Cjelobrojne funkcije i primjene

Piškorjanac, Marina

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Marina Piškorjanac

Cjelobrojne funkcije i primjene

Diplomski rad

Osijek, 2019.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Marina Piškorjanac

Cjelobrojne funkcije i primjene

Diplomski rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2019.

Sadržaj

Uvod

U svakodnevnom se životu često služimo cijelim brojevima. Prirodne brojeve koristimo za prebrojavanje različitih objekata, dok su pozitivni i negativni cijeli brojevi potrebni za prikaz stanja na bankovnom računu, definiranje mjernih ljestvica, npr. pri mjerenju temperature, brzine, sile, nadmorske visine i slično. U matematici se skup cijelih brojeva $\mathbb{Z}$ ubraja u prebrojive skupove, koje uz konačne skupove zajedničkim imenom nazivamo diskretnim skupovima. Problemima vezanim uz diskretne strukture bavi se diskretna matematika koja obuhvaća različita područja matematike poput teorije brojeva, algebre, računalne znanosti, kombinatorike, matematičke logike, teorije grafova i drugih.

Pri modeliranju i rješavanju problema iz područja diskretne matematike koja se bave prirodnim i cijelim brojevima često se koriste cjelobrojne funkcije. To su funkcije koje elementima svoje domene pridružuju cjelobrojne vrijednosti, odnosno, njihova je slika skup cijelih brojeva ili neki od njegovih podskupova. Matematički: za funkciju f čija je domena proizvoljan, (ne nužno diskretan) skup D kažemo da je cjelobrojna ako je $f(D) \subseteq \mathbb{Z}$.

Pri analiziranju i interpretaciji podataka iz svakodnevnog života, može se dogoditi da egzaktni matematički izračuni daju rezultate koji u stvarnosti nemaju smisla te ih je potrebno doraditi primjenjujući neku cjelobrojnu funkciju.

Primjerice, prema Eurostatovom istraživanju 2017. godine, broj članova po kućanstvu u Republici Hrvatskoj iznosi 2.8 članova[1], no prirodnije je taj podatak opisati najbližim prirodnim brojem te reći kako on iznosi približno 3. Slično, kada se u Hrvatskom saboru koji trenutno broji 151 zastupnika treba apsolutnom većinom izglasati neki važni zakon, nema smisla govoriti o 75.5 glasova potrebnih za njegovo usvajanje nego tu vrijednost zaokružimo na prvi veći cijeli broj, koji je 76.

Različite funkcije za zaokruživanje brojeva na cjelobrojne vrijednosti implementirane su i u računalima. Ubrzanim razvojem računalne znanosti, stvorila se potreba za upotrebom i detaljnijim proučavanjem cjelobrojnih funkcija. Bez elementarnog znanja o njima gotovo je nemoguće razumjeti rad računala i brojnih programskih algoritama u kojima se koriste.

[1] `https://ec.europa.eu/eurostat/statistics-explained/index.php/Household_composition_statistics\#Household_size`

U ovom ćemo radu definirati izabrane cjelobrojne funkcije, navesti neka njihova svojstva i osnovne rezultate te ih potkrijepiti odgovarajućim primjerima. Ograničit ćemo se na funkcije realne varijable, čija je domena skup realnih brojeva ili neki njegov podskup. U duhu konkretne matematike više ćemo se koncentrirati na primjenu na numeričkim primjerima i primjerima iz svakodnevnog života, a manje na primjenu pri dokazivanju matematičkih tvrdnji i opisivanje apstraktnih svojstava i struktura vezanih uz cjelobrojne funkcije.

U prvom ćemo poglavlju definirati karakterističnu (indikator) funkciju, općenito reći nešto o neprekidnosti cjelobrojnih funkcija te pomoću karakteristične funkcije definirati stepenaste funkcije. Navest ćemo i neke njihove primjene.

U drugom poglavlju posebno ćemo izdvojiti stepenaste cjelobrojne funkcije najveće i najmanje cijelo zbog potrebe navođenja različitih primjena u nastavi, teoriji brojeva i računalnoj znanosti.

U trećem ćemo poglavlju spomenuti nekoliko važnih funkcija iz teorije brojeva koje se koriste pri proučavanju svojstava prirodnih brojeva i njihovih djelitelja, a u posljednjem, četvrtom poglavlju, skup svih cjelobrojnih funkcija karakterizirat ćemo kao prsten te kratko navesti neka algebarska svojstva skupa cjelobrojnih polinoma kao njegovog podskupa.

1 Karakteristična funkcija

Korisna funkcija za ispitivanje pripadnosti nekog elementa skupa X nekom podskupu od X je tzv. **karakteristična ili indikator funkcija**. Intuitivno, za njenu sliku možemo uzeti bilo koji dvočlani skup, npr. {istinito, lažno} u ovisnosti pripada li element danom podskupu ili ne. Ipak, u standardnoj matematičkoj definiciji za sliku karakteristične funkcije uzima se skup $\{0, 1\}$ pa ju možemo promatrati kao cjelobrojnu funkciju.

1.1 Definicija i svojstva

Definicija 1. *Neka je X neki skup i $A \subseteq X$. Funkciju $\chi_A : X \to \{0, 1\}$ definiranu s*

$$\chi_A(x) = \begin{cases} 1, & \text{ako} \quad x \in A \\ 0, & \text{ako} \quad x \notin A \end{cases}$$

nazivamo karakteristična funkcija podskupa $A \subseteq X$.

U nastavku rada karakterističnu funkciju označavat ćemo s $\mathbb{1}_A$ što je najčešće korištena oznaka u literaturi, a još se koriste i oznake I_A, K_A te $[x \in A]$, pri čemu su $[\cdot]$ Iversonove zagrade[2].

Navedimo neka od svojstava karakteristične funkcije:

Propozicija 1. (vidi [1, Theorem 2, Theorem 3, Theorem 4, Theorem 5])
Neka su $A, B, A_1, A_2, \ldots, A_n \subseteq X$. Tada vrijedi:

(a) $\mathbb{1}_{A^C} = 1 - \mathbb{1}_A$,

(b) $\mathbb{1}_{A \cap B} = \mathbb{1}_A \cdot \mathbb{1}_B$,

(c) $\mathbb{1}_{\bigcap_{i=1}^{n} A_i} = \prod_{i=1}^{n} \mathbb{1}_{A_i}$,

(d) $\mathbb{1}_A^n = \mathbb{1}_A, \quad \forall n \in \mathbb{N}$,

(e) $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \cdot \mathbb{1}_B$.

[2] $[P] = 1$, ako je logički izraz P istinit; $[P] = 0$, ako je lažan

Primjer 1. *Jedan od standardnih primjera karakteristične funkcije jest* ***Dirichletova funkcija****, definirana kao* $f : \mathbb{R} \to \{0, 1\}$ *s pravilom pridruživanja*

$$f(x) = \begin{cases} 1, & \text{ako } x \in \mathbb{Q} \\ 0, & \text{ako } x \notin \mathbb{Q} \, . \end{cases} \tag{1}$$

Dirichletova se funkcija najčešće navodi kao primjer funkcije neprekidne u svakoj točki svoje domene (vidjeti [12, Zadatak 1.85]).

Općenito, za primjer funkcija koje imaju prekid u jednoj ili više točaka, nerijetko se uzimaju upravo cjelobrojne funkcije definirane na skupu realnih brojeva ili nekom njegovom povezanom podskupu. Dakle, ako cjelobrojna funkcija definirana na povezanom skupu nije konstantna, sigurno ima prekid. Kako bismo se uvjerili u istinitost te tvrdnje, prisjetimo se osnovnih pojmova i rezultata metričkih prostora.

Definicija 2. *Par* (X, d) *nepraznog skupa* X *i realne funkcije* $d : X \times X \to \mathbb{R}$ *koja zadovoljava uvjete:*

(M_1) $d(x, y) \geqslant 0, \quad \forall x, y \in X,$

(M_2) $d(x, y) = 0 \iff x = y,$

(M_3) $d(x, y) = d(y, x), \quad \forall x, y \in X,$

(M_4) $d(x, y) \leqslant d(x, z) + d(z, y), \quad \forall x, y, z \in X$

naziva se metrički prostor. Funkciju d *nazivamo metrikom na* X*.*
(Ukoliko je nevažno o kojoj se točno funkciji d radi, možemo govoriti samo o metričkom prostoru X.)

Definicija 3. *Neka je* (X, d) *metrički prostor. Skup*

$$K(x_0, r) \coloneqq \{x \in X : d(x, x_0) \leqslant r\} \subseteq X$$

zovemo otvorenom kuglom oko x_0 *radijusa* r*.*

Definicija 4. *Neka je* X *metrički prostor. Za skup* $U \subseteq X$ *kažemo da je otvoren ako za svaku točku* $x \in U$ *postoji realan broj* $r > 0$ *takav da je* $K(x, r) \subseteq U$*. Za skup* $F \subseteq X$ *kažemo da je zatvoren ako je njegov komplement* $X \backslash F$ *otvoren skup.*

Primjer 2. (vidi [22, Primjer 1.1])
Skup $\mathbb{R}^n$ *je metrički prostor uz metriku* $d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$*. Svaka otvorena kugla u* $\mathbb{R}^n$ *je otvoren skup.*

U [22] se može vidjeti kako familija $\mathcal{U}$ svih otvorenih skupova u metričkom prostour (X, d) ima sljedeća svojstva:

(T_1) prazan skup $\varnothing$ i cijeli skup X su otvoreni skupovi,

(T_2) unija proizvoljne familije otvorenih skupova je otvoren skup,

(T_3) presjek svake konačne familije otvorenih skupova je otvoren skup.

Općenito, uz familiju podskupova nekog skupa koja zadovoljava ova svojstva vežemo sljedeću definiciju:

Definicija 5. *Neka je X neprazan skup i $\mathcal{U} \subseteq \mathcal{P}(X)$ neka familija podskupova od X koja ima svojstva $(T_1), (T_2)$ i (T_3). Tada uređeni par $(X,\mathcal{U})$ zovemo topološki prostor, familiju $\mathcal{U}$ topologijom na X, a elemente familije $\mathcal{U}$ otvorenim skupovima.*

Teorem 1. (vidi [22, Teorem 2.1])
Neka su X i Y metrički prostori. Preslikavanje $f : X \to Y$ je neprekidno ako i samo ako je za svaki zatvoreni skup $F \subseteq Y$ njegova praslika $f^{\leftarrow}(F) := \{x \in X : f(x) \in Y\} \subseteq X$ zatvoren skup u X.

Definicija 6. *Za metrički prostor X kažemo da je nepovezan ako postoje neprazni otvoreni podskupovi $U, V \subseteq X$ takvi da je $X = U \cup V$ i $U \cap V = \varnothing$. Prostor X je povezan ako nije nepovezan, tj. ako se ne može prikazati kao unija dvaju disjunktnih nepraznih otvorenih podskupova. Skup $A \subseteq X$ je povezan ako je A povezan kao topološki prostor.*
(Riječ "otvoren", u ovoj se definiciji može zamijeniti riječju "zatvoren", pri čemu se smisao definicije ne mijenja.)

Primjer 3. (vidi [15, Primjer 3.26. c)])
Skup $\mathbb{R}$ je povezan.

Teorem 2. (vidi [22, Teorem 2.14])
Topološki prostor X je nepovezan ako i samo ako postoji neprekidna surjekcija $f : X \to \{0, 1\}$.

Dokaz:
$\boxed{\Rightarrow}$ Neka je X nepovezan. Po Definiciji 6 postoje disjunktni zatvoreni neprazni skupovi $U, V \subseteq X$ takvi da je $X = U \cup V$. Tada je karakteristična funkcija od $U \subseteq X$, $f : X \to \{0, 1\}$ definirana s

$$f(x) = \begin{cases} 1, & \text{ako } x \in U \\ 0, & \text{ako } x \in V \end{cases}$$

neprekidna surjekcija.

$\boxed{\Leftarrow}$ Neka je $f : X \to \{0, 1\}$ neprekidna surjekcija. Tada su prema Teoremu 1 skupovi $U \coloneqq f^{\leftarrow}(0)$ i $V \coloneqq f^{\leftarrow}(1)$ neprazni zatvoreni disjunktni podskupovi od X za koje vrijedi $X = U \cup V$. Prema tome, X nije povezan. □

Dakle, ako bi postojala neprekidna nekonstantna cjelobrojna funkcija definirana na skupu realnih brojeva, slično dokazu Teorema 2, skup $\mathbb{R}$ bi mogli prikazati kao disjunktnu uniju njegovih zatvorenih podskupova koju bi činile praslike elemenata iz skupa cijelih brojeva koji se nalaze u slici. To bi značilo da skup $\mathbb{R}$ ne bi bio povezan, što je u kontradikciji s Primjerom 2.

1.2 Karakteristična funkcija u teoriji vjerojatnosti i statistici

U teoriji vjerojatnosti se za funkciju iz Definicije 1 uvijek koristi naziv indikator funkcija jer je izraz karakteristična funkcija rezerviran za nešto drugačije definiranu, kompleksnu funkciju (vidi [10, stranica 12]). Stoga ćemo se i mi u nastavku držati takve terminologije.

Osnovni predmet proučavanja teorije vjerojatnosti je vjerojatnosni prostor. Za njegovo precizno definiranje potrebno je poznavati pojmove σ-algebre i funkcije vjerojatnosti koje se mogu pogledati u [2, Definicija 1.3, Definicija 1.4].

Definicija 7. *Neka je Ω prostor elementarnih događaja slučajnog pokusa. Neka je $\mathcal{F}$ σ-algebra na Ω i P vjerojatnost na $\mathcal{F}$. Uređenu trojku $(\Omega, \mathcal{F}, P)$ zovemo vjerojatnosni prostor. Ako je Ω konačan ili prebrojiv skup, onda $(\Omega, \mathcal{F}, P)$ zovemo diskretan vjerojatnosni prostor.*

Iz sljedeće definicije vidljivo je kako indikator funkciju možemo promatrati kao diskretnu slučajnu varijablu te pomoću nje opisati određene slučajne pokuse.

Definicija 8. *Neka je dan diskretan vjerojatnosni prostor $(\Omega, \mathcal{P}(\Omega), P)$. Svaku funkciju $f : \Omega \to \mathbb{R}$ nazivamo diskretna slučajna varijabla.*

Pojasnimo kako to radimo na primjeru.

Primjer 4. *Promotrimo slučajni pokus bacanja dviju simetričnih igraćih kockica. Pomoću indikator funkcije modelirajmo događaj ako su se okrenula dva ista broja.*

Neka je $\Omega = \{(\omega_1, \omega_2) : \omega_i \in \{1, \ldots, 6\}\}$ *i* $A = \{(\omega_1, \omega_2) \in \Omega : \omega_1 = \omega_2\}$. *Vjerojatnost događaja* A *iznosi* $P(A) = \frac{k(A)}{k(\Omega)} = \frac{6}{36} = \frac{1}{6}$, *gdje je* $k(A)$ *broj elemenata skupa* A. *Tražena slučajna varijabla definirana je s* $X : \Omega \to \{0, 1\}$ *i*

$$X\left((\omega_1, \omega_2)\right) = \begin{cases} 1, & \text{ako } (\omega_1, \omega_2) \in A \\ 0, & \text{ako } (\omega_1, \omega_2) \notin A \end{cases} = \mathbb{1}_A\left((\omega_1, \omega_2)\right).$$

Varijabla X *očito ima Bernoullijevu distribuciju (vidi [2, Poglavlje 2.4.2]) s parametrom* $p = \frac{1}{6}$, *tj.*

$$X \sim \begin{pmatrix} 0 & 1 \\ \frac{5}{6} & \frac{1}{6} \end{pmatrix}.$$

Općenito, iz činjenice da indikator funkcija ima Bernoullijevu distribuciju, možemo izvesti korisnu vezu između vjerojatnosti slučajnog događaja i matematičkog očekivanja slučajne varijable

$$E[\mathbb{1}_A] = 0 \cdot (1 - p) + 1 \cdot p = p = P(A)$$

koja se, uz svojstva karakteristične funkcije iz Propozicije 1, koristi za elegantno dokazivanje složenih tvrdnji, npr. vidi [2, Teorem 2.4.].

U statistici, indikator funkciju možemo koristiti za definiranje empirijske funkcije distribucije dane slučajne varijable (vidi [7, Definition 1.]).

1.3 Stepenaste cjelobrojne funkcije

U ovom ćemo potpoglavlju pomoću karakteristične funkcije definirati veliku klasu stepenastih funkcija, a posebno ćemo spomenuti cjelobrojne stepenaste funkcije.

Definicija 9. *Neka su* A_i, $i = 1, \ldots, n$ *u parovima disjunktni intervali realnih brojeva takvi da vrijedi* $\bigcup_{i=1}^{n} A_i = \mathbb{R}$ *i neka su* a_i, $i = 1, \ldots, n$ *realni brojevi. Za funkciju* $f : \mathbb{R} \to \mathbb{R}$ *kažemo da je* ***stepenasta*** *ako ju možemo prikazati kao linearnu kombinaciju karakterističnih funkcija podskupova* A_i *s koeficijentima* a_i*:*

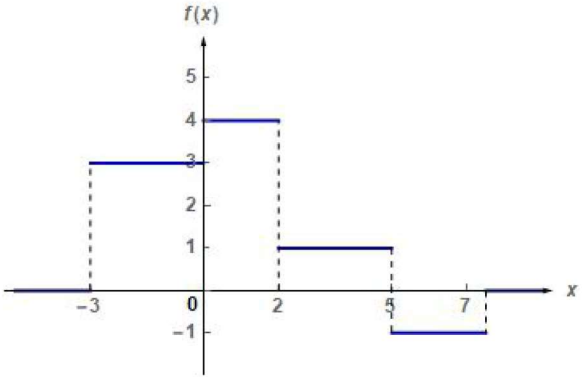
$$f = \sum_{i=1}^{n} a_i \mathbb{1}_{A_i}.$$

Ako su svi koeficijenti $a_i \in \mathbb{Z}$, $i = 1, \ldots, n$, *riječ je o cjelobrojnoj stepenastoj funkciji.*

Stepenaste funkcije ime su dobile zbog svojih grafova koji se sastoje od dijelova pravaca paralelnih s osi apscisa (npr. Slika 1), a koji podsjećaju na stepenice.

Primjer 5. *Promotrimo stepenastu funkciju $f : \mathbb{R} \to \mathbb{Z}$ definiranu s*

$$f(x) = \begin{cases} 3, & x \in \langle -3, 0] \\ 4, & x \in \langle 0, 2] \\ 1, & x \in \langle 2, 5] \\ -1, & x \in \langle 5, 7.5] \\ 0, & \text{inače.} \end{cases}$$



Slika 1: Graf funkcije f

Prema Definiciji 9, funkciju f možemo zapisati u obliku

$$f = 0 \cdot \mathbb{1}_{\langle -\infty, -3]} + 3 \cdot \mathbb{1}_{\langle -3, 0]} + 4 \cdot \mathbb{1}_{\langle 0, 2]} + 1 \cdot \mathbb{1}_{\langle 2, 5]} - 1 \cdot \mathbb{1}_{\langle 5, 7.5]} + 0 \cdot \mathbb{1}_{\langle 7.5, \infty \rangle}.$$

Radi jednostavnosti zapisa, u nekim slučajevima smijemo zanemariti uvjete disjunktnosti intervala pomoću kojih definiramo stepenastu funkciju, te uvjet da njihova unija mora biti skup $\mathbb{R}$. Tada funkciju f možemo prikazati u ekvivalentnom obliku

$$f = 3 \cdot \mathbb{1}_{\langle -3, 2]} + 1 \cdot \mathbb{1}_{\langle 0, 5]} - 1 \cdot \mathbb{1}_{\langle 5, 7.5]}.$$

Heavisideova funkcija

Jednu stepenastu cjelobrojnu funkciju, važnu u matematičkoj analizi, koriste fizičari i elektroinženjeri za opisivanje mehaničkih vibracija i analiziranje strujnih krugova. To je tzv. **Heavisideova funkcija**, koju ćemo označiti s H, definirana s

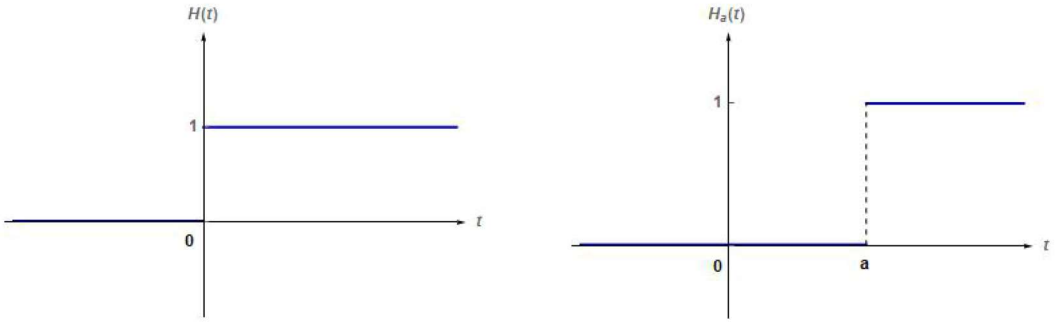
$$H(t) = \begin{cases} 0, & t < 0 \\ 1, & t \geqslant 0 \end{cases}$$

ili s pomakom kao

$$H(t - a) \coloneqq H_a(t) = \begin{cases} 0, & t < a \\ 1, & t \geqslant a \end{cases}, \quad \text{gdje je } a \geqslant 0.$$

Pri računanju s Heavisideovom funkcijom najčešće se koriste operacije u kojima nije bitna vrijednost funkcije u svakoj pojedinoj točki pa se, u ovisnosti o problemu, vrijednost Heavisideove funkcije može dogovorno posebno definirati za $t = 0$, najčešće sa $H(t) = \frac{1}{2}$.

U literaturi se može pronaći i pod nazivom skok funkcija, u oznakama u, S, Y ili Θ. Na Slici 2 možemo vidjeti grafove funkcija H i H_a.

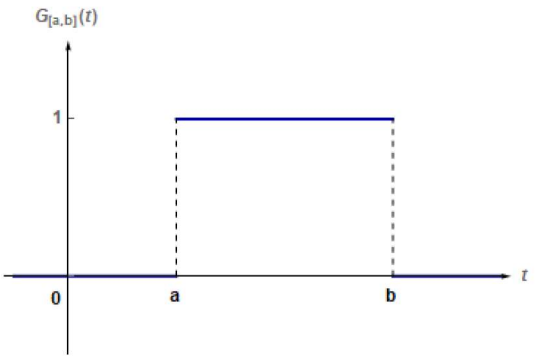


(a) Graf funkcije H (b) Graf funkcije H_a

Slika 2: Graf Heavisidove funkcije

U ovom kontekstu pomoću Heavisidove funkcije možemo definirati i karakterističnu funckiju intervala $[a, b]$ pod imenom **pravokutna ili "gate" funkcija** u oznaci $G_{[a,b]}$, na način

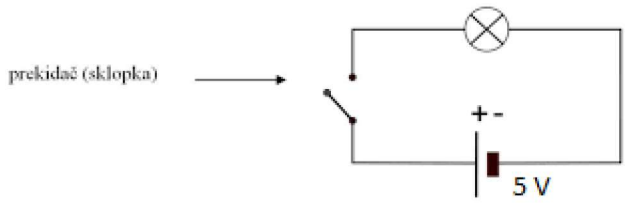
$$\begin{aligned} G_{[a,b]}(t) &= H(t-a) - H(t-b) \\ &= \begin{cases} 1, & t \in [a,b] \\ 0, & \text{inače} \end{cases} \\ &= \mathbb{1}_{[a,b]}(t). \end{aligned}$$



Slika 3: Graf funkcije $G_{[a,b]}$

Pomoću Heavisideove i gate funkcije mogu se modelirati vrijednosti napona ili struje u strujnom krugu, u ovisnosti je li i kada sklopka zatvorena. Pogledajmo kako to izgleda na jednostavnom primjeru.

Primjer 6. *Promatramo strujni krug koji se sastoji od izvora napona od* $5V$*, sklopke i trošila (vidjeti Sliku 4).*



Slika 4: Jednostavan strujni krug

Opišimo pad napona u strujnom krugu u sljedećim situacijama:

(*a*) *ako je sklopka jednokratno zatvorena u trenutku* $t = 0$*, pad napona opisujemo Heavisideovom funkcijom:* $5H(t)$*;*

(*b*) *ako je sklopka jednokratno zatvorena u trenutku* $t = 3$*, pad napona opisujemo Heavisideovom funkcijom s pomakom:* $5H(t-3)$*;*

(*c*) *ako je sklopka zatvorena u trenutku* $t = 1$*, te ponovno otvorena u trenutku* $t = 15$*, pad napona opisujemo gate funkcijom:* $5G_{[1,15]}(t)$*.*

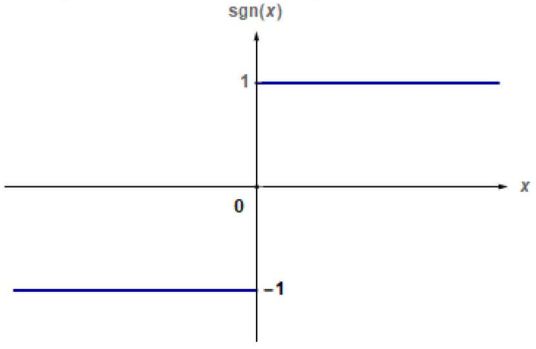
U složenijim se strujnim krugovima veze između napona, struje, otpora i ostalih veličina opisuju diferencijalnim jednadžbama. Pri njihovom rješavanju koriste se Laplaceove transformacije (vidi [4, Chapter 6]). Prethodno navedene funkcije prigodne su za opisivanje danih veličina upravo zbog jednostavnosti primjene Laplaceove transformacije nad njima, u odnosu na transformiranje funkcije dio po dio.

Funkcija predznaka

Funkcija predznaka $sgn : \mathbb{R} \to \{-1, 0, 1\}$ negativnim brojevima pridružuje vrijednost -1, a pozitivnima 1. Dodatno se broju 0 pridružuje vrijednost 0. Dakle,

$$sgn(x) = \begin{cases} -1, & x < 0 \\ 0, & x = 0 \\ 1, & x > 0 \end{cases}$$

ili $\quad sgn(x) = \dfrac{x}{|x|}, \ x \neq 0.$



Slika 5: Graf funkcije *sgn*

Ova funkcija svoju primjenu nalazi u matematičkoj analizi kao derivacija funkcije apsolutne vrijednosti, a zbog toga što ima prekid (kao nekonstantna cjelobrojna funkcija definirana na $\mathbb{R}$), korisna je i u konstruiranju kontraprimjera brojnim tvrdnjama (vidi [3, page 62., Remark 1]).

U inženjerstvu se pomoću funkcije predznaka mogu modelirati binarni kontrolni sustavi paljenja i gašenja različitih uređaja.

Primjer 7. *Ako želimo dizajnirati termostat kućnog klima uređaja tako da se upali kada je sobna temperatura viša od* $T = 26^{\circ c}$ *i ugasi kada rashladi sobu na željenu temperaturu, električni uređaj koji očitava trenutnu sobnu temperaturu i signalizira potrebu za paljenjem (šalje signal* 1*) ili gašenjem (šalje vrijednost* 0*) uređaja treba modelirati pomoću funkcije*

$$f(t) = 0.5 + 0.5 \cdot sgn(t-26) = \begin{cases} 0, & t < 26 \\ (0.5, & t = 26) \\ 1, & t > 26\ . \end{cases} \tag{2}$$

(Vrijednost u trenutku $t = 26$ *možemo i izostaviti iz definicije funkcije, zbog pretpostavke da je temperatura vrlo promjenjiva i vrlo kratko će iznositi točno* $26^{\circ c}$*).*

Uočimo iz (2) općenitu vezu funkcije predznaka i Heavisidove funkcije

$$\frac{1}{2} + \frac{1}{2} \cdot sgn(t-T) = H(t-T),\ T \geqslant 0.$$

2 Funkcije "pod" i "strop"

Nastavljajući se na navođenje primjera cjelobrojnih stepenastih funkcija iz prethodnog poglavlja, zbog brojnih zanimljivih primjena u svakodnevnom životu, zadacima iz nastave, teoriji brojeva i računalnoj znanosti, u ovom ćemo poglavlju posebnu pažnju posvetiti cjelobrojnim stepenastim funkcijama najveće i najmanje cijelo, jednostavnije zvanima funkcije pod i strop.

2.1 Definicija i osnovna svojstva

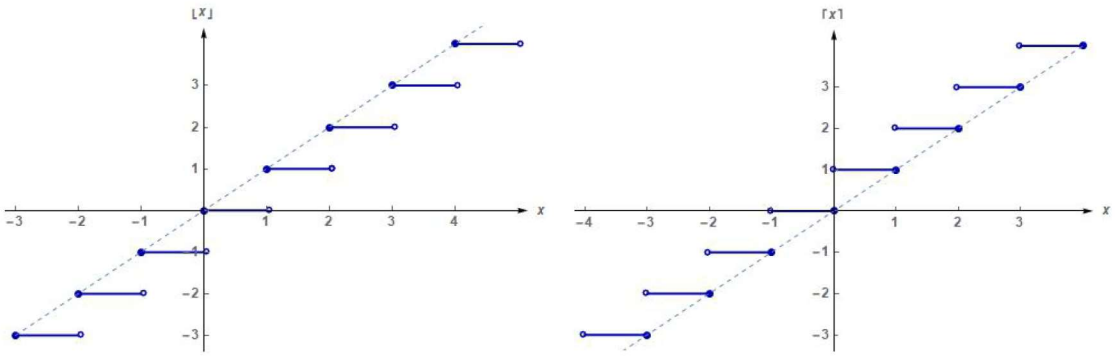
Definicija 10.
Funkciju $\lfloor\cdot\rfloor : \mathbb{R} \to \mathbb{Z}$ *koja realnom broju* x *pridružuje najveći cijeli broj manji ili jednak od* x *nazivamo funkcija najveće cijelo ili funkcija pod (eng. floor).*
Funkciju $\lceil\cdot\rceil : \mathbb{R} \to \mathbb{Z}$ *koja realnom broju* x *pridružuje najmanji cijeli broj veći ili jednak od* x *nazivamo funkcija najmanje cijelo ili funkcija strop (eng. ceiling).*

Primjer 8. *Uočimo kako vrijedi:*

$$\lfloor e \rfloor = 2, \quad \lceil e \rceil = 3,$$
$$\lfloor -0.3 \rfloor = -1, \quad \lceil -0.1 \rceil = 0.$$

Oznake $\lfloor x \rfloor$, $\lceil x \rceil$ te nazive pod i strop, uveo je Kenneth E. Iverson 1960.-ih. Do tada nisu postojale zasebne oznake za ove funkcije. Funkcija pod uobičajeno se označavala s $[x]$, uz uvijek potrebno dodatno pojašnjenje oznake. Izrazi koji su zahtijevali upotrebu funkcije strop zapisivali su se pomoću odgovarajuće veze s funkcijom pod.

Za lakše razumijevanje svojstava ovih dvaju funkcija, korisno je najprije promotriti njihove grafove koji imaju karakterističan oblik stepenica.



(a) Graf funkcije $\lfloor x \rfloor$ (b) Graf funkcije $\lceil x \rceil$

Slika 6: Grafovi funkcija pod i strop

Iz definicije i grafa, za svaki $x \in \mathbb{R}$ očigledno vrijede nejednakosti

$$x - 1 < \lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil < x + 1 \tag{3}$$

$$\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1 \quad \text{i} \quad \lceil x \rceil - 1 < x \leqslant \lceil x \rceil. \tag{4}$$

Posebno, za cjelobrojne argumente vrijedi

$$\lfloor x \rfloor = x \iff x \in \mathbb{Z} \iff \lceil x \rceil = x.$$

Uočimo i kako su grafovi funkcija pod i strop simetrični obzirom na ishodište, pa je lako zapisati vezu između ovih dvaju funkcija

$$\lfloor x \rfloor = -\lceil -x \rceil \quad \text{i} \quad \lceil x \rceil = -\lfloor -x \rfloor.$$

Izravno iz definicije, za $x \in \mathbb{R}$ i $n \in \mathbb{Z}$, slijedi i

$$\lfloor x \rfloor = n \iff n \leqslant x < n + 1 \tag{5}$$

$$\lfloor x \rfloor = n \iff x - 1 < n \leqslant x$$

$$\lceil x \rceil = n \iff n - 1 < x \leqslant n \tag{6}$$

$$\lceil x \rceil = n \iff x \leqslant n < x + 1.$$

Ako u (4) pribrojimo $n \in \mathbb{Z}$, dobivamo sljedeće nejednakosti

$$\lfloor x \rfloor + n \leqslant x + n < \lfloor x \rfloor + n + 1 \tag{7}$$

$$\lceil x \rceil + n - 1 < x + n \leqslant \lceil x \rceil + n. \tag{8}$$

Kako su $\lfloor x \rfloor, \lceil x \rceil, n \in \mathbb{Z}$, onda su i sume $\lfloor x \rfloor + n$ i $\lceil x \rceil + n$ cjelobrojne.
Iz (5) i (7), te (6) i (8) tada slijedi

$$\lfloor x + n \rfloor = \lfloor x \rfloor + n \tag{9}$$

$$\lceil x + n \rceil = \lceil x \rceil + n. \tag{10}$$

Iz posljednjih svojstava intuitivno se nameće da bi slično moglo vrijediti i za množenje: $\lfloor nx \rfloor \stackrel{?}{=} n\lfloor x \rfloor$, te da za sve $x, y \in \mathbb{R}$ vrijedi $\lfloor x + y \rfloor \stackrel{?}{=} \lfloor x \rfloor + \lfloor y \rfloor$.

No, treba biti oprezan, jer te jednakosti općenito ne vrijede. Primjerice, za $n = 3$ i $x = \frac{1}{3}$ je $\lfloor 3 \cdot \frac{1}{3} \rfloor = \lfloor 1 \rfloor = 1$, ali je $3 \cdot \lfloor \frac{1}{3} \rfloor = 3 \cdot 0 = 0$. Također, za $x = \frac{1}{2}$ i $y = \frac{1}{2}$ je $\lfloor \frac{1}{2} + \frac{1}{2} \rfloor = \lfloor 1 \rfloor = 1$, ali je $\lfloor \frac{1}{2} \rfloor + \lfloor \frac{1}{2} \rfloor = 0$.

Još neka od brojnih svojstava funkcija pod i strop pokazat ćemo u nastavku, kako nam budu bila potrebna za pojašnjenje različitih primjena.

2.2 Primjene u radu s učenicima

U redovnoj se osnovnoškolskoj i srednjoškolskoj nastavi cjelobrojne funkcije gotovo uopće ne spominju. Tek u ponekom udžbeniku mogu se pronaći definicije i osnovna svojstva, najčešće funkcija pod i strop, u sklopu sadržaja "za one koji žele znati više". Na temelju razumijevanja jednostavnih svojstava cjelobrojnih funkcija mogu se generirati brojni zanimljivi zadaci za učenička natjecanja. Šteta je i ne koristiti ih kao vrlo ilustrativne primjere nekih svojstava funkcija. Zato ćemo u nastavku navesti nekoliko primjera kako uklopiti rezultate vezane uz funkcije pod i strop u redovnu i dodatnu nastavu ili neku zanimljivu radionicu za učenike.

Prilikom obrade navedenih funkcija zbog lakšeg razumijevanja navest ćemo primjere iz svakodnevnog života u kojima se one i koriste.

Primjer 9. *Jedan osječki taxi prijevoznik cijenu usluge prijevoza na području grada Osijeka naplaćuje* 20 *kn za udaljenost do* 5 *km, te* 5 *kn za svaki sljedeći prijeđeni kilometar. U praksi to ne znači da se cijena nakon* 5 *kilometara obračunava proporcionalno prijeđenim kilometrima, nego se broj kilometara* k *zaokružuje na najmanji sljedeći cijeli broj, što odgovara definiciji funkcije strop. Cijenu prijevoza možemo zapisati kao cjelobrojnu funkciju po varijabli* $k \in \mathbb{R}^+$ *na način*

$$C(k) = \begin{cases} 20, & k < 5 \\ 20 + \lceil k - 5 \rceil, & k \geqslant 5. \end{cases}$$

Glavna mjera kuta

Jedino mjesto na kojem se u redovnoj nastavi koristi funkcija pod jest u trećem razredu srednje škole pri uvodu u gradivo trigonometrijskih funkcija, kada se govori o mjeri kuta.

Znamo kako svaki kut ima beskonačno mnogo mjera, a svake se dvije razlikuju za neki višekratnik broja 360. Drugim riječima, ako je α jedna mjera nekog kuta, tada je i svaki broj iz skupa $\{\alpha + k \cdot 360^\circ, k \in \mathbb{Z}\}$ također mjera tog kuta.

Među svim tim mjerama, posebno će nas zanimati ona za koju vrijedi $0^\circ \leqslant \alpha' < 360^\circ$ koju nazivamo glavna mjera kuta, a možemo ju izračunati pomoću formule

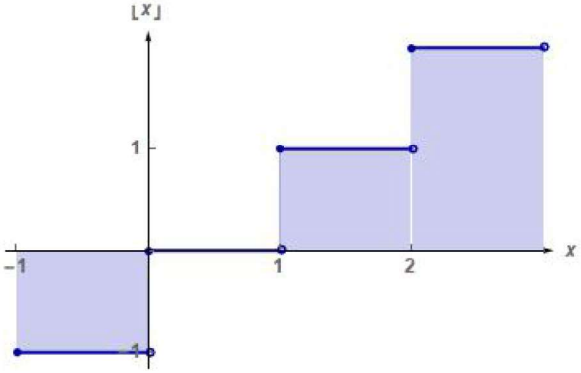
$$\alpha' = \alpha - \left\lfloor \frac{\alpha}{360} \right\rfloor \cdot 360^\circ.$$

Svojstva funkcija

U četvrtom razredu srednje škole sistematizira se i nadograđuje svo znanje o funkcijama i njihovim svojstvima. Upravo je funkcije pod i strop prigodno navesti kao primjer monotono rastućih funkcija ili funkcija koje imaju beskonačno mnogo prekida, što je učenicima vrlo lako zaključiti gledajući grafove tih funkcija.

Također, geometrijsku interpretaciju računanja određenog integrala lako je predočiti učenicima računajući površine pravokutnika što ih "stepenice" grafa funkcije pod zatvaraju s osi apscisa.

Primjer 10. *Vrijedi:* $\int_{-1}^{3} \lfloor x \rfloor \, dx = -1 \cdot 1 + 0 \cdot 1 + 1 \cdot 1 + 2 \cdot 1 = 2.$



Slika 7: Graf funkcije $\lfloor x \rfloor$, za $x \in [-1, 3]$

Broj cijelih brojeva u danom skupu

Na državnoj maturi često se pojavljuju zadaci u kojima treba odrediti broj cijelih brojeva u nekom skupu (intervalu, segmentu).
Primjerice, segment $[-1, 4]$ sadrži 6 cijelih brojeva: $-1, 0, 1, 2, 3$ i 4.

Rješenje se može jednostavno dobiti prebrojavanjem, ali i pomoću formula koje uključuju funkcije pod i strop.

Već u petom razredu osnovne škole, učenicima je jasno kako se broj cijelih brojeva koje sadrži segment $[a, b]$, gdje su $a, b \in \mathbb{Z}, a \leqslant b$, može dobiti pomoću formule $b - a + 1$.

Ako su a i b realni brojevi, tada je najmanji cijeli broj koji se nalazi u segmentu $[a, b]$ prema definiciji funkcije strop, upravo $\lceil a \rceil$, dok je najveći cijeli broj u danom segmentu $\lfloor b \rfloor$, pa se problem svodi na traženje broja cijelih brojeva u segmentu $[\ \lceil a \rceil, \lfloor b \rfloor\ ]$, a on iznosi $\lfloor b \rfloor - \lceil a \rceil + 1$.

Sličnim razmatranjem, za $a, b \in \mathbb{R}, a \leqslant b$, dobiju se sljedeće formule:

Skup	Broj cijelih brojeva u skupu
$[a, b\rangle$	$\lceil b \rceil - \lceil a \rceil$
$\langle a, b]$	$\lfloor b \rfloor - \lfloor a \rfloor$
$\langle a, b\rangle$, $a < b$	$\lceil b \rceil - \lfloor a \rfloor - 1$.

Broj znamenaka u prikazu prirodnog broja u bazi *b*

Pri učenju pretvaranja brojeva iz jednog brojevnog sustava u drugi, može nas zanimati koliko će znamenaka neki broj imati u traženoj bazi b.

Primjer 11. *Koliko će mjesta u memoriji računala zauzeti dekadski broj* 23*, zapisan u binarnom sustavu?*

Rješenje: Kako je $23_{10} = 10111_2$, za zapis u bazi 2 potrebno je 5 znamenaka, odnosno 5 bitova memorije.

Općenito, prirodni broj $n \in \mathbb{N}$, zapisan u bazi $b \in \mathbb{N}$, ima $r \in \mathbb{N}$ znamenki ako je

$$\begin{aligned} b^{r-1} \leqslant n < b^r \quad &\Big/ \log_b \\ r - 1 \leqslant \log_b n < r. & \end{aligned}$$

Uočimo kako je $r - 1$ najveći cijeli broj manji ili jednak od $\log n$, odnosno

$$\lfloor \log_b n \rfloor = r - 1 \quad \Rightarrow \quad r = \lfloor \log_b n \rfloor + 1.$$

Zanimljivi zadaci na ovu temu mogu se pojaviti na učeničkim natjecanjima, nakon obrade logaritamske funkcije.

Zadatak 1. *Neka je x broj znamenaka u decimalnom zapisu broja 2^{2019}, a y broj znamenaka u decimalnom zapisu broja 5^{2019}. Odredi $x + y$.*

Rješenje: Prema prethodno izvedenoj formuli, vrijedi

$$x = \lfloor \log 2^{2019} \rfloor + 1 = \lfloor 2019 \log 2 \rfloor + 1$$
$$y = \lfloor \log 5^{2019} \rfloor + 1 = \lfloor 2019 \log 5 \rfloor + 1.$$

Iz svojstva (4) znamo da vrijedi $\lfloor x \rfloor + 1 > x$, $\forall x \in \mathbb{R}$ iz čega slijedi

$$\lfloor 2019 \log 2 \rfloor + 1 > 2019 \log 2$$
$$\lfloor 2019 \log 5 \rfloor + 1 > 2019 \log 5,$$

pa je

$$\begin{aligned} \underline{x + y} &= \lfloor 2019 \log 2 \rfloor + 1 + \lfloor 2019 \log 5 \rfloor + 1 \\ &\textcircled{>} 2019 \log 2 + 2019 \log 5 \\ &= 2019 \left(\log 2 + \log 5 \right) = 2019 \log 10 = \underline{2019}. \end{aligned}$$

S druge strane, za $x \notin \mathbb{Z}$ zbog (3) vrijedi $\lfloor x \rfloor + 1 < x + 1$. Kako brojevi $2019 \log 2$ i $2019 \log 5$ nisu cijeli, slijedi

$$\lfloor 2019 \log 2 \rfloor + 1 < 2019 \log 2 + 1$$
$$\lfloor 2019 \log 5 \rfloor + 1 < 2019 \log 5 + 1,$$

pa je

$$\begin{aligned} \underline{x + y} &= \lfloor 2019 \log 2 \rfloor + 1 + \lfloor 2019 \log 5 \rfloor + 1 \\ &\textcircled{<} 2019 \log 2 + 2019 \log 5 + 2 \\ &= 2019 \left(\log 2 + \log 5 \right) + 2 = 2019 \log 10 + 2 = \underline{2021}. \end{aligned}$$

Konačno, iz izraza $2019 < x + y < 2021$ i $x + y \in \mathbb{N}$, dobivamo $x + y = 2020$.

Određivanje dana u tjednu iz datuma

Za brojne važne događaje iz osobnog života ili one od povijesne važnosti, znamo točne datume kada su se dogodili, ali za rijetko koji događaj znamo kojeg se dana u tjednu dogodio. Zbog složenosti kalendara koji koristimo, to nije tako lako odrediti.

Za rješenje ovog problema dano je više matematičkih formula, a jedna od njih, koju je osmislio njemački matematičar Karl Zeller, može se izvesti uz elementarno znanje o funkciji pod. Izvod i primjena ove formule može biti zanimljiva tema jedne matematičke radionice za učenike.

Svaki datum možemo prikazati u obliku (d, m, g), gdje d označava redni broj dana u mjesecu, m je broj pridružen svakom mjesecu koji očitavamo iz Tablice 1, a g je godina po Gregorijanskom kalendaru. Zbog specifičnosti formule koju ćemo navesti potrebno je za datume u siječnju i veljači uzeti prethodnu kalendarsku godinu.

	ožujak	travanj	svibanj	lipanj	srpanj	kolovoz	rujan	listopad	studeni	prosinac	siječanj	veljača
m	1	2	3	4	5	6	7	8	9	10	11	12

Tablica 1

Brojeve d, m i g uvrštavamo u formulu

$$D(d, m, g) = d + g + \left\lfloor \frac{g}{4} \right\rfloor - \left\lfloor \frac{g}{100} \right\rfloor + \left\lfloor \frac{g}{400} \right\rfloor + \left\lfloor \frac{13m - 1}{5} \right\rfloor \tag{11}$$

te na osnovu ostatka pri dijeljenju dobivenog broja D brojem 7, iz Tablice 2 doznajemo koji dan u tjednu pripada traženom datumu.

nedjelja	ponedjeljak	utorak	srijeda	četvrtak	petak	subota
0	1	2	3	4	5	6

Tablica 2

Detaljno obrazloženje formule (11) može se pronaći u [9].

Primjer 12. *Koji je dan u tjednu bio* 9. *srpnja* 1995. *godine?*

Rješenje: Stavimo $d = 9$, $m = 5$ i $g = 1995$. Uvrštavanjem u formulu (11) dobivamo $D(9, 5, 1995) = 2499$. Kako ostatak pri dijeljenju broja 2499 sa 7 iznosi 0, prema Tablici 2 znamo da je 9.7.1995. bila nedjelja.

2.3 Primjene u kombinatorici i teoriji brojeva

Koristeći definiciju i svojstva funkcija pod i strop, mnoge se tvrdnje i formule kombinatorne matematike i teorije brojeva mogu (jednostavnije) izraziti pomoću upravo spomenutih funkcija, te pomoću njih riješiti mnoštvo zanimljivih zadataka.

Broj deranžmana

Definicija 11. *Za dani se skup S svaka bijekcija $f : S \to S$ naziva permutacija skupa S. Za $s \in S$ kažemo da je fiksna točka permutacije f ako vrijedi $f(s) = s$.*

Definicija 12. *Permutacije n-članih skupova bez fiksnih točaka nazivamo deranžmanima.*

Primjer 13. *Broj deranžmana tročlanog skupa $\{a, b, c\}$ je 2, jer su $\{b, c, a\}$ i $\{c, a, b\}$ jedine njegove permutacije bez fiksnih točaka.*

Za velike n-ove, broj deranžmana D_n nije jednostavno izračunati prema uobičajenoj formuli

$$D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right).$$

pa se aproksimiranjem broja D_n brojem $n!e^{-1}$ i zaokruživanjem na najbliži cijeli broj (izvod vidjeti u [23, IV, Propozicija 2]) dobiva jednostavnija formula

$$D_n = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor.$$

Tako, jednoga dana na našoj promociji, vjerojatnost da pročelnik podijeli diplome stotini studenata tako da svatko dobije nečiju tuđu diplomu iznosi čak

$$\frac{\text{broj deranžmana}}{\text{ukupan broj permutacija}} = \frac{D_n}{n!} = e^{-1} \approx 0.36788 = 36.79\%.$$

Nadajmo se da se to ipak neće dogoditi.

Dirichletov princip prebrojavanja

Jaku formu Dirichletovog principa možemo izreći u sljedećem obliku:

Propozicija 2. (vidi [11, Excercise 3.8])
Ako n predmeta smjestimo u m kutija, tada barem jedna kutija sadrži najmanje $\lceil n/m \rceil$ predmeta, i barem jedna kutija sadrži najviše $\lfloor n/m \rfloor$ predmeta.

Dokaz: Kada bi sve kutije sadržavale manje od $\lceil n/m \rceil$ predmeta, tada bi ukupan broj predmeta bio $n \leqslant m(\lceil n/m \rceil - 1)$, pa bi vrijedilo $n/m \leqslant \lceil n/m \rceil - 1$, a to je u kontradikciji s (3).

Slično, kada bi sve kutije sadržavale više od $\lfloor n/m \rfloor$ predmeta, ukupan broj predmeta bio bi $n \geqslant m(\lfloor n/m \rfloor + 1)$, iz čega slijedi $n/m \geqslant \lfloor n/m \rfloor + 1$, što ponovno dovodi do kontradikcije s (3). □

Broj višekratnika prirodnog broja manjih ili jednakih od zadanog broja

Primjenom sljedećeg teorema u kojem se koriste osnovna svojstva funkcije pod mogu se riješiti brojni problemi iz teorije brojeva.

Teorem 3. (vidi [17, Lema 1])
Neka je $n \in \mathbb{N}$ i $x \in \mathbb{R}^+ \cup \{0\}$. Tada je broj višekratnika od n koji su manji ili jednaki od x jednak $\left\lfloor \frac{x}{n} \right\rfloor$.

Dokaz: Ako s k označimo broj višekratnika od n manjih ili jednakih od x, onda vrijedi

$$kn \leqslant x < (k+1)n, \quad \text{odnosno} \quad k \leqslant \frac{x}{n} < k+1$$

a prema svojstvu (5) funkcije pod slijedi $k = \left\lfloor \frac{x}{n} \right\rfloor$. □

Primjer 14. *Odredimo broj četveroznamenkastih prirodnih brojeva koji su djeljivi s 4, ali ne i s 20.*

Rješenje: Među brojevima $1000, 1001, \ldots, 9999$ treba odrediti broj višekratnika od 4 koji nisu višekratnici broja 20. Kako je svaki višekratnik od 20 ujedno i višekratnik od 4, treba oduzeti broj višekratnika broja 20 od broja višekratnika od 4.

Broj četveroznamenkastih višekratnika od 4 je

$$\left\lfloor \frac{9999}{4} \right\rfloor - \left\lfloor \frac{999}{4} \right\rfloor = 2250,$$

a broj četveroznamenkastih višekratnika od 20 je

$$\left\lfloor \frac{9999}{20} \right\rfloor - \left\lfloor \frac{999}{20} \right\rfloor = 450.$$

Stoga, traženi broj iznosi $2250 - 450 = 1800$.

Najveća potencija prostog broja p koja dijeli $n!$

Rezultat iz Teorema 3 može se iskoristiti u dokazu sljedeće tvrdnje. Dokaz nećemo navoditi nego se može pogledati u [17], a navest ćemo primjer zadatka u kojem se tvrdnja može iskoristiti.

Teorem 4. (vidi [17, Teorem 1])
Neka je $n \in \mathbb{N}$, p prost broj i $s \in \mathbb{N}$ takav da je $p^s \leqslant n < p^{s+1}$ te a najveći prirodan broj takav da $p^a | n!$. Tada je

$$a = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^s} \right\rfloor.$$

Primjer 15. *S koliko nula završava broj* 2019!*?*

Rješenje: Općenito, broj završava s onoliko nula koliki je eksponent najveće potencije broja 10 koja ga dijeli. Kako je $10 = 2 \cdot 5$, a 2 je prosti faktor s najvećim eksponentom u rastavu broja 2019! na proste faktore, broj nula kojim završava broj 2019! jednak je eksponentu broja 5 u rastavu broja 2019! na proste faktore. Prema Teoremu 15, taj eksponent iznosi

$$\left\lfloor \frac{2019}{5} \right\rfloor + \left\lfloor \frac{2019}{5^2} \right\rfloor + \left\lfloor \frac{2019}{5^3} \right\rfloor + \left\lfloor \frac{2019}{5^4} \right\rfloor = 403 + 80 + 16 + 3 = 502.$$

Prema tome, broj 2019! završava s 502 nule.

Teorem o dijeljenju s ostatkom

Sada ćemo iskazati jedan od polaznih teorema vezan uz djeljivost dvaju cijelih brojeva te ukratko objasniti primjenu funkcije pod pri njegovu dokazivanju.

Teorem 5. (Teorem o dijeljenju s ostatkom, vidi [18, Teorem 1.1.2])
Neka su $a, b \in \mathbb{Z}$ i $a > 0$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je $b = q \cdot a + r$, pri čemu je $0 \leqslant r < a$.

U svrhu dokazivanja egzistencije brojeva q i r iz prethodnog teorema, biramo q takav da za broj $\frac{b}{a}$ vrijedi $q \leqslant \frac{b}{a} < q + 1$. Prema svojstvu (5) funkcije pod to je upravo $q = \left\lfloor \frac{b}{a} \right\rfloor$. Tada je $r = b - a \left\lfloor \frac{b}{a} \right\rfloor$. Broj q nazivamo kvocijent, a r ostatak pri cjelobrojnom dijeljenju.

2.4 Primjene u računalnoj znanosti

Cjelobrojne funkcije pod i strop, kao i brojne druge operacije i funkcije izvedene pomoću njih, implementirane su u gotovo svim računalnim programima te se vrlo često primjenjuju u različitim algoritmima.

Binarne operacije *mod* i *div*

U prethodnom smo potpoglavlju razmatrali kvocijent i ostatak pri cjelobrojnom dijeljenju. Izraze koji ih opisuju možemo generalizirati tako da vrijede za sve realne brojeve x, y, $y \neq 0$ te na taj način definiramo binarne operacije div i mod sa

$$x \text{ div } y = \left\lfloor \frac{x}{y} \right\rfloor,$$
$$x \bmod y = x - y \left\lfloor \frac{x}{y} \right\rfloor.$$

Operacije mod i div u različitim su programskim jezicima implementirane u obliku različitih operatora. Primjerice, u Python-u je // operator koji predstavlja div, a % oznaka za mod.

Pogledajmo primjer trivijalnog algoritma u kojem se koriste ove operacije.

Primjer 16. *Za uneseni troznamenkasti prirodan broj n, program treba ispisati znamenke stotica, desetica i jedinica unesenog broja u obrnutom poretku.*

Rješenje: Pseudokod traženog algoritma glasi:

ulaz(n);
$j \coloneqq n$ **mod 10;**
$d \coloneqq (n$ **div 10) mod 10;**
$s \coloneqq n$ **div 100;**
izlaz(j, d, s);

Nakon unosa željenog troznamenkastog broja n, algoritam računa njegovu znamenku jedinica kao ostatak pri dijeljenju broja n brojem 10 i sprema ju u varijablu j. Zatim pronalazi broj koji predstavlja dvoznamenkasti početak zadanog broja n kao rezultat cjelobrojnog dijeljenja broja n brojem 10, za što se koristi operacija div. Ostatak dijeljenja dvoznamenkastog početka broja n brojem 10 jest znamenka desetica tog broja te se ona sprema u varijablu d. Znamenka stotica dobiva se kao rezultat cjelobrojnog dijeljenja broja n brojem 100 i sprema se u varijablu s. Konačno, u posljednjem se retku znamenke broja n ispisuju redoslijedom: jedinica, desetica, stotica.

Metoda "Podijeli pa vladaj"

Veliki je problem lakše riješiti podjelom na nekoliko manjih istovrsnih problema, pa objedinjenjem njihovih rješenja doći do konačnog rješenja polaznog problema. Metoda "podijeli pa vladaj" koristi se u algoritmima kako bi se smanjila njihova vremenska složenost.

Jednu od podjela problema koji se sastoji od n elemenata, na dva potproblema, možemo načiniti koristeći sljedeću jednakost.

Propozicija 3. (vidi [11])
Za svaki $n \in \mathbb{Z}$ *vrijedi* $n = \lfloor n/2 \rfloor + \lceil n/2 \rceil$.

Dokaz: Ako je n paran, možemo ga prikazati u obliku $n = 2k, k \in \mathbb{Z}$. Tada je $\lfloor n/2 \rfloor = \lfloor 2k/2 \rfloor = \lfloor k \rfloor = k$. Slično je i $\lceil n/2 \rceil = k$, pa tvrdnja vrijedi.

Za n neparan oblika $n = 2k+1, k \in \mathbb{Z}$, imamo $\lfloor n/2 \rfloor = \lfloor (2k+1)/2 \rfloor = \lfloor k + 1/2 \rfloor$. Koristeći svojstvo (9) funkcije pod dobivamo $\lfloor k + 1/2 \rfloor = k + \lfloor 1/2 \rfloor = k$. S druge strane, vrijedi $\lceil n/2 \rceil = \lceil k + 1/2 \rceil$, a zbog svojstva (10) funkcije strop to je jednako $k + \lceil 1/2 \rceil = k + 1$, pa tvrdnja vrijedi i u ovom slučaju. □

Najpoznatiju primjenu ove jednakosti nalazimo u MergeSort algoritmu za sortiranje nekog niza. Algoritam radi na principu podjele niza duljine $n \in \mathbb{N}$ na dva podniza iste duljine (u slučaju neparnog broja $n = 2k+1, k \in \mathbb{N}$ jedan niz sadrži k, a drugi $k+1$ element), sortiranja svake polovice rekurzivno te kombiniranja rezultata spajajući ih u jedan niz (detaljnije vidi u [8, 2.3]).

Zaokruživanje realnog broja na cjelobrojne vrijednosti

Ovisno o prirodi zadanog problema, nekada je potrebno ulazne vrijednosti i/ili (među)rezultate zaokružiti na cjelobrojne. Mnogo je načina na koje to možemo učiniti, pa spomenimo one najčešće korištene, koji se mogu pronaći u obliku gotovih funkcija u programskim jezicima.

- **Zaokruživanje na najveći cijeli broj manji ili jednak od zadanog broja**

Zaokruživanje provodimo tako da na zadani broj primijenimo funkciju pod. U Python-u i Wolfram Mathematica-i na taj način rade funkcije *floor*(), odnosno *Floor*[ ]. Matematički, za uneseni argument $x \in \mathbb{R}$, vraćaju vrijednost $\lfloor x \rfloor$.

- **Zaokruživanje na najmanji cijeli broj veći ili jednak od zadanog broja**

Ovu metodu provodimo tako da na zadani broj primijenimo funkciju strop. U Python-u za to postoji gotova funkcija *ceil*(), a u Wolfram Mathematica-i *Ceil*[ ]. Matematički, broju $x \in \mathbb{R}$ pridružujemo vrijednost $\lceil x \rceil$.

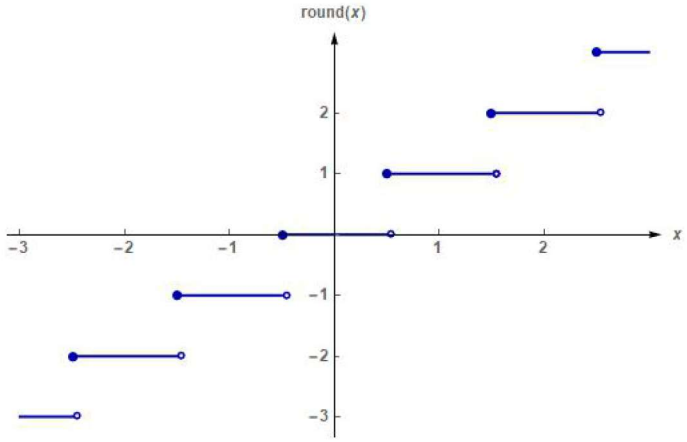
- **Zaokruživanje "prema nuli"**

Još jedna zanimljiva funkcija koja zaokružuje realne brojeve na cijele najčešće se naziva *trunc*(), a ponaša se kao funkcija pod za pozitivne brojeve te kao funkcija strop za negativne brojeve. Često se interpretira i kao funkcija koja jednostavno odbacuje decimalni dio zadanog broja. Pomoću funkcije poda i predznaka možemo ju zapisati kao $trunc(x) = sgn(x) \cdot \lfloor |x| \rfloor$.

Primjer 17. *Vrijedi:* $trunc(1.34) = 1, \quad trunc(-1.34) = -1.$

- **Zaokruživanje na "najbliži" cijeli broj**

Zadani realni broj možemo zaokružiti i na najbliži njemu cijeli broj po apsolutnoj vrijednosti. U Python-u to radi funkcija *round*(), u Wolfram Mathematica-i *Round*[ ], a u njihovoj je pozadini funkcija koja broju $x \in \mathbb{R}$ pridružuje vrijednost $\left\lfloor x + \frac{1}{2} \right\rfloor$. Graf te funkcije možemo vidjeti na sljedećoj slici.



Slika 8: Graf funkcije *round*

Primjer 18. *Vrijedi:* $round(1.4) = 1, \quad round(1.5) = 2, \quad round(1.6) = 2.$

3 Cjelobrojne funkcije u teoriji brojeva

U teoriji brojeva posebno se proučavaju brojne aritmetičke funkcije. To su funkcije čija je domena skup prirodnih brojeva, a poprimaju vrijednosti nekog podskupa skupa kompleksnih brojeva $\mathbb{C}$. Aritmetičke se funkcije često ne mogu opisati jednostavnom formulom, već to činimo opisno ili aproksimativno. U ovom ćemo poglavlju navesti nekoliko cjelobrojnih aritmetičkih funkcija te dati primjere kako i gdje se mogu koristiti.

Kako ćemo se u nastavku poglavlja baviti djeliteljima prirodnih brojeva, prostim brojevima te navesti neka posebna svojstva aritmetičkih funkcija, navedimo najprije njihove definicije i osnovni rezultat na koji ćemo se često pozivati.

Definicija 13. *Neka su a i b cijeli brojevi te neka je $a \neq 0$. Kažemo da a dijeli b ako postoji cijeli broj d takav da vrijedi $b = a \cdot d$. Tada pišemo $a|b$, broj a nazivamo djeliteljem broja b, a broj b višekratnikom broja a.*

Napomena: U nastavku poglavlja bavit ćemo se samo pozitivnim djeliteljima prirodnih brojeva pa to nećemo uvijek posebno naglašavati.

Definicija 14. *Prirodan broj n, $n > 1$ nazivamo prostim ako nema niti jednog djelitelja d za koji vrijedi $1 < d < n$. Broj koji nije prost naziva se složen.*

Definicija 15. *Za cijele brojeve a i b kažemo da su relativno prosti ako je njihov najveći zajednički djelitelj jednak 1. Tada pišemo $(a, b) = 1$.*

Primjer 19. *Broj 3 dijeli broj 15, u oznaci $3|15$, jer postoji $d = 5 \in \mathbb{Z}$ takav da vrijedi $15 = 3 \cdot 5$. Svi pozitivni djelitelji broja 15 su $1, 3, 5$ i 15, pa je on složen broj. Broj 23 je prost broj. Jedini njegovi djelitelji su broj 1 i on sam. Brojevi 15 i 23 su relativno prosti.*

Teorem 6. *(Osnovni teorem aritmetike, vidi [18, Teorem 1.4.3])*
Svaki prirodan broj n, $n > 1$ možemo zapisati u obliku produkta potencija prostih brojeva, jedinstvenog do na poredak faktora.

Primjer 20. *Broj 360 možemo zapisati kao $360 = 2^3 \cdot 3^2 \cdot 5$.*

Definicija 16. *Aritmetička funkcija $f : \mathbb{N} \to \mathbb{C}$ je multiplikativna ako vrijedi $f(1) = 1$ i za sve parove relativno prostih prirodnih brojeva a i b vrijedi $f(a \cdot b) = f(a) \cdot f(b)$.*

Svojstvo multiplikativnosti općenito ima važnu primjenu u gotovo svakom dokazu tvrdnje vezane uz multiplikativne funkcije, a olakšava i računanje vrijednosti samih funkcija.

3.1 Broj djelitelja prirodnog broja

Definicija 17. *Broj djelitelja prirodnog broja opisan je funkcijom* $\tau : \mathbb{N} \to \mathbb{N}$ *koja prirodnom broju* n *pridružuje broj različitih djelitelja od* n*.*

Vrijednosti funkcije τ se u literaturi mogu pronaći u oznakama $d(n), v(n)$ i $\sigma_0(n)$, a definirane su kao

$$\tau(n) = \sum_{d|n} 1.$$

Broj djelitelja nekog prirodnog broja n možemo odrediti postupkom sličnim traženju prostih brojeva pomoću Eratostenovog sita. Postupamo na sljedeći način: redom zapišemo brojeve $1, 2, \ldots, n$ te svaki od njih podcrtamo. Zatim u zapisanom nizu dodamo još jednu crticu ispod svih višekratnika broja 2, pa još jednu crticu ispod svih višekratnika broja 3, itd. Na kraju dodamo crticu ispod broja n. Broj crtica ispod svakog od brojeva u nizu predstavlja broj njegovih djelitelja.

Primjer 21. *Odredimo broj djelitelja prirodnih brojeva od* 1 *do* 12 *pomoću prethodno opisanog postupka.*

Rješenje: Zapišemo brojeve od 1 do 12 te ih podcrtamo na opisani način pa imamo

$$\underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}, \underline{9}, \underline{10}, \underline{11}, \underline{12}.$$

Prebrojavanjem crtica ispod svakog od brojeva dobivamo:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6

.

Sljedeći teorem daje nam matematičku formulu za određivanje $\tau(n)$.

Teorem 7. (vidi [20, CH IV, Theorem 2.])
Broj djelitelja, $\tau(n)$*, prirodnog broja* n *čiji je rastav na faktore dan s*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \alpha_i \geqslant 0, \forall i = 1, \ldots, k.$$

iznosi:

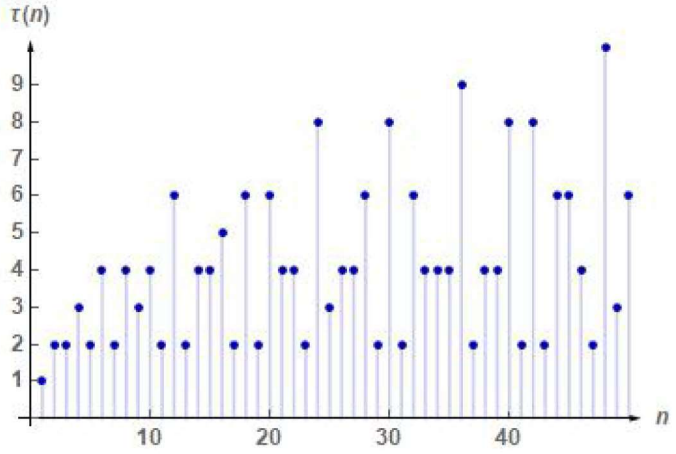
$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1). \tag{12}$$

Primjer 22. *Odredimo* $\tau(360)$ *pomoću formule iz prethodnog teorema.*

Rješenje: U Primjeru 20 vidjeli smo kako je rastav broja 360 na proste faktore oblika $360 = 2^3 \cdot 3^2 \cdot 5$ pa je $\tau(360) = (3 + 1) \cdot (2 + 1) \cdot (1 + 1) = 24$.

Graf i svojstva funkcije τ

Graf na Slici 9 prikazuje vrijednosti funkcije τ za prvih 50 prirodnih brojeva.



Slika 9: Graf funkcije τ

Uočimo na grafu kako je $\tau(n) = 1 \iff n = 1$, a to slijedi i iz (12) jer je $\tau(n) = 1 \iff \alpha_i = 0$, $\forall i = 1, \ldots, n$, tj. $n = 1$. Iz Definicije 14 slijedi kako svaki prost broj ima točno 2 djelitelja, a to je ponovno vidljivo i iz (12) jer je $\tau(n) = 2$ samo ako je $a_i = 1$ za točno jedan $i \in \{1, \ldots, k\}$, a svi ostali a_j, $j \neq i$ su jednaki 0. Dakle, bez smanjenja općenitosti možemo staviti $\alpha_1 = 1$ i slijedi kako je n prost broj. Također, za sve složene prirodne brojeve vrijedi $\tau(n) \geqslant 3$, a za svaki $n \in \mathbb{N}$ vrijedi i ocjena $\tau(n) \leqslant 2\sqrt{n}$ (ideja dokaza može se vidjeti u [20, CH IV, Excercise 1]).

Pokažimo sada još neka svojstva funkcije τ.

- *$\tau(n)$ je neparan prirodan broj ako i samo ako je n potpun kvadrat.*

Zaista, prema formuli (12) vrijedi da je $\tau(n)$ neparan ako i samo ako je $\alpha_i + 1$ neparan za svaki $i = 1, \ldots, k$, a to vrijedi ako i samo ako je α_i paran za svaki $i = 1, \ldots, k$. Tada n možemo zapisati u obliku $n = \left(p_1^{\frac{\alpha_1}{2}} p_2^{\frac{\alpha_2}{2}} \cdots p_k^{\frac{\alpha_k}{2}}\right)^2$, tj. postoji cijeli broj $m \coloneqq p_1^{\frac{\alpha_1}{2}} p_2^{\frac{\alpha_2}{2}} \cdots p_k^{\frac{\alpha_k}{2}}$ takav da je $n = m^2$, pa je n potpun kvadrat.

- *Za svaki prirodan broj $s > 1$ postoji beskonačno mnogo prirodnih brojeva n koji imaju točno s djelitelja.*

Dokaz prethodne tvrdnje također slijedi iz (12). Za svaki $n \in \mathbb{N}$ oblika $n = p^{s-1}$, p prost, vrijedi $\tau(n) = s - 1 + 1 = s$. Kako je prostih brojeva beskonačno mnogo (vidi [18, Teorem 1.4.5.]), slijedi da je i prirodnih brojeva n takvih da je $\tau(n) = s$ beskonačno mnogo.

Primjer 23. *Odredimo sve prirodne brojeve n koji imaju točno 15 djelitelja.*

Rješenje: Vrijedi $\tau(n) = 15 \overset{(12)}{\iff} (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1) = 15$. Broj 15 možemo rastaviti na umnožak nekoliko prirodnih brojeva na dva načina: $15 = 1 \cdot 15$ ili $15 = 3 \cdot 5$. U prvom slučaju mora biti $k = 2$ i bez smanjenja općenitosti možemo staviti $\alpha_1 = 2, \alpha_2 = 4$, a u drugom je $k = 1$ i bez smanjenja općenitosti $\alpha_1 = 14$. To znači da su svi prirodni brojevi koji imaju točno 15 djelitelja oblika $n = p^2q^4$ ili $n = p^{14}$, za međusobno različite proste brojeve p i q.

Nadalje, vrijedi:

- *Funkcija τ je multiplikativna.*

Ovo svojstvo slijedi direktno iz (12) i Osnovnog teorema aritmetike, a dokaz se može vidjeti u [18, 1.4.3.].

Od primjena funkcije τ spomenimo kako se pojavljuje kao koeficijent u razvoju nekih funkcija u redove potencija.

Primjer 24. (detaljnije vidi u [20, CH IV, §3.])

(*a*) *U razvoju Lambertovog reda u red potencija, $\tau(n)$ je koeficijent uz član x^n.*

$$\sum_{k=1}^{\infty} \frac{x^k}{1 - x^k} = \sum_{n=1}^{\infty} \tau(n) x^n.$$

(*b*) *Funkcija τ pojavljuje se u razvoju u red potencija kvadrata Riemannove zeta funkcije ζ, koja ima oblik Dirichletovog reda $\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$. Vrijedi*

$$(\zeta(s))^2 = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}.$$

3.2 Suma djelitelja prirodnog broja

Razmotrimo još jednu cjelobrojnu aritmetičku funkciju uz koju se vežu zanimljivi rezultati u teoriji brojeva.

Definicija 18. *Funkcija $\sigma : \mathbb{N} \to \mathbb{N}$ prirodnom broju n pridružuje vrijednost sume svih njegovih pozitivnih djelitelja.*

Ponekad se za sumu djelitelja prirodnog broja koristi i oznaka σ_1, a matematički se može zapisati kao $\sigma(n) = \sum_{d|n} d$.

Vrijednosti $\sigma(n)$ možemo izračunati pomoću formule iz sljedećeg teorema:

Teorem 8. (vidi [20, CH IV, Theorem 3.])
Suma svih pozitivnih djelitelja prirodnog broja n, čiji je rastav na proste faktore dan s $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ iznosi:

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_1+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \tag{13}$$

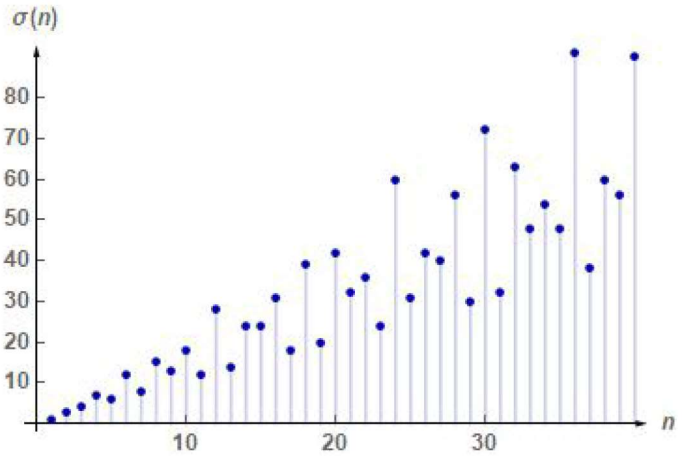
Primjer 25. *Izračunajmo $\sigma(360)$.*

Rješenje: Budući je $360 = 2^3 \cdot 3^2 \cdot 5$, prema formuli (13) imamo

$$\sigma(360) = \sigma(2^3 \cdot 3^2 \cdot 5) = \frac{2^{3+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} = 1170.$$

Graf i svojstva funkcije σ

Na sljedećem grafu vidimo vrijednosti funkcije σ za prvih 40 prirodnih brojeva.



Slika 10: Graf funkcije σ

Gledajući graf, uočimo kako bi donja granica ove funkcije mogao biti zamišljeni pravac $n+1$. Opravdajmo tu pretpostavku sljedećom tvrdnjom.

- *Za svaki prirodan broj $n > 1$ vrijedi $\sigma(n) \geqslant n+1$.*

Naime, prost proj p ima samo dva djelitelja, 1 i p, pa je $\sigma(p) = p+1$. Nadalje, za složen broj n, neka su $a, b > 1$ takvi da je $n = ab$. Tada n ima barem tri djelitelja, $1, a$ i n, pa je $\sigma(n) \geqslant 1 + a + n > n + 1$.

Broj 1 možemo zapisati kao p^0, pri čemu je p bilo koji prost broj. Tada je

$$\sigma(1) = \sigma(p^0) \overset{(13)}{=} \frac{p^1 - 1}{p - 1} = 1.$$

Osim toga, može se pokazati i sljedeća tvrdnja:

- *Postoji beskonačno mnogo prirodnih brojeva s takvih da je $\sigma(n) \neq s, \forall n \in \mathbb{N}$.*

Dokaz se može vidjeti u [20, CH IV, Theorem 4.], a mi pokažimo kako je, primjerice, broj 10 jedan od takvih brojeva. Vrijednosti funkcije σ za prvih 9 prirodnih brojeva dane su u tablici:

n	1	2	3	4	5	6	7	8	9
$\sigma(n)$	1	2	4	7	6	12	8	15	13

Uočimo kako je za svaki $n \leqslant 9, \sigma(n) \neq 10$. Prema prethodno pokazanom svojstvu, za svaki $n \geqslant 10$ vrijedi $\sigma(n) \geqslant 11$, pa broj 10 zaista nije vrijednost funkcije $\sigma(n)$ niti za jedan prirodan broj n.

Nadalje, u [18, 1.4.3.] je pokazano je kako je i funkcija σ multiplikativna.

Slično kao i funkcija τ, funkcija σ pojavljuje se u razvoju nekih posebnih funkcija u redove potencija (detaljnije vidjeti u [20, CH IV, §8.]).

Savršeni i prijateljski brojevi

Kada je riječ o funkciji σ, gotovo je neizostavno spomenuti brojeve čija su egzistencija i svojstva vrlo zanimljiv predmet proučavanja teoriji brojeva. To su savršeni i prijateljski brojevi. Više o njima može se pročitati u [18] ili [20], a mi ćemo navesti njihove definicije i jednostavne primjere.

Definicija 19. *Prirodan broj n nazivamo savršenim ako vrijedi $\sigma(n) = 2n$.*

Primjer 26. *Broj 6 je savršen broj. Zaista,* $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$.

Definicija 20. *Prirodne brojeve m i n nazivamo prijateljskima ako je* $\sigma(m) = m + n = \sigma(n)$.

Primjer 27. *Prvi (ujedno i najmanji) par prijateljskih brojeva otkrili su još Pitagorejci. To su brojevi* 220 *i* 284. *Zaista:*

$$\sigma(220) = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 + 220 = 504$$
$$\sigma(284) = 1 + 2 + 4 + 71 + 142 + 284 = 504.$$

Ako bismo gledali samo sume pravih djelitelja d broja n $(d|n, d \neq n)$, uočimo kako za prijateljske brojeve $m = 220$ i $n = 284$ vrijedi $\sigma(m) = n$ i $\sigma(n) = m$. Prijateljski se brojevi ponekad definiraju i na taj način.

3.3 Eulerova funkcija

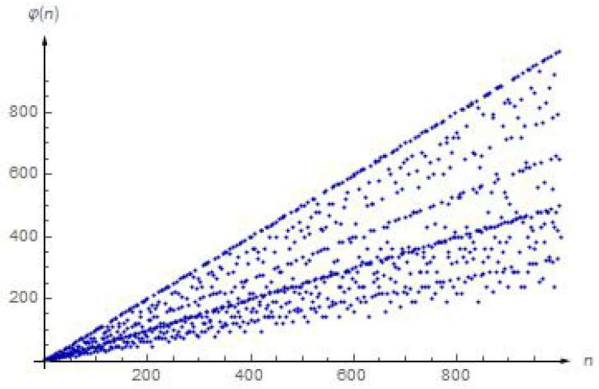
Eulerova funkcija jedna je od najvažnijih funkcija u teoriji brojeva. U mnogim su radovima detaljno opisana svojstva, rezultati i problemi vezani uz ovu funkciju, pa ćemo, kako se ne bi ponavljali, u ovom potpoglavlju, uz definiciju i primjer računanja vrijednosti Eulerove funkcije, navesti samo neke od njenih primjena.

Definicija 21. *Eulerova funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ definirana je s*

$$\varphi(n) = \#\{k \in \mathbb{N} : 1 \leqslant k \leqslant n \text{ i } (k, n) = 1\}.$$

Dakle, Eulerova funkcija prirodnom broju n pridružuje broj prirodnih brojeva manjih ili jednakih od n, koji su relativno prosti s n.

Uočimo odmah kako vrijedi $\varphi(1) = 1$ te kako za svaki prost broj p vrijedi da je relativno prost sa svim prirodnim brojevima strogo manjim od samog sebe, tj. $\varphi(p) = p - 1$. Da je $p - 1$ maksimalna moguća vrijednost Eulerove funkcije vidljivo je i iz njezinog grafa.



Slika 11: Graf Eulerove funkcije

Vrijedi i sljedeći rezultat:

Teorem 9. (vidi [18, Teorem 2.2.7])
Eulerova funkcija φ je multiplikativna.

Svojstvo multiplikativnosti ponekad uvelike olakšava računanje vrijednosti $\varphi(n)$.

Primjer 28. *Izračunajmo* $\varphi(2019)$.

Rješenje: Rastavimo broj 2019 na proste faktore. Dakle, $2019 = 3 \cdot 673$. Kako su 3 i 673 relativno prosti, primjenom svojstva multiplikativnosti lako se izračuna

$$\varphi(2019) = \varphi(3) \cdot \varphi(673) = 2 \cdot 672 = 1344.$$

Vrijednosti Eulerove funkcije za proizvoljan $n \in \mathbb{N}$, čiji je rastav na proste faktore oblika $n = \prod_{i=1}^{k} p_i^{\alpha_i}, \alpha_i \geqslant 0, i = 1, \ldots, k$ možemo izračunati pomoću formule

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) \tag{14}$$

čiji se izvod može vidjeti u [20, CH VI, Theorem 3].

Primjer 29. *Izračunajmo* $\varphi\left(20^{19}\right)$.

Rješenje: Kako je $20^{19} = \left(2^2 \cdot 5\right)^{19} = 2^{38} \cdot 5^{19}$, prema (14) je

$$\varphi(20^{19}) = 2^{37} \cdot (2-1) \cdot 5^{18} \cdot (5-1) = 2^{39} \cdot 5^{18}.$$

Eulerova je funkcija sastavni dio dvaju važnih teorema teorije brojeva na koje se nadovezuju brojne njezine primjene. U njima se spominju kongruencije, pa ih prije navođenja samih teorema definirajmo, a više o njihovim svojstvima može se pronaći u [18, 2.1].

Definicija 22. *Neka je $n \in \mathbb{N}$ te $a, b \in \mathbb{Z}$. Ako n dijeli razliku $a - b$, tada kažemo da je a kongruentan b modulo n i pišemo $a \equiv b \pmod{n}$.*

Primjer 30. $5 \equiv 1 \pmod{2}$, *jer* 2 *dijeli razliku* $5 - 1 = 4$.

Teorem 10. (**Eulerov teorem**, vidi [18, Teorem 2.2.2])
Neka su $a \in \mathbb{Z}$ i $n \in \mathbb{N}$ takvi da je $(a, n) = 1$. Tada vrijedi

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Kao direktna posljedica Eulerovog teorema slijedi Mali Fermatov teorem:

Teorem 11. (**Mali Fermatov teorem**, vidi [18, Korolar 2.2.3])
Neka su $a \in \mathbb{Z}$ i p prost broj. Ako $p \nmid a$, vrijedi $a^{p-1} \equiv 1 \pmod{p}$. Nadalje, za svaki $a \in \mathbb{Z}$ vrijedi $a^p \equiv a \pmod{p}$.

Primjene Eulerove funkcije

Koristeći prethodne rezultate, pokažimo primjenu Eulerove funkcije na nekoliko različitih primjera.

Primjer 31. *Odredimo ostatak pri dijeljenju broja* 2019^{20} *brojem* 22.

Rješenje: Zbog $\varphi(22) = \varphi(2) \cdot \varphi(11) = (2-1) \cdot (11-1) = 10$ i $(2019, 22) = 1$, prema Eulerovom teoremu vrijedi

$$2019^{10} \equiv 1 \pmod{22}$$

pa je

$$2019^{20} \equiv (2019^{10})^2 \equiv 1 \pmod{22},$$

tj. traženi ostatak je 1.

Na sličan se način Eulerova funkcija koristi pri rješavanju linearnih kongruencija (primjere pogledati u [20, CH VI]), a važnu ulogu ima i u kriptografiji, posebice RSA kriptosustavu.

Definicija 23. *Neka je $n = pq$ gdje su p i q prosti brojevi. Neka je $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ skup svih mogućih elemenata otvorenih tekstova i šifrata, a*

$$\mathcal{K} = \{(n, p, q, d, e) : n = pq,\ p, q \text{ prosti, } de \equiv 1 \pmod{\varphi(n)}\}$$

skup svih mogućih ključeva.
Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo funkcije šifriranja i dešifriranja

$$e_K(x) = x^e \bmod n \quad i \quad d_K(y) = y^d \bmod n$$

gdje su $x, y \in \mathbb{Z}_n$. Vrijednosti n i e su javne, a p, q i d tajne.

Eulerov teorem koristi se u dokazu da su gore navedene funkcije međusobno inverzne, tj. da je $d_k(e_k(x)) = x$, a to je najvažnije svojstvo kriptosustava (vidi [13]).

Primjer 32. *Korištenjem RSA kriptosustava šifrirajmo poruku NE.*

Rješenje: Slovima iz otvorenog teksta pridružimo broj koji predstavlja njihovu poziciju u međunarodnom (engleskom) alfabetu koristeći dogovorenu korespondenciju A$-$0, B$-$1, C$-$2, $\ldots$, Z$-$25. Dakle, slovu N pridružujemo broj 13, a slovu E broj 4, pa numerički ekvivalent otvorenog teksta glasi 134.

Odaberimo $p = 5$ i $q = 13$. Tada je $n = 65$ i $\varphi(65) = 4 \cdot 12 = 48$. Odaberimo e relativno prost s $\varphi(65)$, npr. $e = 11$.

Za $x = 13$ i $x = 4$ odredimo $e_K(13) = 13^{11} \bmod 65$ i $e_K(4) = 4^{11} \bmod 65$. Imamo:

$$13^{11} \equiv 13^3 \cdot 13^3 \cdot 13^3 \cdot 13^2 \equiv 52 \cdot 52 \cdot 52 \cdot 39 \equiv 52 \pmod{65}$$
$$4^{11} \equiv 4^4 \cdot 4^4 \cdot 4^3 \equiv 61 \cdot 61 \cdot 64 \equiv 49 \pmod{65},$$

tj. $e_K(13) = 52$, $e_K(4) = 49$, pa uz javni ključ $(n, e) = (65, 11)$ šifrat glasi 52 49. Pri dešifriranju bi bilo potrebno odrediti d takav da je $11d \equiv 1 \pmod{\varphi(65)}$. Nekom od metoda rješavanja linearne kongruencije dobili bi $d = 35$ i polazni tekst NE.

Obrat Malog Fermatovog teorema općenito ne vrijedi, ali može poslužiti za ispitivanje prostosti prirodnih brojeva. Naime, ako postoji prirodan broj $a < n - 1$ takav da $a^{n-1} \not\equiv 1 \pmod{n}$, tada n nije prost. No, treba biti oprezan, ako za prirodan broj n vrijedi $a^{n-1} \equiv 1 \pmod{n}$, za svaki $a \in \{2, 3, \ldots, n-1\}$, ne znači da je n prost. Stoga se za brojeve koji zadovoljavaju neka od ovih svojstava uvode pojmovi pseudoprostih i Carmichaelovih brojeva o kojima se detaljnije može pročitati u [18], a mi ćemo navesti samo njihove definicije.

Definicija 24. *Neka je n neparan složen broj i a cijeli broj takav da je $(n, a) = 1$ i $a^{n-1} \equiv 1 \pmod{n}$. Tada za n kažemo da je pseudoprost u bazi a.*

Definicija 25. *Složen prirodan broj n naziva se Carmichaelov broj ako za sve prirodne brojeve a koji su relativno prosti s n vrijedi $a^{n-1} \equiv 1 \pmod{n}$.*

Primjer 33. *Za $n = 8$ i $a = 3$ vrijedi $3^7 \equiv 3 \not\equiv 1 \pmod{8}$ pa broj 8 nije prost. S druge strane, za $n = 91$ i $a = 3$ vrijedi $3^{90} \equiv 1 \pmod{91}$, ali $91 = 7 \cdot 13$ nije prost broj. On je pseudoprost u bazi 3.*

Zanimljiv problem vezan uz Eulerovu funkciju javlja se i u konstruktivnoj geometriji.

Teorem 12. (Gauss - Wantzelov teorem, vidi [16])
Pravilan n-terokut može se konstruirati ravnalom i šestarom ako i samo ako je n prirodan broj veći od 2 takav da je $\varphi(n)$ potencija broja 2.

Dakle, neki konstruktibilni pravilni $n-$terokuti su $3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots -$ erokuti.

3.4 Još neke cjelobrojne aritmetičke funkcije

Navedimo definicije i eventualne primjene još nekoliko zanimljivih cjelobrojnih aritmetičkih funkcija, uz izuzetak funkcije π za čiju se domenu najčešće uzima skup realnih brojeva.

- **$\sigma_k(n)$ - suma k-tih potencija pozitivnih djelitelja od n**

Definicija 26. *Funkcija $\sigma_k : \mathbb{N} \to \mathbb{R}$ definirana sa $\sigma_k(n) = \sum_{d|n} d^k$ prirodnom broju n pridružuje sumu $k-$tih potencija njegovih pozitivnih djelitelja.*

Ako je k prirodan broj, onda je σ_k cjelobrojna funkcija. Primijetimo kako su funkcije τ i σ zapravo specijalni slučajevi ove funkcije za $k = 0$, odnosno $k = 1$.

Primjer 34. *Pozitivni djelitelji broja 10 su $1, 2, 5$ i 10 pa je $\sigma_3(10) = 1^3 + 2^3 + 5^3 + 10^3 = 1134$.*

- **$\omega(n)$ - broj različitih prostih faktora od n**

Definicija 27. *Funkcijom $\omega : \mathbb{N} \to \mathbb{N}_0$ definiranom s*

$$\omega(n) = \begin{cases} 0, & n = 1 \\ k, & n = \prod_{i=1}^{k} p_i^{\alpha_i}, \end{cases} \qquad tj. \quad \omega(n) = \sum_{p|n} 1, \text{p prost}$$

dan je broj različitih prostih faktora prirodnog broja n.

Primjer 35. *Vrijedi:*

(a) $\omega(p) = 1$, *za prost broj p;*

(b) $\omega(900) = \omega(2^2 \cdot 3^2 \cdot 5^2) = 3$.

- **Möbiusova funkcija**

Definicija 28.
Funkcija $\mu : \mathbb{N} \to \{-1, 0, 1\}$ definirana s

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^k, & n = \prod_{i=1}^{k} p_i, \text{ gdje su } p_i \text{ različiti prosti brojevi} \\ 0, & \text{inače} \end{cases}$$

zove se Möbiusova funkcija.

Primjer 36. *Vrijedi:* $\mu(2) = 1, \quad \mu(4) = \mu(2 \cdot 2) = 0, \quad \mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1.$

Kako bismo lakše izračunali vrijednosti $\mu(n)$ za složene prirodne brojeve n, navedimo i sljedeći rezultat:

Teorem 13. (vidi [14, Theorem 2.1.])
Möbiusova funkcija je multiplikativna.

Möbiusovu je funkciju moguće dovesti u vezu s Eulerovom (vidi [14, Theorem 2.8.]). Vrijedi:

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{15}$$

Primjer 37. *Pomoću formule* (15) *mogu se računati vrijednosti funkcije* φ. *Primjerice, djelitelji broja* 20 *su* $1, 2, 4, 5, 10, 20$, *pa je*

$$\varphi(20) = 20 \sum_{d|20} \frac{\mu(d)}{d} = 20 \cdot \left(\frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(4)}{4} + \frac{\mu(5)}{5} + \frac{\mu(10)}{10} + \frac{\mu(20)}{20} \right).$$

Kako je $\mu(1) = 1$, $\mu(2) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(10) = \mu(2 \cdot 5) = 1$, $\mu(20) = 0$, *slijedi*

$$\varphi(20) = 20 \cdot \left(1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{10} \right) = 8.$$

Neke zanimljive primjene Möbiusove funkcije mogu se detaljnije vidjeti u [14, 3.2].

- **Liouvilleova funkcija**

Definicija 29. *Funkcija* $\lambda : \mathbb{N} \to \mathbb{N}$ *definirana s*

$$\lambda(n) = \begin{cases} 1, & n = 1 \\ (-1)^{\alpha_1 + \alpha_2 + \cdots + \alpha_k}, & n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \end{cases}$$

zove se Liovilleova funkcija.

Može se pokazati (vidjeti u [20, CH IV, Theorem 7.]) da je

$$\sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{ako je } n \text{ potpun kvadrat} \\ 0, & \text{ako } n \text{ nije potpun kvadrat.} \end{cases}$$

Liouvilleova se funkcija, kao i neke prethodno spomenute aritmetičke funkcije, može pronaći u razvoju određenih funkcija u redove potencija. Primjerice:

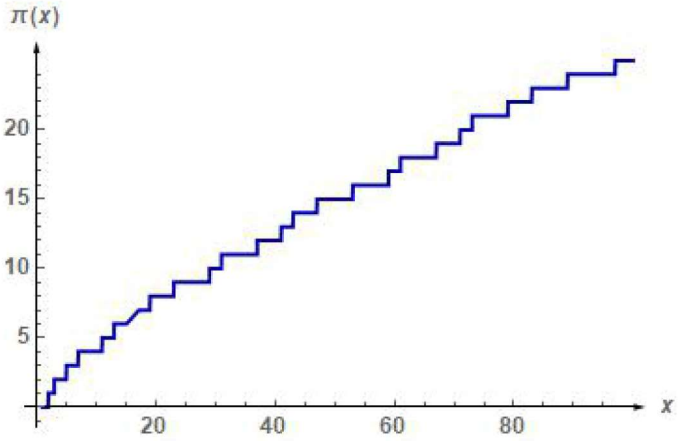
$$\frac{\zeta(2s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s},$$

gdje je ζ Riemannova zeta funkcija.

- **$\pi(x)$ - broj prostih brojeva manjih ili jednakih od x**

Definicija 30. *Funkcija* $\pi : \mathbb{R} \to \mathbb{N}_0$ *svakom realnom broju* x *pridružuje broj prostih brojeva koju su manji ili jednaki od* x.

Na Slici 12 vidimo vrijednosti funkcije π za pozitivne brojeve $x \leqslant 100$. Uočimo kako je $\pi(x) = 0$, $\forall x < 2$.



Slika 12: Vrijednosti funkcije π

Za male vrijednosti varijable x, vrijednost $\pi(x)$ moguće je pronaći tako da pomoću algoritma Eratostenovog sita pronađemo sve proste brojeve manje od x te ih prebrojimo. No, taj postupak predugo traje za velike vrijednosti od x. Zato su za funkciju π dane brojne numeričke aproksimacije, a najčešće korištenu, predstavljenu kao *Prime Number Theorem*, dokazali su Hadamarde i de la Valée Poussin 1896. godine (vidi [24]). Ona govori o asimptotskom ponašanju funkcije π kada x teži u beskonačnost:

$$\pi(x) \sim \frac{x}{\ln x}, \quad x \to \infty.$$

Korisna interpretacija funkcije π jest da vjerojatnost da je slučajno izabran pozitivan cijeli broj prost iznosi približno

$$\frac{\pi(x)}{x} \sim \frac{\frac{x}{\ln x}}{x} = \frac{1}{\ln x}.$$

Primjerice, imamo li kriptosustav u kojem su za sigurno šifriranje potrebni vrlo veliki prosti brojevi, čak do 1000 znamenaka, i pokrenemo li neki algoritam koji generira slučajne brojeve do 10^{1000} te provjerava jesu li prosti, vjerojatnost da će prvi generirani broj biti prost iznosi

$$\frac{\text{broj prostih brojeva manjih od } 10^{1000}}{10^{1000}} = \frac{\pi(10^{1000})}{10^{1000}} \sim \frac{1}{\ln 10^{1000}},$$

što znači da u prosjeku treba testirati $\ln(10^{1000}) \approx 2302$ broja dok ne pronađe prvog koji je prost.

4 Cjelobrojni polinomi

U ovom ćemo poglavlju izdvojiti skup cjelobrojnih polinoma kao podskup skupa cjelobrojnih funkcija te pojasniti zašto je zanimljiv predmet proučavanja u algebri.

Definicija 31. *Neka je* $n \in \mathbb{N}_0$ *te* $a_0, a_1, \ldots, a_n \in D$, *pri čemu je* $D \subseteq \mathbb{R}$ *ili* $D \subseteq \mathbb{C}$ *i* $a_n \neq 0$. *Funkcija*

$$p_n(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

naziva se polinom n-tog stupnja u varijabli x *nad skupom* D. *Brojeve* $a_0, a_1, \ldots, a_n$ *nazivamo koeficijentima polinoma* p_n.

Polinome koji za svaki element domene poprimaju cjelobrojne vrijednosti nazivamo **cjelobrojnim polinomima**.

Napomena: U daljnjem ćemo radu promatrati polinome cjelobrojne varijable, što ponekad nećemo više posebno naglašavati.

Ako promatramo polinome čija je domena skup cijelih brojeva, očito je kako tada polinom s cjelobrojnim koeficijentima uvijek poprima cjelobrojne vrijednosti. Pitanje je možemo li i kako konstruirati cjelobrojne polinome cjelobrojne varijable s koeficijentima iz nekog drugog skupa. Pokušajmo to učiniti induktivno u ovisnosti o stupnju polinoma u varijabli $x \in \mathbb{Z}$:

- $\underline{n = 1}$:
  polinom $a \cdot x$ je cjelobrojan za svaki $x \in \mathbb{Z}$ samo ako je $a \in \mathbb{Z}$ (jer je skup $\mathbb{Z}$ zatvoren obzirom na množenje);
- $\underline{n = 2}$:
  polinom $a \cdot \frac{x(x-1)}{2}$, $a \in \mathbb{Z}$ je cjelobrojan jer je $\frac{x(x-1)}{2} = \binom{x}{2}$ binomni koeficijent[3];
- $\underline{n = 3}$:
  za $a \in \mathbb{Z}$ je $a \cdot \frac{x(x-1)(x-2)}{2 \cdot 3} = a \cdot \binom{x}{3} \in \mathbb{Z}$;
  $\vdots$
- $\underline{n \in \mathbb{N}}$ proizvoljan:
  za $a \in \mathbb{Z}$ je $a \cdot \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!} = a \cdot \binom{x}{n} \in \mathbb{Z}$.

[3]binomni je koeficijent pozitivan cijeli broj (vidi [23, strana 81.])

Na ovaj smo način definirali cjelobrojne polinome cjelobrojne varijable s koeficijentima iz skupa racionalnih brojeva. Ispravnost ovog razmatranja i jedinstvenost ovakve konstrukcije potvrđuje sljedeći teorem:

Teorem 14. (vidi [19, Chapter 2., 85.])
Polinom $p_n(x)$ cjelobrojne varijable x, stupnja n, je cjelobrojan ako i samo ako se može prikazati kao linearna kombinacija polinoma definiranih pomoću binomnih koeficijenata

$$p_n(x) = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \cdots + a_1 \binom{x}{1} + a_0,$$

pri čemu su $a_0, a_1, \ldots, a_n \in \mathbb{Z}$.

Prema [19], ovaj su rezultat već u 17. stoljeću neformalno poznavali poznati matematičari poput Newtona i Briggsa, no tada su cjelobrojne polinome koristili samo u sklopu tehnika računanja poput Gregory - Newtonove formule za određivanje interpolacijskog polinoma uz ekvidistantne čvorove ili pri izradi logaritamskih tablica. Tek su u 20. stoljeću Georg Pólya i Alexander Ostrowsky u svojim radovima objavili prve rezultate koji opisuju algebarska svojstva cjelobrojnih polinoma.

Prsten cjelobrojnih polinoma

I danas se u algebri proučavaju brojne tvrdnje vezane uz cjelobrojne polinome, no zbog opsežnosti bi njihovo navođenje izašlo iz okvira ovog rada, pa ćemo samo kratko pokazati algebarsku strukturu prstena cjelobrojnih funkcija i njegovog potprstena cjelobrojnih polinoma te spomenuti primjenu u algebarskoj geometriji.

Definicija 32. *Prsten je neprazan skup R na kome su zadane binarne operacije zbrajanja $(a, b) \mapsto a + b$ i množenja $(a, b) \mapsto ab$ za koje vrijedi:*

(a) *$(R, +)$ je Abelova grupa;*

(b) *$(R, \cdot)$ je polugrupa;*

(c) *množenje je i s lijeva i desna distributivno u odnosu na zbrajanje.*

Primjer 38. $(\mathbb{Z}, +, \cdot)$ *je prsten.*

Rješenje: Za operaciju zbrajanja na skupu $\mathbb{Z}$ očito vrijede svojstva asocijativnosti i komutativnosti. Za zbrajanje je 0 neutralni element, a za svaki element $a \in \mathbb{Z}$ je broj $-a \in \mathbb{Z}$ njemu suprotan element, pa je $(R, +)$ Abelova grupa. Za operaciju množenja očito vrijedi asocijativnost, a broj 1 je neutralni element za množenje, pa je $(R, \cdot)$ polugrupa. U skupu $\mathbb{Z}$ vrijedi i obostrana distributivnost množenja obzirom na zbrajanje.

Primjer 39. *Skup svih funkcija $f : D \to \mathbb{Z}$ je prsten uz binarne operacije zbrajanja i množenja "po točkama" definirane s*

$$\begin{aligned} (f+g)(x) &= f(x) + g(x), \\ (f \cdot g)(x) &= f(x) \cdot g(x), \end{aligned} \tag{16}$$

za svaki $x \in D$, pri čemu su operacije zbrajanja i množenja s desnih strana jednakosti standardne operacije na $\mathbb{Z}$.

Rješenje: Nasljeđujući svojstva skupa $\mathbb{Z}$, na skupu cjelobrojnih funkcija za operaciju zbrajanja i množenja iz (16) vrijede svojstva asocijativnosti. Isto tako vrijedi i komutativnost zbrajanja i obostrana distributivnost množenja u odnosu na zbrajanje. Ulogu neutralnog elementa za zbrajanje ima funkcija $f(x) = 0$, za svaki $x \in D$. Za svaku cjelobrojnu funkciju f postoji funkcija $-f$ koja je također cjelobrojna i funkciji f je suprotan element obzirom na zbrajanje. Ulogu neutralnog elementa za množenje ima funkcija $f(x) = 1$, za svaki $x \in D$.

Navedimo sada definiciju potprstena nekog prstena koja će nam koristiti za jednostavnija pojašnjenja budućih tvrdnji.

Definicija 33. *Potprsten prstena R je podskup S skupa R koji je i sam prsten u odnosu na operacije od R.*

Dakle, kako bi pokazali da je skup cjelobrojnih polinoma prsten, dovoljno je pokazati da je potprsten skupa cjelobrojnih funkcija.

Teorem 15. (Karakterizacija potprstena, vidi [5, Teorem 2.2.2.])
Neprazan podskup S prstena R je potprsten prstena R ako za sve $a, b \in S$ vrijedi $a - b \in S$ i $ab \in S$.

Primjer 40. *Skup cjelobrojnih polinoma je potprsten prstena cjelobrojnih funkcija.*

Rješenje: Označimo sa S skup svih cjelobrojnih polinoma i s R skup svih cjelobrojnih funkcija. Skup S je očito neprazan jer npr. za $h \in R$ definiranu s $h(x) = 1$ za svaki x iz njene domene vrijedi i $h \in S$.

Neka su $f, g \in S$. Razlika i umnožak dvaju polinoma ponovno je polinom. Slično dokazu Primjera 39, zbog svojstava naslijeđenih is skupa cijelih brojeva, polinomi $f - g$ i $f \cdot g$ su cjelobrojni. Prema karakterizaciji iz Teorema 15, skup S je potprsten od R.

Kako smo pokazali da vrijedi tvrdnja iz Primjera 40, prema Definiciji 33 skup svih cjelobrojnih polinoma je i sam prsten uz operacije definirane sa (16).

Proučavanje svojstava prstena cjelobrojnih polinoma i njegovih modula dovodi nas do brojnih primjena u algebarskoj geometriji. Sve se to detaljnije može vidjeti u [21].

Literatura

[1] M. Bencze, F. Smarandache, University of Braşov, University of New Mexico, *About the characteristic function on a set*, dostupno na `https://arxiv.org/ftp/arxiv/papers/0707/0707.2969.pdf`.

[2] M. Benšić, N. Šuvak, *Uvod u vjerojatnost i statistiku*, Odjel za matematiku, Sveučilište u Osijeku, Osijek, 2014.

[3] A. Bourchtein, L. Bourchtein, *Counterexamples on Uniform Convergence; Sequences, Series, Functions and Integrals*, John Willey & Sons, SAD, 2017.

[4] W. E. Boyce, R. C. DiPrima, *Elementary Differential Equations and Boundary Value Problems*, John Willey & Sons, SAD, 2001.

[5] D. Brajković, *Algebra kroz primjere*, Odjel za matematiku, Sveučilište u Osijeku, Osijek, 2018.

[6] P. J. Cahen, J. P. Chabert, *Integer - Valued Polynomials*, AMS, Providence, 1997.

[7] R. Castro, *The Empirical Distribution Function and the Histogram*, Eindhoven University of Technology, dostupno na `https://www.win.tue.nl/~rmcastro/2WS17/files/ecdf_hist.pdf`.

[8] T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein, *Introduction to Algoritms, 2ed*, MIT Press, 2001.

[9] J. Delač-Klepac, *Čarobmatička priča: Određivanje dana u tjednu iz zadanog datuma*, Matka **25**(2016/2017), 2–7.

[10] N. Elezović, *Vjerojatnost i statistika, Slučajne varijable*, Element, Zagreb, 2007.

[11] K. Graham, D. E. Knuth, O. Patashnik, *Concrete mathematics: a foundation for computer science*, Addison – Wesley, Boston, 1994.

[12] I. Gogić, A. Mimica, *Matematička analiza II*, primjeri i zadaci, Matematički odjel PMF, 2010., dostupno na `https://web.math.pmf.unizg.hr/~ilja/ma2_vjezbe.pdf`.

[13] B. Ibrahimpašić, *RSA kriptosustav*, Osječki matematički list **5**(2005), 101–112.

[14] Z. Islek, *Möbius Inversion Formula and Applications to Cyclotomic Polynomials*, Linnaeus University, 2012.

[15] D. Jukić, *Neprekidna preslikavanja*, Nastavni materijali, Odjel za matematiku, Sveučilište u Osijeku, Osijek, dostupno na `https://www.mathos.unios.hr/~jukicd/realna/neprekidnost.pdf`.

[16] D. Kuh, *Constructible Regular n-gons*, Whitman College, 2013.

[17] I. Kuzmanović, *Neke primjene funkcija pod i strop*, Osječki matematički list **8**(2008), 77–82.

[18] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku, Osijek, 2014.

[19] G. Polya, G. Szegö, *Problems and Theorems in Analysis II*, Stanford University, USA, Springer, 1976.

[20] W. Sierpinski, *Elementary theory of numbers*, North - Holland, Amsterdam, 1988.

[21] J. R. Smith, *Introduction to Algebraic Geometry*, Five Dimensions Press, 2014.

[22] Š. Ungar, *Matematička analiza 3*, Matematički odjel PMF, Zagreb, 1994.

[23] D. Veljan, *Kombinatorna i diskretna matematika*, Algoritam, Zagreb, 2001.

[24] D. Zagier, *Newman's Short Proof of the Prime Number Theorem*, The American Mathematical Monthly **104**(1997), 705–708.

Sažetak

Glavni cilj ovog rada jest upoznati čitatelje s nekima od cjelobrojnih funkcija te njihovim primjenama u svakodnevnom životu i raznim područjima matematike i drugih znanosti. Iz same definicije cjelobrojnih funkcija kao funkcija čija je slika podskup skupa cijelih brojeva jasno je kako se radi o vrlo velikom skupu funkcija, pa su za prezentaciju u ovom radu odabrane one od posebne važnosti u teorijskoj matematici te cjelobrojne funkcije sa zanimljivim primjenama u modeliranju situacija iz stvarnog života. Rad je podijeljen u četiri smisleno odijeljena i tematski podosta različita poglavlja.

Na samom smo početku definirali vrlo trivijalnu cjelobrojnu funkciju zvanu karakteristična ili indikator funkcija. Naveli smo neka njena svojstva te pokazali kako se u različitim oblicima može primijeniti u matematičkoj analizi, teoriji vjerojatnosti i statistici. Iskoristili smo ju i pri dokazu tvrdnje da nekonstantne cjelobrojne funkcije imaju prekid. Uzimajući linearnu kombinaciju karakterističnih funkcija, definirali smo veliku klasu stepenastih funkcija te naveli jednostavne primjere s primjenama.

Zbog brojnih zanimljivih primjena, cjelobrojne stepenaste funkcije pod i strop zaslužile su posebno poglavlje u ovom radu. Istaknuli smo kako bi bilo poželjno češće ih obrađivati u redovnoj i dodatnoj nastavi, zbog lakog razumijevanja i predočavanja njihovih svojstava te brojnih primjena u bliskim situacijama iz svakodnevnog života. Pomoću funkcija pod i strop pojednostavili smo neke složenije matematičke formule te definirali druge operacije i funkcije koje primjenu nalaze u kombinatorici, teoriji brojeva i računalnoj znanosti.

U trećem je poglavlju dan pregled cjelobrojnih aritmetičkih funkcija u teoriji brojeva. Najpoznatije od njih, broj i suma djelitelja te Eulerova funkcija, detaljnije su opisane te su kratko navedene njihove primjene. Definirali smo i nekoliko zanimljivih funkcija koje se vežu uz svojstva prirodnih, posebice prostih brojeva.

Na kraju smo se dotaknuli algebarskih svojstava skupa cjelobrojnih funkcija te izdvojili njegov podskup cjelobrojnih polinoma, čija struktura prstena vodi do brojnih primjena u algebri i algebarskoj geometriji.

Ključne riječi: cjelobrojne funkcije, karakteristična funkcija, stepenaste funkcije, funkcije pod i strop, aritmetičke funkcije, cjelobrojni polinomi

Integer-valued functions and applications

Summary

The aim of this paper is to introduce the readers to some of integer-valued functions, their real-life applications, and applications in different fields of mathematics and other sciences. The integer-valued functions are functions whose image is some subset of integers. It yields from the definition that the set of integer functions includes a large number of functions. In this paper, we chose and present those with great importance in theoretical mathematics and has an application in real-life.

In Chapter 1, we defined a trivial integer function called characteristic or indicator function and gave some of its properties and applications in analysis, probability, and statistics. It is used to show that every integer function, not equal to constant, has discontinuity. By taking the linear combination of characteristic functions, we defined a big class of step functions. Through examples we illustrated some of their applications.

The next chapter deals with interesting properties and applications of floor and ceiling function. Since they are easily understandable and have lots of applications in familiar real-life situations, we pointed out that they should be more involved in school curriculum. Moreover, by using these functions we simplified some complex formulae and defined some other operations and functions, used in combinatorics, number theory and computer science.

The Chapter 3 of this paper gives the review of integer-valued arithmetic functions in number theory. We shortly listed the most important of them, i.e., number and sum of divisors of positive integer, Euler function and their applications. Moreover, we defined some other interesting functions which mostly deal with primes.

Finally, we explained the algebraic properties of integer-valued functions and integer-valued polynomials whose ring structure leads to numerous applications in algebra and algebraic geometry.

Keywords: integer-valued functions, characteristic function, step functions, floor and ceiling functions, arithmetic functions, integer-valued polynomials

Životopis

Rođena sam 9. srpnja 1995. godine u Osijeku. Pohađala sam Osnovnu školu Antuna Mihanovića i III. gimnaziju u Osijeku te nakon toga, 2014. godine, upisala Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku u Osijeku. Sudjelovala sam na brojnim osnovnoškolskim i srednjoškolskim natjecanjima, te kroz cijelo školovanje primala stipendije za izvrnost. U akademskoj godini 2018./2019. nagrađena sam Rektorovom nagradom za izvrstan seminarski rad iz kolegija Matematički modeli. Prezime Lacković, udajom 2017. godine, promijenila sam u Piškorjanac, a iste sam godine postala majka djevojčice Lene.