,* LMS Lecture note series 154, Cambridge Univ. Press., Cambridge 1990.
[5] G. Mackiw, *Applications of abstract algebra,* J. Wiley&Sons, New York 1985.
[6] I. Vidav, *Algebra,* Matematika-Fizika 4, DMFA, Ljubljana 1989.
[7] J. Zupan, *Nekaj kriptografskih metod,* Obzornik Mat. fiz. 25 (1978) 129-136.

VABILO

Zavod Republike Slovenije za šolstvo in Oddelek za fiziko Univerze v Ljubljani prirejata v sodelovanju z Evropskim fizikalnim društvom mednarodno konferenco o pouku fizike z naslovom

VLOGA EKSPERIMENTA PRI POUKU FIZIKE

Konferenca — v angleškem jeziku — bo trajala 4 dni, in sicer od 26. do 29. avgusta v Škofji Loki. Pri organizaciji konference sodelujemo tudi s skupnostjo Alpe-Jadran.

Konferenca bo namenjena proučevanju vloge eksperimenta pri pouku fizike od osnovne šole do univerze, s poudarkom na srednji šoli. Posebno pozornost bomo namenili sodobni učni tehnologiji, saj je računalniško vodeno eksperimentiranje odprlo nove razsežnosti in spodbudilo živahen razvoj tudi pri našem projektu, tako da bomo na konferenci aktivno sodelovali s svojimi prispevki.

Konferenca pa naj bi nudila več kot samo predstavitev najnovejših dosežkov učne tehnologije. Spregovorili naj bi tudi o vlogi eksperimenta pri pouku in o njegovem pomenu za razvoj mišljenja. Zelo aktualno vprašanje za nas je eksperimentalno delo učenca kot sestavina pouka, se pravi učne ure in ocenjevanja. Razprava bo za nas zelo dragocena, saj želimo s posodabljanjem pouka fizike omejiti pretirani pomen in obseg računskih nalog, zlasti v srednji šoli, in bolj poudariti razumevanje fizikalnih zakonov.

Na konferenci naj bi aktivno sodelovalo okoli 70 udeležencev, od tega kakih 50 iz drugih držav. Dopoldneve nameravamo nameniti za predavanja, popoldneve za predstavitve, diskusije in delavnice. Za praktični del konference bodo na razpolago laboratoriji škofjeloškega srednješolskega centra.

Vabimo vse, ki želijo aktivno sodelovati na konferenci, naj se povežejo s prireditelji na Zavodu Republike Slovenije za šolstvo, Poljanska cesta 28, 61001 Ljubljana, tel. 319-066.

Seta Oblak

TRAJNI MAGNETI PRI SLIKANJU Z MAGNETNO RESONANCO

GORAZD PLANINŠIČ

PACS a8715Mv a0758-j

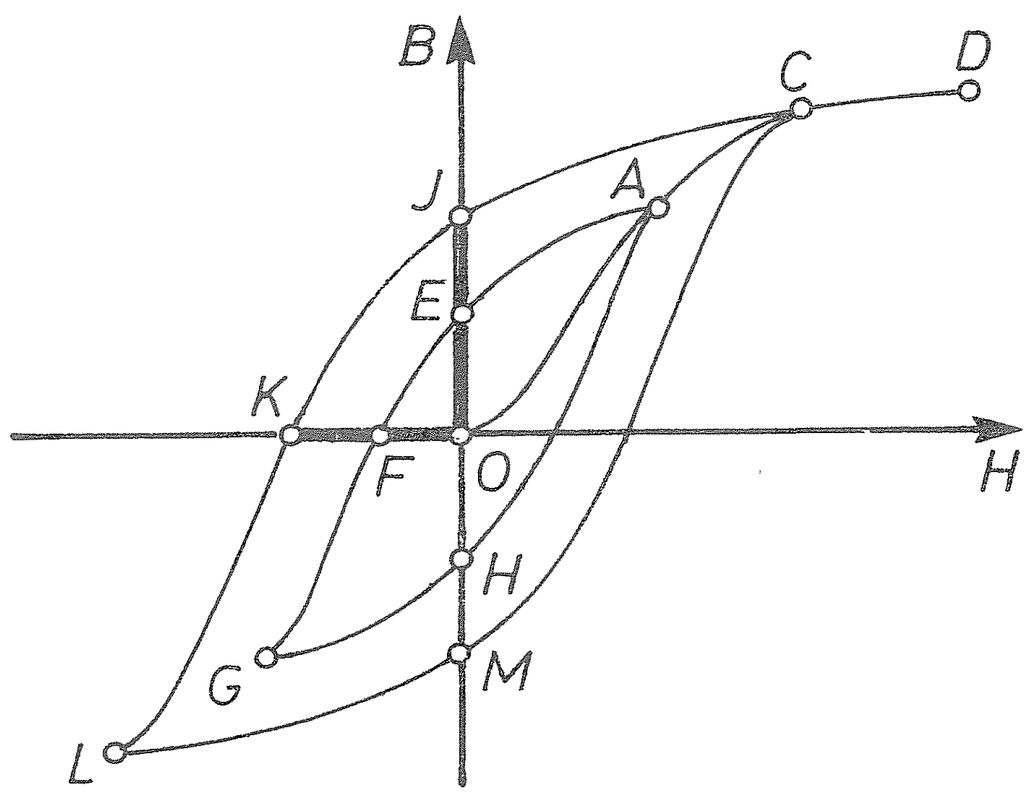
V prvem delu članka so opisane osnovne lastnosti trajnih magnetov. Pri tem si pomagamo s pojmom površinske gostote magnetnega naboja. Omenjeni so nekateri magnetni materiali in njihove fizikalne lastnosti. Trajne magnete uporabljamo tudi v magnetizacijskem delu tomografa na magnetno resonanco. Več pozornosti posvetimo sistemu prizmatične oblike z dodatki za izboljšanje homogenosti magnetnega polja.

PERMANENT MAGNETS IN NMR IMAGING

In the beginning of the article the characteristics of permanent-magnet materials are described. The surface density of magnetic charge is introduced and physical properties of some magnetic materials are given. Permanent magnets can be used as magnetising part of NMR tomography systems. The evolution of prismatic magnetic system is discussed and some ideas for correction of field inhomogeneity are given.

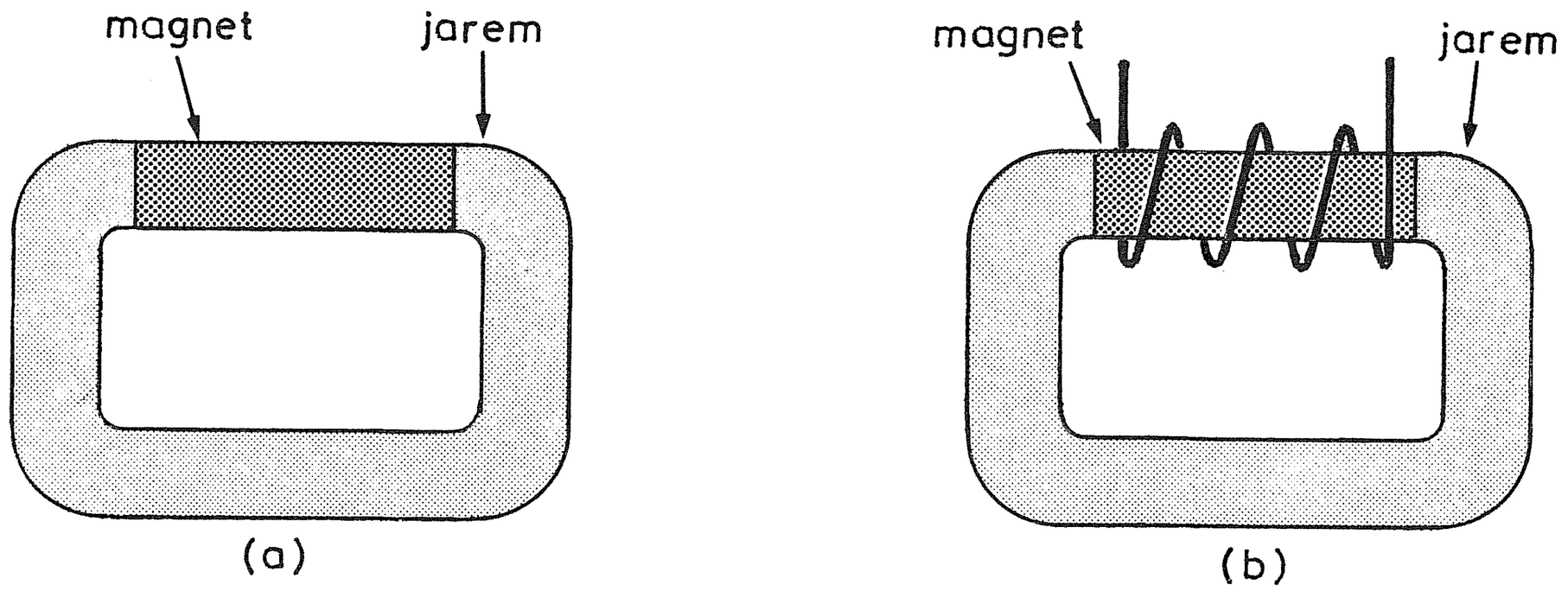
1. Trajni magneti

Lastnosti feromagnetnih snovi se ne da opisati s konstantno permeabilnostjo μ kot pri diamagnetnih in paramagnetnih snoveh. Gostota magnetnega polja B pri njih ni sorazmerna z jakostjo magnetnega polja H. Poleg tega kažejo feromagnetne snovi histerezo: njihovo trenutno stanje določajo še stanja v preteklosti. V vzorcu, ki še ni bil v magnetnem polju, z naraščajočo jakostjo magnetnega polja narašča gostota magnetnega polja, kar kaže magnetilna krivulja ($OACD$) (Sl. 1). Če v nekem stanju (A) pričnemo jakost magnetnega polja zmanjševati, jo obrnemo v nasprotno smer in nato povečamo do prvotne vrednosti, dobimo notranjo histerezno zanko ($AEFGHA$). Vsaki točki na magnetilni krivulji ustreza druga taka zanka. Z nadaljnjim večanjem začetne jakosti ploščina notranje histerezne zanke narašča. Prej ali slej dosežemo nasičenje: zveza med jakostjo in gostoto postane linearna in magnetizacija konstantna. Zanka z največjo ploščino je za snov značilna *histerezna zanka*.



Slika 1: Histerezna zanka feromagnetne snovi

Za magnetne materiale sta pomembna dva podatka. *Remanentna gostota magnetnega polja*, pri kateri je jakost magnetnega polja enaka nič (J), in *koercitivna jakost magnetnega polja*, pri kateri pade gostota magnetnega polja na nič (K).



Slika 2: Trajni magnet, sklenjen z visokopermeabilnim jarmom: (a) v jarmu je $B_j = B_r$, $H_m = 0$ (a), (b) v jarmu je $B_j = 0$, jakost magnetnega polja H, ki jo povzroča tok v navitju, je enaka H_c

Pomena količin se posebej zavemo, če sklenemo pola trajnega magneta z jarmom iz mehkega železa (Sl. 2). Permeabilnost mehkega železa ima velikostno stopnjo tisoč in zanjo lahko večkrat privzamemo, da naraste prek vsake meje. Zato ostane ves magnetni pretok v notranjosti in iz enačbe $\Phi_m = \Phi_j$ sledi

$$B_m = B_j \tag{1}$$

Indeksa m in j zaznamujeta količine, ki se nanašajo na magnet in jarem. Jakost magnetnega polja v jarmu je enaka

$$H_j = B_j/(\mu_j \mu_0) \tag{2}$$

Iz Amperovega zakona

$$\oint H\,dl = I \tag{3}$$

v našem primeru sledi

$$H_m l_m + H_j l_j = 0 \tag{4}$$

ker ni tokov (l_m in l_j sta dolžina magneta in srednja dolžina jarma). Približno lahko privzamemo, da sta dolžini l_m in l_j enaki, če pola magneta povežemo tako, da je dolžina jarma čim krajša. Iz enačbe

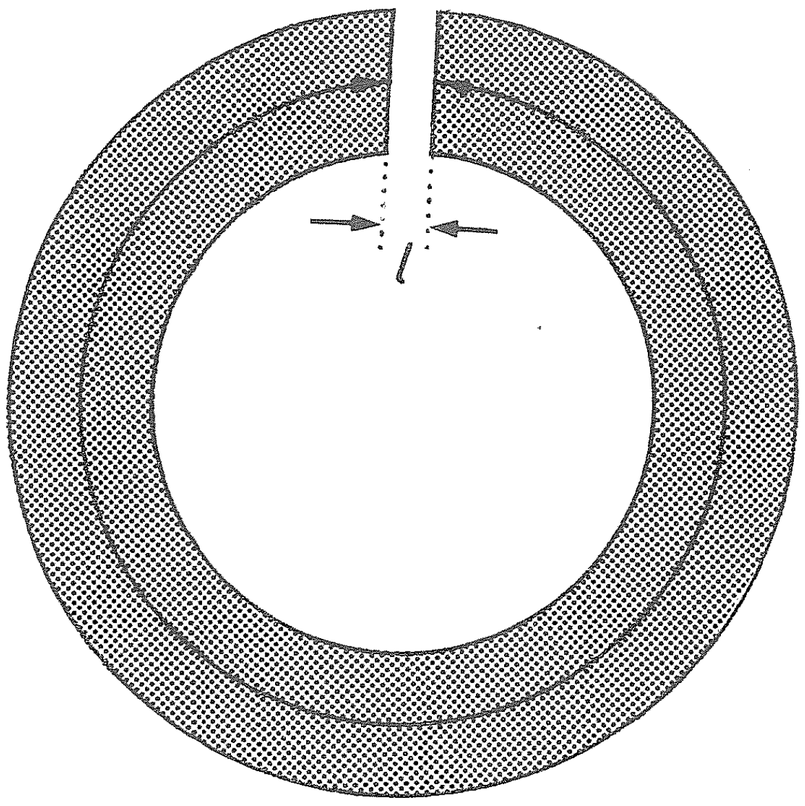
$$B_m - \mu_0 M + B_j/\mu_j = 0 \tag{5}$$

izhaja

$$\mu_0 M = B_m(1 + 1/\mu_z) \approx B_m \tag{6}$$

in $H_m = (B_m - \mu_0 M)/\mu_0$.

Histerezna zanka kaže, da sta gostota magnetnega polja v magnetu in v jármu enaki remanentni gostoti B_r, to je največji gostoti magnetnega polja, ki jo lahko dosežemo v trajnem magnetu (ker je $H_m \approx 0$). Navijmo okrog trajnega magneta žico in poženimo po njej tok tako, da ustvari magnetno polje v nasprotni smeri v jarmu (Sl. 2). Ko je jakost zunanjega magnetnega polja H enaka koercitivni jakosti H_c, pade gostota magnetnega polja v jarmu na nič.



Slika 3: Trajni magnet toroidne oblike z režo.

Trajni magneti delujejo na območju, na katerem je $B > 0$ in $H < 0$ (Sl. 1). Naredimo kratek račun za toroidni magnet (Sl. 3). Vzemimo, da je gostota magnetnega polja zunaj toroida sicer enaka nič, le na mestu reže se silnice razširijo v prostor in zopet poniknejo v magnet. Magnetni pretok v reži je enak kot v magnetu

$$B_g S_g = B_m S_m \tag{7}$$

Indeksa g in m se nanašata na režo in magnet. V reži je $\mu = 1$ in

$$B_g = \mu_0 H_g \tag{8}$$

Amperov zakon (3)

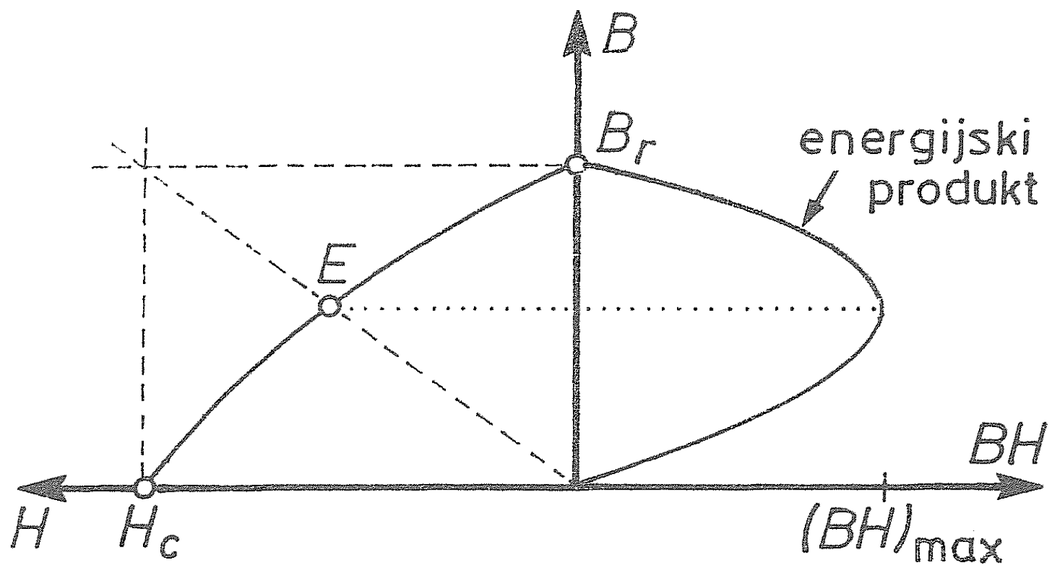
$$\int_{mag} H_m dl = -(1/\mu_0) \int_{reža} B_g dl \tag{9}$$

kaže, da ima jakost magnetnega polja H v magnetu nasprotno smer kot v reži.

Smer jakosti magnetnega polja v trajnem magnetu je nasprotna magnetizaciji in gostoti magnetnega polja v magnetu — magnet deluje nase razmagnetilno. Jakost magnetnega polja in magnetizacijo povezuje demagnetizacijski faktor D

$$H_m = -DM \tag{10}$$

Faktor je odvisen od oblike trajnega magneta in zavzame vrednosti med nič in ena. V tankem ploščatem magnetu je $B_m \approx 0$ in $H_m \approx -M$, tako da je $D \approx 1$. V dolgem magnetu ali v magnetu s sklenjenim jarmom je $H_m \approx 0$ in zato $D \approx 0$. Faktor D se da izračunati za trajni magnet elipsoidne oblike [1],[5] in je za dano smer magnetizacije v tem primeru konstanten. Za drugačne oblike trajnih magnetov je lahko D (in s tem tudi H_m) različen za različne dele magneta. Tedaj lahko izračunamo jakost magnetnega polja le za nekatere preproste primere.



Slika 4: Histerezna zanka in energijski produkt

Gostoto magnetnega polja v magnetu izrazimo z magnetizacijo in s faktorjem D takole: $B_m = \mu_0(1 - D)M$, torej velja $B_g \leq B_m$. Neenakost potrjuje tudi predstavo o obliki magnetnega polja v reži.

Še naprej razmišljajmo o trajnem magnetu. Privzemimo, da je magnetno polje v magnetu in v reži homogeno. Amperov zakon dobi preprostejšo obliko

$$H_g l_g = -H_m l_m \tag{11}$$

Enačbo zmnožimo z enačbo (7) in z 1/2:

$$\frac{1}{2} B_g H_g V_g = -\frac{1}{2} B_m H_m V_m \tag{12}$$

Ker je $H_g = B_g/\mu_0$, velja

$$\frac{1}{2}\mu_0 B_g^2 = -\frac{1}{2} B_m H_m V_m / V_g \tag{13}$$

Energijski produkt trajnega magneta $B_m H_m$ je pomemben podatek pri izbiri magneta. Iz enačbe (13) razberemo, da je gostota magnetnega polja v reži z njim sorazmerna. Material in obliko magneta poskušamo izbrati tako, da je energijski produkt na delovnem območju magneta največji. Stanja na histerezni krivulji in ustrezne energijske produkte za dan magnetni material lahko narišemo na istem grafu (Sl. 4). Največje vrednosti energijskih produktov za določene materiale $(BH)_{max}$ podajamo v tabelah (Tab. 1). Približen račun pokaže, da velja v točki največjega energijskega produkta $B/H = B_g/H_c$. To vrednost energijskega produkta na histerezni zanki lahko določimo grafično (točka E Sl. 4). V kateri točki na grafu bo trajni magnet deloval, je seveda odvisno od faktorja demagnetizacije D, torej od oblike magneta [1].

Posvetimo nekaj vrstic *površinski gostoti magnetnega naboja.* Iz zakona o magnetnem pretoku

$$\oint \mathbf{B} d\mathbf{S} = 0 \tag{14}$$

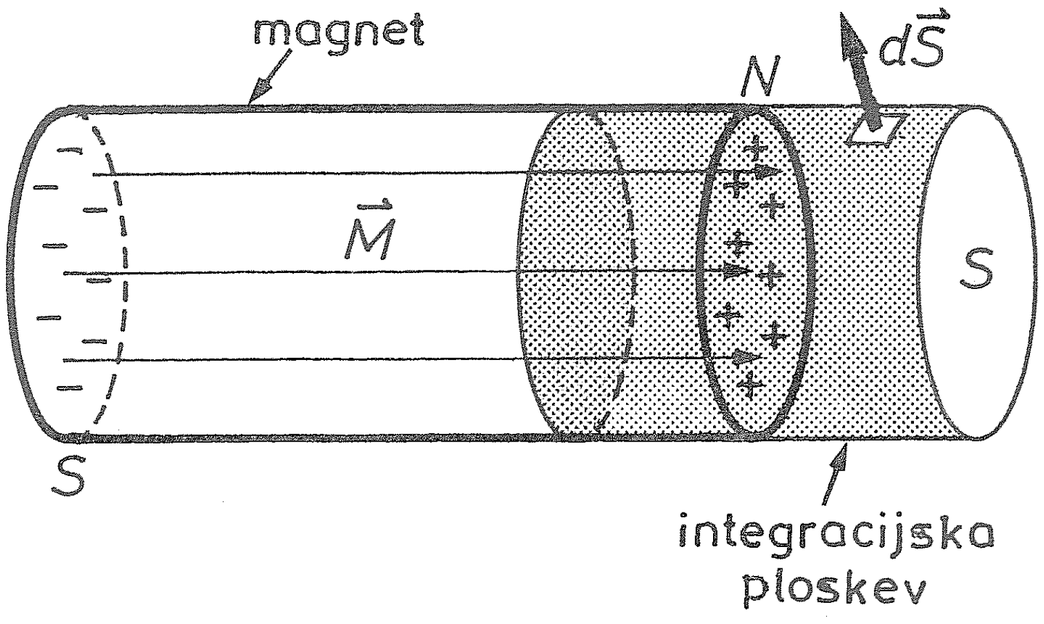
izhaja

$$\oint \mathbf{H} d\mathbf{S} = -\oint \mathbf{M} d\mathbf{S} \tag{15}$$

Enačba

$$\oint \mathbf{H} d\mathbf{S} = 0 \tag{16}$$

velja le v vakuumu ali v izotropni snovi. Na mejnih ploskvah magnetiziranega telesa pa so izviri in ponori jakosti magnetnega polja in magnetizacija doživi skok [4]. Integrala v enačbi (15) sta v splošnem različna od nič, če poteka integracijska ploskev čez meje magnetiziranega telesa.



Slika 5: Porazdelitev magnetnih nabojev na osnovnih ploskvah enakomerno magnetiziranega valja

Namesto da bi snov v magnetnem polju opisali s permeabilnostjo, vpeljimo magnetne naboje q_m. Na ploskvah vzorca ustvarijo ti naboji magnetizacijo, kot ustvari v elektrostatiki polarizacijo površinski vezani naboj na površini dielektrika. Po zgledu Gaussovega zakona za električni pretok zapišemo

$$\oint \mathbf{H} d\mathbf{S} = q_m \tag{17}$$

Magnetni naboj ima enoto Am.

Vzemimo za primer enakomerno magnetiziran valj (Sl. 5) s presekom S. Integral magnetizacije po označeni ploskvi je enak

$$\oint \mathbf{M} d\mathbf{S} = -MS \tag{18}$$

(vektor S kaže iz telesa, ki ga obdaja ploskev). Magnetni naboj na severnem polu magneta je pozitiven, na južnem negativen. Gostoto površinskega magnetnega naboja vpeljemo po vzoru iz elektrostatike:

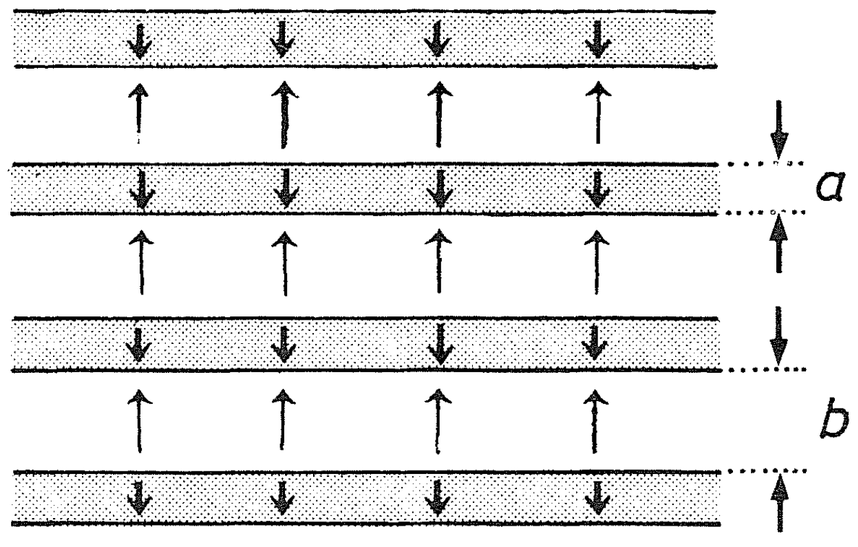
$$\sigma = \mathbf{M} \cdot \mathbf{n} \tag{19}$$

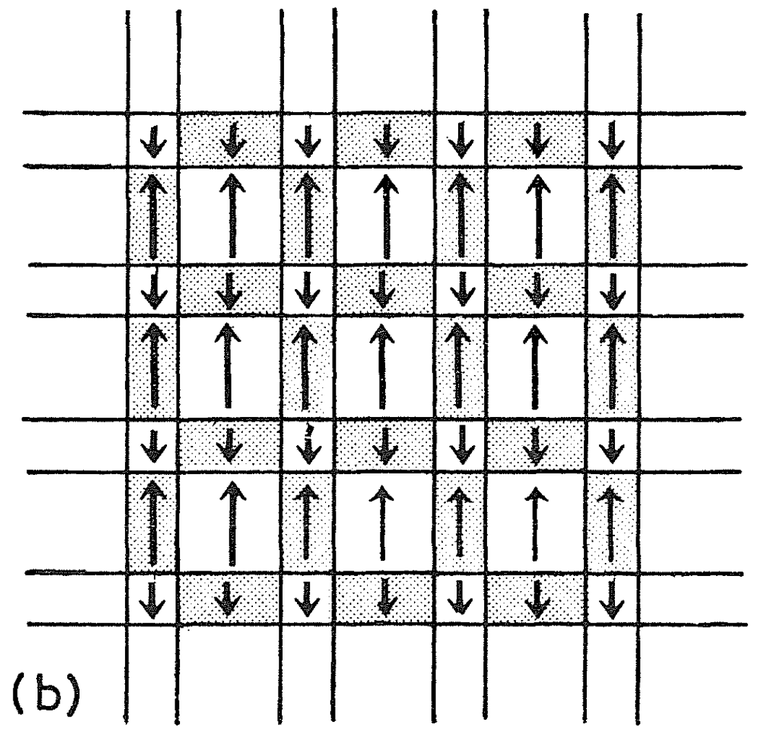
n je enotski vektor v smeri vektorja S. Za valj (Sl. 5) je gostota površinskega naboja na osnovnih ploskvah enaka $+M$ in $-M$, na plašču pa je enaka nič.

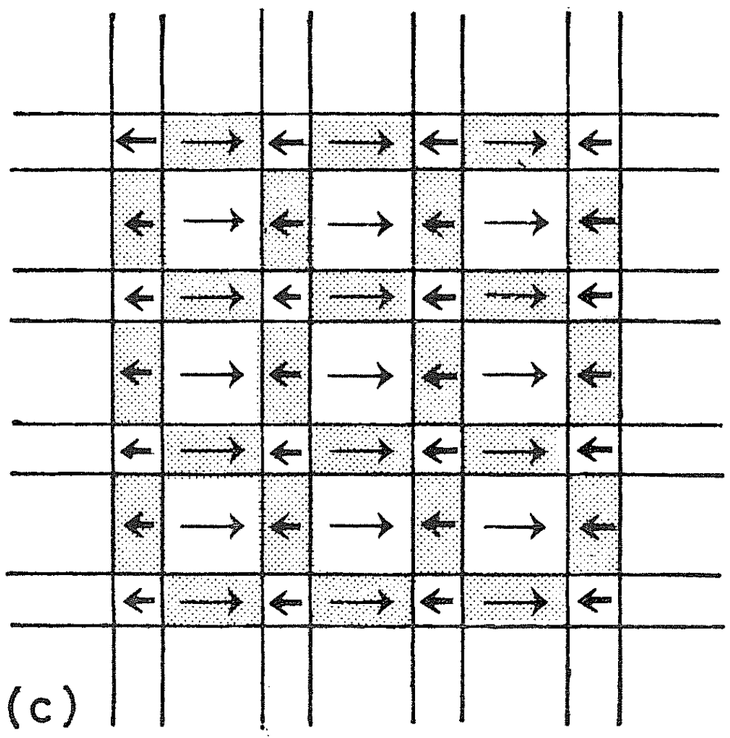
lastnost	alnico 5-7	keramika	Sm_2Co_{17}	NdFeB
B_r	1,35	0,405	1,06	1,12 T
$\mu_0 H_c$	0,074	0,37	0,94	1,06 T
$(BH)_{max}$	59,7	30,56	206,9	238,7 kJ/m^3
ρ	7,31	4,8	8,2	7,4 kg/dm^3
$\mu_0 H_s$	0,35	1,4	> 4	> 3 T

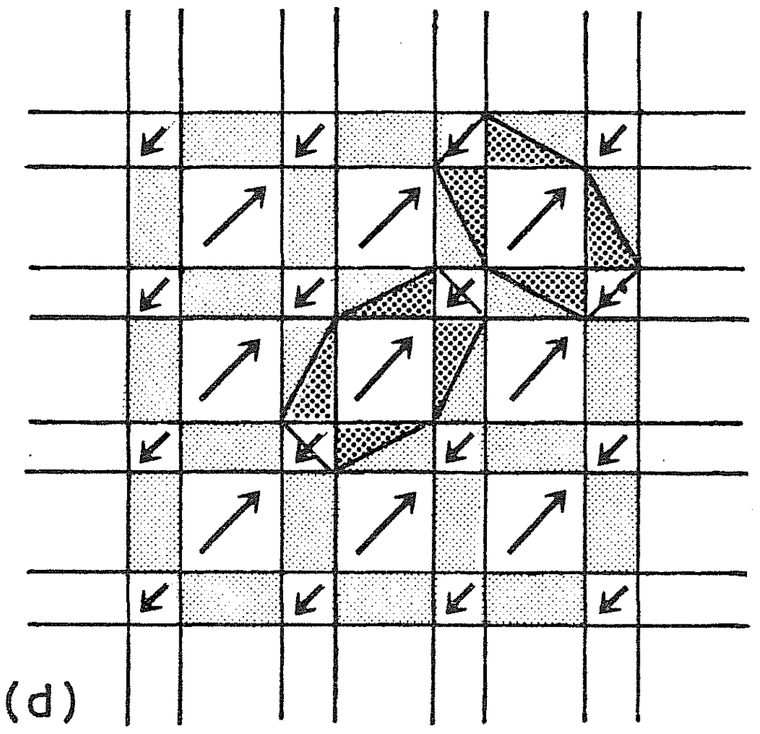
Tabela 1: Lastnosti nekaterih magnetnih materialov (ρ gostota snovi, H_s magnetna poljska jakost nasičenja) [3]

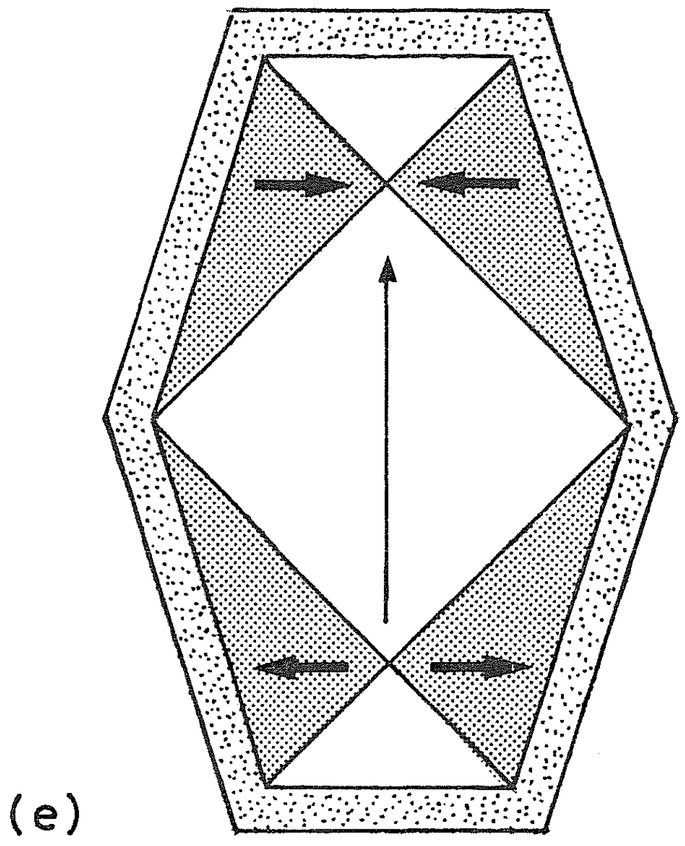
O magnetnih materialih povejmo le nekaj besed. Delimo jih na *trde* (keramike, redke zemlje z dodatkom kobalta, NdFeB) in *mehke* (alnico). Demagnetizacijska krivulja prvih je premica s smernim koeficientom med $1.0\mu_0$ in $1,1\mu_0$. Ta linearni model je posebej uporaben za numerično računanje lastnosti trajnih magnetov. Demagnetizacijska krivulja drugih ima koleno.

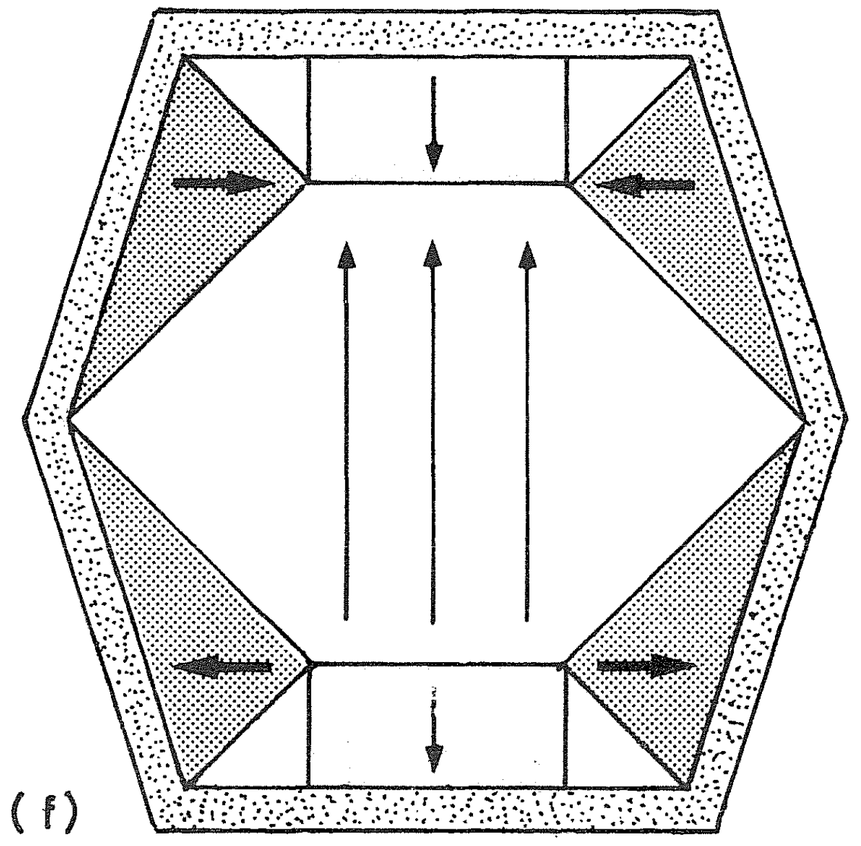












Slika 6: Razvoj trajnega magneta prizmatične oblike. Vektorji $\mathbf{H}_m$ so risani z debelejšo, vektorji $\mathbf{H}_g$ pa s tanjšo črto

Oblika magneta vpliva na lastnosti pri mehkih magnetih precej bolj kot pri trdih magnetih.

2. Uporaba trajnih magnetov pri slikanju z magnetno resonanco

Tomografija na magnetno resonanco se je uveljavila v sodobni medicini predvsem kot dopolnilna tehnika slikanja različnih mehkih tkiv in ožilja [6].

Pri tem potrebujemo na opazovanem mestu magnetno polje z nehomogenostjo, manjšo od 100 ppm. Izviri magnetnega polja so tuljave z uporom (navitja), supraprevodne tuljave, zemeljsko magnetno polje ali trajni magneti. Zadnji imajo cilindrično ali prizmatično geometrijo. Poglejmo podrobneje druge.

Magnetno polje med neskončnima, vzporednima, namagnetenima ploščama je homogeno. Kako pa dobimo sistem s homogenim magnetnim poljem, v obliki neskončno visoke prizme [2]? Vzemimo nešteto vzporednih, namagnetenih plošč z debelino a, ki so med seboj razmaknjene za b (Sl. 6a). Jakost in gostota magnetnega polja znotraj in zunaj magnetnih plošč sta homogeni. Jakost magnetnega polja v magnetu H_m kaže v nasprotno smer kot jakost magnetnega polja H_g zunaj magneta.

Mislimo si, da so magnetne plošče razporejene kot lopatice na mlinskem kolesu z neskončnim radijem. Ker ni tokov, je integral po sklenjeni krivulji, to je po obodu "mlinskega kolesa", pravokotni na plošče,

$$aH_m + bH_g = 0 \tag{20}$$

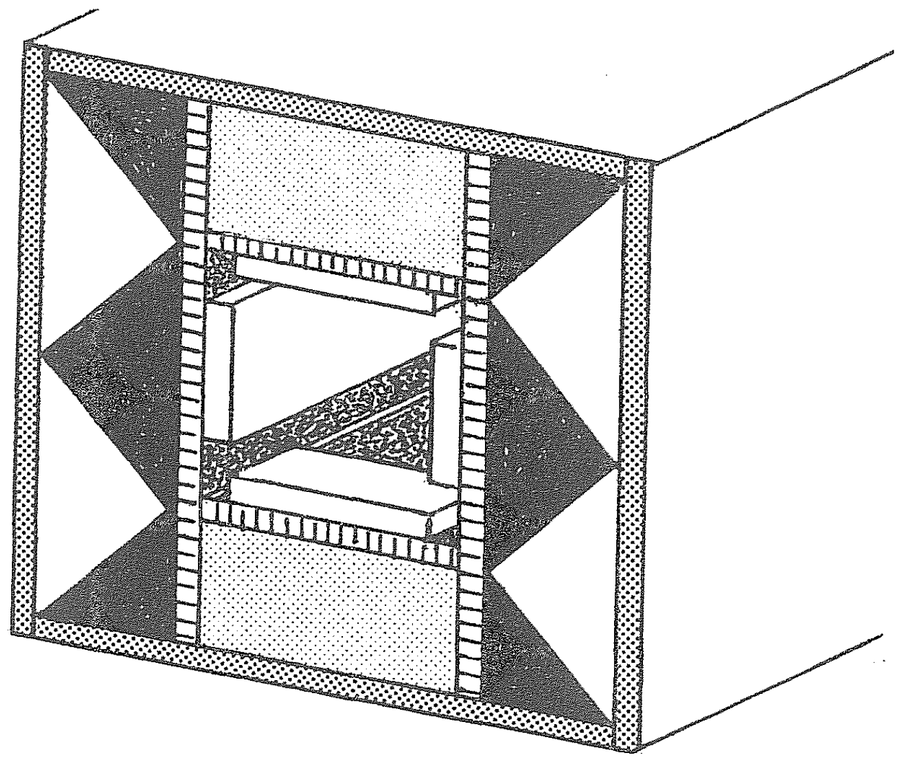
enak nič. Magnetni pretok je povsod enak, zato je $B_m = B_g$. Znotraj magnetov velja zveza $B = \mu_0 H_m + \mu_0 M$, v plasteh med njimi pa $B = \mu_0 H_g$. Hitro izpeljemo izraza za jakost magnetnega polja v reži

$$H_g = (M/\mu_0)(a/(a+b)) \tag{21}$$

in v magnetu

$$H_m = (M/\mu_0)(-b/(a+b)) \tag{22}$$

Razporedimo magnete v šahovnico (Sl. 6b). Sistem je neskončen v smeri pravokotno na ravnino slike. Magnetizacija M naj bo enaka kot v prejšnem primeru. Gostota površinskega naboja na vodoravnih ploskvah (črte na sl. 6b) je enaka kot gostota površinskega naboja na ploskvah magnetnih plasti (Sl. 6a). Jakost magnetnega polja v prostoru med magneti je torej v prvem in v drugem primeru homogena, njeno velikost določa izraz (21).



Slika 8: Magnetni sistem z dodatnimi elementi za izboljšanje homogenosti magnetnega polja

Sestavimo opisani magnetni sistem (Sl. 6b) in enak sistem, zasukan za pravi kot (Sl. 6c). V nastalih magnetnih poljih (Sl. 6d) so velikosti vektorjev jakosti magnetnega polja za $\sqrt{2}$-krat večje kot prej. Iz sestavljenega magnetnega polja lahko izrežemo več različnih osnovnih celic. Mnogokotnik je osnovna celica, če lahko s takšnimi mnogokotniki pokrijemo celotno sliko (Sl. 6d). Vzemimo eno od osnovnih celic in jo obdajmo z oklepom iz feromagnetne

snovi z veliko permeabilnostjo. Gostota magnetnega polja se pri prehodu v feromagnetno snov praktično ne spremeni, zato so razmere enake kot na mestu osnovne celice (Sl. 6d). Tako smo dobili sistem s homogenim magnetnim poljem na sredini pri pogoju, da so magneti homogeno magnetizirani. Majhni trikotni *parazitski reži* znižujeta magnetno energijo (Sl. 6e), igrata pa pomembno vlogo pri homogenizaciji polja.

Delovno območje homogenega polja povečamo s trajnima magnetoma s pravokotnim presekom, ki ju vložimo v omenjeni sistem (Sl. 6f). Gostote površinskih nabojev na stičiščih morajo biti enake. Doslej smo opisali razvoj magneta prizmatične oblike. Z izbiro drugačne osnovne celice ali šahovnice (Sl. 6b) sestavljene iz romboidov, dobimo nove oblike prizmatičnih magnetnih sistemov (Sl. 7 je na prvi strani ovitka). Magnetni sistem, ki smo ga na koncu dobili, je neskončen v smeri pravokotno na ravnino slike in zato še vedno praktično ni uporaben. Odločimo se za sistem z enakim presekom in končno dolžino. Popačitve, ki jih prinese končna dolžina, pa odpravimo z dodatnimi elementi iz feromagnetnih snovi.

Nehomogenost magnetnega polja nastane zaradi končne dolžine magnetnega sistema in nehomogenosti magnetizacije trajnih magnetov. V magnetnem sistemu s končno dolžino dodatni elementi popravijo homogenost polja na delovnem območju. Navpični steni delovnega območja pokrivata plošči, ki ju sestavljajo železni lističi, ločeni med seboj z lističi iz nemagnetnega materiala. Takšna plošča ima veliko permeabilnost v smeri lističev in majhno v prečni smeri. Plošči izenačita lokalne razlike v lastnostih trajnih magnetov in poskrbita, da sta pola vloženih trajnih magnetov ekvipotencialni ploskvi. Magnetno polje na delovnem območju zmanjšata približno za tretjino. Na zunanjih robovih vloženih trajnih magnetov dodamo feritne palice, namagnetene v isti smeri kot magneta. Palice preprečujejo zmanjševanje magnetnega polja proti odprtinama. Morebitne dodatne nehomogenosti v smeri prečno na os sistema uravnovešata podobni palici na notranjih stranicah delovnega območja. Palici sta magnetizirani v nasprotni smeri od smeri glavnega magnetnega polja. Plasti, ki prekrivata pola vloženih magnetov, izenačujeta lokalne razlike v lastnostih materialov. Sestavljajo ju vzporedni lističi, čeprav glede na to, da sta pola ekvipotencialni ploskvi, to ne bi bilo potrebno. S takšno zgradbo zmanjšamo inducirane tokove pri vklapljanju in izklapljanju gradientnih tuljav v tomografu.

LITERATURA

[1] D. Hadfield, *Permanent Magnets and Magnetism* J. Willey and Sons, New York 1963.
[2] H. Zijlstra, *Permanent Magnet System for NMR Tomography,* Philips J. Res., **40** (1985) 259–288.
[3] T. J. E. Miller, *Brushless Permanent-Magnet and Reluctance Motor Drivers,* Clarendon Press, Oxford 1989.
[4] A. F. Kip, *Electricity and Magnetism,* Mc-Graw Hill, (1969).
[5] D. J. Craik, *Structure and Properties of Magnetic Materials,* Pion Limited, London 1971.
[6] J. Stepišnik, *Slikanje z jedrsko magnetno resonanco v medicini,* Obzornik mat. fiz., **34** (1987) 9–17.

VESTI

42. OBČNI ZBOR DRUŠTVA MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE

Pri letošnjem občnem zboru smo napravili prijetno spremembo: podaljšali smo ga za en dan v korist delovnega programa.

V četrtek, 11. oktobra, je bil astronomski dan. Črni vrh nad Idrijo smo za kraj občnega zbora izbrali iz dveh razlogov: zaradi 500-letnice mesta Idrije in zaradi bližine slovenskega ljudskega observatorija na Javorniku. Sodelovali so astronomi iz Ljubljane pod vodstvom dr. Andreja Čadeža in člani Astronomskega društva Javornik. Seznanili so nas z organizacijo astronomske noči za učence. Pri tem ima Astronomsko društvo Javornik bogate izkušnje, saj je za letos organiziralo mednarodni tabor iz astronomije za srednješolce. Po večerji smo astronomsko noč tudi praktično preskusili. Razdelili smo se na dve skupini: prva je opazovala nebo na observatoriju Javornik, druga pa na observatoriju Hermana Mikuža, prvenstveno namenjenem za fotografiranje neba. Vreme je bilo kot naročeno za opazovanje, v čistem in neosvetljenem ozračju je bil že pogled na nebo enkratno doživetje. Še več lepote je pričaral pogled skoz daljnogled. Opazovali smo zvezdne kopice, meglice, planete, najbolj vneti opazovalci so vztrajali do Luninega vzhoda. Zaradi velikega zanimanja smo astronomsko noč ponovili še v petek.

V petek, 12. oktobra, smo se udeleženci občnega zbora razdelili na dva dela. Matematiki so poslušali štiri predavanja iz uporabne matematike — dr. Marko Petkovšek, *Program za simbolično računanje*, dr. Bojan Magajna, *Uporaba končnih obsegov*, dr. Peter Petek, *Kaos ni nered*, dr. Vladimir Batagelj, *Večkriterijski optimizacijski problemi.* Udeležencev je bilo približno 40, kar kaže, da je delo sekcije za uporabno matematiko prav zelo potrebno.

Tudi pri fiziki je bilo lepo število udeležencev: 70. *Projekt prenove pouka fizike v srednji šoli* je predstavil Fedor Tomažič. Delovna skupina za prenovo pouka fizike je pod vodstvom Nade Razpet pripravila razstavo učil, ki so jih učitelji razvili v okviru projekta. Učila so razstavljali: Stane Kodba *optični mikrometer, daljinomer, ki deluje na osnovi paralakse, merilnik naboja* in *pripravo za merjenje površinske napetosti.* Andrej Kuhar *zračno drčo*; *računalniške programe za poskuse na zračni drči* je pripravil Vincenc Petruna. Aktiv fizikov iz Velenja je pokazal *tehtnico na upogib in torzijsko tehtnico, vmesnik za IBM PC-združljive računalnike* pa Silvo Kocjančič. Seta Oblak je predstavila *uvajanje nacionalnega programa pouka fizike v Angliji.* Razstavili so tudi nova gradiva iz fizike za srednjo šolo in tujo literaturo.

Dr. Marko Valič je skušal prikazati *delo fizikov v Elektrooptiki.* Za razstavo je prinesel laserski stimulator, laserski označevalec, Šolski He-Ne laser, prospekt za oftalmološki laser MOL 01 in univerzalno namizno hobi stružnico. Boris Kham je poskrbel za razstavo posterjev, s katerimi so srednješolci prikazali svoje raziskovalne naloge iz astronomije letošnjega maja v Angliji.

Komisija za tisk je razstavila letošnje publikacije. Izdala je 35 publikacij, všteti so tudi ponatisi, ki so pogosti zlasti pri učbeniikih in priročnikih. V letošnjem letu je izdala publikacijo z zaporedno številko 1000.

Strokovni del v petek smo zaključili z dvema predavanjema. Janez Kavčič je imel zelo zanimivo predavanje *O pomenu Idrije pri razvoju slovenske znanosti in tehnike.* Predavanje je popestril z vzorci rud, rudarskega orodja, s knjigami, ki so jih napisali idrijski znanstveniki. Marijan Prosén pa je na kratko poročal o *slovenskem matematiku, astronomu in zdravniku Andreju Perlahu*, ki se je rodil pred petsto leti.

V soboto, 13. oktobra je občni zbor potekal po ustaljenem redu. V imenu Krajevne skupnosti Črni vrh ga je pozdravil Benedikt Bajec, v imenu občine Idrija pa njen predsednik dr. Janez Podobnik. Občni zbor so pozdravili dr. Peter Petek v imenu IMFM, dr. Mitja Rosina v imenu IJS, dr. Milan Hladnik v imenu oddelka za matematiko in mehaniko in dr. Janez Strnad v imenu oddelka za fiziko. Spomnili smo se v zadnjem letu umrlih članov, med njimi Marije Pilgram in Franca Bezjaka.

Društvena priznanja za popularizacijo matematike, fizike, astronomije in računalništva so prejeli: **dr. Izidor Hafner**, profesor matematike na Fakulteti za elektrotehniko in računalništvo v Ljubljani, za pobudo in sodelovanje pri izdaji knjig iz logike, za sodelovanje pri matematičnih učbenikih za osnovne šole in za organizacijo tekmovanj iz logike. **Anton Podvršnik**, profesor matematike na gimnaziji v Kopru, je dobil priznanje za požrtvovalno pedagoško delo pri matematiki, **Nika Šilc**, profesorica matematike na gimnaziji v Celju, za zavzeto in zagnano delo z mladimi. **Gimnazija Idrija** je dobila priznanje za dolgoletno načrtno in živahno delo na področju matematike in fizike.

Poročila o delu društva so tudi letos zbrana v biltenu. Še vselej smo uspešno izpeljali vsa matematična in fizikalna tekmovanja v osnovni in srednji šoli, se udeležili zveznih tekmovanj. Za najboljše tekmovalce smo tudi letos organizirali matematično in fizikalno poletno šolo in raziskovalne dneve iz matematike in fizike za srednješolce.

Komisija za pedagoško dejavnost je za učitelje matematike organizirala 4 predavanja, prav toliko za učitelje fizike. Dvodnevni društveni seminar o grafih v februarju je strokovno vodil dr. Vladimir Batagelj. Na obeh oddelkih za matematiko in za fiziko poteka permanentno izobraževanje za učitelje obeh strok.

Tudi podružnice kažejo pestro dejavnost. Poleg priprav in izvedb tekmovanj iz matematike, fizike in logike za osnovno in srednjo šolo so organizirale predavanje za člane. V Mariboru je bilo teh predavanj 10, v Kopru 6, v Celju 2.

9. kongres Zveze društev matematikov, fizikov in astronomov Jugoslavije, ki bi moral biti v septembru v Ljubljani, smo preložili. Vzrokov je več: premalo prijav, nezadostna finančna sredstva, nezainteresiranost nekaterih republiških društev za kongres.

Po razpravi o poročilih smo sprejeli naslednje sklepe: na vse dejavnosti društva v okviru dela z mladimi, kot so tekmovanja, poletne šole in tabori, je

treba vabiti tudi učence in učitelje iz naših zamejskih šol. Za te dejavnosti je treba pripraviti ustrezne diplome, potrdila. Poiskati je treba ime za fizikalna tekmovanja osnovnošolcev in srednješolcev, podobno kot so Vegova priznanja. Društvo naj aktivno sodeluje pri oblikovanju kriterijev za napredovanje učiteljev. Upravni odbor naj pregleda tisti del verifikacijskega postopka za ustanavljanje šol, ki se tiče dejavnosti društva. Prav tako naj prouči in določi pogoje za organiziranje aktivnosti iz dejavnosti društva. Druge naloge upravnega odbora so: ustanovi naj posebno skupino članov društva, ki bo skrbela za informiranje ožje strokovne in širše javnosti o aktivnostih društva; prouči naj možnost za čimbolj ugoden nakup računalniške in tudi matematične, fizikalne in astronomske opreme za člane društva; koordinira naj aktivnosti pri pripravah strokovnih srečanj, ki so načrtovani v prihodnjih letih, in naj določi višino članarine za člane iz tujine. Statutarna komisija iz treh članov naj do naslednjega občnega zbora uskladi statut društva s spremenjenimi družbenimi razmerami.

Posebna točka je bila sprememba imena društva, ki se sedaj imenuje **Društvo matematikov, fizikov in astronomov Slovenije**.

Po poročilu nadzornega odbora in po razrešnici staremu odboru smo izvolili novi odbor. V upravnem odboru so: predsednik Peter Petek, podpredsednica Martina Koman, tajnica Maja Bleiweis, blagajničarka Helena Velikonja; sekretarji komisij so: za pedagoško dejavnost Milena Strnad, za uporabno matematiko Marko Razpet, za uporabno fiziko Dušan Brajnik. Komisija za popularizacijo matematike in fizike ima sekretarje: Aleksander Potočnik — matematika OŠ in poletna šola iz matematike, Franci Prijatelj — fizika OŠ, Rubin Belina — fizika 1. letnik SŠ, Darjo Felda — matematika SŠ in raziskovalni dnevi iz matematike, Iztok Kukman — fizika SŠ, Boris Kham — astronomija, Branko Borštnik — vodja raziskovalnih dni za fiziko, Nada Razpet — poletna šola iz fizike, Blaža Cedilnik — predavanja učencem, Izidor Hafner — razvedrilna matematika.

V upravnem odboru Komisije za tisk so: predsednik in glavni urednik Marko Petkovšek, tajnik in urednik Ciril Velkovrh, blagajnik Janez Markelj, odgovorni uredniki: Obzornik za matematiko in fiziko — Milan Hladnik, Presek — Boris Lavrič, Presekova knjižnica — Edvard Kramar, učbeniki in priročniki — Ciril Velkovrh, Knjižnica Sigma ter Izbrana poglavja iz matematike in računalništva — Ivan Vidav, Izbrana poglavja iz fizike — Janez Strnad. Za zbirko Matematika-Fizika in Postdiplomski seminar iz matematike je bil kasneje imenovan Bojan Magajna.

V nadzornem odboru so Ivan Kuščer, Darka Hvastija, Pavle Zajc, v častnem razsodišču pa Ivan Vidav, Peter Gosar, Dušan Modic.

Občni zbor smo v soboto popoldne zaključili z ogledom Idrije, zlasti njenega muzeja, pod vodstvom Janeza Kavčiča. Zanimive so bile makete o nekdanjem in sodobnem pridobivanju živega srebra, o klavžah, prav tako veliko vodno kolo — idrijska kamšt — v originalu. Najbolj vneti so končali tudi najbolj optimistično v gostilni Nebesa.

Martina Koman

IZ SREDNJE ŠOLE PRED STO LETI

Nedavno sem dobil v roke letno poročilo gimnazije v Gorici iz leta 1876 in nekaj letnih poročil gimnazije v Ljubljani iz časa med leti 1879 in 1899. Pri prelistavanju sem opazil nekaj podrobnosti, ki bodo morda zanimale tudi bralce Obzornika.

V Gorici je bilo od 295 dijakov 124 Slovencev, v Ljubljani pa l. 1879 od 509 dijakov kar 376 Slovencev. Po priimkih profesorjev sodeč, je bila v Gorici skoraj polovica profesorjev slovenskega rodu, v Ljubljani pa so bili v večini. V goriškem letnem poročilu so bili objavljeni pogoji za vpis v nemškem, italijanskem in slovenskem jeziku. Skoraj polovico letnega poročila je zavzemal članek *O določevanju časa, poldnevnika in zemljepisne širjave po solnčnih opazovanjih.* Članek je v slovenščini.

Učni jezik je bil nemški razen v nižjih razredih, v katerih so prevladovali slovenski učenci. Pouk slovenščine je bil v vseh razredih obvezen, prav tako je bila slovenščina maturitetni predmet. Slovenščine je bilo 2–3 ure tedensko, nemščine 3–4, matematike 3 ure. Največ je bilo latinščine, celo do 10 ur tedensko.

Najbolj zanimiva so naslednja dejstva.

V nobenem razredu od 1. do 8. ni bilo več kot 9 predmetov letno, vključno z veronaukom.

Število tedenskih ur obveznih predmetov je bilo od 24 do največ 28. Ker je bil delovni teden 6-dneven, pomeni, da so imeli dijaki 4–5 ur pouka dnevno.

Kreatorjem nove srednje šole priporočam, da o teh podatkih resno razmislijo. Zmožnost sprejemanja in učenja dijakov se v zadnjih sto letih gotovo ni kaj prida, če sploh, povečala.

Anton Suhadolc

OBVESTILO

ČLANOM DRUŠTVA

V letošnjem letu je članarina za Društvo matematikov, fizikov in astronomov Slovenije 200,00 din. Člani bodo prejemali društveno glasilo Obzornik za matematiko in fiziko brezplačno. Prosimo pa, da nam članarino nakažete čimprej. Višino članarine bomo v kasnejših mesecih morali spreminjati v skladu z inflacijo. Na priloženi položnici ne pozabite vpisati svojega popolnega naslova.

Milan Hladnik, Janez Strnad, Ciril Velkovrh

NOVE KNJIGE

RIBARIČ, M., ŠUŠTERŠIČ, L., Conservation laws and open questions of classical electrodynamics, World Scientific, Singapore 1990, 333 str.

Obzornik je doslej le malokrat imel priložnost poročati o knjigah, ki so jih izdali domači matematiki ali fiziki v tujini. Ribaričeva in Šušteršičeva knjiga *Ohranitveni zakoni in odprta vprašanja v klasični elektrodinamiki* sodi med take knjige.

Knjiga ima dva dela. Prvi je posvečen ohranitvenim zakonom klasične elektrodinamike in vsebuje osem poglavij: Osnovne enačbe klasične elektrodinamike, Ohranitveni zakoni za zvezni elektromehanični sistem, Elektrodinamična stacionarna stanja, Formulacije, ki so kovariantne po Lorentzu, Elektromagnetno sevanje, Energija, gibalna količina in vrtilna količina, ki jo izseva naelektreni mehanični sistem, Primerjava lastnosti Maxwellove in elektrodinamične gostote energije, gibalne količine in vrtilne količine in njihovih tokov in Fizikalni pomen retardiranih potencialov v Lorentzovi umeritvi. Tri poglavja drugega dela obravnavajo klasična naelektrena točkasta telesa: Točkasti naboj, Gibanje klasičnih točkastih teles v zunanjih poljih, Asimptotični tiri klasičnih naelektrenih točkastih teles v odzivu na šibko in počasi se spreminjajočo zunanjo silo. Epilogu, ki pogleda na fizikalne teorije z nekoliko širšega gledišča, sledi več dodatkov, predvsem z definicijami količin in nekaterimi izpeljavami.

Knjiga sodi na območje, ki ga navadno imenujemo *raziskovanje osnov*. S težavnimi vprašanji te vrste se ne ukvarja veliko fizikov, ker delo velja večinoma za nehvaležno. Ni veliko upanja, da bi uspešno, že dobro stoletje veljavno Maxwellovo klasično elektrodinamiko vrgli s prestola ali bistveno preoblikovali. Početje ima vendar smisel, ker opozarja na to, da veliko fizikov odrine v podzavest pomanjkljivosti teorije, ki se razkrijejo tudi, ko jo hočemo dosledno prilagoditi kvantnemu pogledu. Kaže, da sta si Ribarič in Šušteršič predvsem prizadevala sistematično našteti in razčleniti pomanjkljivosti, kar jima je dobro uspelo. Fiziki, ki se bodo ukvarjali z osnovami klasične elektrodinamike, ne bodo mogli mimo njune knjige.

V uvodu sta naštela glavne skupine nerešenih vprašanj. Ali naj damo prednost opisu z jakostjo električnega in gostoto magnetnega polja ali opisu s skalarnim in vektorskim potencialom? Kje je sedež energije in gibalne in vrtilne količine, ko delujejo naelektrena telesa in vodniki s tokom drug na drugega? Ali je vrtilna količina sevanja lokalna lastnost kot energija ali izhaja iz robnega pogoja, kot bi sklepali po Maxwellovem napetostnem tenzorju? Kako naj vpeljemo energijo in gibalno in vrtilno količino sevanja, ne da bi se odločili za to ali drugo obliko napetostnega tenzorja? Ali obstaja klasična enačba gibanja za točkasti naboj, ki vključuje nasprotno silo sevanja in ne nasprotuje kavzalnosti in ne skriva singularnosti? Ali je torej točkaste naboje mogoče zares vgraditi v klasično elektrodinamiko ali je bolje v njih videti le pripravno računsko pomagalo? Čeprav ta vprašanja ne omejujejo

uporabnosti elektrodinamike in se jih veliko učbenikov komaj dotakne ali gre celo mimo njih, se jih je koristno zavedati. Le tako lahko vidimo klasično elektrodinamiko v pravi luči kot usklajeno in na določenem območju uspešno, a vendar ne dokončno teorijo. Tak trezni pogled je vredno večkrat poudariti kot protistrup misli, da pozna fizika odgovore na vsa vprašanja.

Janez Strnad

ATIYAH M. in drugi (uredniki), Physics and mathematics of strings, The royal society, London 1989, 96 str.

Konec predlanskega leta je Kraljeva družba, ki ima vlogo angleške akademije znanosti, v Londonu priredila znanstveni sestanek o teoriji strun. Udeležili so se ga številni znani matematiki in fiziki, ki delajo v teoriji strun in na sorodnih območjih. Teorija zajame kvantno gravitacijo, kot je ni nobena druga teorija doslej. Postavlja globoka matematična vprašanja in je povezana s teorijo faznih prehodov. Razprava je segala od razmišljanj o prostoru in času do poskusov, da bi pojasnili standardni model osnovnih delcev. Matematiki so razpravljali o tem, kakšno orodje potrebujejo fiziki, ti pa so ga poskušali uporabiti.

Knjiga je zbornik s tega sestanka, pravzaprav ponatis v velikem formatu člankov iz *Proceedings of the Royal Society.* Vsebuje prispevke: D. I. Olive, *Uvod v teorijo strun: zgradba in vprašanja*, P. Goddard, *Umeritvena simetrija in teorija strun*, J. H. Schwarz, *Iskanje realističnega superstrunskega vakuma*, G. G. Ros, *Fizika supersimetrij (pri nizki energiji)*, A. Strominger, *Tretja kvantizacija* in D. J. Gross, *Strune pri energiji nad Planckovo: iskanje simetrije strun.* Zbornik bo prišel prav vsem tistim, ki se ukvarjajo s teorijo strun, kolikor si niso pomagali že prej s prednatisi ali z revijo.

Janez Strnad

POPRAVKI

V članku Davida J. Grossa *Fizika in matematika na meji* v zadnji lanski številki Obzornika za matematiko in fiziko je prišlo do neprijetnih tiskovnih napak, za katere se bralcem opravičujemo in jih prosimo, da jih popravijo:

na str. 178 v peti vrstici z dna mora biti od sedmega do devetega mesta za decimalno vejico 652 (ne 625).

na str. 179 v četrti vrsti z dna mora biti prvi oklepaj na začetku enačbe:

$$(A^{\alpha\gamma}A^{\beta\delta} + \mathrm{Tr}\, B^{\alpha\gamma}B^{\beta\delta} + \mathrm{Tr}\, C^{\alpha\gamma}C^{\beta\delta}),$$

na str. 182 v drugi vrstici za enačbo mora biti: osemnajst (ne osem) velikostnih stopenj.

Janez Strnad

PUBLIKACIJE DMFA SLOVENIJE, IMFM ter FNT — oddelka za matematiko in mehaniko ter oddelka za fiziko v letu 1990

1.–6. **Obzornik za matematiko in fiziko 37** (1990) številke 1, 2, 3, 4, 5, 6 (992, 1010, 1016, 1025, 1026, 1034). V četrti številki so bila objavljena predavanja na društvenem seminarju iz matematike z naslovom *Izbrane teme iz teorije grafov.*

7.–12. **Presek** — list za mlade matematike, fizike, astronome in računalnikarje **17** (1989/90) številke 4, 5, 6; **18** (1990/91) številke 1, 2, 3 (996, 1001, 1056, 1023, 1032, 1036)

Presekova knjižnica

13. **30.** Plevnik F., Bradač Z., Cvahte M., Naloge s tekmovanj iz fizike v osnovni šoli, 1. del, 1982–1988 (2. natis) (1027)
14. **33.** Ranzinger P, Hržič M., Vidrih R., Cecić I., Naše nebo in Zemlja 1991. Astronomske efemeride. Umetni sateliti. Potresi. (1041)

Učbeniki in priročniki

15. Uršič S., Matematične tabele in formule (2. natis) (1003)

Štalec I. in dr., Zbirke vaj iz aritmetike, algebre in analize za

16. 1. razred srednjih šol (13. natis) (1011)
17. 2. ——— " ——— (12. natis) (1012)
18. 3. ——— " ——— (10. natis) (1013)
19. 4. ——— " ——— (8. natis) (1014)
20. Vadnal A., Matematika. Mali leksikon CZ (3. natis) (995)
21. Batagelj V., Golli B., TEX. Povabilo v TEX, LATEX, BIBTEX, PICTEX (1029)
22. Programski paket TEX (z 18 disketami) (1038))

Račkova knjižnica

23. **1.** Klavžar S., Mali priročnik operacijskega sistema MS DOS (2. natis) (1008)

24.–25. **2.** Lokar M., Turbo pascal (1. in 2. natis) (994, 1035)

Knjižnica Sigma

26. **15.** Prijatelj N., Matematične strukture II (4. natis) (997)
27. **47.** Sadovski L. E., Sadovski A. L., Matematika in šport (prevedel B. Hvala) (1020)
28. **48.** Virčenko N. A., Matematika v aforizmih, citatih in izrekih (prevedel D. Pagon) (1033)

Matematični rokopisi

29. **18.** Vrabec J., Tri teme iz teorije vrst (1018)
30. **19.** Suhadolc A., Robni problemi za linearne diferencialne enačbe drugega reda (1019)

Izbrana poglavja iz matematike in računalništva

31. **20.** Dobovišek M., Kobal D., Magajna B., Naloge iz algebre I (4. razširjena in popravljena izdaja) (999)
32. **24.** Kramar E., Rešene naloge iz linearne algebre (2. natis) (1031)

Zbirka izbranih poglavij iz fizike

33. **17.** Ahlin F. in dr., Fizikalni praktikum I (5. natis) (1037)

Matematika–Fizika — Zbirka univerzitetnih učbenikov in monografij

34. **6.** Vidav I., Višja matematika I (10. natis) (1004)
35. **9.** Strnad J., Fizika, 1. del, Mehanika. Toplota (6. natis) (1040)
36. **16.** Jamnik R., Matematika (4. natis) (1007)
37. **23.** Grasselli J., Linearna Algebra
    Vadnal A., Linearno programiranje (2. natis) (1006)
38. **25.** Krušič B., Dvojni in mnogoterni integral. Vidav I., Diferencialna geometrija v prostoru. Vencelj M., Vektorska analiza (2. natis) (1039)
39. **31.** Vrabec J., Metrični prostori (1000)

Inštitut za matematiko, fiziko in mehaniko

40. **30.** Poročilo za leto 1989 (998)
41. **27.** Preprint series of the department of mathematics 1989 (993)
42. **28.** ——————— " ——————— (separati) 1990 (1015)

Seminar za računalniško matematiko

43. **547.** Sraka R., Optični računalniki (1021)
44. **549.** Dacar F., Sistemi dinamičnih neenačb (1022)

Društvo matematikov, fizikov in astronomov Slovenije

45. **42.** občni zbor (1030)

Tekmovanja

46. **34.** republiško tekmovanje srednješolcev iz matematike, Idrija (1002)
47. **10.** republiško tekmovanje iz fizike za osnovnošolce, Maribor (1024)
48. **9.** področno tekmovanje fizikov, Koper (1009)
49. **26.** republiško tekmovanje osnovnošolcev iz matematike, Postojna (1017)

Na koncu naslovov so v oklepajih vpisane zaporedne številke izdaj Komisije za tisk DMFAS od leta 1951 do danes.

OBVESTILO

MAGISTRSKI ŠTUDIJ ZA UČITELJE MATEMATIKE

V šolskem letu 1991/92 bomo začeli z novim ciklom predavanj magistrskega študija matematike — izobraževalna smer. Do sedaj smo imeli dva cikla s po 15 udeleženci, predavanja so bila raztegnjena na tri leta. Enak ritem predvidevamo tudi tokrat. Na vse srednje šole v Sloveniji bomo poslali prijavnice za vpis. Pogoj za vpis je diploma iz matematike in opravljen strokovni izpit.

Za pojasnila se obrnite na naslov VTO Matematika in mehanika FNT, Jadranska 19, 61111 Ljubljana, pp. 64, tel. (061) 265-061.

Vodja podiplomskega študija
Peter Petek