Multiplikativne funkcije

Vuletić, Ivana

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Sveučilišni diplomski studij matematike
smjer: Financijska matematika i statistika

Multiplikativne funkcije

Diplomski rad

Mentor:
prof. dr. sc. Ivan Matić

Student:
Ivana Vuletić

Osijek, 2024.

Sadržaj

1 | Uvod

Teorija brojeva, često nazvana "kraljica matematike", grana je matematike koja se bavi svojstvima i odnosima između brojeva. Važnu ulogu u analiziranju tih svojstava i odnosa imaju aritmetičke funkcije. Njih možemo definirati kao funkcije kod kojih je domena skup prirodnih brojeva, a čiju kodomenu čini neki podskup skupa kompleksnih brojeva. Od posebne važnosti su funkcije koje zadovoljavaju svojstvo multiplikativnosti. Takve funkcije pripadaju velikoj klasi aritmetičkih funkcija koje se nazivaju multiplikativne funkcije. U ovom radu bit će predstavljeno nekoliko funkcija koje zadovoljavaju to svojstvo.

U prvom poglavlju rada navest ćemo definicije i osnovne pojmove teorije brojeva koji su nam potrebni za razumijevanje sadržaja ovog rada. Također, spomenut ćemo jednu od najvažnijih funkcija teorije brojeva - Eulerovu funkciju. U drugom poglavlju definirat ćemo multiplikativne funkcije, te ćemo iskazati i dokazati Fundamentalni teorem za multiplikativne funkcije. Vratit ćemo se na ranije spomenutu Eulerovu funkciju i pokazat ćemo da je ona multiplikativna funkcija. Nadalje, definirat ćemo funkcije broj djelitelja i suma djelitelja, te ćemo se dotaknuti nekih njihovih svojstva koja su rezultat multiplikativnosti tih funkcija. U četvrtom poglavlju, spomenut ćemo se savršenih i Mersenneovih brojeva. Uz kratak prikaz povijesti, navest ćemo i neka njihova osnovna svojstva. Na kraju rada upoznat ćemo se Möbiusovom funkcijom te ćemo pokazati njenu povezanost s Eulerovom funkcijom koristeći se teoremom poznatim pod nazivom Möbiusova formula inverzije.

2 | Definicije i osnovni pojmovi teorije brojeva

U ovom poglavlju definirat ćemo neke od osnovnih pojmova koji čine temelj teorije brojeva. Za početak imamo definiciju djeljivosti, koja je jedan od najjednostavnijih i najznačajnijih pojmova.

Definicija 1 ([1], Definicija 1.1)**.** *Neka su $a \neq 0$ i b dva cijela broja. Reći ćemo da a dijeli b ako postoji cijeli broj d za koji vrijedi $b = a \cdot d$. Tada je broj b višekratnik broja a, a broj a je djelitelj broja b. U slučaju kada a dijeli b pišemo $a|b$, a kada a ne dijeli b pisat ćemo $a \nmid b$.*

Primjer 1. $7|21$ *jer je* $21 = 7 \cdot 3$.

Neka su a i b dva cijela broja. Reći ćemo da je cijeli broj d zajednički djelitelj brojeva a i b ako d dijeli oba broja a i b. Ako je barem jedan od brojeva a i b različit od nule, tada taj broj ima konačno mnogo djelitelja. U tom slučaju postoji i konačno mnogo zajedničkih djelitelja brojeva a i b. Najvećeg među njima označavamo s (a, b) te izraz (a, b) nazivamo najveći zajednički djelitelj brojeva a i b.

Možemo primijetiti da je $(a, b) \geq 1$.

Definicija 2 ([1], Definicija 1.4.)**.** *Kažemo da je prirodan broj p, $p > 1$, prost ako nema niti jednog djelitelja d takav da vrijedi $1 < d < p$. Za prirodan broj a, $a > 1$, koji nije prost, kažemo da je složen.*

Primjer 2. *Broj* 13 *je prost broj, dok je broj* $15 = 5 \cdot 3$ *složen.*

Definicija 3 ([1], Definicija 1.3.)**.** *Za cijele brojeve a i b reći ćemo da su relativno prosti ako je $(a, b) = 1$. Analogno, reći ćemo da su cijeli brojevi $a_1, a_2, \ldots, a_n$ relativno prosti ako je $(a_1, a_2, \ldots, a_n) = 1$, a da su u parovima relativno prosti ako je $(a_i, a_j) = 1$ za sve i i j takve da je $i \neq j$ i $1 \leq i, j \leq n$.*

Primjer 3. *Jedan od primjera relativno prostih brojeva su brojevi* 9 *i* 14 *jer je* $(9, 14) = 1$. *S druge strane, brojevi* 60 *i* 36 *nisu relativno prosti jer je* $(36, 60) = 12$.

Teorem 1 ([1], Teorem 1.8.)**.** *Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Dokaz. Vidjeti [1]. □

Iz prethodnog teorema slijedi da se svaki prirodan broj n možemo zapisati u obliku
$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$
gdje su $p_1, \ldots, p_k$ različiti prosti brojevi, a $e_1, \ldots, e_k$ prirodni brojevi. Takav zapis broja n zvat ćemo kanonski rastav broja n na proste faktore. Broj e_i nazivamo kratnošću prostog broja p_i.

Primjer 4. $5445 = 3^2 \cdot 5 \cdot 11^2$

Važan teorem u teoriji brojeva je idući teorem pod nazivom *Osnovni teorem aritmetike* koji će nam biti koristan pri dokazivanju mnogih tvrdnji:

Teorem 2 ([6], Teorem 1.4.3.). *Prikaz svakog prirodnog broja većeg od* 1 *u obliku produkta potencija prostih brojeva je jedinstven do na poredak faktora.*

Dokaz. Vidjeti [6]. □

2.1 Eulerova funkcija

Eulerova funkcija (engl. Euler's totient function) jedna je od najvažnijih funkcija teorije brojeva. Prvobitna oznaka Eulerove funkcije bila je π koju je uveo Euler 1784. godine, dok se danas koristi oznaka φ predstavljena u Gaussovoj knjizi *Disquisitiones Arithmeticae* iz 1801. godine.

Za prirodan broj n, vrijednost Eulerove funkcije $\varphi(n)$ označava broj prirodnih brojeva manjih ili jednak broju n koji su relativno prosti s n. Vrijedi $\varphi(1) = 1$.

Primjer 5. *Odredimo* $\varphi(13)$ *i* $\varphi(16)$.
Rješenje: Kako je 13 *prost broj, svaki prirodan broj manji od* 13 *je relativno prost s* 13. *Stoga je* $\varphi(13) = 12$.
Brojevi manji od 16 *koji su relativno prosti sa* 16 *su* $1, 3, 5, 7, 9, 11, 13$ *i* 15. *Dakle,* $\varphi(16) = 8$.

Možemo uočiti da za prost broj p vrijedi da je relativno prost sa svim brojevima strogo manjim od samog sebe, osnosno $\varphi(p) = p - 1$.

Lema 1 ([6], Lema 2.2.4). *Neka je p prost broj i k prirodan broj. Tada vrijedi*
$$\varphi(p^k) = p^k - p^{k-1}.$$

Dokaz. U nizu prirodnih brojeva $1, 2, 3, \ldots, p^k$ oni koji nisu relativno prosti s p^k su $1p, 2p, 3p, \ldots, p^{k-1} \cdot p = p^k$. Kada ih prebrojimo, ukupno ih je p^{k-1}. Stoga vrijedi
$$\varphi(p^k) = p^k - p^{k-1}.$$
□

Uočimo da se prethodni rezultat može zapisati i kao
$$\varphi(p^k) = p^k \left(1 - \frac{1}{p}\right).$$

Primjer 6. *Odredimo* $\varphi(1024)$ *koristeći se prethodnom lemom.*
Rješenje: Kako je $1024 = 4^5$, *onda je* $\varphi(1024) = \varphi(4^5) = 4^5 - 4^4 = 768$.

3 | Multiplikativne funkcije

Definicija 4 ([9], Definition 7.1)**.** *Aritmetička funkcija je funkcija definirana za sve prirodne brojeve.*

U ovom poglavlju bavit ćemo se klasom aritmetičkih funkcija koje zadovoljavaju svojstvo multiplikativnosti. Takve funkcije nazivamo multiplikativne funkcije.

Definicija 5 ([1], Definicija 2.4.)**.** *Aritmetička funkcija $f : \mathbb{N} \to \mathbb{C}$ je multiplikativna ako vrijedi*

1) $f(1) = 1$
2) $f(mn) = f(m)f(n)$ *za sve* m, n *takve da je* $(m, n) = 1$.

Pogledajmo neke od primjera multiplikativnih funkcija.

Primjer 7. *Konstantna funkcija $f(n) = 1$ je multiplikativna jer je $f(1) = 1$ i*

$$f(mn) = 1 = 1 \cdot 1 = f(m)f(n).$$

Primjer 8. *Funkcija $f(n) = n^k$ je multiplikativna jer je $f(1) = 1$ i*

$$f(mn) = (mn)^k = m^k n^k = f(m)f(n).$$

Neka su p i q dva različita prosta broja. Pretpostavimo da je funkcija f multiplikativna i da znamo vrijednosti $f(p^a)$ i $f(q^b)$. Tada možemo odrediti i $f(p^a q^b)$ jer vrijedi $f(p^a q^b) = f(p^a)f(q^b)$. Ova tvrdnja može se generalizirati kroz sljedeći važni teorem pod nazivom Fundamentalni teorem za multiplikativne funkcije.

Teorem 3 ([5], Theorem 8.1)**.** *Neka je funkcija f multiplikativna i neka je $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ kanonski rastav broja n na proste faktore. Tada je*

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k}).$$

Dokaz. Tvrdnja se dokazuje matematičkom indukcijom po broju k. Kada je $k = 1$ imamo $n = p_1^{e_1}$ i $f(n) = f(p_1^{e_1})$ te je tvrdnja trivijalno ispunjena. Pretpostavimo da tvrdnja vrijedi za bilo koji prirodan broj n s kanonskim rastavom na proste faktore sastavljenim od k različitih prostih brojeva, tj.

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k}).$$

Nadalje, neka je m neki prirodan broj čiji kanonski rastav na proste faktore sadrži $k + 1$ različitih prostih brojeva, odnosno $m = p_1^{e_1} p_2^{e_2} \cdots p_{k+1}^{e_{k+1}}$. Kako je

$(p_1^{e_1} \cdots p_k^{e_k}, p_{k+1}^{e_{k+1}}) = 1$ i funkcija f multiplikativna, iz pretpostavke indukcije slijedi

$$f(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} p_{k+1}^{e_{k+1}}) = f(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) f(p_{k+1}^{e_{k+1}}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k}) f(p_{k+1}^{e_{k+1}}).$$

□

Dakle, vrijednost multiplikativne funkcije $f(n)$ za bilo koji prirodan broj n može se jednostavno izračunati koristeći se kanonskim rastavom broja n na proste faktor. Dovoljno je poznavati vrijednosti $f(p_i^{e_i})$, za sve $1 \leq i \leq k$. Tako npr. za $n = 3528$ imamo $f(3528) = f(2^3)f(3^2)f(7^2)$.

3.1 Multiplikativnost Eulerove funkcije

Vratimo se na Eulerovu funkciju, htjeli bi smo provjeriti je li ona multiplikativna funkcija. Pogledajmo idući primjer kojim ćemo predstaviti algoritam potreban za dokaz multiplikativnosti Eulerove funkcije. Za početak, pretpostavimo da je φ multiplikativna funkcija i da želimo izračunati npr. $\varphi(24)$. To bi značilo da je $\varphi(24) = \varphi(3 \cdot 8) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8$, što ćemo i pokazati u primjeru.

Primjer 9. *Neka je $m = 3$ i $n = 8$. Tada je $(m, n) = 1$ i $mn = 24$. Kako bi odredili $\varphi(mn) = \varphi(24)$ u Tablici 3.1.1 smo ispisali sve prirodne brojeve manje ili jednake broju 24 u tri retka i u svakom retku 8 brojeva: Pogledamo li prvi broj u trećem retku, uočavamo kako*

1	4	7	10	13	16	19	22
2	5	8	11	14	17	20	23
3	6	9	12	15	18	21	24

Tablica 3.1.1

on nije relativno prost s brojem $m = 3$. Također niti jedan broj iz tog retka nije relativno prost s brojem $m = 3$, pa niti jedan od njih nije relativno prost s brojem $mn = 24$.
Dakle, brojevi koji su relativno prosti s 24 i koji su manji ili jendaki 24 nalaze se u preostala $2 = \varphi(3)$ retka:

1	4	7	10	13	16	19	22
2	5	8	11	14	17	20	23

Tablica 3.1.2

Odnosno brojevi iz prethodne tablice relativno su prosti s $m = 3$, a svaki redak te tablice sadrži $4 = \varphi(8)$ broja relativno prosta s brojem 8:

1	7	13	19
5	11	17	23

Tablica 3.1.3

Ukupno nam je ostalo 8 *brojeva u Tablici* 3.1.3*, a to su upravo svi brojevi manji ili jendak broju* 24 *koji su relativno prosti s* 24*. Dakle, vrijedi* $\varphi(24) = 8 = 2 \cdot 4 = \varphi(3)\varphi(8)$.

Sada ćemo dokazati da je funkcija φ multiplikativna funkcija.

Teorem 4 ([5], Theorem 8.3)**.** *Funkcija* φ *je multiplikativna.*

Dokaz. Neka su m i n dva relativno prosta prirodna broja, odnosno $(m, n) = 1$. Trebamo pokazati da vrijedi $\varphi(mn) = \varphi(m)\varphi(n)$.
Poredajmo brojeve od 1 do mn u m redaka i n stupaca, kako je prikazano u Tablici 3.1.4.

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \ldots & (n-1)m+3 \\
 & & & \vdots & \\
r & m+r & 2m+r & \ldots & (n-1)m+r \\
 & & & \vdots & \\
m & 2m & 3m & \ldots & nm
\end{array}$$

Tablica 3.1.4

Neka je r prirodan broj takav da je $1 \leq r \leq m$ i $(r, m) > 1$. Pokazat ćemo da u r-tom redu Tablice 3.1.4 niti jedan broj nije relativno prost s brojem mn. Neka je $d = (r, m)$. Tada $d|r$ i $d|m$ iz čega slijedi da $d|km + r$ za bilo koji cijeli broj k.
Dakle, niti jedan element r-tog reda nije relativno prost s m, pa onda nije ni relativno prost s brojem mn. Stoga se brojevi koji su relativno prosti s mn nalaze u retcima za koje je $(r, m) = 1$, a takvih redaka je upravo $\varphi(m)$.

Uzmimo neki $\varphi(m)$ redak, npr. k-ti redak. Sa S_k označimo skup kojeg čine svi elementi tog retka, tj. $S_k = \{k, m + k, 2m + k, \ldots, (n-1)m + k\}$. Dokazat ćemo da su svi elementi skupa S_k međusobno nekongruentni modulo n. Pretpostavimo suprotno, odnosno neka postoje $i, j \in \{0, 1, \ldots n-1\}$ za koje vrijedi

$$im + k \equiv jm + k \pmod{n},$$

slijedi da $n|(i-j)m$. Kako je $(m, n) = 1$ i $0 \leq i, j < n$ dolazimo do zaključka da je $i = j$. Dakle, skup S_k se sastoji od n međusobno nekongruentnih elemenata modulo n, pa možemo zaključiti da je skup S_k potpun sustav ostataka modulo n. S R_k označimo skup svih brojeva iz S_k koji su relativno prosti s brojem n. Tada je R_k reduciran sustav ostataka modulo n te sadrži $\varphi(n)$ elemenata. Budući da u k-tom retku imamo $\varphi(n)$ elemenata relativno prostih s n, onda imamo točno $\varphi(n)$ elemenata relativno prostih s mn.

Zaključujemo da se u $\varphi(m)$ redaka nalaze brojevi relativno prosti s brojem mn i da svaki taj redak sadrži $\varphi(n)$ brojeva relativno prostih s mn. Dakle, imamo $\varphi(m)\varphi(n)$ brojeva manjih ili jednak broju mn koji su relativno prosti s mn. Slijedi da je $\varphi(mn) = \varphi(m)\varphi(n)$. $\square$

Primjer 10. *Izračunajmo* $\varphi(943)$, $\varphi(5184)$.
Rješenje:

$$\begin{aligned}\varphi(943) &= \varphi(23 \cdot 41) = \varphi(23) \cdot \varphi(41)\\ &= 22 \cdot 40\\ &= 880\\ \varphi(5184) &= \varphi(2^6 \cdot 3^4) = \varphi(2^6) \cdot \varphi(3^4)\\ &= (2^6 - 2^5) \cdot (3^4 - 3^3)\\ &= 1728.\end{aligned}$$

Koristeći se Teoremom 4 i Lemom 1 dolazimo do formule za $\varphi(n)$.

Teorem 5 ([9], Theorem 7.5)**.** *Neka je* $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ *kanonski rastav broja* n *na proste faktore. Tada je*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Dokaz. Funkcija $\varphi(n)$ je multiplikativna pa vrijedi sljedeće:

$$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}).$$

Iz Leme 1 imamo

$$\varphi(p_j^{e_j}) = p_j^{e_j} - p_j^{e_j - 1} = p_j^{e_j}\left(1 - \frac{1}{p_j}\right)$$

za sve $j \in \{1, 2, \ldots, k\}$. Dakle,

$$\begin{aligned}\varphi(n) &= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{e_k}\left(1 - \frac{1}{p_k}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).\end{aligned}$$

□

Primjer 11. $\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = 600\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 160.$

4 | Funkcije broj djelitelja i suma djelitelja

U ovom poglavlju pokazat ćemo da su funkcije broj djelitelja i suma djelitelja multiplikativne funkcije. Koristeći se tim svojstvom i kanonskim rastavom broja na proste faktore izvest ćemo formule za određivanje vrijednosti navedenih funkcija. Za početak ćemo ih definirati.

Neka je n prirodan broj. Broj djelitelja je funkcija $\tau(n)$ koja broji sve pozitivne djelitelje broja n, odnosno

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

Primjer 12. *Odredimo $\tau(36)$ i $\tau(37)$.*
Rješenje: Pozitivni djelitelji broja 36 su $1, 2, 3, 4, 6, 9, 12, 18$ i 36, pa je $\tau(36) = 9$. Broj 37 je prost broj pa su jedini djelitelji tog broja 1 i 37. Dakle, $\tau(37) = 2$.

Uočimo, ako je p prost broj, onda su jedini pozitivni djelitelji broja p upravo 1 i p. Dakle, $\tau(p) = 2$. Vrijedi i obrat. Ako je $\tau(n) = 2$, onda je n prost broj.

Suma djelitelja je funkcija $\sigma(n)$ koja zbraja sve pozitivne djelitelje broja n, odnosno

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

Primjer 13. *Odredimo $\sigma(32)$ i $\sigma(41)$.*
Rješenje: Pozitivni djelitelji broja 32 su $1, 2, 4, 8, 16$ i 32, pa je

$$\sigma(32) = 1 + 2 + 4 + 8 + 16 + 32 = 63.$$

Pozitivni djelitelji broja 41 su 1 i 41, pa je

$$\sigma(41) = 1 + 41 = 42.$$

Uočimo, za p prost broj vrijedi $\sigma(p) = p + 1$. Vrijedi i obrat. Ako je $\sigma(n) = n + 1$, onda je n prost broj.

Kako bi dokazali multiplikativnosti prethodno definiranih funkcija $\tau(n)$ i $\sigma(n)$ uvodimo novu funkciju $F(n)$ definiranu formulom

$$F(n) = \sum_{d|n} f(d),$$

pri čemu je f multiplikativna funkcija.

Primjer 14.

$$\begin{aligned} F(45) &= \sum_{d|45} f(45) \\ &= f(1) + f(3) + f(5) + f(9) + f(15) + f(45). \end{aligned}$$

Postavlja se pitanje, je li ovako definirana funkcija $F(n)$ multiplikativna. Poglejdajmo sljedeći primjer.

Primjer 15. *Pokažimo da vrijedi $F(24) = F(3)F(8)$.*
Rješenje: Kako je $(3, 8) = 1$, svaki se pozitivan djelitelj broja 24 može zapisati kao produkt jednog djelitelja broja 3 i jednog djelitelja broja 8. Odnosno, $1 = 1 \cdot 1$, $2 = 1 \cdot 2$, $3 = 3 \cdot 1$, $4 = 1 \cdot 4$, $6 = 3 \cdot 2$, $8 = 1 \cdot 8$, $12 = 3 \cdot 4$ i $24 = 3 \cdot 8$ (u svakom produktu, prvi faktor predstavlja djelitelja broja 3, dok drugi faktor predstavlja djelitelja broja 8).

$$\begin{aligned} F(24) = F(3 \cdot 8) &= \sum_{d|24} f(24) \\ &= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24) \\ &= f(1 \cdot 1) + f(1 \cdot 2) + f(3 \cdot 1) + f(1 \cdot 4) + f(3 \cdot 2) + f(1 \cdot 8) \\ &\quad + f(3 \cdot 4) + f(3 \cdot 8) \\ &= f(1)f(1) + f(1)f(2) + f(3)f(1) + f(1)f(4) + f(3)f(2) + f(1)f(8) \\ &\quad + f(3)f(4) + f(3)f(8) \\ &= f(1)\left(f(1) + f(2) + f(4) + f(8)\right) + f(3)(f(1) + f(2) + f(4) + f(8)) \\ &= \left(f(1) + f(3)\right)\left(f(1) + f(2) + f(4) + f(8)\right) \\ &= \sum_{d|3} f(d) \cdot \sum_{d|8} f(d) \\ &= F(3) \cdot F(8). \end{aligned}$$

Koristeći se idejom prikazanom u ovom primjeru sada možemo dokazati da je funkcija $F(n)$ multiplikativna.

Teorem 6 ([5], Theorem 8.6)**.** *Ako je funkcija f multiplikativna, onda je i*

$$F(n) = \sum_{d|n} f(d)$$

multiplikativna funkcija.

Dokaz. Za $n = 1$ vrijedi

$$F(1) = \sum_{d|1} f(d) = f(1) = 1.$$

Neka su m i n dva relativno prosta prirodna broja. Trebamo pokazati da je $F(mn) = F(m)F(n)$. Iz definicije funkcije F imamo

$$F(mn) = \sum_{d|mn} f(d).$$

Kako su brojevi m i n relativno prosti, svaki djelitelj d broja mn možemo na jedinstven način zapisati kao produkt djelitelja d_1 broja m i djelitelja d_2 broja n. Tada je $(d_1, d_2) = 1$ i vrijedi sljedeće

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2).$$

Funkcija f je multiplikativna pa vrijedi $f(d_1 d_2) = f(d_1) f(d_2)$. Tada je

$$\begin{aligned} F(mn) &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) = \sum_{d_1|m} \left(f(d_1) \sum_{d_2|n} f(d_2) \right) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) = F(m)F(n). \end{aligned}$$

□

Iskoristimo rezultat ovog teorema za dokaz multiplikativnosti funkcija τ i σ.

Korolar 1 ([5], Corollary 8.1)**.** *Funkcije τ i σ su multiplikativne funkcije.*

Dokaz. U Primjeru 7 pokazali smo da je konstantna funkcija $f(n) = 1$ multiplikativna funkcija. Koristeći se prethodnim teoremom možemo zaključiti da je funkcija

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

također multiplikativna funkcija.

U Primjeru 8 pokazali smo da je funkcija $f(n) = n^k$ multiplikativna funkcija. Koristeći se prethodnim teoremom možemo zaključiti da je i funkcija

$$\sigma(n) = \sum_{d|n} f(d) = \sum_{d|n} d$$

također multiplikativna funkcija. Dakle, za $(m, n) = 1$ vrijedi

$$\tau(mn) = \tau(m)\tau(n)$$

i

$$\sigma(mn) = \sigma(m)\sigma(n).$$

□

Primjer 16. *Odredimo $\tau(42)$ i $\sigma(42)$.*
Rješenje: Rastav broja 42 je oblika $42 = 6 \cdot 7$ pa je

$$\tau(42) = \tau(6) \cdot \tau(7) = 4 \cdot 2 = 8$$

i

$$\sigma(42) = \sigma(6) \cdot \sigma(7) = 12 \cdot 8 = 96.$$

Sada kada znamo da su funkcije τ i σ multiplikativne možemo odrediti formule za $\tau(n)$ i $\sigma(n)$. Prije toga, odredimo forumle za $\tau(p^e)$ i $\sigma(p^e)$ gdje je p prost broj.

Teorem 7 ([5], Theorem 8.7)**.** *Neka je p prost broj i e prirodan broj. Tada je*

$$\tau(p^e) = e + 1$$

i

$$\sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}.$$

Dokaz. Bojevi $1, p, p^2, \dots, p^e$ su pozitivni djelitelji broja p^e. Ima ih ukupno $e + 1$ pa je

$$\tau(p^e) = e + 1.$$

Nadalje,

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \sum_{i=0}^{e} p^i.$$

Uočimo da je $\sigma(p^e)$ zapravo suma prvih $e + 1$ članova geometrijskog niza pa vrijedi

$$\sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}.$$

□

Primjer 17. *Odredimo $\tau(5^4)$ i $\sigma(5^4)$.*
Rješenje:

$$\tau(5^4) = 1 + 4 = 5$$

i

$$\sigma(5^4) = \frac{5^5 - 1}{5 - 1} = 781.$$

Na kraju, koristeći se Korolarom 1 i Teoremom 7 dolazimo do formula za $\tau(n)$ i $\sigma(n)$.

Teorem 8 ([5], Theorem 8.8)**.** *Neka je n prirodan broj čiji je kanonski rastav na proste faktore $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Tada je*

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

i

$$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1}.$$

Dokaz. Kako su funkcije τ i σ multiplikativne vrijedi

$$\tau(n) = \tau(p_1^{e_1})\tau(p_2^{e_2}) \cdots \tau(p_k^{e_k})$$

i

$$\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k}).$$

Uvrstimo li vrijednosti za $\tau(p_i^{e_i})$ i $\sigma(p_i^{e_i})$ iz Teorema 7 imamo sljedeće

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

i

$$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1}.$$

□

Rezultat prethodnog teorema kraće možemo zapisati kao

$$\tau(n) = \prod_{i=1}^{k} (e_i + 1),$$
$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

Primjer 18. *Odredimo $\tau(4725)$ i $\sigma(4725)$.*
Rješenje: Kanonski rastav broja 4725 je oblika $4725 = 3^3 \cdot 5^2 \cdot 7$ pa je

$$\tau(4725) = (3 + 1)(2 + 1)(1 + 1) = 24$$

i

$$\sigma(4725) = \frac{3^{3+1} - 1}{3 - 1} \cdot \frac{5^{2+1} - 1}{5 - 1} \cdot \frac{7^{1+1} - 1}{7 - 1} = 40 \cdot 31 \cdot 8 = 9920.$$

5 | Savršeni i Mersenneovi brojevi

Funkciju $\sigma(n)$, definiranu u prethodnom poglavlju, vežemo uz jednu klasu prirodnih brojeva pod nazivom savršeni brojevi. Za prirodan broj n reći ćemo da je savršen ako je $\sigma(n) = 2n$, odnosno ako je jednak sumi svojih pravih djelitelja.

Primjer 19. *Kako vrijedi*

$$\sigma(6) = 1+2+3+6 = 12 = 2\cdot 6 \quad i \quad \sigma(28) = 1+2+4+7+14+28 = 56 = 2\cdot 28,$$

brojevi 6 *i* 28 *su primjeri savršenih brojeva.*

Izraz "savršen" potječe još iz doba Pitagorejaca. Oni su savršenim brojevima pripisivali mistična značenja, pa su tako broj 6 smatrali simbolom braka, zdravlja i ljepote. Osim mističnih, savršenim brojevima su se kroz povijest pripisivala i religijska značenja. Biblijski znanstvenici su vjerovali da je broj 6 savršen jer je Bog stvorio svijet u 6 dana, a Božije djelo je savršeno. Sveti Augustin sr pak suprostavio toj tvrdnji. Broj 6 je savršen sam po sebi te je Bog izabrao stvoriti svijet u 6 dana simbolizirajući njegovo djelo kao savršeno.

Prva četiri savršena broja, 6, 28, 496 i 8128, bila su poznata starim Grcima. Njihov zapis pronalazimo u Nicomachusovoj knjizi *Introductio Arithmetica* (oko 100. godine). Na osnovu prva četiri broja, Nicomachus je došao do zaključka da n-ti savršen broj čini točno n broj znamenki te da parni savršeni brojevi naizmjence završavaju na znamenke 6 i 8. Obje tvrdnje su se kroz povijest pokazale pogrešnima. Naime, tek 1536. godine, grčki matematičar H. Regius otkrio je peti savršeni broj sastavljen od 8 znamenki koji je jednak 33550336. Drugu tvrdnju opovrgnuo je talijanski matematičar Cataldi pronalaskom šestog savršenog broja koji kao i peti završava znamenkom 6, a jednak je 8589869056.

Prvi matematički rezultat vezan uz savršene brojeve predstavio je Euklid u IX. knjizi *Elemenata* (oko 300. godine prije Krista). On je dokazao sljedeće: ako je vrijednost sume $1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = p$ prost broj, tada je broj $2^{n-1}p$ savršen broj. Tako je npr. $1 + 2 + 4 = 7$ prost broj i broj $4 \cdot 7 = 28$ savršen broj. Dokažimo tu tvrdnju sljedećim teoremom koji nosi naziv Euklidov teorem.

Teorem 9 ([5], Theorem 8.9.)**.** *Neka je $n \geq 2$ prirodan broj. Ako je broj $2^n - 1$ prost, onda je broj $N = 2^{n-1}(2^n - 1)$ savršen broj.*

Dokaz. Kako je $2^n - 1$ neparan prost broj i 2^{n-1} paran broj dolazimo do zaključka da je $(2^{n-1}, 2^n - 1) = 1$. Funkcija σ je multiplikativna pa vrijedi

$$\begin{aligned}\sigma(N) &= \sigma(2^{n-1})\sigma(2^n - 1) \\ &= \frac{2^n - 1}{2 - 1} \cdot (1 + 2^n - 1) \\ &= (2^n - 1) \cdot 2^n \\ &= 2 \cdot 2^{n-1} \cdot (2^n - 1) \\ &= 2N.\end{aligned}$$

Dakle, broj N je savršen. □

Nakon 2000 godina, Euler je dokazao da svi parni savršeni brojevi moraju imati oblik prikazan Euklidovim teoremom.

Teorem 10 ([5], Theorem 8.10)**.** *Ako je $N = 2^{n-1}(2^n - 1)$ savršen broj, onda je $2^n - 1$ prost broj.*

Dokaz. Neka je N oblika $N = 2^{n-1} \cdot s$, gdje je s neparan prirodan broj. Budući da 2 ne djeli s, onda je $(2^{n-1}, s) = 1$. Znamo da je funkcija σ multiplikativna pa vrijedi

$$\sigma(N) = \sigma(2^{n-1}s) = \sigma(2^{n-1})\sigma(s) = (2^n - 1)\sigma(s).$$

Kako je $\sigma(N) = 2N = 2^n s$ imamo

$$2^n s = (2^n - 1)\sigma(s).$$

Budući da je $2^n - 1$ neparan, $2^n - 1$ dijeli s. Stoga je s oblika $s = (2^n - 1)k$, pa možemo pisati

$$2^n(2^n - 1)k = (2^n - 1)\sigma(s)$$

iz čega slijedi

$$\sigma(s) = 2^n k = (2^n - 1)k + k = s + k.$$

Kako $k|s$ i $\sigma(s) = s + k$ to znači da s ima samo dva pozitivna djelitelja pa je $k = 1$. Prema tome, s je prost broj oblika $s = 2^n - 1$. Dakle, $N = 2^{n-1}(2^n - 1)$, gdje je $2^n - 1$ prost broj. □

Brojeve oblika $M_n = 2^n - 1$ nazivamo Mersenneovi brojevi, a proučavao ih je francuski redovnik i matematičar Marin Mersenne. One brojeve $M_n = 2^n - 1$ koji su prosti nazivamo Mersenneovi prosti brojevi.

Stoga se, prema Euklidovom teoremu, problem pronalaska parnih savršenih brojeva svodi na traženje Mersenneovih prostih brojeva. Sljedeći teorem nam govori kako pri tom pronalasku možemo zanemariti one Mersenneove brojeve M_n čiji je indeks n složen broj.

Teorem 11 ([9], Theorem 7.11.)**.** *Ako je Messeneov broj $M_n = 2^n - 1$ prost broj, onda je i n prost broj.*

Dokaz. Pretpostavimo da je n složen broj takav da je $n = ab$, za $1 < a < n$ i $1 < b < n$. Tada je broj

$$M_n = 2^n - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)+\dots 2^a+1})$$

djeljiv s $2^a - 1$, pa nije prost broj. □

Iako se isprva mislilo da vrijedi obrat prethodnog teorema, 1536. godine matematičar H. Regius pokazao je da je za prost broj $m = 11$, broj $2^{11} - 1 = 2047 = 23 \cdot 89$ složen broj.

Marin Marsenne je u svojoj knjizi *Cogitata Physica-Mathematica* iz 1644. tvrdio, bez dokaza, da je broj M_p prost za $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ i 257, a složen za ostale proste brojeve $p < 257$. Tek 1947. godine, uz pomoć mehaničkog kalkulatora, testirali su se svi M_p za proste brojeve $p \leq 257$. Ispostavilo se da je Mersenne napravio 5 grešaka. Pogrešno je tvrdio da su brojevi M_{67} i M_{257} prosti te je zaboravio uključiti brojeve M_{61}, M_{89} i M_{107} u svoju listu. Poslije 1950. godine, moderna računala postaju snažan alat za pronalaženje većih Mersenneovih brojeva.

GIMPS (Great Internet Mersenne Prime Search) je projekt pokrenut 1996. godine s ciljem pronalaženja novih sve većih Mersenneovih prostih brojeva. Do danas je u okviru tog projekta pronađeno 17 Mersenneovih prostih brojeva, a najveći pronađeni je $2^{282589933} - 1$. U tom projektu sudjeluju volonteri iz cijelog svijeta koristeći se besplatnim softverima. Glavni algoritam na kojem se temelji GIMPS projekt je Lucas-Lehmarov test prostosti opisan u idućem teoremu.

Teorem 12 ([9], Theorem 7.13.)**.** *Neka je p prost broj i M_p p-ti Mesrenneov broj. Definirajmo niz prirodnih brojeva rekurzivnom formulom*

$$r_1 = 4,$$

te za $k \geq 2$

$$r_k \equiv r_{k-1}^2 - 2 \pmod{M_p}, \quad 0 \leq r_k \leq M_p.$$

Broj M_p je prost ako i samo ako je $r_{k-1} \equiv 0 \pmod{M_p}$.

Primjer 20. *Niz brojeva definiran u Lucas-Lehmerovom testu za broj $127 = 2^7 - 1$ je $14, 167, 42, 11$ i 0. Kako je $r_6 = 0$, $M_7 = 127$ je prost broj.*

Do danas je poznat ukupno 51 Mersenneov prost broj, pa nam je poznat i jednak broj parnih savršenih brojeva.

Napomenimo kako do danas nije dokazano postojanje savršenih brojeva koji su neparni, iako su postavljeni mnogi uvjeti koje bi oni trebali zadovoljiti.

6 | Möbiusova funkcija i Möbiusova formula inverzije

Ranije u ovom radu uveli smo funkciju $F(n)$ definiranu formulom $F(n) = \sum_{d|n} f(n)$, pod pretpostavkom da je f neka multiplikativna funkcija. Tako definirana funkcija F izražena je u terminima funkcije f. Zanima nas može li se ova veza između funkcija zamijeniti, tj. možemo li funkciju f izraziti u terminima funkcije F. Odgovor na to pitanje slijedi u nastavku ovog poglavlja.

Za početak pretpostavimo da je f aritmetička funkcija i $F(n) = \sum_{d|n} f(d)$. Raspišemo li $F(n)$ za $n = 1, 2, 3, 4, 5, 6$ i 7 dobivamo sljedeće

$$\begin{aligned}
F(1) &= f(1) \\
F(2) &= f(1) + f(2) \\
F(3) &= f(1) + f(3) \\
F(4) &= f(1) + f(2) + f(4) \\
F(5) &= f(1) + f(5) \\
F(6) &= f(1) + f(2) + f(3) \\
F(7) &= f(1) + f(7).
\end{aligned}$$

Rješavanjem gornjih jednadžbi po $f(n)$ za $n = 1, 2, 3, 4, 5, 6$ i 7 imamo

$$\begin{aligned}
f(1) &= F(1) \\
f(2) &= F(2) - f(1) = F(2) - F(1) \\
f(3) &= F(3) - f(1) = F(3) - F(1) \\
f(4) &= F(4) - f(1) - f(2) = F(4) - (F(2) - F(1)) - F(1) \\
&= F(4) - F(2) \\
f(5) &= F(5) - f(1) = F(5) - F(1) \\
f(6) &= F(6) - f(3) - f(2) - f(1) \\
&= F(6) - (F(3) - F(1)) - (F(2) - F(1)) - F(1) \\
&= F(6) - F(3) - F(2) + F(1) \\
f(7) &= F(7) - F(1).
\end{aligned}$$

Na osnovu prethodnog možemo zaključiti kako funkciju $f(n)$ možemo zapisati u obliku sume čiji su članovi oblika $\pm F(n/d)$, pri čemu je d djeljitelj od n. Odnosno, funkciju $f(n)$ možemo definirati sljedećom formulom:

$$f(n) = \sum_{d|n} \mu(d) F(n/d),$$

pri čemu je μ neka aritmetička funkcija koju trebamo odrediti.

Iz prethodnog računa možemo zaključiti kako funkcija μ prima vrijednosti iz skupa $\{-1, 0, 1\}$. Kako je $f(1) = F(1)$, onda je $\mu(1) = 1$. Za prost broj p je $F(p) = f(1) + f(p)$ pa vrijedi $f(p) = F(p) - F(1)$. Dakle, $\mu(p) = -1$. Nadalje, kako je

$$F(p^2) = f(1) + f(p) + f(p^2)$$

vrijedi

$$f(p^2) = F(p^2) - (F(p) - F(1)) - F(1) = F(p^2) - F(p).$$

Iz tog slijedi da je $\mu(p^2) = 0$. Također, može se pokazati da je $f(p^k) = F(p^k) - F(p^{k-1})$ pa je $\mu(p^k) = 0$ za p prost broj i $k > 1$.

Dakle, $\mu(p) = -1$ i $\mu(p^k) = 0$ za sve proste brojeve p i prirodne brojeve $k > 1$. Stoga, ako pretpostavimo da je funkcija μ multiplikativna možemo odrediti vrijednost funkcije $\mu(n)$ za bilo koji prirodan broj n koristeći se Fundamentalnim teoremom za multiplikativne funkcije.

Na osnovu prethodnog razmatranja, definiramo funkciju $\mu(n)$ koja se naziva Möbiusova funkcija. Tu važnu funkciju u teoriji brojeva uveo je njemački matematičar August Ferdinand Möbius po kojem je i dobila ime.

Za prirodan broj n, Möbiusova funkcija $\mu(n)$ definirana je sa

$$\mu(n) = \begin{cases} 1, & \text{ako je } n = 1 \\ 0, & \text{ako } p^2 | n \text{ za neki prost broj } p \\ (-1)^k, & \text{ako je } n = p_1 p_2 \cdots p_k \text{ gdje su } p_i \text{ različiti prosti brojevi.} \end{cases}$$

Drugim riječima, $\mu(n) = 0$ ako je n djeljiv s kvadratom prostog broja, a $\mu(n) \neq 0$ ako je n kvadratno slobodan.

Primjer 21. *Odredimo vrijednost Möbiusove funkcije $\mu(n)$ za $n = 5, 20$ i 210.*
Rješenje:

$$\begin{aligned} \mu(5) &= -1 \\ \mu(20) &= \mu(2^2 \cdot 5) = 0 \\ \mu(210) &= \mu(2 \cdot 3 \cdot 5 \cdot 7) = (-1)^4 = 1 \end{aligned}$$

Prije nego pokažemo da je Möbiusova funkcija $\mu(n)$ multiplikativna, pogledajmo idući primjer.

Primjer 22. *Pokažimo da vrijedi $\mu(mn) = \mu(m)\mu(n)$, za $m = 12$ i $n = 35$.*
Rješenje: Brojevi m i n su relativno prosti. Kako je $m = 12 = 2^2 \cdot 3$, vrijedi $\mu(m) = 0$. Kako je $n = 35 = 5 \cdot 7$, vrijedi $\mu(n) = (-1)^2 = 1$. Nadalje, $mn = 2^2 \cdot 3 \cdot 5 \cdot 7$ pa je mn djeljiv s kvadratom prostog broja. Stoga slijedi da je $\mu(mn) = 0$. Dakle, $\mu(mn) = 0 = 0 \cdot 1 = \mu(m)\mu(n)$.

Dokažimo da je Möbiusova funkcija $\mu(n)$ multiplikativna koristeći se njezinom definicijom.

Teorem 13 ([5], Theorem 8.16)**.** *Funkcija μ je multiplikativna.*

Dokaz. Neka su m i n dva relativno prosta broja. Trebamo pokazati da je $\mu(mn) = \mu(m)\mu(n)$. Moguća su tri slučaja:
1. Ako je $m = 1$ i $n = 1$, očito je $\mu(mn) = \mu(m)\mu(n)$.
2. Pretpostavimo da je jedan od brojeva m ili n djeljiv s p^2, za neki p prost broj. Tada je $\mu(m)\mu(n) = 0$. Kako $p^2|m$ ili $p^2|n$ slijedi $p^2|mn$. Stoga je $\mu(mn) = 0$. Dakle,

$$\mu(mn) = 0 = \mu(m)\mu(n).$$

3. Neka su $m = p_1 p_2 \cdots p_s$ i $n = q_1 q_2 \cdots q_t$ dva kvadratno slobodna broja. Tada imamo

$$\mu(m) = (-1)^s \quad \text{i} \quad \mu(n) = (-1)^t.$$

Kako je $(m, n) = 1$, slijedi da su p_i i q_j različiti prosti brojevi. Stoga je produkt mn sastavljen od $s + t$ različitih prostih brojeva, odnosno $mn = p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$. Vrijedi

$$\mu(mn) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = \mu(m)\mu(n).$$

□

Zanimljivo svojstvo ima funkcija definirana formulom

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

Za $n = 1$ je $\sum_{d|1} \mu(n) = \mu(1) = 1$, dok za $n > 1$ vrijednost sume možemo odrediti koristeći se kanonskim fastavom broja n na proste faktore i Teoremom 13. Najprije odredimo $\sum_{d|n} \mu(n)$, za n oblika $n = p^e$.

Lema 2 ([5], Lemma 8.3)**.** *Neka je* $F(n) = \sum_{d|n} \mu(d)$*. Tada je* $F(p^e) = 0$*, za* $e > 1$*.*

Dokaz. Pozitivni djelitelji broj p^e su $1, p, p^2, \ldots, p^e$. Vrijedi

$$\begin{aligned} F(p^e) &= \sum_{d|p^e} \mu(d) \\ &= \sum_{j=0}^{e} \mu(p^j) \\ &= \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^e) \\ &= 1 + (-1) + 0 + \ldots + 0 = 0. \end{aligned}$$

□

Primjer 23. *Za* $n = 4^5$*, pokažimo da vrijedi rezultat dan u prethodnoj lemi.*
Rješenje:

$$\begin{aligned} \sum_{d|4^5} \mu(d) &= \mu(1) + \mu(4) + \mu(4^2) + \mu(4^3) + \mu(4^4) + \mu(4^5) \\ &= 1 + (-1) + 0 + 0 + 0 + 0 = 0. \end{aligned}$$

Teorem 14 ([5], Theorem 8.17)**.** *Neka je n prirodan broj. Tada je*

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

Dokaz. Za slučaj $n = 1$ već smo pokazali da je

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

Nadalje, neka je $n > 1$, $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ kanonski rastav broja n na proste faktore i neka je

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

Kako je funkcija μ multiplikativna, iz Teorema 6 slijedi da je i funkcija F multiplikativna. Odnosno,

$$F(n) = F(p_1^{e_1}) F(p_2^{e_2}) \cdots F(p_k^{e_k}).$$

Koristeći se rezultatom prethodne leme, zaključujemo da je svaki od faktora s desne strane jednakosti jednak nuli. Dakle, $F(n) = 0$ za $n > 1$. □

Ilustraciju ovog teorema imamo u sljedećem primjeru.

Primjer 24.

$$\begin{aligned} \sum_{d|45} \mu(d) &= \mu(1) + \mu(3) + \mu(5) + \mu(9) + \mu(15) + \mu(45) \\ &= 1 + (-1) + (-1) + 0 + (-1)^2 + 0 = 0 \end{aligned}$$

Važan rezultat u ovom poglavlju je idući teorem koji nosi naziv Möbiusova formula inverzije. Möbiusova formula inverzije izražava funkciju f u terminima funkcije F, pri čemu je $F(n) = \sum_{d|n} f(d)$. Ovaj rezultat daje nam odgovor na pitanje postavljeno na početku ovog poglavlja.

Teorem 15 ([5], Theorem 8.18)**.** *Neka je f aritmetička funkcija i $F(n) = \sum_{d|n} f(d)$. Tada je*

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Dokaz. Kako je $F(n) = \sum_{d|n} f(d)$, onda je $F(n/d) = \sum_{d'|(n/d)} f(d')$. Imamo

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

Sumiramo li obje strane jednakosti po svim pozitivnim djeliteljima d od n dobivamo

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

Lako se može pokazati da $d|n$ i $d'|(n/d)$ ako i samo ako $d'|n$ i $d|(n/d')$. Stoga se desna strana prethodne jednakosti može zapisati kao

$$\sum_{d|n} \sum_{d'|(n/d)} \mu(d) f(d') = \sum_{d'|n} \sum_{d|(n/d')} \mu(d) f(d').$$

Vrijedi

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

Prema Teoremu 14 je $\sum_{d|(n/d')} \mu(d) = 0$, osim u slučaju kada je $n/d' = 1$, odnosno $n = d'$. Za $n = d'$ vrijednost sume jednaka je 1 te je

$$\sum_{d|n} \mu(d) F(n/d) = f(n) \cdot 1 = f(n).$$

Dakle, $f(n) = \sum_{d|n} \mu(d) F(n/d)$ i time je tvrdnja dokazana. □

Napomena 1. *Primijetimo da u prethodnoj formuli d prolazi po svim pozitivnim djeliteljima od n, a isto je i s n/d. Stoga Möbiusovu formulu inverzije možemo zapisati i na sljedeći način:*

$$f(n) = \sum_{d|n} \mu(n/d) f(d).$$

U dokazu prethodnog teorema javlja se potreba za promjenom redoslijeda sumacije varijabli. Ilustrirajmo tu promjenu na primjeru koji slijedi.

Primjer 25. *Neka je f aritmetička funkcija. Pokažimo da vrijedi*

$$\sum_{d|8} \sum_{d'|(8/d)} \mu(d) f(d') = \sum_{d'|8} \sum_{d|(8/d')} f(d') \mu(d).$$

Rješenje:

$$\begin{aligned}
&\sum_{d|8} \sum_{d'|(8/d)} \mu(d) f(d') \\
&\qquad = \sum_{d'|8} \mu(1) f(d') + \sum_{d'|4} \mu(2) f(d') + \sum_{d'|2} \mu(4) f(d') + \sum_{d'|1} \mu(8) f(d') \\
&\qquad = \mu(1) \sum_{d'|8} f(d') + \mu(2) \sum_{d'|4} f(d') + \mu(4) \sum_{d'|2} f(d') + \mu(8) \sum_{d'|1} f(d') \\
&\qquad = \mu(1)(f(1) + f(2) + f(4) + f(8)) + \mu(2)(f(1) + f(2) + f(4)) \\
&\qquad\qquad \mu(4)(f(1) + f(2)) + \mu(8) f(1) \\
&\qquad = f(1)(\mu(1) + \mu(2) + \mu(4) + \mu(8)) + f(2)(\mu(1) + \mu(2) + \mu(4)) \\
&\qquad\qquad f(4)(\mu(1) + \mu(2)) + f(8)\mu(1) \\
&\qquad = f(1) \sum_{d|8} \mu(d) + f(2) \sum_{d|4} \mu(d) + f(4) \sum_{d|2} \mu(d) + f(8) \sum_{d|1} \mu(d) \\
&\qquad = \sum_{d'|8} f(d') \sum_{d|(8/d')} \mu \\
&\qquad = \sum_{d'|8} \sum_{d|(8/d')} f(d') \mu(d).
\end{aligned}$$

Prisjetimo se funkcija broj djelitelja $\tau(n)$ i suma djelitelja $\sigma(n)$. One su definirane na sljedeći način:

$$\tau(n) = \sum_{d|n} 1 \quad \text{i} \quad \sigma(n) = \sum_{d|n} d.$$

Stoga bi dobri primjeri Möbiusove formule inverzije bili inverzija funkcija τ i σ. Primjenom Teorema 15 dolazimo do sljedećih formula

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

i

$$n = \sum_{d|n} \mu(d)\sigma(n/d) = \sum_{d|n} \mu(n/d)\sigma(d).$$

Primjer 26. *Provjerimo prethodne formule za $n = 26$.*
Rješenje:

$$\begin{aligned}\sum_{d|26} \mu(26)\tau(26/d) &= \mu(1)\tau(26) + \mu(2)\tau(13) + \mu(13)\tau(2) + \mu(26)\tau(1) \\ &= 1 \cdot 4 + (-1) \cdot 2 + (-1) \cdot 2 + (-1)^2 \cdot 1 = 1\end{aligned}$$

i

$$\begin{aligned}\sum_{d|26} \mu(26)\sigma(26/d) &= \mu(1)\sigma(26) + \mu(2)\sigma(13) + \mu(13)\sigma(2) + \mu(26)\sigma(1) \\ &= 1 \cdot 42 + (-1) \cdot 14 + (-1) \cdot 3 + (-1)^2 \cdot 1 = 26.\end{aligned}$$

Koristeći Möbiusovu formulu inverzije možemo izvesti još jednu formulu za Eulerovu funkciju $\varphi(n)$. Za to nam je potreban sljedeći teorem.

Teorem 16 ([5], Theorem 8.5)**.** *Za svaki prirodan broj n je $\sum_{d|n} \varphi(n) = n$.*

Dokaz. Označimo s $F(n) = \sum_{d|n} \varphi(n)$. Kako je Eulerova funkcija multiplikativna, prema Teoremu 6 je i funkcija F multiplikativna.

Neka je $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ kanonski rastav broja n na proste faktore. Trebamo pokazati da je $F(n) = n$.

Dokažimo prvo da je $F(p^e) = p^e$. Za bilo koji p prost broj i e prirodan broj je

$$\begin{aligned}F(p^e) &= \sum_{d|p^e} \varphi(d) = \sum_{j=1}^{e} \varphi(p^j) \\ &= \varphi(1) + \varphi(p) + \varphi(p^2) + \varphi(p^3) + \ldots \varphi(p^e) \\ &= 1 + (p-1) + (p^2 - p) + (p^3 - p^2) \ldots + (p^e - p^{e-1}) \\ &= p^e,\end{aligned}$$

gdje predzadnja jednakost slijedi iz Leme 1. Kako je funkcija F multiplikativna vrijedi

$$\sum_{d|n} \varphi(n) = F(n) = F(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = F(p_1^{e_1}) \cdots F(p_k^{e_k}) = p_1^{e_1} \cdots p_k^{e_k} = n.$$

□

Teorem 17 ([5], Theorem 8.19)**.** $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.

Dokaz. U prethodnom teoremu pokazali smo da je $F(n) = \sum_{d|n} \varphi(d) = n$. Tada je $F(n/d) = n/d$. Primjenimo li Möbiusovu formulu inverzije dobivamo

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

□

Već smo ranije u radu pokazali da je Eulerova funkcija multiplikativna. Koristeći se formulom za $\varphi(n)$ iz prethodnog teorema dolazimo do još jednog dokaza. Naime, kako je funkcija μ multiplikativna funkcija, onda je i Eulerova funkcija prema Teoremu 6 multiplikativna.

Također, za prost broj p i prirodan broj i, koristeći se formulom za $\varphi(n)$ iz prethodnog teorema dolazimo do sljedećeg

$$\varphi(p^i) = p^i \sum_{d|p^i} \frac{\mu(d)}{d} = p^i \sum_{j=1}^{i} \frac{\mu(p^j)}{p^j} = p^i \left(1 - \frac{1}{p}\right)$$

što nam daje rezultat pokazan Lemom 1.

Idući teorem pokazuje da vrijedi obrat Teorema 15.

Teorem 18 ([5], Theorem 8.20)**.** *Neka su F i f dvije aritmetičke funkcije takve da je $f(n) = \sum_{d|n} \mu(d) F(n/d)$. Tada je $F(n) = \sum_{d|n} f(d)$.*

Dokaz. Prema definiciji funkcije f imamo

$$f(d) = \sum_{d'|d} \mu(d') F(d/d').$$

Sumiranjem prethodne jednakosti po svim djeliteljima d od n dobivamo

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

Stavimo li $d/d' = k$, slijedi

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} \sum_{kd'=d} \mu(d') F(k) \\ &= \sum_{kd'|n} \mu(d') F(k) \\ &= \sum_{k|n} F(k) \left[\sum_{d'|(n/k)} \mu(d') \right]. \end{aligned}$$

Koristeći se Teoremom 14 možemo zaključiti da je $\sum_{d'|(n/k)} \mu(d') = 1$ za $n = k$, a inače je ta suma jednaka 0. Stoga je

$$\sum_{d|n} f(d) = F(k) \cdot 1 = F(n).$$

□

Često smo se u ovom radu koristili rezultatom Teorema 6 u kojem smo pokazali da je za multiplikativnu funkciju f i funkcija F definirana formulom $F(n) = \sum_{d|n} f(d)$ također multiplikativna. Još jedna od posljedica Möbiusove formule inverzije je da vrijedi i obrat ove tvrdnje.

Teorem 19 ([9], Theorem 7.17.). *Neka je f aritmetička funkcija i $F = \sum_{d|n} f(d)$. Ako je funkcija F multiplikativna, onda je i funkcija f multiplikativna.*

Dokaz. Pretpostavimo da su m i n dva relativno prosta prirodna broja. Trebamo pokazati da je $f(mn) = f(m)f(n)$. Vrijedi

$$\begin{aligned}
f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\
&= \sum_{d_1|m, d_2|n} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\
&= \sum_{d_1|m, d_2|n} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\
&= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\
&= f(m)f(n).
\end{aligned}$$

□

Literatura

[1] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[2] D. Cortild, A. Villegas Sanabria, *Lucas-Lehmer Primality Test*, University of Groningen, 2022., dostupno na https://www.researchgate.net/publication/358646149_Lucas-Lehmer_Primality_Test

[3] B. Ibrahimpašić, E. Liđan, *Mersenneovi i savršeni brojevi*, Matematički kolokvijum (MAT-KOL), Banja Luka, Vol. XV (2) (2009), 51-60.

[4] M. Jukić Bokun, A. Behin, *Eulerova funkcija*, Math.e: hrvatski matematički elektonički časopis, (1334-6083) 31 (2017), 1-9.

[5] T. Koshy, *Elementary Number Theory with Applications*, Elsevier Inc., Amsterdam, 2007.

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

[7] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, New York, 1991.

[8] J. J. O'Connor, E. F. Robertson, *MacTutor Perfect numbers*, University of St. Andrews, Scotland, 2020.

[9] K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Boston, 2011.

[10] *List of Known Mersenne Prime Numbers*, dostupno na https://www.mersenne.org/primes/

Sažetak

Ovaj rad proučava multiplikativne funkcije teorije brojeva i njihova svojstva, a strukturiran je u pet poglavlja.

Na početku rada definirani su temeljni pojmovi teorije brojeva. Zatim se uvodi definicija multiplikativnosti funkcije te pokazujemo da su Eulerova funkcija, funkcija suma djelitelja i funkija broj djelitelja primjeri multiplikativnih funkcija. Za svaku navedenu funkciju određena je eksplicitna formula.

Za kraj je uvedena Möbiusova funcija koju vežemo uz Möbiusovu formulu inverzije. Primjer Möbiusove formule inverzije pokazan je na funkcijama broj djelitelja i suma djelitelja. Osim toga, izvedena je još jedna formula za Eulerovu funkciju korištenjem Möbiusove formule inverzije.

Ključne riječi

aritmetičke funkcije, multiplikativne funkcije, Eulerova funkcija, broj djelitelja, suma djelitelja, savršeni brojevi, Mersenneovi brojevi, Möbiusova funkcija, Möbiusova formula inverzije

Multiplicative functions

Summary

This paper examines multiplicative functions in number theory and their properties, and is structured into five chapters.

The fundamental concepts of number theory are defined at the start of the paper. Next, the definition of a multiplicative function is introduced, and it is shown that Euler's function, the sum of divisors function, and the number of divisors function are examples of a multiplicative function. For each of the mentioned functions, an explicit formula is provided.

Lastly, the Mobius function is introduced, which is related to the Möbius inversion formula. An example of the Mobius inversion formula is shown for the number of divisors function and the sum of divisors function. Additionaly, one more formula for Euler's function is derived using the Möbius inversion formula.

Keywords

arithmetic functions, multiplicative functions, Euler's function, number of divisors function, sum of divisors function, perfect numbers, Mersenne primes, Möbius function, Möbius inversion formula

Životopis

Moje ime je Ivana Vuletić. Rođena sam 7. prosinca 1996. godine u Slavonskom Brodu. Nakon završene Osnovne škole Antun Mihanović upisujem Tehničku školu u Slavonskom Brodu koju završavam 2015. godine i stječem strukovnu kvalifikaciju/zanimanje arhitektonska tehničarka. U Osijeku sam iste godine upisala preddiplomski studij matematike na Odjelu za matematiku. Akademski naziv sveučilišna prvostupnica matematike stječem 2019. godine sa završnim radom na temu *Algebarska, analitička i geometrijska svojstva vektorskih normi* pod mentorskim vodstvom doc. dr. sc. Ivane Kuzmanović Ivičić. Nakon završenog preddiplomskog studija upisujem diplomski studij, smjer Financijska matematika i statistika. Na Filozofskom fakultetu u Osijeku 2022. godine upisujem i završavam PPDM izobrazbu. Trenutno sam zaposlena u Osnovnoj školi Sibinjskih žrtava u Sibinju na mjestu učiteljica matematike.