Funkcije u teoriji brojeva

Živković, Antonio

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:744551

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Antonio Živković

Funkcije u teoriji brojeva

Završni rad

Osijek, 2019.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Antonio Živković

Funkcije u teoriji brojeva

Završni rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2019.

Sadržaj

Uvod **iv**

1 Funkcija najveće cijelo **1**

2 Aritmetičke funkcije **5**

3 Möbiusova funkcija **11**

Literatura **17**

Sažetak

U ovome radu proučit ćemo neke aritmetičke funkcije,funkciju najveće cijelo i Möbiusovu funkciju. Upoznat ćemo se s njihovim osnovnim svojstvima, objasniti kako se računa vrijednost pojedine funkcije te sve upotpuniti odgovarajućim primjerima

Ključne riječi

Funkcija najveće cijelo, aritmetičke funkcije, Möbiusova funkcija, multiplikativna funkcija, prosti brojevi

Abstract

In this paper, we will consider some arithmetic functions, greatest integer function and Möbius function. We will talk about their basic properties, explain how to calculate their value and illustrate all of that with suitable examples.

Key words

Floor function, arithmetic functions, Möbius function, , multiplicative function, prime numbers.

Uvod

Jedna od najstarijih grana matematike je aritmetika (grč. arithmos - broj i techne - umijeće) koja se bavi proučavanjem računskih operacija s brojevima. Svojstva cijelih brojeva izučava teorija brojeva, koja je ustvari dio aritmetike. Osnovni pojam u teoriji brojeva je pojam djeljivosti. Pomoću definicije djeljivosti možemo složene brojeve rastavljati na proste faktore.

Među najznačajnijim funkcijama u teoriji brojeva su Möbiusova te aritmetičke funkcije koje su osnova ovog rada. Proučavana su njihova važna svojstva te kao bitan zaključak napomenuto je svojstvo multiplikativnosti zbog kojeg imaju veliku primjenu u matematici. U radu je primjena aritmetičkih funkcija posebno prikazana u proučavanju savršenih brojeva. Pokazali smo na koji način nam Möbiusova funkcija može poslužiti u računanju ciklotomskih polinoma.

1 Funkcija najveće cijelo

Krenemo li iz skupa realnih brojeva, ali i dalje su nam u interesu svojstva cijelih brojeva, sljedeća funkcija nam za dani realan broj vraća cijeli broj.

Definicija 1.1. *Za realan broj x, oznaka $[x]$ znači najveći cijeli broj manji ili jednak broju x.*

Funkcija je definirana za sve realne brojeve te uzima samo njihov cijeli dio, tj. $[x]$ je jedinstveni cijeli broj takav da vrijedi

$$[x] \leq x < [x] + 1.$$

Razliku nekog realnog broja x i njegovog najvećeg cijelog broja zovemo razlomljeni dio, a označavamo s $\{x\}$. Dakle, vrijedi

$$\{x\} = x - [x], 0 \leq \{x\} < 1.$$

Primjer 1.1. *Odredimo vrijednost funkcije najveće cijelo za dane brojeve:*

x	$[x]$	$\{x\}$
2.51	2	0.51
-3.88	-4	0.12
-7	-7	0
6	6	0

Osnovna svojstva funkcije $x \mapsto [x]$ dana su u sljedećem teoremu.

Teorem 1.1. *Neka su x i y realni brojevi. Tada vrijedi:*

1. $[x] \leq x < [x] + 1$, $x - 1 < [x] \leq x$, $0 \leq x - [x] < 1$,
2. $[x] = \sum_{1 \leq i \leq x} 1$, *za* $x \geq 0$,
3. $[x + m] = [x] + m$, *za cijeli broj* m.
4. $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$,
5. $[x] + [-x] = \begin{cases} 0, & \text{ako je } x \text{ cijeli broj} \\ -1, & \text{inače} \end{cases}$,
6. $[\frac{[x]}{m}] = [\frac{x}{m}]$, *za prirodan broj* m,
7. $-[-x]$ *je najmanji cijeli broj veći ili jednak* x,
8. $[x + \frac{1}{2}]$ *je najbliži cijeli broj broju* x. *Ako su dva cijela broja jednako udaljena od* x, *tada uzimamo veći od ta dva.*
9. $-[-x + \frac{1}{2}]$ *je najbliži cijeli broj broju* x. *Ako su dva cijela broja jednako udaljena od* x, *tada uzimamo manji od ta dva.*
10. *Ako su* a *i* n *prirodni brojevi, tada je* $[\frac{n}{a}]$ *broj cijelih brojeva između* 1 *i* n *koji su djeljivi sa* a.

Dokaz.

1. Slijedi iz definicije funkcije najveće cijelo zapisane u algebarskom obliku.

2. Za $x < 1$ je suma prazna, a dogovor je da je takva suma 0. Za $x \geq 0$ suma broji pozitivne i koji su manji ili jednaki od x, a taj broj je upravo $[x]$.

3. Očito iz definicije.

4. Neka je $x = n+\nu$ i $y = m+\mu$ gdje su m i n cijeli brojevi takvi da je $0 \leq \nu < 1$ i $0 \leq \mu < 1$. Tada vrijedi

$$\begin{aligned}[x] + [y] = n + m \leq [n + \nu + m + \mu] = [x + y] = \\ = n + m + [\nu + \mu] \leq n + m + 1 = [x] + [y] + 1.\end{aligned}$$

5. Neka je $x = n + \nu$. Odatle je $-x = -n - 1 + 1 - \nu$ za $0 < 1 - \nu \leq 1$. Tada slijedi

$$[x] + [-x] = n + [-n - 1 + 1 - \nu] = n - n - 1 + [1 - \nu] = \begin{cases} 0, & \text{ako je } \nu = 0 \\ -1, & \text{ako je } \nu > 0 \end{cases}.$$

6. Neka je $x = n + \nu$ i $n = qm + r$ gdje je $0 \leq \nu < 1$ i $0 \leq r \leq m - 1$. Tada slijedi

$$\left[\frac{x}{m}\right] = \left[\frac{qm + r + \nu}{m}\right] = q + \left[\frac{r + \nu}{m}\right] = q$$

   za $0 \leq r + \nu < m$. Tada zbog jednakosti

$$\left[\frac{[x]}{m}\right] = \left[\frac{n}{m}\right] = \left[q + \frac{r}{m}\right] = q$$

   slijedi tvrdnja teorema.

7. U prvoj tvrdnji ovog teorema zamijenimo x sa $-x$ i dobijemo $-x - 1 < [-x] \leq -x$ pa vrijedi $x \leq -[-x] < x + 1$ što dokazuje 7.

8. Neka je n najbliži cijeli broj broju x, odnosno veći ako su jednako udaljeni. Tada

$$\begin{aligned} n = x + \theta - \frac{1}{2} < \theta \leq \frac{1}{2} \\ \left[x + \frac{1}{2}\right] = n + \left[-\theta + \frac{1}{2}\right] = n \end{aligned}$$

   za $0 \leq -\theta + \frac{1}{2} < 1$.

9. Slično kao prethodni dokaz.

10. Sve prirodne brojeve koji su manji ili jednaki od n označimo s a, $2a$, $3a$, $\ldots$, $j \cdot a$. Oni su djeljivi s a pa moramo dokazati da je $[\frac{n}{a}] = j$. No, vidimo da je $(j+1)a > n$ pa vrijede

$$\begin{aligned} j \cdot a \leq n < (j+1)a \\ j \leq \frac{n}{a} < j+1 \\ \left[\frac{n}{a}\right] = j. \end{aligned}$$

□

Sljedeći teorem daje dekompoziciju od $n!$ za cijeli broj $n \geq 1$.

Teorem 1.2 (de Polignacova formula)**.** *Neka je p prost broj. Najveća potencija e takva da $p^e \mid n!$ dana je izrazom*

$$e = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

Dokaz. Za slučaj kada je $p^i > n$ imamo $[\frac{n}{p^i}] = 0$ pa je prethodna suma konačna. Drugi slučaj lako se pokaže matematičkom indukcijom.

Baza Za 1! tvrdnja vrijedi.

Pretpostavka Pretpostavimo da tvrdnja vrijedi za $(n-1)!$.

Korak Označimo s j najveći cijeli broj takav da $p^j \mid n$. Kako je $n! = n(n-1)!$, treba pokazati da je

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] - \sum_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right] = j.$$

Vrijedi

$$\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right] = \begin{cases} 1, & \text{ako } p^i \mid n \\ 0, & \text{inače} \end{cases}$$

i stoga

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] - \sum_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right] = j.$$

Teorem možemo dokazati i na drugi način tako da promatramo nenegativne cijele brojeve a_1, a_2, $\ldots$, a_n. Označimo s $f(1)$ broj svih takvih brojeva koji su veći ili jednaki od 1, s $f(2)$ broj svih većih ili jednakih od 2 i tako redom. Tada imamo

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{\infty} f(i)$$

budući da a_i doprinosi 1 na svaki od brojeva $f(1)$, $f(2)$, $\ldots$, $f(a_i)$. Za $1 \leq j \leq n$ neka je a_j najveći cijeli broj takav da $p^{a_j} \mid j$. Tada vidimo da je $e = a_1 + a_2 + \cdots + a_n$. Osim toga, $f(i)$ broji koliko ima cijelih brojeva manjih ili jednakih n koji su djeljivi s p^i.

Dakle, $f(k)$ broji cijele brojeve p^k, $2p^k$, $3p^k$, $\ldots$, $[\frac{n}{p^k}]p^k$ te je $f(k) = [\frac{n}{p^k}]$. Tada vidimo da je

$$e = \sum_{i=1}^{n} a_i = \sum_{i=1}^{\infty} f(i) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

Pomoću formule (6) Teorema 1.1 možemo lakše odrediti e iz gornjeg teorema.

□

Primjer 1.2. *Odredimo najveću potenciju broja* 7 *kojom je djeljivo* 1000!.

Računamo:

$$[\tfrac{1000}{7}] = 142 \quad [\tfrac{1000}{49}] = 20 \quad [\tfrac{1000}{343}] = 2 \quad [\tfrac{1000}{2401}] = 0.$$

Zbrajanjem rezultata dobivamo $7^{164} \mid 1000!$, *a* $7^{165} \nmid 1000!$.

2 Aritmetičke funkcije

Funkcije definirane za sve prirodne brojeve n nazivaju se aritmetičke funkcije ili funkcije u teoriji brojeva. Aritmetička funkcija f za domenu ima prirodne brojeve dok joj je kodomena podskup skupa kompleksnih brojeva.

Svojstvo multiplikativnosti funkcija u teoriji brojeva vrlo je važno svojstvo koje ima primjenu u gotovo svakom dokazu. Sve funkcije navedene dalje u radu imaju stvojstvo multiplikativnosti. Definirajmo to svojstvo odmah na samom početku promatranja aritmetičkih funkcija.

Definicija 2.1. *Funkcija $f\colon \mathbb{N} \to \mathbb{C}$ je multiplikativna ako vrijedi*

- $f(1) = 1$,
- $f(mn) = f(m)f(n)$ *za relativno proste brojeve m i n.*

Napomena 2.1. *Aritmetička funkcija je potpuno multiplikativna ako vrijedi*

$$f(mn) = f(m)f(n)$$

za sve cijele brojeve m i n.

Definicija 2.2. *Neka je n prirodan broj. Broj prirodnih brojeva u nizu $1, \ldots, n$ koji su relativno prosti s n oznaava se s $\varphi(n)$. Ovim je definirana funkcija $\varphi\colon \mathbb{N} \to \mathbb{N}$ koja se naziva Eulerova funkcija.*

Primjer 2.1.

$$\varphi(7) = 6 \quad \varphi(6) = 2 \quad \varphi(1) = 1.$$

Ako je p prost broj, tada je $\varphi(p) = p - 1$. Osim toga, ako za neki prirodan broj n vrijedi $\varphi(n) = n - 1$, možemo zaključiti da je n relativno prost sa svakim manjim prirodnim brojem. Prema tome, n nema djeljitelja većeg od 1 i manjeg od n pa je prost.

Lema 2.1. *Neka je p prost broj i $k \in \mathbb{N}$. Tada je $\varphi(p^k) = p^k - p^{k-1}$.*

Dokaz. Neka je $1 \leq n \leq p^k$. Ako p ne dijeli n, tada su n i p^k relativno prosti. Prema tome, jedini brojevi u nizu $1, 2, \ldots, p^k$ koji nisu relativno prosti s p^k su $p, 2p, \ldots, p^k = p^{k-1} \cdot p$. Takvih brojeva ima p^{k-1} te slijedi da je $\varphi(p^k) = p^k - p^{k-1}$. □

Pokažimo svojstvo multiplikativnosti Eulerove funkcije koje će nam kasnije biti od velike koristi.

Teorem 2.1. *Eulerova funkcija je multiplikativna.*

Dokaz. Od prije znamo da je $\varphi(1) = 1$. Nadalje, neka su m i n relativno prosti cijeli brojevi. Definirajmo skupove $S_1 = \{a \in \mathbb{N}\colon a \leq mn, (a, mn) = 1\}$, $S_2 = \{a \in \mathbb{N}\colon a \leq m, (a, m) = 1\}$ i $S_3 = \{a \in \mathbb{N}\colon a \leq n, (a, n) = 1\}$. Očito je $|S_1| = \varphi(mn)$, $|S_2| = \varphi(m)$ i $|S_3| = \varphi(n)$.

Za $t \in \{0, 1, \ldots, mn - 1\}$ neka je $i(t) = (a, b)$ gdje je $i\colon \{0, 1, \ldots, mn - 1\} \to \{0, 1, \ldots, m - 1\} \times \{0, 1, \ldots, n - 1\}$ definirano s

$$i(t) = (t \bmod m, t \bmod n).$$

Primijetimo da je $(t, mn) = 1$ ako i samo ako je $(a, m) = (b, n) = 1$.

Kako je $t = k_1 m + a = k_2 n + b$, slijedi da je svaki zajednički prost djelitelj brojeva t i m (odnosno, b i n) ujedno i zajednički prost djelitelj brojeva a i m (odnosno, b i n). Prema tome, restrikcija preslikavanja i na skup S_1 je bijekcija sa skupa S_1 u skup $S_2 \times S_3$ iz čega slijedi $\varphi(mn) = \varphi(m)\varphi(n)$. □

Pokažimo primjenu gore dokazane multiplikativnosti Eulerove funkcije na neki složeni prirodan broj.

Primjer 2.2. *Izračunajmo* $\varphi(756)$.

Broj 756 *možemo zapisati na sljedeći način:*

$$756 = 2^2 \cdot 3^3 \cdot 7.$$

Tada imamo

$$\varphi(756) = \varphi(2^2 \cdot 3^3 \cdot 7) = \varphi(2^2) \cdot \varphi(3^3) \cdot \varphi(7).$$

Sada iskoristimo Lemu 2.1 za računanje vrijednosti Eulerove funkcije

$$\begin{aligned} \varphi(2^2) &= 2^2 - 2^1 = 2 \\ \varphi(3^3) &= 3^3 - 3^2 = 18 \\ \varphi(7) &= 7^1 - 7^0 = 6. \end{aligned}$$

Traženi rezultat je

$$\varphi(756) = 2 \cdot 18 \cdot 6 = 216.$$

Sljedeći rezultat može nam poslužiti za računanje vrijednosti Eulerovih funkcija za veće prirodne brojeve.

Neka je $n > 1$ prirodan broj čiji je zapis u obliku umnoška prostih faktora oblika

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Tada je

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) = \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Pokažimo gornji iskaz na primjeru složenog broja.

Primjer 2.3. *Izračunajmo vrijednost Eulerove funkcije za brojeve* 36 *i* 85.

$$\begin{aligned} \varphi(36) &= 36 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 12 \\ \varphi(85) &= 85 \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{17}\right) = 64. \end{aligned}$$

Teorem 2.2. *Za svaki prirodan broj n vrijedi*

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

Dokaz. Neka je $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Zbog multiplikativnosti funkcije φ imamo:

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{\alpha_i})).$$

Nadalje, množenjem desne strane gornjeg izraza dobivamo sumu faktora

$$\varphi(p_1^{\beta_1}) \cdots \varphi(p_k^{\beta_k}) = \varphi(p_1^{\beta_1} \cdots p_k^{\beta_k})$$

gdje je $0 \leq \beta_i \leq \alpha_1$, $i = 1, \ldots, k$ što je upravo lijeva strana izraza. Tada je

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + (p_i - 1) + (p_i^2 - p_i) + \cdots + (p_i^{\alpha_i} - p_i^{\alpha_i - 1})) = \prod_{i=1}^{k} p_i^{\alpha_i} = n.$$

□

Osim Eulerove funkcije, za prirodne brojeve možemo definirati broj i sumu djelitelja koje su također sve aritmetičke funkcije. Navedene su u definiciji.

Definicija 2.3. *Za prirodne brojeve n definiramo sljedeće funkcije*

- *$d(n)$ je broj pozitivnih djelitelja od n,*
- *$\sigma(n)$ je suma pozitivnih djelitelja od n,*
- *$\sigma_k(n)$ je suma k-tih potencija pozitivnih djelitelja od n,*
- *$\omega(n)$ je broj različitih prostih brojeva koji dijele n,*
- *$\Omega(n)$ je broj prostih brojeva koji dijele n, računajući kratnost.*

Primjer 2.4. *Neka je $n = 12$. Djelitelji broja 12 su $1, 2, 3, 4, 6, 12$. Tada je*

$$d(12) = 6 \quad \sigma(12) = 28 \quad \sigma_2(12) = 210 \quad \omega(12) = 2 \quad \Omega(12) = 3.$$

Broj k iz definicije može biti bilo koji realan broj. Kompleksna vrijednost broja k koristi se samo u naprednim istraživanjima. Funkcija djelitelja $d(n)$ je specijalan slučaj za $k = 0$, tj. $d(n) = \sigma_0(n)$. Slično, vrijedi i $\sigma(n) = \sigma_1(n)$. Zbog lakšeg razumijevanja i jednostavnosti koristimo se simbolima za sumu $\sum_{d|n} f(d)$ i produkt $\prod_{d|n} f(d)$ za $f(d)$ za sve pozitivne djelitelje d broja n. Stoga pišemo:

$$d(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d, \qquad \sigma_k(n) = \sum_{d|n} d^k$$

$$\omega(n) = \sum_{p|n} 1, \qquad \Omega(n) = \sum_{p^\alpha || n} \alpha = \sum_{p^\beta | n} 1.$$

Teorem 2.3. *Neka je $f(n)$ multiplikativna funkcija i neka je $F(n) = \sum_{d|n} f(d)$. Tada je $F(n)$ multiplikativna.*

Dokaz. Pretpostavimo da je $m = m_1 m_2$ gdje su m_1 i m_2 relativno prosti. Ako $d|m$, tada uzmemo $d_1 = (d, m_1)$ i $d_2 = (d, m_2)$. Prema tome, $d = d_1 d_2$, $d_1|m_1$ i $d_2|m_2$.

Obratno, za dane d_1, d_2 djelitelje od m_1 i m_2 redom vrijedi da je $d = d_1 d_2$ djelitelj od m i $d_1 = (d, m_1)$, $d_2 = (d, m_2)$. Na osnovu toga imamo jedan-jedan korespondenciju (vezu) između pozitivnih djelitelja d od m i parova pozitivnih djelitelja. Stoga, vrijedi

$$F(m) = \sum_{d|m} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2)$$

za svaku funkciju f. Kako je $(d_1, d_2) = 1$, iz pretpostavke da je f multiplikativna slijedi da je desna strana jednakosti

$$\sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1) f(d_2) = \left(\sum_{d_1|m_1} f(d_1) \right) \left(\sum_{d_2|m_2} f(d_2) \right) = F(m_1) F(m_2).$$

□

Trebamo li izračunati vrijednost funkcije σ za velike prirodne brojeve, sljedeći teorem olakšava nam računanje sume djelitelja.

Teorem 2.4. *Za svaki prirodan broj n vrijedi*

$$\sigma(n) = \prod_{p^\alpha || n} \left(\frac{p^{\alpha+1} - 1}{p - 1} \right).$$

Dokaz. U slučaju $n = 1$, $\alpha = 0$ za sve proste brojeve p, tada je svaki faktor u produktu jednak 1 pa slijedi da je $\sigma(1) = 1$.

Nadalje, na definiciju $\sigma(n) = \sum_{d|n} d$ možemo primijeniti prethodni teorem $f(n) = n$, $F(n) = \sigma(n)$. Prema tome, $\sigma(n)$ je multiplikativna pa je $\sigma(n) = \prod \sigma(p^\alpha)$. No, pozitivni djelitelji od p^α su $1, p, p^2, \ldots, p^\alpha$ čija je suma $\frac{p^{\alpha+1}-1}{p-1}$. □

Primjer 2.5. *Neka je $n = 120$ koji smo raspisali u obliku $120 = 2^3 \cdot 3 \cdot 5$.*

Tada računamo:

$$\sigma(120) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 360.$$

Pokažimo da σ ima svojstvo multiplikativnosti. Očito je da vrijedi $\sigma(1) = 1$. Osim toga, za prosti broj p vrijedi

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

Promotrimo slučaj kada je $n = p^k q^l$ gdje su p i q prosti brojevi. Tada imamo:

$$\begin{aligned}
\sigma(p^k q^l) &= 1 + p + p^2 + \cdots + p^k + q + pq + p^2 q + \cdots + p^k q + \cdots + \\
&\quad + q^l + pq^l + p^2 q^l + \cdots + p^k q^l = \\
&= (1 + p + p^2 + \cdots + p^k)(1 + q + q^2 + \cdots + q^l) = \\
&= \frac{p^{k+1} - 1}{p - 1} \cdot \frac{q^{l+1} - 1}{q - 1} = \sigma(p^k) \cdot \sigma(q^l).
\end{aligned}$$

Generalizacijom gornjeg izraza dobivamo

$$\sigma(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}) = \prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1} = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\cdots\sigma(p_k^{\alpha_k})$$

Slično kao i za sumu djelitelja, broj djelitelja d za velike prirodne brojeve n možemo na lakši način izračunati primjenom formule iz sljedećeg teorema.

Teorem 2.5. *Za svaki prirodan broj n vrijedi*

$$d(n) = \prod_{p^\alpha||n}(\alpha+1).$$

Dokaz. Neka je $n = \prod p^\alpha$ prikaz broja n u obliku produkta potencija prostih brojeva. Pozitivan cijeli broj $d = \prod p^\beta$ dijeli n ako i samo ako $0 \leq \beta(p) \leq \alpha(p)$ za sve proste brojeve p. Kako $\beta(p)$ može imati neke od sljedećih vrijednosti: $0, 1, \ldots, \alpha(p)$, slijedi da postoji $\alpha(p)+1$ mogućih vrijednosti za $\beta(p)$. Stoga je broj djelitelja od n dan izrazom $\prod_{p^\alpha||n}(\alpha+1)$. □

Posljedica ovog teorema je sljedeće svojstvo: ako je $(m,n) = 1$, onda $d(mn) = d(m)d(n)$.

Primjer 2.6. *Neka je $n = 120$. Rastavom na proste faktore dobivamo $120 = 2^3 \cdot 3 \cdot 5$ pa je $d(120) = (3+1)(1+1)(1+1) = 16$.*

Posebno, izraz vrijedi ako su cijeli brojevi $m_1, m_2, \ldots, m_r$ potencije različitih prostih brojeva. Kako se svaki prirodan broj veći od 1 može faktorizirati kao produkt potencija različitih prostih brojeva,ako je f multiplikativna funkcija za koju znamo vrijednost $f(p^\alpha)$ za svaki prosti broj p i svaki prirodan broj α tada vrijednost $f(n)$ za svaki prirodan broj n može se lako odrediti multipliciranjem.

Primjerice, $f(3600) = f(2^4)f(3^2)f(5^2)$.

Neka su a i b relativno prosti prirodni brojevi. Prikažimo ih u obliku $a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ i $b = q_1^{\beta_1}q_2^{\beta_2}\cdots q_l^{\beta_l}$. Budući da su a i b relativno prosti, mora vrijediti $p_i \neq q_j$ za sve i, j. Dakle, $a \cdot b = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \cdot q_1^{\beta_1}q_2^{\beta_2}\cdots q_l^{\beta_l}$ odakle slijedi

$$d(ab) = (\alpha_1+1)\cdots(\alpha_k+1)\cdot(\beta_1+1)\cdots(\beta_l+1) = d(a)d(b).$$

Primjer 2.7. *Za prirodan broj n kažemo da je savršen ako je $\sigma(n) = 2n$, tj. ako je n jednak sumi svojih pravih djelitelja.*

Na primjer, 6 i 28 su savršeni brojevi.

$$n = 6 \qquad \sigma(6) = 1+2+3+6 = 12 = 2\cdot 6$$
$$n = 28 \qquad \sigma(28) = 1+2+4+7+14+28 = 56 = 2\cdot 28$$

Primjer 2.8. *Dokažimo da je $\sum_{d|n} d^{-1} = 2$ ako i samo ako je n savršen.*

Naime,

$$\sum_{d|n} d^{-1} = \sum_{d|n}\frac{1}{d} = \sum_{d|n}\frac{1}{\frac{n}{d}} = \sum_{d|n}\frac{d}{n} = \frac{\sum_{d|n} d}{n} = \frac{\sigma(n)}{n}.$$

Dakle, $\frac{\sigma(n)}{n} = 2$ ako i samo ako je $\sigma(n) = 2n$ ako i samo ako je n savršen.

Primjer 2.9. *Pokažimo da je paran broj savršen ako i samo ako je oblika* $2^{p-1}(2^p-1)$ *gdje su* p *i* 2^p-1 *prosti brojevi.*

Neka je $m = 2^{n-1}(2^n-1)$. *Tada imamo* $\sigma(m) = 2m$.

$$\sigma(m) = \sigma(2^{n-1}(2^n-1)) = \sigma(2^{n-1})\sigma(2^n-1) = \frac{2^n-1}{2-1}\cdot 2^n = (2^n-1)2^n =$$
$$= 2\cdot 2^{n-1}(2^n-1) = 2m.$$

Primjenili smo formule $\sigma(p^j) = \frac{p^{j+1}-1}{p-1}$ *i* $\sigma(p) = p+1$.
Nije poznato postoji li neki neparan broj koji je savršen.

Starim Grcima, oko 100 godina poslije Krista, bila su poznata samo četiri savršena broja. Nikomah je u svojoj knjizi „Introductio Arithmeticae" kao savršene brojeve naveo

$$P_1 = 6 \qquad P_2 = 28 \qquad P_3 = 496 \qquad P_4 = 8128$$

te je zaključio da postoji jedan jednoznamenkasti, jedan dvoznamenkasti, jedan troznamenkasti i jedan četveroznamenkasti savršen broj. Na osnovu toga postavio je sljedeće hipoteze koje su pogrešne

1. n-ti savršen broj P_n sadrži točno n znamenki,
2. parni savršeni brojevi završavaju naizmjence na 6 i 8.

3 Möbiusova funkcija

Definicija 3.1. *Neka su $f(x)$ i $g(x)$ funkcije kojima je domena skup prirodnih ili realnih brojeva. Pišemo $f(x) = O(g(x))$ ako postoji konstanta C takva da je*

$$|f(x)| \leq Cg(x)$$

za svaki x.

Napomena 3.1. *Za funkciju najveće cijelo, $[x] = x - \{x\}$, možemo pisati $[x] = x + O(1)$ budući da je $\{x\}$ funkcija odozgo omeđena s 1.*

U narednim dokazima koristit ćemo $\left[\frac{x}{n}\right] = \frac{x}{n} + O(1)$. Nadalje, zbog

$$\int_1^{[x]} \frac{1}{t} dt \leq \sum_{n \leq x} \frac{1}{n} < 1 + \int_1^x \frac{1}{t} dt,$$

što možemo zapisati i na sljedeći način

$$0 \leq \ln[x] \leq \sum_{n \leq x} \frac{1}{n} < 1 + \ln x,$$

možcmo pisati

$$\sum_{n \leq x} \frac{1}{n} = \ln x + O(1).$$

Definicija 3.2. *Ako za prirodne brojeve n vrijedi*

$$\mu(n) = \begin{cases} 1, & \text{ako je } n = 1 \\ 0, & \text{ako je } n \text{ kvadratno slobodan} \\ (-1)^k, & \text{ako je } n \text{ kvadratno slobodan} \end{cases},$$

pri čemu je k broj prostih faktora broja n, onda kažemo da je $\mu(n)$ Möbiusova funkcija.

Primjer 3.1. *Pogledajmo kako izgleda Möbiusova funkcija za neke prirodne brojeve:*

$$\begin{aligned} \mu(2) &= (-1)^1 = -1 \\ \mu(3) &= (-1)^1 = -1 \\ \mu(4) &= \mu(2^2) = 0 \\ \mu(6) &= (-1)^2 = 1 \\ \mu(8) &= \mu(2^3) = 0. \end{aligned}$$

Ako je p prost broj, onda je $\mu(p) = -1$.

Pokažimo neke zanimljive rezultate za prirodne brojeve koji se odnose na Möbiusovu funkciju.

Primjer 3.2. *Dokažite da za svaki $n \in \mathbb{N}$ vrijedi*

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

Naime, $n, n+1, n+2, n+3$ su četiri uzastopna prirodna broja pa je točno jedan od njih djeljiv s 4. Zbog toga je vrijednost Möbiusove funkcije u tom broju jednaka 0 te je i produkt jednak 0.

Primjer 3.3. *Nađimo prirodan broj n za koji vrijedi*

$$\mu(n) + \mu(n+1) + \mu(n+2) = 3.$$

Iz zadane jednadžbe zaključujemo da mora vrijediti

$$\mu(n) = \mu(n+1) = \mu(n+2) = 1.$$

Prema tome, $n, n+1, n+2$ su tri uzastopna prirodna broja od kojih niti jedan nije prost jer je vrijednost Möbiusove funkcije za prost broj jednaka -1. Nadalje, niti jedan od ta tri broja ne smije biti višekratnik od 4 jer je $\mu(4) = 0$. Zaključujemo da su to brojevi oblika $4k+1$, $4k+2$ i $4k+3$. Traženi brojevi su 33, 34 i 35 koje rastavljamo na $3 \cdot 11$, $2 \cdot 17$ i $5 \cdot 7$ te za svaki od njih vrijedi $\mu(n) = (-1)^2 = 1$ što u sumi zadovoljava zadani izraz.

Nadalje, pokažimo koja svojstva ima Möbiusova funkcija.

Teorem 3.1. *Funkcija $\mu(n)$ je multiplikativna i vrijedi*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{ako je } n = 1 \\ 0, & \text{ako je } n > 1 \end{cases}.$$

Dokaz. Iz definicije zaključujemo da je $\mu(n)$ multiplikativna. Ako je $F(n) = \sum_{d|n} \mu(d)$, tada je $F(n)$ multiplikativna po Teoremu 2.3.

Vidimo da je $F(1) = \mu(1) = 1$. Ako je $n > 1$, $\alpha > 0$ za neki prosti broj p, tada je $F(p^\alpha) = \sum_{\beta=0}^{\alpha} \mu(p^\beta) = 1 + (-1) = 0$ što je željeni rezultat.

Isto možemo dokazati pomoću kvadratno slobodnih djelitelja d od n s točno k prostih faktora. Takvih djelitelja ima $\binom{\omega(n)}{k}$ od kojih svaki pridonosi $\mu(d) = (-1)^k$. Tada je...

$$\sum_{k=0}^{\omega(n)} \binom{\omega(n)}{k} (-1)^k = (1-1)^{\omega(n)}.$$

□

Budući da smo pokazali da je μ multiplikativna funkcija, također slijedi da je i funkcija $\nu \colon \mathbb{N} \to \mathbb{C}$ definirana s

$$\nu(n) = \sum_{d|n} \mu(d)$$

multiplikativna. To znači da je $\nu(1) = 1$, dok za $n > 1$ vrijedi

$$\begin{aligned} \nu(n) &= \nu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \nu(p_1^{\alpha_1}) \cdots \nu(p_k^{\alpha_k}) = \\ &= (\mu(1) + \mu(p_1) + \mu(p_1^2) + \cdots) \cdots (\mu(1) + \mu(p_k) + \mu(p_k^2) + \cdots) = \\ &= (1 - 1 + 0 + \cdots) \cdots (1 - 1 + 0 + \cdots) = 0. \end{aligned}$$

Dobiveni rezultat ima ključnu ulogu u dokazu sljedećeg teorema.

Teorem 3.2 (Möbiusova formula inverzije). *Neka je $f\colon \mathbb{N} \to \mathbb{C}$ proizvoljna funkcija te neka je $F(n) = \sum_{d|n} f(d)$, $n \in \mathbb{N}$. Tada je*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Obratno, ako je $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ za svaki $n \in \mathbb{Z}$, onda je $F(n) = \sum_{d|n} f(d)$.

Dokaz. Imamo

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} f(d') \nu\left(\frac{n}{d'}\right) = f(n).$$

Da bismo dokazali obrat, zapišimo $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ na sljedeći način:

$$f(n) = \sum_{d'|n} \mu\left(\frac{n}{d'}\right) F(d').$$

Pomoću tog zapisa dobijemo

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu\left(\frac{n}{dd'}\right) F(d') = \sum_{d'|n} F(d') \nu\left(\frac{n}{d'}\right) = F(n).$$

□

Primijenimo li gornji teorem na rezultat Teorema 2.2 $\sum_{d|n} \varphi(d) = n$, dobijemo

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

Na taj način vidimo kako povezati Möbiusovu i Eulerovu funkciju što ćemo pokazati u sljedećem primjeru

Primjer 3.4. *Izračunajmo ponovno $\varphi(756)$ koristeći vrijednosti Möbiusovih funkcija.*

Djelitelji broja 756 su: 1, 2, 3, 4, 7, 9, 12, 14, 18, 21, 27, 28, 36, 42, 54, 63, 84, 108, 126, 189, 252, 378 *i* 756. *Po formuli imamo*

$$\begin{aligned}\varphi(756) &= n \sum_{d|n} \frac{\mu(d)}{d} = 756 \sum_{d|756} \frac{\mu(d)}{d} = \\ &= 756 \left(\frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \cdots + \frac{\mu(378)}{378} + \frac{\mu(756)}{756}\right).\end{aligned}$$

Vrijednosti Möbiusove funkcije su: $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(14) = 1$, $\mu(21) = 1$ i $\mu(42) = -1$. Ostale vrijednosti su 0. *Konačno dobivamo*

$$756 \left(\frac{1}{1} + \frac{-1}{2} + \frac{-1}{3} + \frac{1}{6} + \frac{-1}{7} + \frac{1}{14} + \frac{1}{21} + \frac{-1}{42}\right) = 216.$$

Primjenu Möbiusove funkcije možemo naći računajući ciklotomske polinome. Na samom početku prisjetiti ćemo se osnovnih pojmova te problema koji se javljaju rješavajući polinome u skupu prirodnih brojeva $\mathbb{R}$ te proširenje rješena na skup kompleksih brojeva $\mathbb{C}$.

Neka je a n-ti korijen broja b što zapisujemo $b^n = a$. Kvadratni korijen broja 1 je 1 jer je $1 \cdot 1 = 1$, ali (-1)(-1) = 1, te je -1 isto kvadratni korijen od 1. Kažemo da postoje dva kvadratna korijena broja 1. Ako pogledamo kubni korijen broja 1 tada 1 nije rješenje jer je (-1)(-1)(-1) = -1. Dakle, gledajući u skupu realnih brojeva postoji samo jedno rješenje i to je broj 1, no u skupu kompleksnih brojeva $\mathbb{C}$ možemo pronaći tri kubna korijena broja 1.

Broj možemo zapisati u obliku

$$e^{i(nx)} = \cos(nx) + i\sin(nx),$$

gdje je n cijeli broj, a x može biti kompleksan broj.Tražeći rješenje u skupu kompleksnih brojeva postoji točno n različitih n-tih korijena broja 1. Podijelimo li jediničnu kružnicu na n jednakih dijelova, koristeći n točaka lako je pronaći rješenja.

Kompleksan broj z nazivamo n-tim korijenom iz jedinice, gdje je n prirodan broj, ako je $z^n = 1$.

Uzmemo li kompleksan broj z kojemu je apsolutna vrijednost jednaka 1 te ga zapišemo u polarnim koordinatama

$$z = \cos\theta + i\sin\theta,$$

tada ga možemo lako potencirati koristeći formulu za potenciranje kompleksnog broja

$$z^n = (\cos\theta + i\sin\theta)^n = \cos(n \cdot \theta) + i\sin(n \cdot \theta).$$

Tada iz jednakosti $n\theta = 0 + 2k\pi$ za $k = 0, 1, \ldots, n-1$ slijedi da je $\theta = \frac{2k\pi}{n}$. Korijeni iz jedinice dani su s $e^{\frac{2k\pi}{n}}$, za $k = 0, 1, \ldots, n-1$.

Definicija 3.3. *Kažemo da je n-ti korijen iz jedinice primitivan ako je oblika ζ_n^k (ζ_n je kompleksan broj $e^{\frac{2\pi i}{n}}$) gdje su n i k relativno prosti.*

Definicija 3.4. *Neka je n cijeli broj te neka je ζ_n^k primitivni n-ti korijen iz jedinice. Tada n-ti ciklotomski polinom $\Phi_n(x)$ glasi*

$$\Phi_n(x) = \prod_{1 \le k \le n} (x - \zeta_n^k),$$

gdje su korijeni primitivni n-ti korijeni iz jedinice.

Teorem 3.3. *Neka je n cijeli broj. Tada vrijedi*

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

gdje je d pravi dijelitelj od n.

Dokaz. Korijeni od $x^n - 1$ su upravo n-ti korijeni iz jedinice. Nadalje, ako je ζ n-ti korijen iz jedinice reda d, tada je ζ primitivni d-ti korijen iz jedinice pa je i nultočka od $\Phi_d(x)$.

Kako $d \mid n$, ζ je korijen desne strane izraza teorema. Iz toga zaključujemo da su polinomi s lijeve i desne strane istog stupnja te imaju iste korjene. □

Postoji jedan način za pronalaženje n-tog ciklotomskog polinoma koji je ponekad jednostavniji i brži:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_d \Phi_d(x)},$$

gdje je d prolazi po skupu pravih dijelitelja od n.

Primjer 3.5. *Pokazat ćemo neke vrijednosti ciklotomskih polinoma*

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= \frac{x^2 - 1}{\Phi_1(x)} = \frac{x^2 - 1}{x - 1} = x + 1 \\
\Phi_3(x) &= \frac{x^3 - 1}{\Phi_1(x)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 \\
\Phi_4(x) &= \frac{x^4 - 1}{\Phi_1(x)\Phi_2(x)} = x^2 + 1 \\
\Phi_5(x) &= \frac{x^5 - 1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = x^2 - x + 1
\end{aligned}$$

Sljedećim teoremom povezati ćemo izraz iz prethodnog teorema sa Möbiusovom funkcijom preko koje ćemo računati polinome.

Teorem 3.4. *Neka je n pozitivan cijeli broj te μ Möbiusova funkcija. Tada vrijedi*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

Dokaz se može pronaći u [2].

Primjer 3.6. *Izračunajmo $\Phi_4(x)$ pomoću gornjeg teorema.*

$$\begin{aligned}
\Phi_4(x) &= (x-1)^{\mu\left(\frac{4}{1}\right)} + (x^2-1)^{\mu\left(\frac{4}{2}\right)} + (x^4-1)^{\mu\left(\frac{4}{4}\right)} = \\
&= (x-1)^0 + (x-1)^{-1} + (x-1)^1 = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1.
\end{aligned}$$

Dokazano je da su svi koeficijenti ciklotomskih polinoma $\Phi_n(x)$ cijeli brojevi.

Vrlo važno pitanje je kako se asimptotski ponašaju aritmetičke funkcije tj. kako izgledaju sume oblika $\sum_{n \leq x} f(n)$ za dovoljno veliki realan broj x. Na to pitanje pokušati ćemo odgovoriti za vec spomenute funkcije d, σ i φ.

Propozicija 3.1. *Za aritmetičke funkcije vrijedi:*

1. $\sum_{n\leq x} d(n) = x\ln x + O(x)$,
2. $\sum_{n\leq x} \sigma(n) = \frac{1}{12}\pi^2 x^2 + O(x\ln x)$,
3. $\sum_{n\leq x} \varphi(n) = \frac{3}{\pi^2}\cdot x^2 + O(x\ln x)$.

Dokaz.

1.
$$\sum_{n\leq x} d(n) = \sum_{n\leq x}\sum_{d|n} 1 = \sum_{d\leq x}\sum_{m\leq \frac{x}{d}} 1 = \sum_{d\leq x}\left[\frac{x}{d}\right] = \sum_{d\leq x}\left(\frac{x}{d} + O(1)\right) = x\ln x + O(x).$$

Dokazi ostalih tvrdnji mogu se naći u [1].

□

Može se pokazati da je

$$\sum_{n\leq x}\varphi(n) \sim \frac{3}{\pi^2}x^2 \quad \text{i} \quad \sum_{n\leq x} n \sim \frac{3}{\pi^2}x^2.$$

Rezultat možemo interpretirati tako da kažemo da je vjerojatnost da su dva nasumce izabrana cijela broja relativno prosta jednaka

$$\frac{\sum_{n\leq x}\varphi(n)}{\sum_{n\leq x} n} \approx \frac{\frac{3}{\pi^2}x^2}{\frac{1}{2}x^2} = \frac{6}{\pi^2} \approx 0.6079.$$

Literatura

[1] A. DUJELLA, Uvod u teoriju brojeva (skripta), PMF-MO, Zagreb, 2009.

[2] Z. ISLEK, Möbius Inversion Formula and Applications to Cyclotomic Polynomials, Linnaeus University, 2012.

[3] I. NIVEN, H.S. ZUCKERMAN, H.L. MONTGOMERY, An Introduction to the Theory of Numbers,John Wiley Sons, Inc., USA, 1991.