

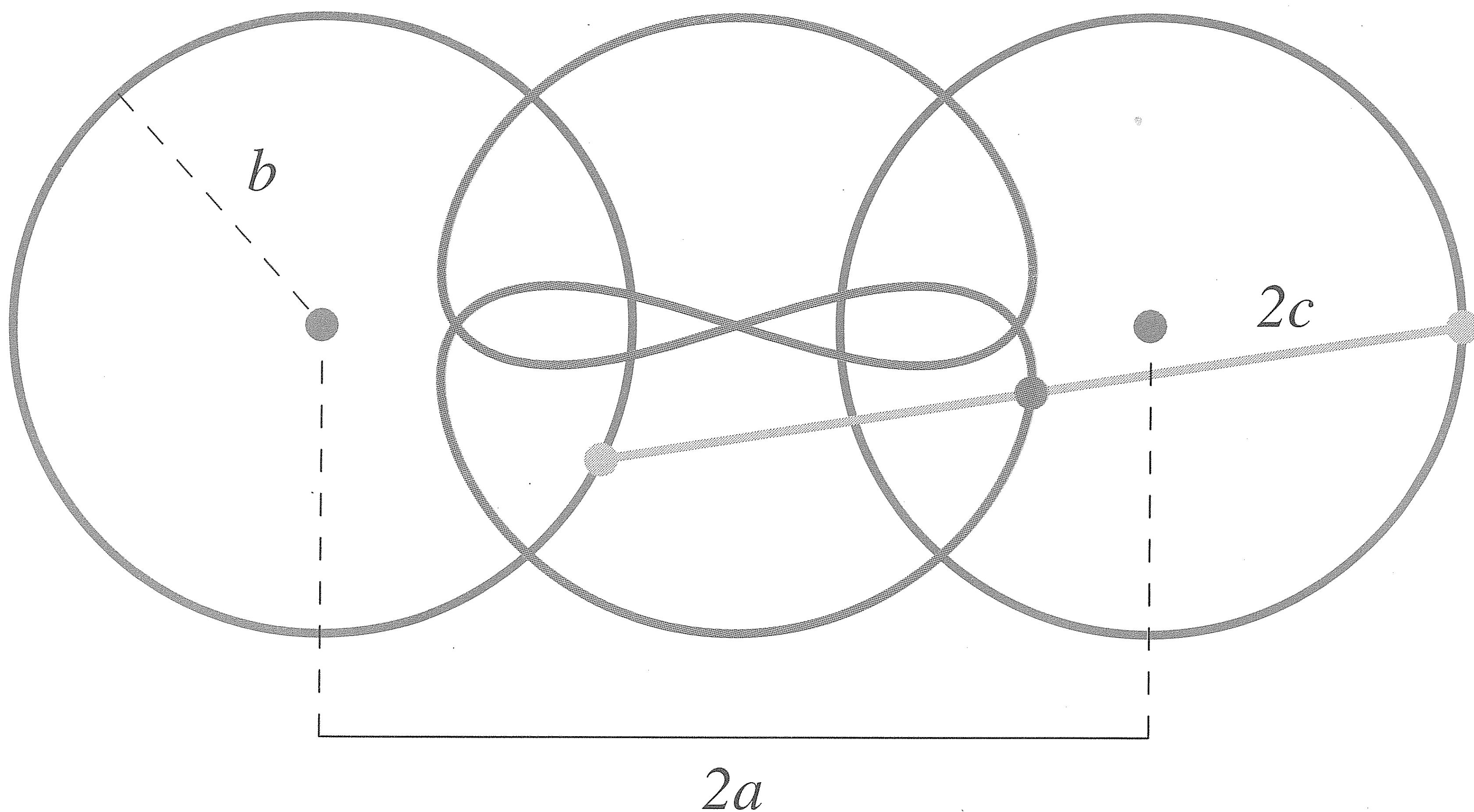
OPISANO

2002

Letnik 49

4

OBZORNIK ZA MATEMATIKO IN FIZIKO



OBZORNIK ZA MATEMATIKO IN FIZIKO

LJUBLJANA, JULIJ 2002

letnik 49, številka 4, strani 97–128

Glasilo Društva matematikov, fizikov in astronomov Slovenije

Naslov uredništva:

DMFA – založništvo, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana.

Telefon (01) 4766 553, 4232 460 Telefaks (01) 2517 281

Devizna nakazila: SKB banka d. d., Ajdovščina 4, Ljubljana

SWIFT: SKBASI2X

Transakcijski račun: 03100-1000018787

Uredniški odbor: Mirko Dobovišek (glavni urednik), Roman Drnovšek (urednik za matematiko in odgovorni urednik), Marko Zgonik (urednik za fiziko), Alenka Klokočovnik (društvene novice), Marjan Jerman (tehnični urednik).

Jezikovno pregledal Janez Juvan, računalniško oblikoval Martin Zemljič.

Člani društva prejemajo Obzornik brezplačno. Celoletna članarina je 4000 SIT, za študente 2000 SIT. Naročnina v knjigarnah in za ustanove je 8000 SIT, za tujino 30 EUR. Posamezna številka za člane je 800 SIT, stare številke 520 SIT.

Tisk: Tiskarna KURIR. Naklada 1450 izvodov.

Revijo sofinancira Ministrstvo za šolstvo, znanost in šport.

DMFA je včlanjeno v Evropsko matematično društvo (EMS), v Mednarodno matematično unijo (IMU), v Evropsko fizikalno društvo (EPS) in v Mednarodno združenje za čisto in uporabno fiziko (IUPAP). DMFA ima pogodbo o recipročnosti z Ameriškim matematičnim društvom (AMS).

© 2002 DMFA Slovenije – 1503

Poštnina plačana na pošti 1102 Ljubljana

VSEBINA — CONTENTS

Članki – Articles

Str.–Page

Kolobar aritmetičnih funkcij — Ring of arithmetical functions (Janko Bračič) 97–108

Spekter in realni spekter kolobarja zveznih realnih funkcij — The spectrum and the real spectrum of the ring of real-valued continuous functions (Igor Klep) 109–117

Verjetnost zaporednih števil v dobitni kombinaciji lota — Probabilities of consecutive integers in lotto (Stanley P. Gudder, James N. Hagler, prev. in prir. Marjan Jerman) 118–127

Vesti — News

Deveto mednarodno tekmovanje študentov matematike (Marjan Jerman) 127–III

Vabilo (Darjo Felda in Janez Krušič) IV

Na naslovnici, ki jo je oblikoval Bor Plestenjak, je Wattova krivulja, imenovana po škotskem izumitelju parnega stroja. Oboda koles polmera b , ki imata osi razmaknjeni za $2a$, povezuje drog dolžine $2c$. Krivuljo sestavljajo vsi možni položaji sredine droga. Njena enačba v polarni obliki je $r^2 = b^2 - (a \sin \varphi \pm \sqrt{c^2 - a^2 \cos^2 \varphi})^2$.

KOLOBAR ARITMETIČNIH FUNKCIJ

JANKO BRAČIČ

Math. Subj. Class. (2000) 11A25

Aritmetične funkcije imajo pomembno vlogo pri študiju deljivosti naravnih števil in porazdelitvi praštevil. V članku na popolnoma elementaren način dokažemo nekatere izreke, ki se nanašajo na Dirichletovo konvolucijo. V zadnjem razdelku obravnavamo aditivne preslikave na Dirichletovem kolobarju. Na koncu zastavimo tudi nekaj vprašanj, ki so verjetno še odprta.

RING OF ARITHMETICAL FUNCTIONS

Arithmetical functions play an important role in the study of divisibility properties of positive integers and the distribution of primes. In this article we prove some theorems which are related to the Dirichlet convolution. In the last section we consider additive mappings on the Dirichlet ring. At the end a few (probably still open) questions are given.

Aritmetična funkcija je preslikava iz množice naravnih števil $\mathbb{N}$ v obseg kompleksnih števil $\mathbb{C}$. Čeprav lahko primere takšnih funkcij definiramo na popolnoma poljuben način, so najbolj zanimive tiste aritmetične funkcije, ki nam nekaj povedo o naravnih številih. Za zgled navedimo naslednje dobro znane funkcije.

Eulerjeva funkcija φ , ki pri vsakem naravnem številu n prešteje, koliko števil v množici $\{1, \dots, n\}$ je tujih n .

Funkcija τ , ki nam pove število različnih deliteljev danega naravnega števila n .

Vsota vseh deliteljev naravnega števila — funkcija σ . Tudi ta funkcija je dobro znana. Z njo je povezan zelo star še nerešen problem o lihih popolnih številih, ki sprašuje, ali obstaja takšno liho naravno število n , za katero velja $\sigma(n) = 2n$.

Möbiusova funkcija μ . Kot bomo videli v drugem razdelku, ima ta funkcija eno od ključnih vlog v teoriji aritmetičnih funkcij. Definirana je takole: $\mu(1) = 1$, $\mu(n) = 0$, če kvadrat kakšnega praštevila deli n , in $\mu(n) = (-1)^k$, če je $n = p_1 \cdots p_k$, kjer so p_i različna praštevila.

Zanimive so tudi razne posplošitve omenjenih funkcij. Na primer, naj bo r poljubno celo število. Označimo s σ_r funkcijo, ki naravnemu številu n priredi vsoto r -tih potenc vseh deliteljev števila n . V posebnem je torej $\sigma_1 = \sigma$ in $\sigma_0 = \tau$.

V nadaljevanju bomo srečali še nekaj aritmetičnih funkcij in zanimivih zvez med njimi, a naše zanimanje ne bo veljalo le njim. V prvem razdelku bomo pokazali, da lahko v množico vseh aritmetičnih funkcij s pomočjo *Dirichletove konvolucije* vpeljemo strukturo komutativnega kolobarja. Del tega članka je namenjen obravnavi tega kolobarja.

Naš namen je dvojen. Prvič: podati želimo popolnoma elementarne dokaze nekaterih osrednjih izrekov iz teorije aritmetičnih funkcij, ki se nanašajo na Dirichletovo konvolucijo. In drugič: upamo, da bosta elementaren pristop in nabor vprašanj na koncu, ki so verjetno še odprta, spodbudila bralca k samostojnemu razmišljanju in raziskovanju.

Dirichletov kolobar

Običajno množico vseh preslikav iz neprazne množice A v neprazno množico B označimo z B^A . Se pravi, $\mathbb{C}^{\mathbb{N}}$ je množica vseh aritmetičnih funkcij. Ta množica je na naraven način kompleksen vektorski prostor: vsoto dveh aritmetičnih funkcij in produkt aritmetične funkcije s kompleksnim številom definiramo po točkah. To pomeni, da za poljubne aritmetične funkcije f, g, h in poljubno kompleksno število α velja

$$(f + g)(n) = f(n) + g(n) \quad \text{ter} \quad (\alpha h)(n) = \alpha h(n) \quad (n \in \mathbb{N}).$$

Aritmetične funkcije lahko tudi množimo po točkah: produkt poljubnih dveh funkcij f in g iz $\mathbb{C}^{\mathbb{N}}$ je funkcija $f \cdot g$, za katero velja

$$(f \cdot g)(n) = f(n)g(n) \quad (n \in \mathbb{N}).$$

Zlahka se prepričamo, da je $\mathbb{C}^{\mathbb{N}}$, opremljena s seštevanjem in množenjem po točkah, komutativna kompleksna algebra z enoto — enota za množenje je konstantna funkcija 1, ki vsakemu naravnemu številu n priredi vrednost 1.

Za teorijo števil omenjena algebrska struktura na $\mathbb{C}^{\mathbb{N}}$ nima velikega pomena. Rekli bi lahko, da vsebuje množenje po točkah le malo informacije o notranji zgradbi naravnih števil. Bolj uporabno množenje aritmetičnih funkcij je *Dirichletova konvolucija*.

Naj bosta f in g poljubni aritmetični funkciji. Njuna konvolucija je aritmetična funkcija $f * g$, ki naravnemu številu n priredi vrednost

$$f * g(n) := \sum_{d|n} f(d)g(n/d), \quad (1)$$

kjer $\sum_{d|n}$ pomeni, da je vsota vzeta po vseh deliteljih števila n . Če $d | n$, potem je jasno, da tudi število $d' = n/d$ deli n in da je produkt števil d in d' enak n . Se pravi, da lahko (1) zapišemo v bolj simetrični obliki

$$f * g(n) := \sum_{d d' = n} f(d)g(d'), \quad (2)$$

kjer $\sum_{d d' = n}$ označuje, da je vsota vzeta po vseh parih (d, d') naravnih števil, za katere velja $d | n$, $d' | n$ in $d d' = n$. V posebnem primeru, ko je, recimo, n praštevilo p , je

$$f * g(p) = f(1)g(p) + f(p)g(1).$$

Iz zapisa (2) je tudi razvidno, da je Dirichletova konvolucija komutativna.

Opremimo množico vseh aritmetičnih funkcij $\mathbb{C}^{\mathbb{N}}$ z operacijama $+$ in $*$, tj. s seštevanjem po točkah, ter Dirichletovo konvolucijo in nastalo algebrsko strukturo – Dirichletu na čast – označimo z $\mathcal{D}$.

Izrek 1. $\mathcal{D}$ je komutativen kolobar z enoto.

Dokaz. Da je za seštevanje po točkah $\mathcal{D}$ komutativna grupa, ni težko videti. Očitno je nevtralni element za seštevanje funkcija 0, ki je enaka 0 pri vsakem naravnem številu n . Kot smo že omenili, je komutativnost Dirichletove konvolucije razvidna iz (2). Preverjanje asociativnosti in distributivnosti je standardno, zato ga izpustimo. Trdimo, da je funkcija $\delta : \mathbb{N} \rightarrow \mathbb{C}$, ki je dana z

$$\delta(n) = \begin{cases} 1; & n = 1 \\ 0; & n \geq 2, \end{cases}$$

enota za množenje. Res! $\delta * f(n) = \sum_{d|n} \delta(d)f(n/d) = f(n)$. ■

Kolobar $\mathcal{D}$ — odslej ga bomo imenovali *Dirichletov kolobar* — ima enoto, zato se je smiselno vprašati po obrnljivih elementih.

Izrek 2. Funkcija $f \in \mathcal{D}$ je obrnljiva natanko tedaj, ko je $f(1) \neq 0$. Če je f obrnljiva, je njen inverz f^{-1} rekurzivno podan s formulo

$$f^{-1}(1) = \frac{1}{f(1)} \quad \text{in} \quad f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq 1}} f(d)f^{-1}(n/d), \quad \text{za } n \geq 2. \quad (3)$$

Dokaz. Naj bo $f \in \mathcal{D}$ obrnljiva. Obstaja torej takšna funkcija $g \in \mathcal{D}$, da velja $f * g(n) = \delta(n)$. V posebnem, pri $n = 1$, imamo $f(1)g(1) = 1$, od koder res sledi $f(1) \neq 0$.

Vzemimo zdaj, da je $f(1) \neq 0$. Potem je s (3) dobro definirana aritmetična funkcija f^{-1} . Preverimo enakost $f * f^{-1} = \delta$. Pri $n = 1$ je

$$f * f^{-1}(1) = f(1)f^{-1}(1) = 1 = \delta(1).$$

Pri $n \geq 2$ pa imamo

$$\begin{aligned} f * f^{-1}(n) &= \sum_{d|n} f(d)f^{-1}(n/d) = f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d \neq 1}} f(d)f^{-1}(n/d) \\ &= f(1)\left(-\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq 1}} f(d)f^{-1}(n/d)\right) + \sum_{\substack{d|n \\ d \neq 1}} f(d)f^{-1}(n/d) \quad \blacksquare \\ &= 0 = \delta(n). \end{aligned}$$

Označimo z $\mathcal{D}_0$ podmnožico vseh neobrnljivih funkcij v Dirichletovem kolobarju. Očitno je vsota dveh funkcij iz $\mathcal{D}_0$ spet v $\mathcal{D}_0$. Če je f funkcija iz $\mathcal{D}_0$, g pa je poljubna aritmetična funkcija, potem iz $f(1) = 0$ sledi $f * g(1) = f(1)g(1) = 0$, kar nam da $f * g \in \mathcal{D}_0$. To pomeni, da je $\mathcal{D}_0$ ideal v $\mathcal{D}$. Jasno je tudi, da je poljuben pravi ideal $\mathcal{I}$ v $\mathcal{D}$ podmnožica ideala $\mathcal{D}_0$, saj v nobenem kolobarju pravi ideal ne vsebuje obrnljivih elementov.

Naj bo K poljuben komutativen kolobar. Element $a \in K \setminus \{0\}$ je *delitelj nič*, če obstaja takšen element $b \in K \setminus \{0\}$, da velja $a \cdot b = 0$. Kolobar, v katerem ni deliteljev nič, imenujemo *celostna domena*.

Izrek 3. *Dirichletov kolobar $\mathcal{D}$ je celostna domena.*

Dokaz. Naj bosta $f, g \in \mathcal{D}$ poljubni neničelni aritmetični funkciji. Pokazali bomo, da je tedaj tudi $f * g$ neničelna.

Naj bo m najmanjše naravno število, za katero velja $f(m) \neq 0$, z n pa označimo najmanjše naravno število, pri katerem je $g(n) \neq 0$. Trdimo, da je mn najmanjše naravno število, pri katerem je funkcija $f * g$ od 0 različna.

Če je $f(1) \neq 0$ in $g(1) \neq 0$, potem je tudi $f * g(1) = f(1)g(1) \neq 0$. Vzemimo, da je $mn > 1$, in naj bo $k < mn$ naravno število. Potem je

$$f * g(k) = \sum_{dd'=k} f(d)g(d').$$

Če v zgornji vsoti za d velja $d < m$, potem je $f(d) = 0$. Kadar pa je $m \leq d$, imamo $md' \leq dd' = k < mn$, od koder sledi $d' < n$ in zato $g(d') = 0$. Se pravi, da pri vsakem paru deliteljev d in d' , za katera je $dd' = k$, velja $f(d)g(d') = 0$. Od tod seveda sledi $f * g(k) = 0$.

Naj bo $k = mn$. Podoben razmislek kot prej nas pripelje do zaključka, da je $f(d)g(d') = 0$, če velja $dd' = k$ in $d \neq m$. Če je $d = m$, je $d' = n$, zato

$$f * g(k) = \sum_{dd'=k} f(d)g(d') = f(m)g(n) \neq 0. \quad \blacksquare$$

Ker v $\mathcal{D}$ ni deliteljev nič, tudi neničelnih *nilpotentov* ni. Spomnimo, da je neničelni element a iz kolobarja K nilpotent, če obstaja takšno naravno število $n \geq 2$, da je $a^n = 0$ in $a^{n-1} \neq 0$. Iz izreka 3 prav tako sledi, da razen funkcij 0 in δ ni drugih *idempotentov*. Idempotent v kolobarju je takšen element, ki je enak svojemu kvadratu. Da sta funkciji 0 in δ edina idempotenta v $\mathcal{D}$, sledi iz naslednjega razmisleka. Če je $e \in \mathcal{D}$ idempotent, potem iz $e * e = e$ izhaja $e * (e - \delta) = 0$. Ker je $\mathcal{D}$ celostna domena, mora veljati bodisi $e = 0$ bodisi $e = \delta$.

Aditivne in multiplikativne aritmetične funkcije

Navedimo še nekaj zgledov aritmetičnih funkcij. Poleg zelo znanih funkcij, ki smo jih navedli v uvodu, smo srečali že enoto za Dirichletovo konvolucijo δ ter konstantni funkciji 1 in 0, ki vsakemu naravnemu številu n priredita vrednost 1 oziroma 0. Pomembna aritmetična funkcija je tudi identiteta na $\mathbb{N}$, ki jo bomo označili z ι . Se pravi, ι je funkcija, za katero velja $\iota(n) = n$ pri vseh $n \in \mathbb{N}$. Definirajmo še funkcije ι_r , kjer je r celo število, s predpisom $\iota_r(n) = n^r$ ($n \in \mathbb{N}$). V posebnem je torej $\iota_1 = \iota$ in $\iota_0 = 1$.

Da bi lahko definirali še druge aritmetične funkcije, ki so zanimive s stališča teorije števil, potrebujemo *izrek o enoličnem razcepu na prafaktorje* (za dokaz glejte, na primer [2; str. 33]).

Naj bo $p \in \mathbb{N}$ praštevilo. Pri vsakem naravnem številu n definirajmo $v_p(n)$ kot največje celo število r , za katero velja $p^r \mid n$. Če praštevilo p naravnega števila n ne deli, je $v_p(n) = 0$. V posebnem torej velja $v_p(1) = 0$ za vsako praštevilo p . Z enostavno uporabo izreka o enoličnem razcepu na prafaktorje se lahko prepričamo, da imajo funkcije v_p naslednjo lastnost:

$$v_p(mn) = v_p(m) + v_p(n) \quad (m, n \in \mathbb{N}).$$

Definicija 4. Aritmetična funkcija f je *aditivna*, če za poljubni naravni števili m in n , katerih največji skupni delitelj (m, n) je 1, velja

$$f(mn) = f(m) + f(n). \quad (4)$$

Če za aritmetično funkcijo f velja (4) brez predpostavke $(m, n) = 1$, pravimo, da je *popolnoma aditivna*.

Funkcije v_p so torej popolnoma aditivne. Nadaljnji zgled popolnoma aditivne funkcije je zožitev logaritemske funkcije na $\mathbb{N}$. Zgled popolnoma aditivne funkcije je tudi Ω . Ta funkcija je definirana takole: če je $n \geq 2$ in je $n = p_1^{r_1} \cdots p_k^{r_k}$ enolični razcep števila n na praštevila, je $\Omega(n) = r_1 + \dots + r_k$. Postavimo še $\Omega(1) = 0$. Očitno nam funkcija Ω pove celotno število praštevil, ki delijo dano naravno število. Funkcija, ki je aditivna, ni pa popolnoma aditivna, je

$$\omega(n) = \sum_{p \mid n} 1 \quad (n \in \mathbb{N}),$$

kjer teče vsota po vseh različnih praštevilih, ki delijo naravno število n . Funkcija ω nam pove, koliko različnih praštevil deli dano naravno število.

Brez veliko truda lahko vidimo, da je vsaka aditivna aritmetična funkcija v idealu $\mathcal{D}_0$ in da je vsota dveh (popolnoma) aditivnih funkcij spet (popolnoma) aditivna. Izpustimo torej dokaz in nadaljujmo z naslednjo definicijo:

Definicija 5. Aritmetična funkcija $f \neq 0$ je *multiplikativna*, če je

$$f(mn) = f(m)f(n), \quad (5)$$

kakor hitro sta m in n naravni števili z $(m, n) = 1$. *Popolnoma multiplikativna* je vsaka tista funkcija, za katero velja (5) tudi brez pogoja $(m, n) = 1$.

Označimo z $\mathcal{M}$ množico vseh multiplikativnih funkcij v $\mathcal{D}$. Preden na-vedemo nekaj zgledov, dokažimo naslednji izrek – v resnici bomo dokazali le točki (iii) in (iv), saj sta prvi dve trditvi dokaj enostavni.

Izrek 6.

- (i) Za vsako multiplikativno funkcijo f velja $f(1) = 1$, kar pomeni, da je $\mathcal{M} \cap \mathcal{D}_0 = \emptyset$.
- (ii) Če sta f in g (popolnoma) multiplikativni, je tudi njun produkt po točkah $f \cdot g$ (popolnoma) multiplikativna funkcija.
- (iii) Naj bosta f in g takšni aritmetični funkciji, da sta g in $f * g$ multiplikativni. Potem je tudi f multiplikativna.
- (iv) $\mathcal{M}$ je podgrupa v grupi vseh obrnljivih elementov kolobarja $\mathcal{D}$.

Dokaz. (iii) Predpostavili bomo, da f ni multiplikativna, in potem pokazali, da tudi $f * g$ ni multiplikativna. Označimo $h = f * g$. Ker f ni multiplikativna, obstajata takšni naravni števili m in n , za kateri velja $(m, n) = 1$, da je $f(mn) \neq f(m)f(n)$. Izberimo takšen par števil m in n , da bo produkt mn najmanjši.

Če je $mn = 1$, potem iz $f(1) \neq f(1)f(1)$ sledi $f(1) \neq 1$. Ker je $g(1) = 1$, velja $h(1) = f(1)g(1) = f(1) \neq 1$, kar po točki (i) tega izreka pomeni, da h ni multiplikativna.

Naj bo $mn > 1$. Potem za naravni števili d in e , ki zadoščata pogojem $(d, e) = 1$ ter $de < mn$, velja $f(de) = f(d)f(e)$. Se pravi, da velja

$$\begin{aligned} h(mn) &= \sum_{\substack{d|m \\ e|n \\ de < mn}} f(de)g\left(\frac{mn}{de}\right) + f(mn)g(1) \\ &= \sum_{\substack{d|m \\ e|n \\ de < mn}} f(d)f(e)g\left(\frac{m}{d}\right)g\left(\frac{n}{e}\right) + f(mn) \\ &= \sum_{d|m} f(d)g\left(\frac{m}{d}\right) \sum_{e|n} f(e)g\left(\frac{n}{e}\right) - f(m)f(n) + f(mn) \\ &= h(m)h(n) - f(m)f(n) + f(mn). \end{aligned}$$

Zaradi $f(mn) \neq f(m)f(n)$ je tudi $h(mn) \neq h(m)h(n)$.

(iv) Naj bo $f \in \mathcal{M}$ ter f^{-1} njen inverz. Funkciji $f^{-1} * f = \delta$ in f sta multiplikativni, zato je po prejšnji točki tudi f^{-1} multiplikativna.

Pokazati moramo še, da za poljubni $f, g \in \mathcal{M}$ velja $h = f * g \in \mathcal{M}$. Spet uporabimo točko (iii): ker sta g^{-1} in $h * g^{-1} = f$ multiplikativni, je h multiplikativna. ■

Točka (iv) v prejšnjem izreku nam omogoča, da iz znanih multiplikativnih funkcij tvorimo nove funkcije s to lastnostjo, oziroma da poiščemo povezave med že znanimi funkcijami. Na primer, ni težko videti, da pri vsakem celem številu r velja $\sigma_r = \iota_r * 1$. Ker sta ι_r in 1 (očitno) popolnoma multiplikativni, je funkcija σ_r multiplikativna. Med drugim to pomeni, da sta $\sigma = \sigma_1$ in $\tau = \sigma_0$ multiplikativni. Funkciji τ in σ nista popolnoma multiplikativni. Torej točki (iii) in (iv) v izreku 6 ne veljata za popolnoma multiplikativne funkcije: Dirichletova konvolucija dveh popolnoma multiplikativnih funkcij ni nujno popolnoma multiplikativna.

Naslednji izrek nam ponuja še nekaj zanimivih zvez med znanimi aritmetičnimi funkcijami.

Izrek 7. *Veljajo naslednje enakosti*

$$\mu = 1^{-1}, \quad \varphi = \mu * \iota \quad \text{ter} \quad \sigma = \varphi * \tau.$$

Dokaz. Da bi dokazali zvezo $\mu = 1^{-1}$, pogledjmo, kaj nam o naravnem številu pove 1^{-1} . Uporabimo (3). Jasno, $1^{-1}(1) = 1$, zato vzemimo, da je $n \geq 2$. Ker je, po izreku 6, 1^{-1} multiplikativna, je dovolj, da poznamo njeno delovanje na potencah praštevil. Naj bo torej $n = p^r$, kjer je p praštevilo in $r \in \mathbb{N}$. Če je $r = 1$, potem nam (3) da

$$1^{-1}(p) = - \sum_{\substack{d|p \\ d \neq 1}} 1^{-1}(p/d) = -1^{-1}(1) = -1.$$

Za $r = 2$ dobimo

$$1^{-1}(p^2) = - \sum_{\substack{d|p^2 \\ d \neq 1}} 1^{-1}(p/d) = -1^{-1}(p) - 1^{-1}(1) = 0.$$

Z enostavno indukcijo glede na r lahko pokažemo, da je $1^{-1}(p^r) = 0$ za vse $r \geq 2$. Iz vsega povedanega sledi, da se 1^{-1} res povsod ujema s funkcijo μ .

Za dokaz enakosti $\varphi = \mu * \iota$ bomo uporabili formulo

$$\sum_{d|n} \varphi(d) = n \quad (n \in \mathbb{N}), \quad (6)$$

katere dokaz je recimo v [2; str. 52]. Zapisana z Dirichletovo konvolucijo se (6) glasi $\varphi * 1 = \iota$. Če pomnožimo to enakost z μ in upoštevamo, da je $\mu = 1^{-1}$, dobimo

$$\iota * \mu = (\varphi * 1) * \mu = \varphi * (1 * \mu) = \varphi * \delta = \varphi.$$

Da bi dokazali zadnjo identiteto, pomnožimo enakost $\tau = 1 * 1$ z μ in upoštevajmo, da je μ inverz funkcije 1. Dobimo $\mu * \tau = 1$. Upoštevajmo še zvezo $\varphi = \mu * \iota$, pa imamo

$$\varphi * \tau = (\mu * \iota) * \tau = \iota * (\mu * \tau) = \iota * 1 = \sigma. \quad \blacksquare$$

Zdaj, ko vemo, da je $\mu = 1^{-1}$, lahko brez težav dokažemo naslednji znameniti izrek:

Izrek 8 (Möbiusova inverzna formula). Če za aritmetični funkciji f in g velja

$$f(n) = \sum_{d|n} g(d) \quad (n \in \mathbb{N}), \quad (7)$$

potem zanju velja tudi

$$g(n) = \sum_{d|n} f(d) \mu(n/d) \quad (n \in \mathbb{N}). \quad (8)$$

Obratno, če za f in g velja (8), potem zanju velja tudi (7).

Dokaz. Enakost (7) pravi, da je $f = g * 1$. Pomnožimo to enakost z μ in upoštevajmo, da je $\mu = 1^{-1}$, pa imamo $g = f * \mu$, kar ni nič drugega kot (8). Drugi del izreka dokažemo podobno: enakost $g = f * \mu$ pomnožimo z 1, da dobimo $f = g * 1$. ■

Preslikave na $\mathcal{D}$

V tem razdelku nas bodo zanimale nekatere *aditivne* preslikave na Dirichletovem kolobarju $\mathcal{D}$. Začnimo z definicijo.

Definicija 9.

(1) Preslikava $T : \mathcal{D} \rightarrow \mathcal{D}$ je *aditivna*, če velja

$$T(f + g) = T(f) + T(g) \quad (f, g \in \mathcal{D}).$$

(2) *Homomorfizem* kolobarja $\mathcal{D}$ je vsaka takšna aditivna preslikava $\Theta \neq 0$ na $\mathcal{D}$, za katero velja

$$\Theta(f * g) = \Theta(f) * \Theta(g) \quad (f, g \in \mathcal{D}).$$

(3) *Odvajanje* na kolobarju $\mathcal{D}$ je vsaka takšna aditivna preslikava D na $\mathcal{D}$, za katero velja

$$D(f * g) = f * D(g) + D(f) * g \quad (f, g \in \mathcal{D}).$$

Naj bo h aritmetična funkcija. Definirajmo preslikavo $M_h : \mathcal{D} \rightarrow \mathcal{D}$ s predpisom $M_h(f) = h * f$ ($f \in \mathcal{D}$). Zaradi distributivnosti, ki velja v $\mathcal{D}$, je M_h aditivna. Če je $h \neq 0$ in $h \neq \delta$, potem M_h ni homomorfizem niti odvajanje na $\mathcal{D}$, očitno pa zanjo velja

$$M_h(f * g) = M_h(f) * g = f * M_h(g) \quad (f, g \in \mathcal{D}). \quad (9)$$

Preslikavi M na $\mathcal{D}$, ki zadošča (9), pravimo *multiplikator*. Ker ima $\mathcal{D}$ enoto za množenje, razen preslikav oblike M_h ($h \in \mathcal{D}$), drugih multiplikatorjev na tem kolobarju ni. Namreč, naj bo M multiplikator na $\mathcal{D}$. Označimo s h funkcijo $M(\delta)$. Potem pri vsaki funkciji $f \in \mathcal{D}$ velja

$$M(f) = M(f * \delta) = f * M(\delta) = M_h(f),$$

kar nam da $M = M_h$.

Jasno je, da je identična preslikava $I : f \mapsto f$ ($f \in \mathcal{D}$) homomorfizem kolobarja $\mathcal{D}$. Prav tako je očitno, da je $0 : f \mapsto 0$ ($f \in \mathcal{D}$) odvajanje. Iz naslednjega izreka izhaja, da poleg teh dveh trivialnih primerov obstajajo tudi drugi homomorfizmi in odvajanja na $\mathcal{D}$. Spomnimo se, da smo v prvem razdelku z $f \cdot g$ označili produkt po točkah. Za vsak $h \in \mathcal{D}$ definirajmo preslikavo T_h na $\mathcal{D}$ s predpisom $f \mapsto h \cdot f$.

Izrek 10.

- (i) Funkcija $h \in \mathcal{D}$ je popolnoma multiplikativna natanko tedaj, ko je T_h homomorfizem kolobarja $\mathcal{D}$.
- (ii) Funkcija $h \in \mathcal{D}$ je popolnoma aditivna natanko tedaj, ko je T_h odvajanje na kolobarju $\mathcal{D}$.

Dokaz. (i) Naj bo h popolnoma multiplikativna funkcija, f, g pa poljubni. Potem pri vsakem $n \in \mathbb{N}$ velja

$$\begin{aligned} [h \cdot (f * g)](n) &= h(n) \sum_{d d' = n} f(d)g(d') = \sum_{d d' = n} h(d)h(d')f(d)g(d') \\ &= \sum_{s d' = n} [h \cdot f](d)[h \cdot g](d') = [(h \cdot f) * (h \cdot g)](n), \end{aligned}$$

kar dokazuje, da je T_h homomorfizem.

Da bi dokazali obrat, definirajmo pri vsakem naravnem številu k funkcijo δ_k z zahtevo $\delta_k(k) = 1$ in $\delta_k(n) = 0$, če je $k \neq n$. V posebnem je torej $\delta_1 = \delta$. Za poljubni naravni števili m in n velja $\delta_m * \delta_n = \delta_{mn}$.

Predpostavimo, da je h takšna funkcija, da je T_h homomorfizem. Naj bosta m in n poljubni naravni števili. Potem je

$$\begin{aligned} h(mn) &= [h \cdot \delta_{mn}](mn) = [h \cdot (\delta_m * \delta_n)](mn) \\ &= [(h \cdot \delta_m) * (h \cdot \delta_n)](mn) = \sum_{d d' = mn} (h \cdot \delta_m)(d)(h \cdot \delta_n)(d') \\ &= \sum_{d d' = mn} h(d)\delta_m(d)h(d')\delta_n(d') = h(m)h(n). \end{aligned}$$

(ii) Dokaz tega dela izreka je zelo podoben prvemu delu. Če je h popolnoma aditivna funkcija, ni težko videti, da je T_h odvajanje na $\mathcal{D}$. Za dokaz obrata pa spet uporabimo funkcije δ_k . ■

Ali poleg homomorfizmov in odvajanj na $\mathcal{D}$, ki jih določajo popolnoma multiplikativne oziroma popolnoma aditivne funkcije z množenjem po točkah, obstajajo homomorfizmi in odvajanja, ki jih ni mogoče predstaviti na takšen način? Obstajajo. Poglejmo na primer odvajanja.

Naj bo $p \in \mathbb{N}$ praštevilo. Definirajmo preslikavo $D_p : \mathcal{D} \rightarrow \mathcal{D}$ s predpisom

$$D_p f(n) = v_p(pn) f(pn) \quad (n \in \mathbb{N}, f \in \mathcal{D}).$$

Izrek 11. *Za vsako praštevilo $p \in \mathbb{N}$ je D_p surjektivno odvajanje na $\mathcal{D}$.*

Dokaz. Naj bo p poljubno praštevilo, $m \in \mathbb{N}$ število, ki ni deljivo s p , ter k nenegativno celo število. Očitno so delitelji števila $p^k m$ natanko vsa števila oblike $p^j d$, kjer je d delitelj števila m , število j pa je iz množice $\{0, 1, \dots, k\}$. Za poljubni dve aritmetični funkciji f in g torej velja

$$f * g(p^k m) = \sum_{j=0}^k \sum_{d d' = m} f(p^j d) g(p^{k-j} d').$$

To dejstvo nam bo nekoliko olajšalo delo, saj je ideja našega dokaza, da pri danih funkcijah f in g iz $\mathcal{D}$ in danem številu $n \in \mathbb{N}$ pokažemo, da sta števili $D_p(f * g)(n)$ in $(f * D_p g + D_p f * g)(n)$ enaki.

Zapišimo število n kot $n = p^k m$, kjer je k takšno nenegativno celo število, da praštevilo p ne deli naravnega števila m . Potem je

$$\begin{aligned} D_p(f * g)(n) &= D_p(f * g)(p^k m) = v_p(p^{k+1} m) f * g(p^{k+1} m) \\ &= (k+1) \sum_{j=0}^{k+1} \sum_{d d' = m} f(p^j d) g(p^{k+1-j} d'). \end{aligned}$$

Velja pa tudi

$$\begin{aligned} f * D_p g(p^k m) &= \sum_{j=0}^k \sum_{d d' = m} f(p^j d) D_p g(p^{k-j} d') \\ &= \sum_{j=0}^k \sum_{d d' = m} f(p^j d) v_p(p^{k-j+1} d') g(p^{k-j+1} d') \\ &= \sum_{j=0}^k \sum_{d d' = m} (k-j+1) f(p^j d) g(p^{k-j+1} d') \end{aligned}$$

in

$$\begin{aligned}
D_p \mathbf{f} * \mathbf{g}(p^k m) &= \sum_{j=0}^k \sum_{d \mid d'=m} D_p \mathbf{f}(p^j d) \mathbf{g}(p^{k-j} d') \\
&= \sum_{j=0}^k \sum_{d \mid d'=m} \mathbf{v}_p(p^{j+1} d) \mathbf{f}(p^{j+1} d) \mathbf{g}(p^{k-j} d') \\
&= \sum_{j=0}^k \sum_{d \mid d'=m} (j+1) \mathbf{f}(p^{j+1} d) \mathbf{g}(p^{k-j} d').
\end{aligned}$$

Se pravi, da je

$$\begin{aligned}
(\mathbf{f} * D_p \mathbf{g} + D_p \mathbf{f} * \mathbf{g})(p^k m) &= \sum_{j=0}^k \sum_{d \mid d'=m} (k-j+1) \mathbf{f}(p^j d) \mathbf{g}(p^{k-j+1} d') \\
&\quad + \sum_{j=0}^k \sum_{d \mid d'=m} (j+1) \mathbf{f}(p^{j+1} d) \mathbf{g}(p^{k-j} d').
\end{aligned}$$

Združimo na desni strani drugi člen iz prve vsote s prvim členom iz druge vsote, tretji člen iz prve vsote z drugim členom iz druge vsote itd., pa dobimo

$$\begin{aligned}
(\mathbf{f} * D_p \mathbf{g} + D_p \mathbf{f} * \mathbf{g})(p^k m) &= (k+1) \sum_{j=0}^{k+1} \sum_{d \mid d'=m} \mathbf{f}(p^j d) \mathbf{g}(p^{k+1-j} d') \\
&= D_p(\mathbf{f} * \mathbf{g})(p^k m).
\end{aligned}$$

Dokažimo še surjektivnost. Naj bo $\mathbf{g} \in \mathcal{D}$ poljubna aritmetična funkcija. Vzemimo takšno funkcijo $\mathbf{f} \in \mathcal{D}$, za katero velja

$$\mathbf{f}(m) = \frac{\mathbf{g}(m/p)}{\mathbf{v}_p(m)},$$

če $p \mid m$, medtem ko so vrednosti funkcije $\mathbf{f}$ pri tistih $m \in \mathbb{N}$, ki niso večkratniki p , lahko poljubne. Potem velja

$$D_p \mathbf{f}(n) = \mathbf{v}_p(p n) \mathbf{f}(p n) = \mathbf{v}_p(p n) \frac{\mathbf{g}(n)}{\mathbf{v}_p(p n)} = \mathbf{g}(n) \quad (n \in \mathbb{N}). \quad \blacksquare$$

Ker množenje po točkah s popolno aditivno funkcijo preslika vsako aritmetično funkcijo v ideal $\mathcal{D}_0$ – in torej ni surjektivno – lahko sklepamo, da odvajanja D_p niso dobljena kot množenje s kakšno popolnoma aditivno funkcijo.

Če sta p in q praštevili, potem za poljubni funkciji f in g iz $\mathcal{D}$ velja

$$D_p D_q f(n) = D_p(v_q \cdot f)(qn) = (v_p \cdot v_q \cdot f)(pq n) = D_q D_p f(n) \quad (n \in \mathbb{N}),$$

kar pomeni, da D_p in D_q komutirata. Prav tako komutirata dve odvajanja, ki ju z množenjem po točkah določata dve popolnoma aditivni funkciji. Toda če je p praštevilo in h popolnoma aditivna funkcija, je

$$\begin{aligned} [(D_p T_h - T_h D_p)f](n) &= [D_p(T_h f)](n) - [T_h(D_p f)](n) \\ &= v_p(pn)(T_h f)(pn) - h(n)(D_p f)(n) \\ &= v_p(pn)h(pn)f(pn) - h(n)v_p(pn)f(pn) \\ &= v_p(pn)f(pn)[h(p) + h(n) - h(n)] \\ &= h(p)D_p f(n) \quad (n \in \mathbb{N}, f \in \mathcal{D}), \end{aligned}$$

kar nam da $D_p T_h - T_h D_p = h(p)D_p$. Torej D_p in T_h komutirata natanko tedaj, ko je $h(p) = 0$.

Na koncu navedimo nekaj problemov.

1. Ali poleg odvajanj D_p , p praštevilo, in tistih, ki smo jih opisali v izreku 10 (ii), obstajajo še kakšna druga odvajanja na $\mathcal{D}$?
2. Opišite vse homomorfizme kolobarja $\mathcal{D}$.
3. Kaj so multiplikatorji na idealu $\mathcal{D}_0$? Z drugimi besedami, poiščite vse aditivne preslikave $M : \mathcal{D}_0 \rightarrow \mathcal{D}_0$, za katere velja (9) pri vseh $f, g \in \mathcal{D}_0$.
4. Ali ima množica vseh popolnoma aditivnih aritmetičnih funkcij poleg tega, da je zaprta za seštevanje, še kakšno drugo algebrsko strukturo?
5. Raziščite podkolobarje v $\mathcal{D}$, ki jih generirajo končni ali neskončni nabori funkcij δ_n , $n \in \mathbb{N}$ (za definicijo glejte dokaz izreka 10).

LITERATURA

- [1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.
- [2] J. Grasselli, *Osnove teorije števil*, DZS, Ljubljana 1975.
- [3] P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer, 1986.

SPEKTER IN REALNI SPEKTER KOLOBARJA ZVEZNIH REALNIH FUNKCIJ

IGOR KLEP

Math. Subj. Class. (2000): 06F, 13J30, 14P

V članku navajamo nekaj osnovnih rezultatov o kolobarju zveznih realnih funkcij $\mathcal{C}(X, \mathbb{R})$. Poiščemo povezavo med spektrom in realnim spektrom tega kolobarja in nakažemo, kako lahko s pomočjo realne algebre izpeljemo Stone-Čechovo kompaktifikacijo popolnoma regularnega topološkega prostora.

THE SPECTRUM AND THE REAL SPECTRUM OF THE RING OF REAL-VALUED CONTINUOUS FUNCTIONS

In this paper we will mention some results about the ring of the real-valued continuous functions $\mathcal{C}(X, \mathbb{R})$. We will find a relationship between the prime and the real spectrum of this ring. Moreover, we also indicate how to deduce the Stone-Čech compactification of a completely regular topological space with the help of real algebra.

Kolobar zveznih realnih funkcij na topološkem prostoru X , ki ga ponavadi označimo s $\mathcal{C}(X, \mathbb{R})$, je področje aktivnega raziskovanja. Zanimiv je za matematike različnih področij: od tistih, ki se ukvarjajo s topologijo, algebro, geometrijo, funkcionalno analizo, pa vse do tistih, ki se ukvarjajo s teorijo množic. Pionirja na tem področju sta Čech in Stone, ki sta s svojimi raziskavami začela pod vplivom doktorske disertacije Tihonova. Pospešeno raziskovanje kolobarja $\mathcal{C}(X, \mathbb{R})$ je vzpodbudil članek Hewitta [5] iz leta 1948. Bil je nadaljevanje del Čecha in Stona in je postavil temelje za študij povezave med topološkimi lastnostmi prostora X in algebraičnimi lastnostmi kolobarja $\mathcal{C}(X, \mathbb{R})$. Izsledke do leta 1960 sta v knjigi [4] objavila Gillman in Jerison. Ta tekst je še vedno osnova za študij kolobarja $\mathcal{C}(X, \mathbb{R})$.

Tudi s stališča realne algebre je kolobar zveznih realnih funkcij zanimiv. Realna algebra med drugim preučuje kolobarje in njihove ureditve. Kot začetnika realne algebre štejemo Hilberta in Artina. Na znamenitem matematičnem kongresu leta 1900 v Parizu je Hilbert objavil seznam 23 nerešenih problemov, ki so ogromno pripomogli k razvoju matematike v dvajsetem stoletju. Sedemnajsti Hilbertov problem sprašuje, ali je vsak realen polinom v več spremenljivkah $p \in \mathbb{R}[X_1, \dots, X_n]$, ki je povsod nenegativen, vsota kvadratov realnih racionalnih funkcij iz $\mathbb{R}(X_1, \dots, X_n)$. Že Hilbert sam je vedel, da takšen polinom ni nujno vsota kvadratov polinomov iz $\mathbb{R}[X_1, \dots, X_n]$. Pritrdilen odgovor na Hilbertov sedemnajsti problem je podal Artin leta 1927. S tem datumom se je začel razvoj realne algebre, ki je v zadnjih 75 letih prinesla mnogo lepih in zanimivih rezultatov. Literatura na tem področju je zelo obširna, glej npr. [1], [10], [11] in [12] ter reference, podane v teh knjigah.

1. Nekaj dejstev iz realne algebre

Osnovne pojme realne algebre je v slovenski matematični svet prinesel Boris Lavrič [8] in [9]. Eden izmed osrednjih predmetov študija realne algebre so ureditve na kolobarjih in obsegih. Več o ureditvah na obsegih lahko bralec najde v [1] in [7], o ureditvah na kolobarjih pa je pred kratkim za Obzornik pisal Jakob Cimprič [2].

Za začetek nekaj besed o privzetkih in oznakah. Vsi kolobarji bodo komutativni z enico. Za kolobar A bomo z A^2 označili množico vseh kvadratov elementov iz A , za podmnožico $S \subseteq A$ bomo s $\sum S$ zaznamovali aditivno polgrupo, generirano s S .

Množica $P \subsetneq A$ je *ureditev*, če velja $P + P \subseteq P$, $P \cdot P \subseteq P$, $P \cup -P = A$ in je $P \cap -P$ praideal kolobarja A . *Nosilec* ureditve P je praideal $P \cap -P$, ki ga označimo s P^0 . Množico *strogo pozitivnih* elementov $P \setminus -P$ ureditve P zaznamujemo s P^+ . Ureditve na kolobarjih lahko definiramo še na en ekvivalenten način. Par $(\mathfrak{p}, \leq)$ imenujemo *ureditev* kolobarja A , če je $\mathfrak{p} \subsetneq A$ praideal in $\leq$ linearna ureditev (usklajena z algebraičnimi operacijami) na obsegu ulomkov celostnega polja $A/\mathfrak{p}$.

Poglejmo si, zakaj sta ti definiciji ekvivalentni. Iz para $(\mathfrak{p}, \leq)$ tvorimo $P := \{x \in A \mid x + \mathfrak{p} \geq \mathfrak{p}\}$, ki očitno izpolnjuje pogoje prve definicije. Obratno, če imamo podano ureditev $P \subsetneq A$, tvorimo $\mathfrak{p} := P^0$ in postavimo $a + \mathfrak{p} \leq b + \mathfrak{p}$ natanko tedaj, ko $b - a \in P$ ($a, b \in A$). Kratek račun pokaže, da lahko $\leq$ enolično razširimo do linearne ureditve na obsegu ulomkov kolobarja $A/\mathfrak{p}$.

Zgled. Naj bo $A := \mathbb{R}[X]$ kolobar realnih polinomov v eni spremenljivki. Množici

$$P_1 := \{a_n X^n + \dots + a_0 \in \mathbb{R}[X] \mid a_n > 0\} \cup \{0\}$$

$$P_2 := \{p(X) \in \mathbb{R}[X] \mid p(0) \geq 0\}$$

sta ureditvi kolobarja A . Ureditev P_1 ima nosilec $\{0\}$, nosilec ureditve P_2 pa je (X) . Klasifikacijo vseh ureditev kolobarja A si lahko bralec ogleda v [7] in [10].

Kot tehničen pripomoček vpeljemo še en pojem. Podmnožico $T \subseteq A$ imenujemo *predureditev*, če velja $T + T \subseteq T$, $T \cdot T \subseteq T$ in $A^2 \subseteq T$. Če velja še $-1 \notin T$, potem je T *prava predureditev*.

V vsakem kolobarju A obstaja predureditev $\sum A^2$. Nima pa vsak kolobar prave predureditve. V kolobarju $\mathbb{Z}[i]$ velja $i^2 = -1$, zato ta kolobar nima prave predureditve. Očitno je vsaka ureditev kolobarja tudi prava predureditev. Obrat te trditve ne velja. Če vzamemo $A = \mathcal{C}(X, \mathbb{R})$, potem je $T := \sum A^2$ prava predureditev, ki vsebuje natanko vse nenegativne funkcije. Vendar T ni ureditev, saj je $T \cup -T \subsetneq A$. Obstajajo pa tudi

kolobarji, ki imajo natanko eno pravo predureditev (ki je tudi ureditev), npr. kolobar celih števil. Naslednji izrek je posplošitev znanega Artin-Schreierjevega izreka o realnih obsegih. Osnovni izrek sta dokazala Artin in Schreier leta 1926 in je ena izmed dveh temeljnih sestavin Artinove rešitve Hilbertovega sedemnajstega problema. Med drugim nam izrek pove, da obsega kompleksnih števil ne moremo urediti.

Izrek 1. Če $-1 \notin \sum A^2$, potem ima kolobar A ureditev.

Ideja dokaza tega izreka je preprosta. Ker $-1 \notin \sum A^2$, po Zornovi lemi obstaja maksimalna prava predureditev $P \subseteq A$. Z nekoliko truda je možno pokazati, da je P ureditev. Podroben dokaz izreka 1 je najdemo v [2] in [10].

Definicija 2. *Spekter* $\text{Spec } A$ kolobarja A je množica vseh praidealov kolobarja A . Množico maksimalnih idealov kolobarja A označimo s $\text{Specmax } A$. *Realen spekter* $\text{Sper } A$ kolobarja A je množica vseh ureditev kolobarja A . Podmnožico vseh maksimalnih ureditev (glede na inkluzijo) označimo s $\text{Spermax } A$.

2. Praideali in ureditve kolobarja $\mathcal{C}(X, \mathbb{R})$

Kolobar vseh zveznih funkcij, ki slikajo iz topološkega prostora X v $\mathbb{R}$, bomo označili s $\mathcal{C}(X, \mathbb{R})$. V tem razdelku bo X poljuben topološki prostor. Pokazali bomo, da vsakemu praidealu kolobarja $\mathcal{C}(X, \mathbb{R})$ pripada natanko ena ureditev tega kolobarja, ki ima dan praideal za svoj nosilec. Omenimo, da velja $\text{Spec } \mathcal{C}(X, \mathbb{R}) \neq \emptyset$ (vsak kolobar ima maksimalen ideal, ki je praideal), iz posplošenega Artin-Schreierjevega izreka 1 pa sledi, da je $\text{Sper } \mathcal{C}(X, \mathbb{R}) \neq \emptyset$.

Lema 3. Naj bo $\mathfrak{p} \subseteq \mathcal{C}(X, \mathbb{R})$ poljuben praideal in $n \in \mathbb{N}$. Če za elemente $f_1, \dots, f_n \in \mathcal{C}(X, \mathbb{R})$ velja $f_1^2 + \dots + f_n^2 \in \mathfrak{p}$, potem je $f_1, \dots, f_n \in \mathfrak{p}$.

Dokaz. Za $1 \leq i \leq n$ definiramo funkcijo

$$h_i(x) := \begin{cases} f_i(x) \frac{f_i(x)^2}{f_1(x)^2 + \dots + f_n(x)^2}, & f_1(x)^2 + \dots + f_n(x)^2 \neq 0 \\ 0, & f_1(x)^2 + \dots + f_n(x)^2 = 0 \end{cases}.$$

Če za $x \in X$ velja $f_1(x)^2 + \dots + f_n(x)^2 \neq 0$, potem za vsak $i \in \{1, \dots, n\}$ velja $0 \leq \frac{f_i(x)^2}{f_1(x)^2 + \dots + f_n(x)^2} \leq 1$. Ker so funkcije $f_1, \dots, f_n$ realne, iz $f_1(x)^2 + \dots + f_n(x)^2 = 0$ sledi $f_1(x) = \dots = f_n(x) = 0$. Ta premislek pokaže, da je $h_i \in \mathcal{C}(X, \mathbb{R})$ in velja $f_i^3 = h_i(f_1^2 + \dots + f_n^2) \in \mathfrak{p}$. Ker je $\mathfrak{p}$ praideal, sledi $f_i \in \mathfrak{p}$. ■

Izrek 4. *Obstaja naravna bijekcija $\Phi : \text{Sper } \mathcal{C}(X, \mathbb{R}) \rightarrow \text{Spec } \mathcal{C}(X, \mathbb{R})$, ki ureditvi $P \in \text{Sper } \mathcal{C}(X, \mathbb{R})$ priredi njen nosilec P^0 . Njena zožitev je bijekcija med $\text{Spermax } \mathcal{C}(X, \mathbb{R})$ in $\text{Specmax } \mathcal{C}(X, \mathbb{R})$.*

Dokaz. Preslikava Φ je definirana s predpisom $P \mapsto P^0$. Očitno je ta preslikava dobro definirana, pokazati pa moramo, da je bijektivna. V prvem koraku bomo pokazali surjektivnost, v drugem pa injektivnost te preslikave.

Korak 1. Za praideal $\mathfrak{p} \in \text{Spec } \mathcal{C}(X, \mathbb{R})$ je $P_{\mathfrak{p}} := \mathcal{C}(X, \mathbb{R})^2 + \mathfrak{p}$ ureditev z nosilcem $\mathfrak{p}$.

Očitno velja $P_{\mathfrak{p}} + P_{\mathfrak{p}} \subseteq P_{\mathfrak{p}}$ in $P_{\mathfrak{p}} \cdot P_{\mathfrak{p}} \subseteq P_{\mathfrak{p}}$. Za poljubno funkcijo $f \in \mathcal{C}(X, \mathbb{R})$ velja $(f - |f|)(f + |f|) = 0 \in \mathfrak{p}$, torej je $f - |f| \in \mathfrak{p}$ ali $f + |f| \in \mathfrak{p}$. Ker je vsaka nenegativna funkcija v $\mathcal{C}(X, \mathbb{R})$ kvadrat kakšne zvezne funkcije, smo s tem dokazali $f \in P_{\mathfrak{p}} \cup -P_{\mathfrak{p}}$. Vzemimo poljuben $f = a^2 + p = -b^2 - q \in P_{\mathfrak{p}} \cap -P_{\mathfrak{p}}$, kjer $a, b \in \mathcal{C}(X, \mathbb{R})$ in $p, q \in \mathfrak{p}$. Tedaj je $a^2 + b^2 = -p - q \in \mathfrak{p}$ in po prejšnji lemi $a, b \in \mathfrak{p}$. Sledi $P_{\mathfrak{p}} \cap -P_{\mathfrak{p}} \subseteq \mathfrak{p}$. Obratna inkluzija je trivialna.

Korak 2. Za poljubno ureditev P kolobarja $\mathcal{C}(X, \mathbb{R})$ obstaja natanko en praideal $\mathfrak{p} \subseteq \mathcal{C}(X, \mathbb{R})$, da velja $P = P_{\mathfrak{p}}$.

Naj bo $\mathfrak{p} := P^0$ nosilec ureditve P . Trdimo, da je $P = P_{\mathfrak{p}} (= \mathcal{C}(X, \mathbb{R})^2 + \mathfrak{p})$. Ker je $\mathcal{C}(X, \mathbb{R})^2 \subseteq P$ in $\mathfrak{p} = P^0 \subseteq P$, je $P_{\mathfrak{p}} \subseteq P$. Denimo, da je $P_{\mathfrak{p}} \subsetneq P$. Tedaj obstaja element $f \in P \setminus P_{\mathfrak{p}}$. Iz definicije ureditve sledi $-f \in P_{\mathfrak{p}} \subseteq P$. Torej je $f \in P^0 = \mathfrak{p} \subseteq P_{\mathfrak{p}}$, kar je očitno protislovje.

S tem smo dokazali, da je preslikava Φ bijektivna. Dostavek o maksimalnih spektrih je očiten. ■

3. Spektralni prostori in spektra kolobarja $\mathcal{C}(X, \mathbb{R})$

Realna algebra in (realna) algebraična geometrija si pogosto pomagata s splošno topologijo. Prostori, ki jih tukaj srečujemo, so si zelo podobni. Zato vpeljemo posebno kategorijo topoloških prostorov in preslikav med njimi.

Definicija 5. Topološki prostor X imenujemo *spektralen*, če velja:

1. X je kompakten T_0 prostor¹.
2. Presek dveh odprtih kompaktnih množic je kompaktna množica.
3. Odprte kompaktne množice so baza topologije.
4. Vsaka neprazna zaprta nerazcepna podmnožica ima generično točko.

Zvezna preslikava $f : X \rightarrow Y$ med dvema spektralnima prostoroma je *spektralna*, če je praslika poljubne odprte kompaktne množice kompaktna.

Na vsakem spektralnem prostoru lahko uvedemo še eno topologijo, ki nam pogosto rabi kot tehničen pripomoček.

¹ Topološki prostor X je T_0 , če za poljubni različni točki $x, y \in X$ velja $x \notin \overline{\{y\}}$ ali $y \notin \overline{\{x\}}$.

Definicija 6. Naj bo X spektralni prostor.

- (a) S $\mathcal{K}(X)$ označimo družino množic, ki jih dobimo iz odprtih kompaktnih podmnožic prostora X z naslednjimi operacijami: končnimi unijami, končnimi preseki in komplementi. Elemente $\mathcal{K}(X)$ imenujemo *konstruktibilne* množice. S $\mathcal{K}^\circ(X)$ označimo množico odprtih konstruktibilnih množic, $\bar{\mathcal{K}}(X)$ pa je množica zaprtih konstruktibilnih množic.
- (b) $\mathcal{K}(X)$ je baza *konstruktibilne* topologije na X . Ta topologija ima za podbazo zaprtih množic natanko zaprte množice in kompaktne odprte množice v osnovni topologiji prostora X .

Kadar spektralni prostor X opremimo s konstruktibilno topologijo, ga označimo s X_{kon} , osnovno topologijo pa imenujemo *spektralna*.

Literatura o spektralnih prostorih je zelo obširna, glej npr. [6], [10] in [11]. Zato bomo daljše in zahtevnejše dokaze v tem poglavju izpuščali. Nekaj osnovnih lastnosti spektralnih prostorov smo strnili v naslednji izrek.

Izrek 7. *Naj bo X spektralni prostor. Potem je X_{kon} kompakten, Hausdorffov in povsem nepovezan. Identična preslikava $X_{\text{kon}} \rightarrow X$ je spektralna in $(X_{\text{kon}})_{\text{kon}} = X_{\text{kon}}$. Množica odprtih kompaktnih podmnožic v X je ravno $\mathcal{K}^\circ(X)$.*

Iz zadnjega izreka lahko izpeljemo, da je preslikava $f : X \rightarrow Y$ spektralna natanko tedaj, ko sta preslikavi $f : X \rightarrow Y$ in $f : X_{\text{kon}} \rightarrow Y_{\text{kon}}$ zvezni.

Kot smo že prej omenili, si algebraična geometrija pogosto pomaga s topologijo. Na oba prej definirana spektra bomo vpeljali topologijo in si ogledali lastnosti teh topologij.

Definicija 8. Vsakemu elementu f kolobarja A priredimo tri množice: $D(f) := \{\mathfrak{p} \in \text{Spec } A \mid f \notin \mathfrak{p}\}$, $U(f) := \{P \in \text{Sper } A \mid f \in P^+\}$ in $Z(f) := \{P \in \text{Sper } A \mid f \in P^0\}$. Množica $\{D(f) \mid f \in A\}$ je podbaza *spektralne* topologije na $\text{Spec } A$, množica $\{U(f) \mid f \in A\}$ je podbaza *spektralne* topologije na $\text{Sper } A$, $\{U(f), Z(g) \mid f, g \in A\}$ pa je podbaza *konstruktibilne* topologije na $\text{Sper } A$.

Naslednji izrek nakazuje, zakaj so spektralni prostori tako pomembni v (realni) algebraični geometriji. Dokaz prve trditve (o spektru) izreka 9 lahko najdemo v [6], dokaz trditve o realnem spektru pa v [1], [10] in [11].

Izrek 9. *Za poljuben kolobar A sta $\text{Spec } A$ in $\text{Sper } A$ spektralna prostora.*

V svojem članku [6] je Hochster dokazal, da so spektri kolobarjev natanko vsi spektralni prostori; za vsak spektralni prostor X obstaja kolobar A , da velja $X \approx \text{Spec } A$. Analogna trditev za realni spekter ne velja, kot je dokazano v [10].

Definicija 10. V poljuben T_0 topološki prostor X lahko vpeljemo delno urejenost $\leq$ s predpisom $x \leq y \Leftrightarrow y \in \overline{\{x\}}$.

Trditev 11. Za kolobar A velja:

- (a) če je $X = \text{Spec } A$, potem za točki $p, q \in X$ velja $p \leq q \Leftrightarrow p \subseteq q$.
- (b) če je $X = \text{Sper } A$, potem za točki $P, Q \in X$ velja $P \leq Q \Leftrightarrow P \subseteq Q$.

Dokaz. Dokaza sta povsem analogna; kot zgled bomo dokazali točko (b). Velja: $P \leq Q$ natanko tedaj, ko $Q \in \overline{\{P\}}$, natanko tedaj, ko za vsak $f \in A$ iz $Q \in U(f)$ sledi $P \in U(f)$. To je ekvivalentno zahtevi, da za vsak $g \in A$ z lastnostjo $g \in P$ velja $g \in Q$ oziroma $P \subseteq Q$. ■

Naslednja trditev nam pogosto pomaga pri dokazovanju homeomorfnosti dveh spektralnih prostorov. V dokazu trditve bomo potrebovali pomožen rezultat.

Lema 12. Naj bo X spektralni prostor in Y zaprta podmnožica v X_{kon} . Potem je zaprtje $\overline{Y}$ množice Y v spektralni topologiji enako $\bigcup_{y \in Y} \overline{\{y\}}$.

Dokaz. Netrivialna je le inkluzija $\subseteq$. Vzemimo poljuben $z \in \overline{Y}$. Ker ima spektralni prostor bazo iz kompaktnih odprtih množic, ima z bazo kompaktnih odprtih okolic $\{U_\lambda \mid \lambda \in \Lambda\}$. Vsaka okolica točke z ima neprazen presek z množico Y . Če je $\bigcap_{\lambda \in \Lambda} (U_\lambda \cap Y) = \emptyset$, potem je presek zaprtih množic (v konstruktibilni topologiji), ki so vsebovane v kompaktnem prostoru Y , prazna množica. To pomeni, da je že presek končne poddružine prazen: $(U_1 \cap U_2 \cap \dots \cap U_n) \cap Y = \emptyset$. Prišli smo v protislovje, saj je $U_1 \cap \dots \cap U_n$ okolica točke $z \in \overline{Y}$. Za poljubno točko $y \in \bigcap_{\lambda \in \Lambda} (U_\lambda \cap Y)$ velja $z \in \overline{\{y\}}$. ■

Trditev 13. Če je $f : X \rightarrow Y$ spektralna preslikava, ki je urejenostni izomorfizem, potem je f homeomorfizem.

Dokaz. Iz predpostavk sledi, da je preslikava $f : X_{\text{kon}} \rightarrow Y_{\text{kon}}$ zvezna bijekcija, ki slika iz kompaktnega prostora X_{kon} v Hausdorffov prostor Y_{kon} . Zato je $f : X_{\text{kon}} \rightarrow Y_{\text{kon}}$ homeomorfizem (in v posebnem zaprta preslikava). Množica $Z \subseteq X$ je zaprta v spektralni topologiji natanko takrat, ko je zaprta v konstruktibilni topologiji in velja $z \in Z \Rightarrow \overline{\{z\}} \subseteq Z$ (implikacija v desno je trivialna, implikacija v levo pa sledi iz prejšnje leme). Vzemimo poljubno zaprto množico $Z \subseteq X$. Potem je $f(Z)$ zaprta podmnožica v Y_{kon} . Pokažimo še, da vsebuje zaprtja svojih točk. Če to ni res, potem obstaja točka $y = f(x) \in f(Z)$, za katero je presek $\overline{\{y\}} \cap (Y \setminus f(Z))$ neprazen. Naj bo w poljubna točka iz tega preseka. Potem je $y \leq w$ in iz izotonosti preslikave f^{-1} sledi $x = f^{-1}(y) \leq f^{-1}(w)$, oziroma $f^{-1}(w) \in \overline{\{x\}} \subseteq Z$. Dobimo $w \in f(Z)$ kar je protislovje. S tem smo dokazali, da je $f : X \rightarrow Y$ zvezna zaprta bijekcija, torej homeomorfizem. ■

V spektralnem prostoru X je zanimiv tudi podprostor $X^{\max}$ njegovih zaprtih točk. Za $X = \text{Spec } A$ pišemo $X^{\max} = \text{Specmax } A$, za $X = \text{Sper } A$ pa $X^{\max} = \text{Spermax } A$ (ta zapis je upravičen po trditvi 11).

Trditev 14. *Vzemimo poljuben kompakten T_0 topološki prostor X in njegov podprostor zaprtih točk $X^{\max}$. Potem je $X^{\max}$ kompakten in za vsak $x \in X$ velja $\overline{\{x\}} \cap X^{\max} \neq \emptyset$.*

Dokaz. Zadošča dokazati $\overline{\{x\}} \cap X^{\max} \neq \emptyset$ za vsak $x \in X$ (tedaj je X edina odprta okolica množice $X^{\max}$). Za poljuben $x \in X$ naj bo $Y := \overline{\{x\}}$. V Y imamo naravno delno urejenost $x_1 \leq x_2 \Leftrightarrow x_2 \in \overline{\{x_1\}}$. Ker je Y kompakten, za vsako linearno urejeno podmnožico M v Y velja $\bigcap_{y \in M} \overline{\{y\}} \neq \emptyset$. Po Zornovi lemi ima Y maksimalen element. ■

Posledica 15. *Za poljuben kolobar A je prostor maksimalnih idealov $\text{Specmax } A$ kompakten.*

Trditev 16. *Za poljuben kolobar A je prostor maksimalnih ureditev $\text{Spermax } A$ kompakten in Hausdorffov.*

Dokaz. Kompaktnost sledi iz prejšnje trditve, torej moramo dokazati le še, da je izpolnjen T_2 aksiom. Vzemimo dve različni ureditvi $P, Q \in \text{Spermax } A$. Potem je $P \not\subseteq Q$ in $Q \not\subseteq P$. Obstajata elementa $a \in P \setminus Q$ in $b \in Q \setminus P$. Tvorimo $f := a - b$. Ker je $-a \in Q$ in $-b \in P$, je $f \in P$ in $-f \in Q$. Sledi $P \in U(f)$ in $Q \in U(-f)$. To sta iskani disjunktni okolici točk P in Q , saj je $U(f) \cap U(-f) = \emptyset$. ■

Tukaj opazimo prvo pomembno razliko med spektrom in realnim spektrom kolobarja. V primeri s $\text{Spermax } A$ maksimalni spekter $\text{Specmax } A$ ni nujno Hausdorffov topološki prostor (je pa vselej T_1 , saj je sestavljen le iz zaprtih točk).

Ponovno se vrnimo k študiju kolobarja $\mathcal{C}(X, \mathbb{R})$. V drugem razdelku smo našli naravno bijekcijo med spektrom in realnim spektrom tega kolobarja. Ni presenetljivo, da je ta preslikava celo homeomorfizem.

Izrek 17. *Preslikava $\Phi : \text{Sper } \mathcal{C}(X, \mathbb{R}) \rightarrow \text{Spec } \mathcal{C}(X, \mathbb{R})$, ki ureditev $P \in \text{Sper } \mathcal{C}(X, \mathbb{R})$ pošlje v njen nosilec P^0 , je homeomorfizem. Zožitev te preslikave je homeomorfizem med $\text{Spermax } \mathcal{C}(X, \mathbb{R})$ in $\text{Specmax } \mathcal{C}(X, \mathbb{R})$.*

Dokaz. Za poljuben $f \in \mathcal{C}(X, \mathbb{R})$ je $\Phi^{-1}(D(f)) = U(f^2)$, torej je Φ zvezna preslikava. Kompaktne množice v $\text{Spec } \mathcal{C}(X, \mathbb{R})$ so natanko množice oblike $D(f_1) \cup \dots \cup D(f_r)$ za $r \in \mathbb{N}$ in $f_i \in \mathcal{C}(X, \mathbb{R})$. Ker so množice oblike $U(f)$ kompaktne v $\text{Sper } \mathcal{C}(X, \mathbb{R})$, je preslikava Φ spektralna. Pokažimo še, da je urejenostni izomorfizem. Če je $P_p \subseteq P_q$, potem je $p = P_p^0 \subseteq P_q^0 = q$, kar pomeni, da je Φ izotona preslikava. Očitno je tudi Φ^{-1}

izotona preslikava, saj praideal $\mathfrak{p}$ pošlje v $\mathcal{C}(X, \mathbb{R})^2 + \mathfrak{p}$. Po trditvi 13 je Φ homeomorfizem. Dostavek o zožitvi je trivialen, saj zvezna preslikava $\Phi^{-1}|_{\text{Specmax } \mathcal{C}(X, \mathbb{R})}$ slika kompakten prostor $\text{Specmax } \mathcal{C}(X, \mathbb{R})$ injektivno na Hausdorffov prostor $\text{Spermax } \mathcal{C}(X, \mathbb{R})$. ■

4. Stone-Čechova kompaktifikacija

Kolobar zveznih realnih funkcij $\mathcal{C}(X, \mathbb{R})$ je lahko zelo majhen, če topološki prostor X ni dovolj „lep“. Če ima X npr. trivialno topologijo, so edine funkcije v $\mathcal{C}(X, \mathbb{R})$ konstante. Če pa X opremimo z diskretno topologijo, je $\mathcal{C}(X, \mathbb{R})$ kar množica vseh funkcij iz X v $\mathbb{R}$. Obstajajo pa tudi razmeroma zapleteni regularni topološki prostori, kjer so edine zvezne realne funkcije konstantne. Bralec si lahko primer takšnega prostora ogleda v [3].

Definicija 18. Topološki prostor X je *popolnoma regularen* (včasih tudi prostor *Tihonova* ali $T_{3\frac{1}{2}}$), če je T_0 in za vsako točko $x \in X$ in njej disjunktno zaprto množico $F \subseteq X$ obstaja taka zvezna funkcija $f : X \rightarrow [0, 1]$, da je $f(x) = 0$ in $f(F) = \{1\}$.

Iz definicije in Urysohnove leme sledi, da je vsak normalen prostor popolnoma regularen. Zaradi prej opisanih težav se pri študiju kolobarja zveznih realnih funkcij pogosto omejimo na popolnoma regularne topološke prostore X . Vendar to ni zelo huda omejitev. Kot sta dokazala Gillman in Jerison v [4], za vsak topološki prostor X obstajata popolnoma regularen topološki prostor Y in takšna zvezna surjekcija $\varphi : X \rightarrow Y$, da je preslikava $g \mapsto g \circ \varphi : \mathcal{C}(Y, \mathbb{R}) \rightarrow \mathcal{C}(X, \mathbb{R})$ izomorfizem kolobarjev.

Preprosta uporaba Urysohnove leme nam pokaže, da je vsak podprostor kompaktnega Hausdorffovega prostora popolnoma regularen. Velja pa tudi obrat. Vsakemu popolnoma regularnemu prostoru X lahko pripišemo kompakten Hausdorffov prostor βX , v katerem je X gost podprostor. Prostoru βX pravimo Stone-Čechova kompaktifikacija prostora X . V literaturi obstaja mnogo konstrukcij te kompaktifikacije; glej npr. [3] in [4]. Naslednji izrek je karakterizacija Stone-Čechove kompaktifikacije.

Izrek 19. *Naj bo X popolnoma regularen in Y poljuben kompakten Hausdorffov topološki prostor.*

- (a) *Vsako zvezno funkcijo $f : X \rightarrow Y$ je možno razširiti do zvezne funkcije $F : \beta X \rightarrow Y$.*
- (b) *Če je cX takšna Hausdorffova kompaktifikacija prostora X , da je vsako zvezno funkcijo $X \rightarrow Y$ možno razširiti do zvezne funkcije $cX \rightarrow Y$, potem je cX ekvivalentna Stone-Čechovi kompaktifikaciji βX .*

V nadaljevanju bomo nakazali povezavo med Stone-Čechovo kompaktifikacijo popolnoma regularnega prostora X in realno algebro.

Za vsak $x \in X$ definiramo množico $\mathcal{M}_x := \{f \in \mathcal{C}(X, \mathbb{R}) \mid f(x) = 0\}$. Očitno je $\mathcal{M}_x$ ideal v kolobarju $\mathcal{C}(X, \mathbb{R})$ in $\mathcal{C}(X, \mathbb{R})/\mathcal{M}_x \cong \mathbb{R}$. V posebnem je $\mathcal{M}_x \in \text{Specmax}\mathcal{C}(X, \mathbb{R})$. Tako dobimo preslikavo $j : X \rightarrow \text{Spermax}\mathcal{C}(X, \mathbb{R})$, ki točki x priredi ureditev $P_{\mathcal{M}_x} = \mathcal{C}(X, \mathbb{R})^2 + \mathcal{M}_x$. Velja $P_{\mathcal{M}_x} = \{f \in \mathcal{C}(X, \mathbb{R}) \mid f(x) \geq 0\}$, $P_{\mathcal{M}_x}^0 = \mathcal{M}_x$ in zato $P_{\mathcal{M}_x}^+ = \{f \in \mathcal{C}(X, \mathbb{R}) \mid f(x) > 0\}$.

Izrek 20. *Naj bo X popolnoma regularen topološki prostor.*

- (a) *Preslikava $j : X \rightarrow \text{Spermax}\mathcal{C}(X, \mathbb{R})$ je vložitev.*
- (b) *Slika $j(X)$ je gosta podmnožica v $\text{Spermax}\mathcal{C}(X, \mathbb{R})$.*
- (c) *$\text{Spermax}\mathcal{C}(X, \mathbb{R})$ je Stone-Čechova kompaktifikacija prostora X .*

Dokaz tega izreka je razmeroma zapleten in ga bomo izpustili. Za konec le še omenimo, da kot posledico izrekov 17 in 20 dobimo znan rezultat iz topologije in zanimivo karakterizacijo kompaktnih Hausdorffovih prostorov.

Posledica 21. *Za poljuben popolnoma regularen topološki prostor X je spekter maksimalnih idealov $\text{Specmax}\mathcal{C}(X, \mathbb{R})$ homeomorfen Stone-Čechovi kompaktifikaciji βX .*

Posledica 22. *Za topološki prostor X so naslednje trditve ekvivalentne:*

- 1. *X je kompakten in Hausdorffov.*
- 2. *X je homeomorfen $\text{Specmax}\mathcal{C}(X, \mathbb{R})$.*
- 3. *X je homeomorfen $\text{Spermax}\mathcal{C}(X, \mathbb{R})$.*

LITERATURA

- [1] J. Bochnak, M. Coste, M. F. Roy, *Géométrie Algébrique Réelle*, Springer-Verlag, 1987.
- [2] J. Cimprič, *Izrek o pozitivnosti*, Obzornik Mat. Fiz. **46** (1999) 75–82.
- [3] R. Engelking, *General Topology*, PWN – Polish Scientific Publisher, 1977.
- [4] L. Gillman, M. Jerison, *Rings of Continuous Functions*, D. Van Nostrand Publ. Co, 1960.
- [5] E. Hewitt, *Rings of real-valued continuous functions I*, Trans. Amer. Math. Soc. **64** (1948) 54–99.
- [6] M. Hochster, *Prime ideal structure in commutative rings*, Trans. Amer. Math. Soc. **142** (1969) 43–60.
- [7] I. Klep, *Homogeni izrek o pozitivnosti*, Diplomsko delo, 2001.
- [8] B. Lavrič, *Delno urejene grupe in delno urejeni kolobarji*, DMFA, 1993.
- [9] B. Lavrič, *Delno urejeni vektorski prostori*, DMFA, 1995.
- [10] M. Knebusch, C. Scheiderer, *Einführung in die Reele Algebra*, Vieweg & Sohn, 1989.
- [11] M. Marshall, *Spaces of Orderings and Abstract Real Spectra*, Springer-Verlag, 1996.
- [12] A. Prestel, C. N. Delzell, *Positive Polynomials*, Springer-Verlag, 2001.

VERJETNOST ZAPOREDNIH ŠTEVIL V DOBITNI KOMBINACIJI LOTA*

STANLEY P. GUDDER, JAMES N. HAGLER,
prev. in prir. MARJAN JERMAN

Math. Subj. Class. (2000): 60C05

Dobitna kombinacija pri lotu precej pogosto vsebuje dve zaporedni številki. V članku izračunamo verjetnost tega dogodka in jo primerjamo z empiričnimi podatki. Poleg tega obravnavamo nekatera vprašanja, ki se pojavijo pri tem.

PROBABILITIES OF CONSECUTIVE INTEGERS IN LOTTO

We observe that, quite often, the winning numbers in a lotto game of the form “pick m numbers between 1 and n ” contain two consecutive integers. Probabilities of this and related events are computed and compared with empirical results. Further, we show the following using only calculus: for a given n , the smallest n which gives probability greater than or equal to $1/2$ that at least two of the numbers are consecutive is about $\sqrt{n/\ln 2}$.

1. Uvod

Pri slovenskem lotu so v bobnu kroglice, ki so označene s števili od 1 do 39. Med stalnim mešanjem iz bobna naključno odpihne sedem kroglic in še eno rezervno za primer, če ni glavnega dobitka – „sedmice”. V našem članku se bomo ukvarjali zgolj s prvimi sedmimi kroglicami. Žrebanje poteka vsak teden. Glavni dobitek je večji v primeru, če v prejšnjih kolih ni bilo glavnega dobitka. Kadar dobitno kombinacijo ugame več igralcev, se nagrada razdeli med njimi. Verjetnost glavnega dobitka je zelo majhna, enaka je

$$1 / \binom{39}{7} = 1/15\,380\,937.$$

Statistični podatki za pretekla leta (po viru [7]) kažejo, da je zelo velika verjetnost, da se v dobitni kombinaciji pojavita dve zaporedni števili, npr. 31. 12. 2000 je bila dobitna kombinacija 5, 7, 14, 15, 19, 30, 37. Podatki za leta 1998–2001 kažejo, da je bilo v 208 žrebanjih kar 143 (69 %) kombinacij z vsaj dvema zaporednima številoma. Natančneje: bilo je 91 (43 %) kombinacij z natanko enim parom, 45 (22 %) z dvema paroma, šest (3 %) s tremi pari in ena (0,5 %) kombinacija s štirimi pari zaporednih števil.

Za primer navedimo še enega od ameriških lotov, loterijo v zvezni državi Colorado. Tam izmed 42 kroglic izvlečejo dobitno kombinacijo šestih števil. Vsak teden sta dve koli. Verjetnost glavnega dobitka je

$$1 / \binom{42}{6} = 1/5\,245\,786.$$

* Prispevek je prevod članka *Probabilities of Consecutive Integers in Lotto*, Mathematics Magazine **74**, junij 2001, str. 216–222. Prevedel ga je Marjan Jerman, ki ga je tudi dopolnil s podatki iz slovenskega lota.

Statistika za leta 1996–1998 pove, da so v 312 žrebanjih izvlekli 164 (53 %) kombinacij z vsaj enim parom zaporednih števil. V 121 (39 %) primerih sta bila v dobitni kombinaciji po dva para, v preostalih 14 % pa več kot dva para zaporednih števil.

Ker torej loterije nimajo enakih pravil, si bomo ogledali igro lota tipa (n, m) , kjer je dobitna kombinacija podmnožica z m elementi množice $\{1, \dots, n\}$. Najprej bomo teoretično izračunali, kolikšna je verjetnost dveh zaporednih števil v dobitni kombinaciji (trditev 1). Potem bomo ugotovili, da je pri loteriji tipov $(39, m)$ in $(42, m)$ šestica najkrajša dolžina kombinacije, pri kateri je verjetnost, da se pojavita zaporedni števili, še večja od polovice. Če bi šli opazovat še druge tipe loterij, bi lahko domnevali, da ta dolžina približno raste s $\sqrt{n}$. V izreku 5 bomo pokazali, da ta domneva „skoraj drži“.

Naš problem je soroden problemu razporeditve rojstnih dnevor, ki sta ga obravnavala Abrahamson in Moser ([1]). Izračunala sta, kolikšna je verjetnost, da nobena dva rojstna datuma skupine n ljudi nista za k dni narazen. Zelo zanimiva knjiga, ki sta jo napisala Henze in Riedwyl ([4]) pa opisuje strategijo, kako se izogniti delitvi glavnega dobitka (če ga seveda zadanemo). V knjigi je tudi veliko statističnih analiz preteklih iger lota. Naše delo se pokriva s Henzejevim ([3]), kjer je obravnavano pojavljanje vrzeli med števili v dobitnih kombinacijah lota.

2. Verjetnosti pri lotu

Igra lota tipa (n, m) je igra, kjer je zmagovalna kombinacija podmnožica A v $\{1, \dots, n\}$, ki ima m elementov. V tem primeru pravimo, da je A m -podmnožica in pišemo $A = \{a_1, a_2, \dots, a_m\}$. Hkrati bomo privzeli, da je kombinacija urejena po velikosti: $a_1 < a_2 < \dots < a_m$. Če A vsebuje vsaj dve zaporedni števili, bomo rekli, da je A *zaporedna* (v nasprotnem primeru *nezaporedna*) m -podmnožica. Naj $K(n, m)$ in $N(n, m)$ zaporedoma označujeta število zaporednih in nezaporednih m -podmnožic. Verjetnost $P(n, m)$, da je naključno izbrana m -podmnožica zaporedna, je

$$P(n, m) = K(n, m) / \binom{n}{m}.$$

Pri koloradskem lotu je na primer

$$P(42, 6) = K(42, 6) / \binom{42}{6},$$

pri nas pa

$$P(39, 7) = K(39, 7) / \binom{39}{7}.$$

Verjetnost $P(n, m)$ bomo torej našli, če bomo poznali število $K(n, m)$. To sploh ni tako enostavno, kot je videti na prvi pogled. Bralca vabimo, da poskuša število $K(n, m)$ izračunati, preden prebere rešitev. Rezultat (trditev 1) je znan (glej recimo [2, str. 30] ali [5, primer 4c, str. 7]). To je tudi začetni rezultat v Henzejevi knjigi [3], v kateri študira vrzeli v dobitnih kombinacijah lota.

Kot je pogosto pri kombinatoričnih problemih, je lažje najti število $N(n, m)$ in nato uporabiti zvezo

$$K(n, m) = \binom{n}{m} - N(n, m).$$

Seveda v primeru $m > (n+1)/2$ velja $N(n, m) = 0$. Zato lahko privzamemo, da velja $m \leq (n+1)/2$. Podobno sta trivialna primera, ko je $m = 0$ ali $m = 1$, zato lahko privzamemo, da je $m \geq 2$. Dogovorimo se, da je $\binom{r}{j} = 0$ v primerih, ko je $j > r$ ali $r < 0$.

Trditev 1.

$$N(n, m) = \binom{n-m+1}{m}$$

Dokaz. Poiskali bomo bijekcijo med množico m -podmnožic množice

$$\{1, \dots, n-m+1\},$$

katere moč je $\binom{n-m+1}{m}$, in nezaporednimi m -podmnožicami v $\{1, \dots, n\}$. Če je $\{a_1, a_2, \dots, a_m\}$ m -podmnožica v $\{1, \dots, n-m+1\}$, je

$$\{a_1, a_2 + 1, \dots, a_m + m - 1\}$$

nezaporedna m -podmnožica v $\{1, \dots, n\}$. Ta prireditev je jasno bijektivna. ■

Po trditvi 1 je tako

$$K(n, m) = \binom{n}{m} - \binom{n-m+1}{m}. \quad (1)$$

Pri lotu tipa (42, 6) je

$$P(42, 6) = 1 - \binom{37}{6} / \binom{42}{6} \approx 0,557,$$

pri lotu tipa (39, 7) pa je

$$P(39, 7) = 1 - \binom{33}{7} / \binom{39}{7} \approx 0,722.$$

Statistični podatki dajo pri lotu tipa (42, 6) delež 53 %, pri lotu tipa (39, 7) pa 69 %. Idejo v zadnjem dokazu lahko posplošimo in tako dobimo formulo za primer daljših vrzeli med števili v kombinaciji. Rekli bomo, da ima m -podmnožica A v $\{1, \dots, n\}$ vrzeli dolžine vsaj k , če je

$$a_{j+1} - a_j \geq k + 1 \quad \text{za } j = 1, \dots, m - 1.$$

Dokaz trditve 1 se da enostavno posplošiti (glej [3]). Tako dobimo naslednji rezultat.

Trditev 2. Število m -podmnožic v množici $\{1, \dots, n\}$, ki imajo med pari izžrebanih števil vrzeli dolžine vsaj k , je

$$\binom{n - km + k}{m}.$$

Trditev 1 je začetni korak pri izračunu verjetnosti dogodkov, povezanih s porazdelitvijo števil v dobitni kombinaciji. Rekli bomo, da sta v m -podmnožici A v $\{1, \dots, n\}$ natanko dve zaporedni števili, če za neki $k < m$ velja

$$a_k + 1 = a_{k+1} \quad \text{in} \quad a_j + 1 < a_{j+1} \quad \text{za } j \neq k.$$

Naslednji rezultat nam pove, koliko je takih množic.

Trditev 3. Število m -podmnožic v $\{1, \dots, n\}$ z natanko dvema zaporednima številoma je

$$(m - 1) \binom{n - m + 1}{m - 1}.$$

Dokaz. Iz vsake nezaporedne $(m - 1)$ -podmnožice $A = \{a_1, \dots, a_{m-1}\}$ v $\{1, \dots, n - 1\}$ lahko dobimo naslednjih $m - 1$ m -podmnožic z natanko dvema zaporednima številoma:

$$\begin{aligned} &\{a_1, a_1 + 1, a_2 + 1, \dots, a_{m-1} + 1\}, \\ &\{a_1, a_2, a_2 + 1, a_3 + 1, \dots, a_{m-1} + 1\}, \\ &\vdots \\ &\{a_1, a_2, \dots, a_{m-1}, a_{m-1} + 1\}. \end{aligned}$$

Lahko je videti, da se da vsaka m -podmnožica z dvema zaporednima številoma zapisati na natanko enega od zgornjih načinov. Ker vsaka množica A generira $m - 1$ takih množic, je njihovo skupno število

$$\begin{aligned} (m-1)N(n-1, m-1) &= (m-1) \binom{(n-1) - (m-1) + 1}{m-1} = \\ &= (m-1) \binom{n-m+1}{m-1}. \end{aligned} \quad \blacksquare$$

Pri lotu tipa (42, 6) je verjetnost, da se v dobitni kombinaciji pojavita natanko dve zaporedni števili, enaka

$$5 \binom{37}{5} / \binom{42}{6} \approx 0,415,$$

pri lotu tipa (39, 7) pa je ta verjetnost

$$6 \binom{33}{6} / \binom{39}{7} \approx 0,432.$$

(V praksi sta bila ustrezna deleža 39 % in 43 %.)

Definicijo in trditev lahko enostavno razširimo za primer r zaporednih števil. Bralca vabimo, da dokaže naslednji rezultat tako, da oponaša dokaz trditve 3.

Trditev 4.

(a) Število m -podmnožic v množici $\{1, \dots, n\}$ z natanko r zaporednimi števili je

$$(m-r+1) \binom{n-m+1}{m-r+1}.$$

(b) Število m -podmnožic v množici $\{1, \dots, n\}$ z natanko dvema ločenima paroma zaporednih števil je

$$\binom{m-2}{2} \binom{n-m+1}{m-2}.$$

Pri lotu tipa (42, 6) je verjetnost treh zaporednih števil v dobitni kombinaciji enaka

$$4 \binom{37}{4} / \binom{42}{6} \approx 0,050,$$

kar se zelo dobro ujema z izmerjenim rezultatom 17/312 (5,5 %).

Verjetnost dveh ločenih parov zaporednih števil pa je

$$\binom{4}{2} \binom{37}{4} / \binom{42}{6} \approx 0,076.$$

Izmerjen rezultat je 18/312 (5,8 %).

Bralca vabimo, da izračuna ustrezne teoretične in praktične deleže še za naš sistem lota.

3. Mejna števila

Problem rojstnih dni ([5, Primer 5j, str. 40]) sprašuje, kako velika mora biti skupina ljudi, da ima dogodek, ko imata vsaj dve osebi v skupini rojstni dan na isti dan v letu, verjetnost vsaj $1/2$. Podobno razmišljanje lahko naredimo za igro lota tipa (n, m) . V tem primeru se vprašamo, kolikšna mora biti pri fiksnem številu n dolžina dobitne kombinacije m , da je z verjetnostjo vsaj $1/2$ zaporedna. Zanimivo je, da je možno potrebno dolžino napisati skoraj kot zaključen izraz v spremenljivki n samo s pomočjo elementarne analize.

V preteklih računih smo opazili, da je v pri lotu tipa $(42, 6)$ verjetnost, da je dobitna kombinacija zaporedna, več kot $1/2$. Kaj pa, če bi vzeli krajše dobitne kombinacije dolžine pet? Vemo, da je

$$P(42, 5) = 1 - \binom{38}{5} / \binom{42}{5} = 0,41 < 1/2,$$

zato pravimo da je 6 $1/2$ -mejno število v primeru $n = 42$. Nasploh bomo rekli, da je m mejno število za n , če je m najmanjše število, za katero je $P(n, m) > 1/2$. To mejno število bomo označili s $T(n)$. V naslednji tabeli je navedenih nekaj mejnih števil:

n	5	10	12	39	42	49	100	116	10^3	10^4	10^5	10^6
$T(n)$	3	3	4	6	6	7	9	10	27	84	264	833

Če pogledamo tabelo, lahko domnevamo, da so števila $T(n)$ reda velikosti $\sqrt{n}$. Ali obstaja kakšen zaključen izraz za $T(n)$?

Iščemo najmanjše takšno število m , da bo $K(m, n) / \binom{n}{m} > 1/2$. Ta pogoj je po (1) ekvivalenten neenakosti

$$\binom{n-m+1}{m} / \binom{n}{m} < \frac{1}{2}. \quad (2)$$

Ko neenakost razpišemo po faktorjih, dobimo

$$\frac{n-m}{n} \cdot \frac{n-m-1}{n-1} \cdot \dots \cdot \frac{n-m-(m-2)}{n-(m-2)} < \frac{1}{2}. \quad (3)$$

Leva stran v izrazu (3) ima $m-1$ faktorjev, ki padajo od leve proti desni. Zato neenakost (3) zagotovo drži v primeru, ko je

$$\frac{n-m}{n} \leq 2^{-1/(m-1)}, \quad (4)$$

kar je ekvivalentno zahtevi

$$n(2^{1/(m-1)} - 1) \leq m 2^{1/(m-1)}. \quad (5)$$

Ker približno velja $2^{1/(m-1)} \approx 1 + \frac{\ln 2}{m-1}$, lahko neenakost (5) *približno* prevedemo na

$$\frac{n}{m-1} \ln 2 \leq m \left(1 + \frac{\ln 2}{m-1}\right). \quad (6)$$

Iz (6) dobimo

$$n \ln 2 \leq m^2 - m(1 - \ln 2) \leq m^2.$$

Zato je $\sqrt{n \ln 2} \leq m$, in ker je m celo število, tudi $\lceil \sqrt{n \ln 2} \rceil \leq m$. Pri tem $\lceil \cdot \rceil$ označuje zaokroževanje navzgor.

Glede na zgornji hevristični izračun lahko domnevamo, da je najkrajša mejna dolžina dobitne kombinacije $m = S(n) = \lceil \sqrt{n \ln 2} \rceil$. Ta domneva je pravilna za zelo veliko števil n . Pravilna je recimo za vsa števila v zgornji tabeli razen za $n = 5, 12, 49, 116$. Za te vrednosti je

$$\begin{aligned} S(5) &= 2 < 3 = T(5); & S(12) &= 3 < 4 = T(12); \\ S(49) &= 6 < 7 = T(49); & S(116) &= 9 < 10 = T(116). \end{aligned}$$

Zdi se, da naša domneva od pravilnega rezultata odstopa kvečjemu za 1. V naslednjem izreku bomo dokazali tako popravljeno domnevo:

Izrek 5. *Za mejno funkcijo $T(n)$ velja*

$$\left| T(n) - \lceil \sqrt{n \ln 2} \rceil \right| \leq 1.$$

Opomba 6. Izrek 5 bi lahko izostrili in pokazali, da je $T(n)$ bodisi $\lceil \sqrt{n \ln 2} \rceil$ bodisi $\lceil \sqrt{n \ln 2} \rceil + 1$. Tega pa ne bomo storili, ker bi bil ustrezen dokaz bistveno težji in daljši od navedenega.

Dokaz. Naj bo

$$a = \frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2}.$$

(Takšen a smo izbrali zato, ker je blizu številu $\sqrt{n \ln 2}$ in zadošča enostavni kvadratni enačbi $a^2 - a = n \ln 2$.) Posebej velja

$$\frac{\ln 2}{a - 1} = \frac{a}{n}. \quad (7)$$

Najprej pokažimo, da velja neenakost (4) v primeru, ko je $m = \lceil a \rceil$. Z uporabo enakosti (7) dobimo naslednje ekvivalence:

$$\begin{aligned} \frac{n - a}{n} \leq 2^{-1/(a-1)} &\iff 2^{1/(a-1)} \left(1 - \frac{a}{n}\right) \leq 1 \iff \\ &\iff \exp\left(\frac{\ln 2}{a - 1}\right) \left(1 - \frac{a}{n}\right) \leq 1 \iff \\ &\iff \exp\left(\frac{a}{n}\right) \left(1 - \frac{a}{n}\right) \leq 1. \end{aligned}$$

Pokažimo, da velja zadnja neenakost. Naj bo $f(x) = e^x(1 - x)$. Potem je $f(0) = 1$ in $f'(x) < 0$ za $x > 0$. Ker je $0 < \frac{a}{n} < 1$, velja $f(\frac{a}{n}) < f(0) = 1$, zato je

$$\frac{n - a}{n} < 2^{-1/(a-1)}. \quad (8)$$

Če vzamemo $m = \lceil a \rceil > a$, iz neenakosti (8) sledi neenakost (4). Zato velja tudi neenakost (2) in

$$T(n) \leq \left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2} \right\rceil.$$

S tem smo dobili zgornjo mejo za $T(n)$. Poiščimo še spodnjo. Naj bo

$$b = a - 1 = -\frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2}.$$

Podobno kot prej velja $b^2 + b = n \ln 2$ in

$$\frac{\ln 2}{b - 1} = \frac{b(b + 1)}{n(b - 1)}. \quad (9)$$

Ko uporabimo enakost (9), oceno $e^x > 1 + x$ in dejstvo, da je $b^2 < n + 1$, po krajšem izračunu dobimo

$$\exp\left(\frac{\ln 2}{b - 1}\right) \left(1 - \frac{b}{n - b + 2}\right) > 1.$$

Od tod sledi

$$\frac{n - 2b + 2}{n - b + 2} > 2^{-1/(b-1)}. \quad (10)$$

V primeru $m = \lfloor b \rfloor < b$ (kjer $\lfloor \cdot \rfloor$ označuje zaokroževanje navzdol) iz neenakosti (10) dobimo

$$\frac{n - 2m + 2}{n - m + 2} > 2^{-1/(m-1)}. \quad (11)$$

Leva stran v neenakosti (11) je najmanjši izmed faktorjev v neenakosti (3), zato je

$$\binom{n - m + 1}{m} / \binom{n}{m} > 1/2.$$

Odtod dobimo $\lfloor -\frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2} \rfloor < T(n)$, zato je

$$\left\lfloor -\frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2} \right\rfloor \leq T(n) \leq \left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2} \right\rceil. \quad (12)$$

Enostaven račun nam tedaj pove, da je

$$\left\lfloor -\frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2} \right\rfloor \leq \lceil \sqrt{n \ln 2} \rceil \leq \left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + n \ln 2} \right\rceil. \quad (13)$$

Ker sta spodnja in zgornja meja za ena narazen, rezultat izreka sledi iz neenakosti (12) in (13). ■

Dalo bi se izračunati tudi mejna števila $T_\alpha(n)$ za verjetnosti $\alpha \neq \frac{1}{2}$. Tedaj bi prvo domnevo nadomestili s približkom

$$T_\alpha(n) \approx \sqrt{n \ln \left(\frac{1}{1 - \alpha} \right)}.$$

V primeru $\alpha = 1 - e^{-1} \approx 0,6321$ bi recimo enostavno dobili $T_\alpha(n) = \lceil \sqrt{n} \rceil$.

V primeru, ko je $0 < \alpha < 1 - e^{-1}$, lahko enostavno priredimo dokaz izreka 5 in dobimo

$$\left| T_\alpha(n) - \left\lceil \sqrt{n \ln \left(\frac{1}{1 - \alpha} \right)} \right\rceil \right| \leq 1. \quad (14)$$

Numerični poizkusi kažejo, da neenakost (14) velja za dovolj velika števila n tudi v primeru, ko je $1 - e^{-1} \leq \alpha < 1$, a za to še nismo našli dokaza.

LITERATURA

- [1] M. Abrahamson, W. Moser, *More birthday surprises*, Amer. Math. Monthly **77** (1970), 856–85.
- [2] C. Berge, *Principles of Combinatorics*, Academic Press, New York, NY and London, 1971.
- [3] N. Henze, *The distribution of spaces on lottery tickets*, The Fibonacci Quarterly **33** (1995), 426–431.
- [4] N. Henze, H. Riedwyl, *How to win more: Strategies for Increasing a Lotto Win*, A. K. Peters, Natick, MA, 1998.
- [5] S. Ross, *A First Course in Probability* (5. izdaja), Prentice Hall, Upper Saddle River, NJ, 1998.
- [6] Internetna stran koloradske loterije: <http://www.coloradolottery.com>.
- [7] Internetna stran slovenske loterije: <http://www.loterija.si/igre/loto>.

VESTI

Deveto mednarodno tekmovanje študentov matematike

Med 19. in 25. julijem 2002 je bilo v Varšavi deveto mednarodno tekmovanje študentov matematike. Tekmovanje počasi raste in postaja nekakšno logično nadaljevanje mednarodnih srednješolskih matematičnih olimpijad. Letos se je tekmovanja udeležilo že več kot 200 najboljših študentov matematike z vsega sveta. Univerzo v Ljubljani so zastopali: Irena Majcen iz drugega, Dušan Jan in Jure Kališnik iz tretjega ter Tomaž Kosem in Martin Milanič iz četrtega letnika. Tekmovanje je potekalo dva dneva. Vsak dan so imeli študenti po pet ur za reševanje šestih nalog, ki jih je predlagala mednarodna žirija. Pomerili so se v naslednjih nalogah:

I.1. Grafu kvadratnega polinoma, podanega z enačbo $y = x^2 + ax + b$; $a, b \in \mathbb{R}$, rečemo *standardna parabola*. Tri standardne parabole s temeni V_1 , V_2 in V_3 se paroma sečejo v točkah A_1 , A_2 in A_3 . Naj bo $s : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ zrcaljenje čez abscisno os.

Pokaži, da se standardne parabole s temeni $s(A_1)$, $s(A_2)$ in $s(A_3)$ paroma sečejo v točkah $s(V_1)$, $s(V_2)$ in $s(V_3)$.

I.2. Ali obstaja zvezno odvedljiva funkcija $f : \mathbb{R} \rightarrow \mathbb{R}$, za katero velja

$$f(x) > 0 \quad \text{in} \quad f'(x) = f(f(x)) \quad \text{za vsak } x \in \mathbb{R}?$$

I.3. Naj bo n naravno število in

$$a_k = \frac{1}{\binom{n}{k}}, \quad b_k = 2^{k-n} \quad \text{za } k = 1, 2, \dots, n.$$

Pokaži, da velja:

$$\frac{a_1 - b_1}{1} + \frac{a_2 - b_2}{2} + \dots + \frac{a_n - b_n}{n} = 0.$$

I.4. Naj bo $f : [a, b] \rightarrow [a, b]$ zvezna funkcija in $p \in [a, b]$. Rekurzivno definirajmo $p_0 = p$ in $p_{n+1} = f(p_n)$ za $n = 0, 1, 2, \dots$. Recimo, da je množica

$$T_p = \{p_n; n = 0, 1, 2, \dots\}$$

zaprta, tj., če $x \notin T_p$, obstaja tak $\delta > 0$, da za vse $x' \in T_p$ velja $|x' - x| \geq \delta$. Pokaži, da ima tedaj množica T_p le končno elementov.

I.5. Dokaži ali ovrzi naslednji izjavi:

- (a) Obstaja monotona funkcija $f : [0, 1] \rightarrow [0, 1]$, za katero ima pri vsakem $y \in [0, 1]$ enačba $f(x) = y$ več kot števno rešitev.
- (b) Obstaja zvezno odvedljiva funkcija $f : [0, 1] \rightarrow [0, 1]$, za katero ima pri vsakem $y \in [0, 1]$ enačba $f(x) = y$ več kot števno rešitev.

I.6. Za realno matriko M velikosti $n \times n$ naj bo

$$\|M\| = \sup_{x \in \mathbb{R}^n \setminus \{0\}} \frac{\|Mx\|_2}{\|x\|_2},$$

pri čemer $\|\cdot\|_2$ pomeni evklidsko normo na $\mathbb{R}^n$. Recimo, da za realno matriko A velikosti $n \times n$ velja

$$\|A^k - A^{k-1}\| \leq \frac{1}{2002k} \quad \text{za vse } k \in \mathbb{N}.$$

Pokaži, da tedaj velja tudi $\|A^k\| \leq 2002$ za vse $k \in \mathbb{N}$.

II.1. Izračunaj determinanto matrike $A = [a_{ij}]_{i,j=1}^n$, ki je podana takole:

$$a_{ij} = \begin{cases} (-1)^{|i-j|}, & \text{če } i \neq j, \\ 2, & \text{če } i = j. \end{cases}$$

II.2. Dvesto študentov se je udeležilo matematičnega tekmovanja, na katerem je bilo treba rešiti šest nalog. Vsako nalogo je pravilno rešilo

vsaj po 120 študentov. Pokaži, da lahko najdemo dva študenta, za katera velja: vsako od nalog je rešil vsaj eden med njima.

II.3. Naj bo n naravno število in

$$a_n = \sum_{k=0}^{\infty} \frac{k^n}{k!}, \quad b_n = \sum_{k=0}^{\infty} (-1)^k \frac{k^n}{k!}.$$

Pokaži, da je za vsako naravno število n produkt $a_n b_n$ celo število.

II.4. V tristrani piramidi $OABC$ je $\alpha = \angle BOC$, $\beta = \angle COA$ in $\gamma = \angle AOB$. Naj bo σ kot med ploskvama OAB in OAC ter τ kot med ploskvama OBA in OBC . Pokaži, da velja:

$$\gamma > \beta \cos \sigma + \alpha \cos \tau.$$

II.5. Naj bo A kompleksna matrika velikosti $n \times n$. Pokaži, da velja $A\bar{A} = I$ natanko tedaj, ko obstaja obrnljiva matrika S , za katero je $A = S\bar{S}^{-1}$. Pri tem I pomeni identično matriko, prečka pa konjugiranje.

II.6. Naj bo $f : \mathbb{R}^n \rightarrow \mathbb{R}$ konveksna funkcija, katere gradient

$$\nabla f = \left(\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n} \right)$$

obstaja v vsaki točki $\mathbb{R}^n$ in velja

$$\exists L > 0 \forall x_1, x_2 \in \mathbb{R}^n : \|\nabla f(x_1) - \nabla f(x_2)\| \leq L\|x_1 - x_2\|.$$

Pokaži, da tedaj velja tudi:

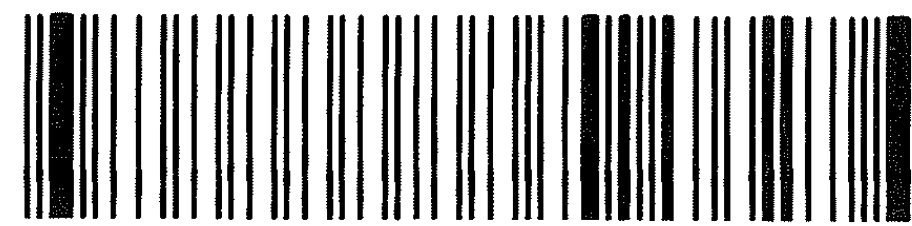
$$\forall x_1, x_2 \in \mathbb{R}^n : \|\nabla f(x_1) - \nabla f(x_2)\|^2 \leq L\langle \nabla f(x_1) - \nabla f(x_2), x_1 - x_2 \rangle.$$

Pri tem $\langle \cdot, \cdot \rangle$ označuje skalarni produkt v $\mathbb{R}^n$.

Teža nalog približno raste z njihovo zaporedno številko. Naši študentje so se v zelo hudi konkurenci že tradicionalno dobro odrezali. Jure Kališnik, Tomaž Kosem, Irena Majcen in Martin Milanič so dobili tretjo nagrado, Dušan Jan pa je dobil pohvalo.

Čeprav je eden od glavnih namenov tekmovanja primerjava kvalitete matematičnih fakultet po vsem svetu, je bil letos še posebej poudarjen neformalni del tekmovanja. Tekmovanje že vsa leta poteka v zelo sproščenem ozračju in najboljši študentje lahko pri skupnih aktivnostih (izleti, nogometne tekme, kosila, sprejemi) spoznajo svoje kolege z vsega sveta.

Marjan Jerman



Vabimo vas na seminar

Elementi vzgoje in izobraževanja pri diferenciranem pouku matematike in fizike.

Seminar bo 11. in 12. 10. 2002 v sklopu strokovnega srečanja ob občnem zboru DMFA Slovenije v poslovnokonferenčnem centru Zdravilišča Laško. Namenjen je predvsem predmetnim učiteljem ter profesorjem matematike in fizike – mentorjem krožkov.

TEME:

- | | | |
|---------------------|---|---------|
| Dr. Gregor Dolinar: | <i>Mednarodne izkušnje pri diferenciranem pouku matematike</i> | (2 uri) |
| Mag. Ciril Dominko: | <i>Reševanje problemskih nalog iz fizike na različnih nivojih</i> | (3 ure) |
| Mag. Darjo Felda: | <i>Delo z nadarjenimi učenci oziroma dijaki</i> | (2 uri) |
| Dr. Bojan Golli: | <i>Eksperimentalni projekti in naloge za nadarjene učence</i> | (3 ure) |
| Mag. Cvetka Rojko: | <i>Zakaj in s kom tekmujemo?</i> | (2 uri) |
| Mag. Gregor Šega: | <i>Uporaba statističnih metod pri analizi rezultatov tekmovanja</i> | (2 uri) |
| Dr. Matjaž Željko: | <i>Reševanje problemskih nalog iz matematike na različnih nivojih</i> | (2 uri) |

Seminar je objavljen v Katalogu programov stalnega strokovnega spopolnjevanja strokovnih delavcev v vzgoji in izobraževanju 2002/2003, stran 244. Ovrednoten je z eno točko. Ker bodo teme izvajane tudi v obliki delavnic, bodo posamezne teme trajale v resnici dlje, kot je zgoraj navedeno. Fizikalne in matematične teme bodo potekale vzporedno, zato bodo udeleženci seminarja morali izbirati med enimi in drugimi (izbor sporočite ob prijavi).

Kotizacija za seminar znasa 10.000 SIT.

Prosimo, da pošljete svoje prijave na predpisanem obrazcu (modri kartončki) najkasneje do 28. 9. 2002 na naslov:

DMFA, Janez Krušič,
Jadranska ul. 19,
1000 Ljubljana.

Lahko se prijavite tudi po elektronski pošti na naslov:

Janez.Krusic@fmf.uni-lj.si.

Koordinatorja seminarja:
Darjo Felda in Janez Krušič