Aritmetičke funkcije teorije brojeva

Vukašinović, Jelena

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Jelena Vukašinović

ARITMETIčKE FUNKCIJE TEORIJE BROJEVA

Diplomski rad

Voditelj rada:
Prof.dr.sc.Sanja Varošanec

Zagreb, rujan, 2017.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Aritmetika je grana matematike koja se bavi brojevima.

U povijesti prvi aritmetički problemi su zapisani u starom Babilonu i Egiptu 2-3 tisuće godina prije Krista. Kroz povijest važna otkrića za aritmetiku su bila otkriće iracionalnih brojeva, te osnovnih svojstava djeljivosti prirodnih brojeva, uporaba pozicijskog sustava i nule. Aritmetika se smatra kraljicom matematike.

Teorija brojeva je grana matematike koja se ponajprije bavi prirodnim brojevima, te cijelim i racionalnim brojevima. Teorija brojeva, poput mnogih drugih grana matematike, se često bavi nizovima realnih ili kompleksnih brojeva, a takvi nizovi brojeva u teorji brojeva se nazivaju aritmetičke funkcije.

Definicija 0.0.1. *Realna ili kompleksna funkcija koja se definira na skupu prirodnih brojeva zove se aritmetička funkcija.*

U ovom diplomskom radu upoznat ćemo se s nekim aritmetičkim funkcijama koje, a posebno s dvije široke klase aritmetičkih funkcija: s multiplikativnoim i aditivnim funkcijama.

U radu ćemo također govoriti i o Dirichletovom produktu (konvoluciji), konceptu koji pomaže razjasniti međusobne odnose između različitih aritmetičkih funkcija.

Također ćemo definirati derivaciju aritmetičke funkcije te opisati kako pomoću njezinog koncepta možemo dokazati Selbergov identitet.

Poglavlje 1

Aditivne i multiplikativne funkcije

1.1 Multiplikativne funkcije

Aritmetička funkcija f je multiplikativna ako je različita od nul funkcije i ako za sve parove relativno prostih brojeva m i n vrijedi

$$f(mn) = f(m)f(n). \tag{1.1}$$

Prema osnovnom stavku aritmetike, svaki se prirodni broj može zapisati u obliku

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$$

pri čemu su $p_1, p_2, ..., p_r$ različiti prosti brojevi, a eksponenti su prirodni brojevi. Brojevi $p_i^{a_i}$ i $p_j^{a_j}$ su relativno prosti za $i \neq j$. Zato se vrijednost multiplikativne funkcije na broju n može napisati u obliku

$$f(n) = f(p_1^{a_1})f(p_2^{a_2})...f(p_r^{a_r}).$$

Funkcija f je potpuno multiplikativna ako je $f(1) = 1$ i ako svojstvo (1.1) vrijedi za svaka dva prirodna broja m i n.

Teorem 1.1.1. *[2] Aritmetička funkcija f je multiplikativna ako i samo ako je* $f(1) = 1$ *i za* $n \geq 2$

$$f(n) = \prod_{p^m | n} f(p^m). \tag{1.2}$$

Funkcija je potpuno multiplikativna ako i samo ako vrijede gornji uvjeti i ako je $f(p^m) = f(p)^m$ *za sve proste brojeve p i prirodne m.*

Dokaz. Pretpostavimo najprije da f zadovoljava $f(1) = 1$ i (1.2) za $n \geq 2$. Neka su n_1 i n_2 relativno prosti brojevi $n_1, n_2 \geq 2$. Tada nijedan prosti faktor od n_1 nije prosti faktor od n_2 i obrnuto. Neka je

$$n_1 = p_1^{a_1} p_2^{a_2} ... p_r^{a_r} \;\; i \;\; n_2 = s_1^{b_1} s_2^{b_2} ... s_k^{b_k}$$

gdje su $p_1, p_2, ..., p_r, s_1, s_2, ..., s_k$ različiti prosti brojevi, $a_1, a_2, ..., a_r, b_1, b_2, ..., b_k$ prirodni brojevi. Tada prema (1.2) vrijedi

$$f(n_1) = f(p_1^{a_1}) f(p_2^{a_2}) ... f(p_r^{a_r}),$$

$$f(n_2) = f(s_1^{b_1}) f(s_2^{b_2}) ... f(s_k^{b_k}),$$

$$f(n_1 n_2) = f(p_1^{a_1}) f(p_2^{a_2}) ... f(p_r^{a_r}) f(s_1^{b_1}) f(s_2^{b_2}) ... f(s_k^{b_k}).$$

Očito je $f(n_1 n_2) = f(n_1) \cdot f(n_2)$. Ako je, bez smanjenja općenitosti, $n_2 = 1$ i $n_1 \geq 2$, tada za par relativno prostih brojeva n_1, n_2 imamo

$$f(n_1 n_2) = f(n_1 \cdot 1) = f(n_1) = f(n_1) \cdot 1 = f(n_1) f(n_2).$$

Dakle, u svakom slučaju dobivamo da vrijedi definicijsko svojstvo multiplikativne funkcije, tj. f je multiplikativna. Ako pretpostavimo da je f multiplikativna, tada f nije jednaka 0 pa postoji $n \in \mathbf{N}$ tako da je $f(n) \neq 0$. Primjenom (1.1) za par $(n_1, n_2) = (n, 1)$ dobivamo $f(n) = f(1 \cdot n) = f(1) f(n)$, odakle dijeljenjem s $f(n)$ slijedi da je $f(1) = 1$. Nadalje, za $n \geq 2$ imamo $n = \Pi_{i=1}^{k} p_i^{a_i}$. Brojevi $p_1^{a_1} ... p_{k-1}^{a_{k-1}}$ i $p_k^{a_k}$ su relativno prosti, pa primjenom svojstva (1.1) imamo

$$f(n) = f(p_1^{a_1} ... p_{k-1}^{a_{k-1}} p_k^{a_k}) = f(p_1^{a_1} ... p_{k-1}^{a_{k-1}}) \cdot f(p_k^{a_k}).$$

Brojevi $p_1^{a_1} ... p_{k-2}^{a_{k-2}}$ i $p_{k-1}^{a_{k-1}}$ su relativno prosti pa je gornji izraz jednak

$$f(n) = f(p_1^{a_1} ... p_{k-2}^{a_{k-2}}) \cdot f(p_{k-1}^{a_{k-1}}) \cdot f(p_k^{a_k}).$$

Nastavljajući dalje, dobivamo

$$f(n) = f(p_1^{a_1}) ... f(p_k^{a_k})$$

što je upravo svojstvo (1.2)

Ako je f potpuno multiplikativna, onda za bilo koji prosti broj p slijedi:

$$f(p^m) = f(p^{m-1} \cdot p) = f(p^{m-1}) f(p) = ... = f(p)^m.$$

Obrnuto, ako je f multiplikativna i zadovoljava $f(p^m) = f(p)^m$ za sve proste brojeve oblika p^m, onda po (1.1) se može zapisati kao $f(n) = \Pi_{i=1}^{r} f(p_i)$, gdje je sada $n = \Pi_{i=1}^{r} p_i$ faktorizacija od n na proste (ne nužno različite) faktore. Neka su n_1 i n_2 prirodni brojevi čije faktorizacije na proste faktore glase ovako:

$$n_1 = p_1 p_2 ... p_r$$

$$n_2 = s_1 s_2 ... s_k.$$

Tada je $f(n_1 n_2) = f(p_1)f(p_2)...f(p_2)f(s_1)f(s_2)...f(s_k) = f(n_1) \cdot f(n_2)$. Stoga je f potpuno multiplikativna. □

Teorem 1.1.2. *[2] Pretpostavimo da su f i g multiplikativne funkcije. Slijedi:*

• *produkt fg je multiplikativan;*

• *ako g nije nula, tada je količnik $\frac{f}{g}$ multiplikativan.*

Dokaz. Rezultat slijedi neposredno iz definicije multiplikativnosti. Produkt fg dviju aritmetičkih funkcija f i g je definiran kao $(fg)(n) = f(n)g(n)$. Dokažimo prvu tvrdnju. Neka su m i n relativno prosti brojevi. Iz multiplikativnosti funkcija f i g slijedi

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

$$g(mn) = g(m)g(n).$$

Tada je

$$(fg)(mn) = f(mn)g(mn) = f(m)f(n)g(m)g(n) = (fg)(m) \cdot (fg)(n),$$

tj. fg je multiplikativna funkcija. Analogno se dokazuje i druga tvrdnja. □

Teorem 1.1.3. *[1] Neka je f multiplikativna funkcija i neka je $F(n) = \sum_{d|n} f(d)$. Tada je F multiplikativna.*

U cijelom radu promatramo isključivo pozitivne djelitelje d prirodnog broja, te to više neće biti posebno napominjano. Također za zajedničkog djelitelja dva broja m i n koristit ćemo oznaku (m, n).

Dokaz. Pretpostavimo da je $m = m_1 m_2$ i $(m_1, m_2) = 1$. Ako je $d|m$, onda je $d_1 = (d, m_1)$ i $d_2 = (d, m_2)$. Tako imamo $d = d_1 d_2$, $d_1|m_1$ i $d_2|m_2$. Obrnuto, ako su d_1, d_2 dijelitelji od m_1 i m_2, tada je $d = d_1 d_2$ djelitelj od m i $d_1 = (d, m_1)$, $d_2 = (d, m_2)$. Tako smo uspostavili vezu između djelitelja d od m i d_1, d_2 kao djelitelja od m_1 i m_2. Stoga vrijedi

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

Osim toga vrijedi i $(d_1, d_2) = 1$, pa iz pretpostavke da je f multiplikativna desna je strana jednaka

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

□

Istaknute multiplikativne funkcije su: Eulerova funkcija, zbroj djelitelja σ, poopćen zbroj djelitelja σ_α, broj djelitelja τ, Liouvilleova funkcija λ, Möbiusova funkcija μ. Recimo nešto o svakoj od tih funkcija.

1.1.1 Eulerova funkcija

Eulerova funkcija ϕ je funkcija koja prirodnom broju n pridružuje broj prirodnih brojeva manjih od n koji su relativno prosti s n.

Primjer 1.1.4. *Izračunajmo $\phi(n)$ za $n = 12$ i $n = 11$.*

Rješenje: Brojevi manji od 12 koji su relativno prosti s 12 su 1, 5, 7 i 11, pa je $\phi(12) = 4$. Broj 11 je prost broj te su svi brojevi manji od njega ujedno relativno prosti s njim. Dakle, $\phi(n) = 10$. Ovaj zaključak za $n = 11$ se može poopćiti za bilo koji prosti broj.

Ako je n prost broj, onda vrijedi $\phi(n) = n - 1$. Vidimo odmah da vrijedi i obrat, ako je $\phi(n) = n - 1$, broj n mora biti prost.

Teorem 1.1.5. *[2] Eulerova funkcija ϕ je multiplikativna.*

Dokaz. Neka su m i n relativno prosti. Sve brojeve koji ne premašuju mn možemo poredati u tablicu:

1	$m+1$	$2m+1$	...	$(n-1)m+1$
2	$m+2$	$2m+2$	...	$(n-1)m+2$
3	$m+3$	$2m+3$	...	$(n-1)m+3$
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
r	$m+r$	$2m+r$	...	$(n-1)+r$
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
m	$2m$	$3m$	...	nm

Želimo izračunati $\phi(mn)$. Dakle, naš je zadatak prebrojati koliko je elemenata ove tablice relativno prosto s mn.

Neka je $1 \leq r \leq m$. Pretpostavimo da je $(m, r) = d > 1$. No, tada nijedan broj iz r-tog retka nije relativno prost s mn. Naime, brojevi u tom retku su oblika $km + r$ i vrijedi da je $d \mid (km + r)$ budući da je $d \mid m$ i $d \mid r$.

Prema tome, brojeve koji su relativno prosti s mn možemo pronaći samo u onim retcima za koje je $(m, n) = 1$. Takvih redaka ima $\phi(m)$. Promotrit ćemo sad bilo koji od njih.

Neka je r relativno prost s m. Tada svi brojevi u r-tom retku daju različite ostatke pri dijeljenju s n. Naime, iz pretpostavke

$$k_1 m + r \equiv k_2 m + r (mod\ n)$$

slijedi $n \mid (k_1 - k_2)m$. Budući da su m i n relativno prosti, a k_1, k_2 manji od n, zaključujemo da mora biti $k_1 = k_2$.

Neki je broj relativno prost sa n onda i samo onda ako je njegov ostatak pri dijeljenju s n relativno prost s n. To znači da u r-tom retku ima točno $\phi(n)$ brojeva koji su relativno prosti s n. Budući da su svi brojevi u tom retku relativno prosti s m, onda ima točno $\phi(n)$ brojeva u tom retku relativno prostih s mn.

U ovoj tablici smo prebrojali $\phi(m)$ redaka, od kojih svaki sadrži $\phi(n)$ brojeva relativno prostih s mn. Zato je $\phi(mn) = \phi(m)\ \phi(n)$. □

Teorem 1.1.6. *[2] Ako je p prost broj i k prirodan, onda je*

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Za bilo koji prirodan broj n vrijedi

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_r}\right)$$

gdje su p_1, p_2,...,p_r svi njegovi različiti prosti faktori.

Dokaz. Ako neki broj manji od p^k nije relativno prost s p^k, onda je on višekratnik od p, jer je to jedini prosti faktor broja p^k. Svi takvi višekratnici su oblika mp, pri čemu je $1 \leq m \leq p^{k-1}$ i ima ih točno p^{k-1}. To znači da brojeva manjih od p^k koji jesu relativno prosti s p^k ima $p^k - p^{k-1}$ i time je dokazana prva formula. Ako je n prirodni broj oblika $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$, tada imamo

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1} p_2^{a_2} ... p_r^{a_r}) \\
&= f(p_1^{a_1}) f(p_2^{a_2}) ... f(p_r^{a_r}) \\
&= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) ... (p_r^{a_r} - p_r^{a_r-1}) \\
&= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right) ... p_r^{a_r}\left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

□

Teorem 1.1.7. *[2]Eulerova funkcija ϕ zadovoljava:*

(i) $\sum_{d|n} \phi(d) = n$ *za sve prirodne brojeve.*

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

Dokaz. (i) Podijelimo skup $A = \{1, 2, ..., n\}$ na disjunktne podskupove $A_d = \{m \in A : (m, n) = d, d \mid n\}$. Pisanjem jednog elementa $m \in A_d$ kao $m = dm'$, vidimo da je $A_d = \{dm' : 1 \leq m' \leq n/d, (m', n/d) = 1\}$, i da je $|A_d| = \phi(n/d)$. Zbog $n = |A| = \sum_{d|n} |A_d|$, slijedi da je $n = \sum_{d|n} \phi(n/d)$.

(ii) Iz definicije Eulerove funkcije ϕ slijedi da je $\phi(n) = \sum_{m \leq n, (m,n)=1} 1$. Uklanjanjem uvjeta $(m, n) = 1$, kao što je navedeno, dobivamo identitet

$$\phi(n) = \sum_{m \leq n} \sum_{d|(m,n)} \mu(d) = \sum_{d|n} \mu(d) \sum_{m \leq n, d|m} 1 = \sum_{d|n} \mu(d)(n/d)$$

.

□

Teorem 1.1.8. *[1](Mali Fermatov teorem) Neka je p prost broj i a prirodan. Ako p ne dijeli a, tada je* $a^{p-1} \equiv 1(mod\ p)$.

Dokaz ovog teorema ćemo odgoditi te ćemo ga shvatiti kao korolar sljedećeg teorema.

Teorem 1.1.9. *[1](Eulerov teorem) Ako je* $(a, n) = 1$ *tada je*

$$a^{\phi(n)} \equiv 1(mod\ n).$$

Dokaz. Neka je $r = \phi(n)$. Označimo s $k_1, ..., k_r$ brojeve manje od n i relativno proste s n. S obzirom da su a i n relativno prosti, tada su i brojevi $ak_1, ..., ak_r$ relativno prosti s n. Ujedno, njihovi ostatci pri dijeljenju s n su međusobno različiti. Naime, pretpostavimo li da ak_i i ak_j za $k_i \neq k_j$ daju isti ostatak pri dijeljenju s n, slijedilo bi da je $a(k_i - k_j)$ djeljivo s n, što nije moguće, jer je a relativno prost s n, dok je $k_i - k_j$ manje od n. Zato imamo

$$ak_i \equiv a_i(mod\ n),$$

za svaki $i = 1, ..., r$, pri čemu su $a_1, a_2, ..., a_r$ isti kao i brojevi $k_1, k_2, ..., k_r$, ali ne nužno u istom redoslijedu. Množenjem ovih kongruencija dobivamo $a^r \equiv 1(mod\ n)$. □

Napravimo sad dokaz teorema 1.1.8

Dokaz. Ako p ne dijeli a tada je $(a, p) = 1$ i $a^{\phi(p)} \equiv 1(mod\ p)$. Trebamo izračunati $\phi(p)$. Svi brojevi $1, 2, ..., p-1, p$ osim p, su relativno prosti za p. Tako imamo $\phi(p) = p - 1$, čime je dokazan mali Fermatov teorem. □

1.1.2 Zbroj djelitelja

Zbroj djelitelja je funkcija σ koja prirodnom broju n pridružuje zbroj svih djelitelja broja n. Drugim riječima, $\sigma(n) = \sum_{d|n} d$.

Primjer 1.1.10. *Izračunajmo* $\sigma(n)$ *za* $n = 12$ *i* $n = 11$.

Rješenje: Brojevi manji od 12 koji su djelitelji od 12 su 1, 2, 3, 4, 6, 12, pa je $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$. *Brojevi manji od 11 koji su djelitelji do 11 su 1, 11, pa je* $\sigma(11) = 1 + 11 = 12$.

Ako n ima prikaz

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}, \quad 1 \leq a_1,$$

gdje su $p_1, ...p_r$ prosti brojevi, $a_1, ...a_r$ prirodni, onda je svaki djelitelj tog broja oblika

$$p_1^{b_1} p_2^{b_2} ... p_r^{b_r}, \quad 0 \leq b_i \leq a_i.$$

Vrijedi stoga

$$\sigma(n) = \sum p_1^{b_1} p_2^{b_2} ... p_r^{b_r},$$

gdje se sumira po svim vrijednostima eksponenata b_i. Ova se suma lako računa jer je to opći član u razvoju izraza

$$\sigma(n) = (1 + p_1 + ... + p_1^{a_1})...(1 + p_r + ... + p_r^{a_r})$$

$$= \frac{p_1^{a_1+1} - 1}{p_1 - 1} ... \frac{p_r^{a_r+1} - 1}{p_r - 1}.$$

Odavde slijedi: ako je $(x, y) = 1$, tada je $\sigma(xy) = \sigma(x)\sigma(y)$. Drugim riječima, σ je multiplikativna funkcija.

Napomenimo još i ovo: ako je d djelitelj, tada je $\frac{n}{d}$ djelitelj broja n. Zato je i

$$\sigma(n) = n\left(\frac{1}{d_1} + ... + \frac{1}{d_k}\right),$$

gdje su $d_1, ..., d_k$ svi djelitelji od n.

1.1.3 Poopćen zbroj djelitelja

Definicija 1.1.11. *Za realni ili kompleksni broj α i za bilo koji prirodni broj n definiramo*

$$\sigma_\alpha(n) = \textstyle\sum_{d|n} d^\alpha.$$

Funkciju σ_α nazivamo poopćeni zbroj djelitelja.

Kada je $\alpha = 0$, $\sigma_0(n)$ je broj od djelitelja broja n, koji smo u sljedećem tekstu označili s $\tau(n)$.

Kada je $\alpha = 1$, $\sigma_1(n)$ je zbroj djelitelja broja n, koji smo u prethodnom poglavlju označili sa $\sigma(n)$.

Za izračunavanje $\sigma_\alpha(p^a)$ napominjemo da su djelitelji prostog broja p^a:

$$1, p, p^2, ..., p^a,$$

stoga je

$$\sigma_\alpha(p^a) = 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{\alpha\alpha} = \begin{cases} \dfrac{p^{\alpha(a+1)} - 1}{p^\alpha - 1} & ; \alpha \neq 0 \\ a + 1 & ; \alpha = 0. \end{cases}$$

Na isti način kao u prethodnom poglavlju dokazuje se da za $\alpha \neq 0$ vrijedi

$$\sigma_\alpha(n) = \frac{p_1^{\alpha(a_1+1)} - 1}{p_1^\alpha - 1} ... \frac{p_r^{\alpha(a_r+1)} - 1}{p_r^\alpha - 1}$$

, gdje je $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$. Odavde se lako vidi da je σ_α multiplikativna funkcija.

1.1.4 Broj djelitelja

Broj djeljitelja je funkcija τ koja prirodnom broju n pridružuje broj različitih djelitelja broja n.

Primjer 1.1.12. *Izračunajmo $\tau(n)$ za $n = 12$ i $n = 11$.*

Rješenje: Brojevi koji su djelitelji od 12 su 1, 2, 3, 4, 6, 12, pa je $\tau(12) = 6$. Brojevi manji od 11 koji su djelitelji od 11 su 1, 11, pa je $\tau(11) = 2$.

Neka je $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ faktorizacija broja n na proste faktore. Kako izgleda njegov djelitelj? To je broj oblika

$$m = p_1^{b_1} p_2^{b_2} ... p_r^{b_r}$$

gdje je $0 \leq b_j \leq a_j$. Različitih djelitelja ima onoliko koliko i različitih r-torki $(b_1, ..., b_r)$. Svaki takav izbor određuje jedan djeljitelj broja n. Stoga je njihov broj

$$\tau(n) = (a_1 + 1)(a_2 + 1)...(a_r + 1).$$

Primjer 1.1.13. *Iz $12 = 2^2 \cdot 3$ dobivamo $\tau(12) = (2 + 1)(1 + 1) = 6$. Ovaj isti rezultat smo dobili u prethodnom primjeru kad smo računali $\tau(12)$ po definiciji.*

Navedimo nekoliko posljedica:

Korolar 1.1.14. *$\tau(n) = 2$ ako i samo ako je n prost.*

Dokaz. Ako je n prost broj, onda je on djeljiv s brojem 1 i sa samim sobom pa je $\tau(n) = 2$. S druge strane, ako je $\tau(n) = 2$, a u djelitelje su uključeni 1 i n, tada je n prost. □

Korolar 1.1.15. *$\tau(n) = 3$ ako i samo ako je n oblika $n = p^2$, p prost.*

Dokaz. Ako je n oblika $n = p^2$ gdje je p prost broj tada je broj p^2 djeljiv s brojevima 1, p i p^2 pa je $\tau(n) = 3$. S druge strane, ako je $\tau(n) = 3$ znamo da n ima tri djelitelja. U djelitelje su uključeni brojevi 1 i n, pa tada je broj n oblika $n = p^2$, prost broj. □

1.1.5 Savršeni brojevi

Postoji beskonačno mnogo brojeva n za koje je $\sigma(n) < 2n$. Na primjer, za prosti broj p je $\sigma(p) = 1 + p < 2p$. Budući da prostih brojeva ima beskonačno mnogo, slijedi da postoji beskonačno mnogo brojeva za koje je $\sigma(n) < 2n$.

Postoji beskonačno mnogo brojeva n za koji je $\sigma(n) > 2n$. Na primjer,

$$\sigma(2^k \cdot 3) = \sigma(2^k) \cdot \sigma(3) = \frac{2^{k+1} - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1}$$

$$= (2^{k+1} - 1) \cdot 4 > 2^{k+1} \cdot 3 = 2n$$

.

Međutim, ne znamo postoji li beskonačno mnogo brojeva za koje je $\sigma(n) = 2n$.

Takvi se brojevi nazivaju savršenim.

Algoritam za nalaženje parnih savršenih brojeva dao je Euklid. Računamo parcijalne sume reda $1 + 2 + 4 + 8 + ...$ Ako je zbroj prost, pomnožimo ga s posljednjim pribrojnikom i dobijemo savršeni broj.

Tako na primjer

$$1 + 2 = 3, 3 \cdot 2 = 6$$

$$1 + 2 + 4 = 7, 7 \cdot 4 = 28$$

$$1 + 2 + 4 + 8 + 16 = 31, 31 \cdot 16 = 496$$

$$1 + 2 + 4 + 8 + 16 + 32 + 64 = 127, 127 \cdot 64 = 8128.$$

Ovi su brojevi bili poznati još starim Grcima.

Do današnjeg dana je poznato 48 savršenih brojeva.

Teorem 1.1.16. *Parni broj n je savršen onda i samo onda ako je oblika*

$$n = 2^{p-1}(2^p - 1)$$

pri čemu je $2^p - 1$ *prost broj.*

Dokaz. Neka je n oblika $2^{p-1}(2^p - 1)$, $2^p - 1$ prost. Onda imamo

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

$$= 2n$$

pa je n savršen.

Neka je sada n savršen parni broj. On se može napisati u obliku $n = 2^{p-1} \cdot k$ pri čemu je $p \geq 2$ cijeli broj i k neparan broj. 2^{p-1} i k su relativno prosti pa zbog multiplikativnosti funkcije σ imamo

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

S druge strane, budući da je n savršen, vrijedi $\sigma(n) = 2n$ pa dobivamo

$$(2^p - 1)\sigma(k) = 2^p \cdot k.$$

Brojevi $(2^p - 1)$ i 2^p su relativno prosti, pa je ova relacija moguća samo ako za neki cijeli broj q vrijedi

$$\sigma(k) = 2^p \cdot q.$$

No onda mora biti ispunjeno i

$$(2^p - 1)q = k.$$

Odavde slijedi

$$\sigma(k) = \left(\frac{k}{p} + 1\right) q = k + q.$$

Iz prethodne relacije vidimo da je q djelitelj broja k, a odavde čitamo da je q jedini djelitelj broja k različit od k, pa mora biti $q = 1$. Sada je $\sigma(k) = k + 1$ pa je k prost. Dalje vidimo da je on jednak $k = 2^p - 1$ i time je tvrdnja dokazana.

□

1.1.6 Neparni savršeni brojevi

Ne zna se postoji li ijedan neparan savršen broj. Ako postoji, dokazano je da mora imati sljedeća svojstva:

- mora biti veći do 10^{1500},
- mora imati više od 101 prostih faktora, od koji je barem 9 različito,
- najveći prosti faktor je veći od 10^8,
- drugi po veličini prosti faktor je veći od 10^4,
- treći po veličini prosti faktor jeveći od 100,
- mora biti oblika $n \equiv 1 (mod\ 12)$, $n \equiv 117 (mod\ 468)$, ili $n \equiv 81 (mod\ 324)$.

1.1.7 Möbiusova funkcija

Definicija 1.1.17. *Möbiusova funkcija μ se definira ovako*

$$\mu(n) = \begin{cases} 1; & za\ n = 1 \\ (-1)^k; & ako\ je\ n = \Pi_{i=1}^{k} p_i \\ 0; & za\ ostale\ n. \end{cases}$$

Definicija 1.1.18. *Aritmetička funkcija I definira se ovako:*

$$I(n) = \begin{cases} 1; & n = 1 \\ 0; & n > 1 \end{cases}.$$

Očio je da je $I(n) = \left[\frac{1}{n}\right]$, *gdje je* [] *oznaka za najveće cijelo.*

Teorem 1.1.19. *[1] Funkcija μ je multiplikativna.*

Dokaz. Neka su m i n relativno prosti brojevi, $m, n \geq 2$ koji imaju prikaze

$$m = p_1^{a_1} ... p_k^{a_k}$$

$$n = s_1^{b_1} ... s_r^{b_r}$$

gdje su $p_1, ..., p_k, s_1, ..., s_r$ različiti prosti brojevi, $a_1, ..., a_k, b_1, ..., b_r$ prirodni. Ako je neki od eskponenata u broju m strogo veći od 1, tada je $\mu(m) = 0$. Ali tada je i u faktorizaciji broja mn taj eskponent veći od 1 pa je $\mu(mn) = 0$. Dakle, vrijedi $\mu(mn) = 0 = \mu(m) \cdot \mu(n)$. Analogno se dobije ako je neki od eksponenata u broju n veći od 1. Ako su svi eksponenti jednaki 1, tada je

$$\mu(m) = (-1)^k, \ \ \mu(n) = (-1)^r \ \ i \ \ \mu(mn) = (-1)^{k+r}$$

pa vrijedi $\mu(mn) = \mu(m)\mu(n)$. U ostalim slučajevima, kad je neki od brojeva m ili n jednak 1 također se lako dokaže multiplikativnost od μ. Ako je $F(n) = \sum_{d|n} \mu(d)$, tada je $F(n)$ multiplikativna po teoremu 1.1.3. Slijedi $F(1) = \mu(1) = 1$. Za $n > 1$, $\alpha > 0$ i proste brojeve p vrijedi $F(p^\alpha) = \sum_{\beta=0}^{\alpha} \mu(p^\beta) = 1 + (-1) = 0$. □

Temeljno svojstvo Möbiusove funkcije dano je sljedećim teoremom.

Teorem 1.1.20. *[2] Za sve $n \in \boldsymbol{N}$, $\sum_{d|n} \mu(d) = I(n)$.*

Dokaz. Ako je $n = 1$, formula je vidljiva iz definicije. Zatim, pretpostavimo da je $n \geq 2$ i neka je $n = \Pi_{i=1}^{k} p_i$ faktorizacija broja n. Budući da je $\mu(d) = 0$ ako d ima neki prosti faktor više puta, to znači da se možemo ograničiti na djelitelje oblika $d = \Pi_{i \in I} p_i$ gdje je $I \subseteq \{1, 2, ...k\}$, a svaki takav djelitelj pridonosi sa izrazom $\mu(d) = (-1)^{|I|}$. Stoga,

$$\sum_{d|n} \mu(d) = \sum_{I \subseteq \{1,2,...k\}} (-1)^{|I|}.$$

Sada imajmo na umu da za bilo koji $r \in \{0, 1, ...k\}$ postoji $\binom{k}{r}$ r-članih podskupova I i za svaki takav podskup pribrojnik $(-1)^{|I|}$ jednak je $(-1)^r$. Stoga se zbroj svodi na

$$\sum_{r=0}^{k} (-1)^r \binom{k}{r} = (1-1)^k = 0$$

pri čemu je upotrebljen binomni teorem. Dakle, imamo $\sum_{d|n} \mu(d) = 0$ za $n \geq 2$, kao što smo i trebali dokazati. □

Teorem 1.1.21. *[2] Za svaki realni $x \geq 1$ imamo*

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1.$$

Dokaz. Pretpostavimo, bez smanjenja općenitosti, da je $x = N$, gdje je N prirodan broj. Zatim izračunajmo zbroj $S(N) = \sum_{n \leq N} I(n)$ na dva različita načina. S jedne strane, po definiciji $I(n)$, imamo $S(N) = 1$, a s druge strane koristeći $I(n) = \sum_{d|n} \mu(d)$ i zamjenom sumiranja dobivamo $S(N) = \sum_{d \leq N} \mu(d)[N/d]$, gdje $[t]$ označava najveći cijeli broj manji ili jednak od t. Sada, za $d \leq N - 1$, $[N/d]$ se razlikje od N/d za iznos koji je po apsolutnoj vrjednosti najviše 1, dok za $d = N$, brojevi $[N/d]$ i N/d su jednaki. Zamjenom $[N/d]$ s N/d i ograničavanjem dobivene pogreške dobivamo

$$\left| S(N) - N \sum_{d \leq N} \frac{\mu(d)}{d} \right| \leq \sum_{d \leq N} |\mu(d)| \cdot |[N/d] - (N/d)| \leq \sum_{d \leq N-1} |\mu(d)| \leq N - 1.$$

Stoga,

$$\left| N \sum_{d \leq N} \frac{\mu(d)}{d} \right| \leq (N-1) + |S(N)| = (N-1) + 1 = N.$$

□

Teorem 1.1.22. *[1] Ako je* $g(n) = \sum_{d|n} f(d)$ *za sve prirodne brojeve n, tada je* $f(n) = \sum_{d|n} \mu(d)g(n/d)$.

Dokaz. Vidimo da je

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

$$= \sum_{dk|n} \mu(d)f(k)$$

pri čemu se sumira po svim parovima (d, k) za koje vrijedi da je $dk \mid n$. Zadnja formula pokazuje da možemo obrnuti uloge od d i k te zapisati kao

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

i to je $f(n)$ prema teoremu 1.1.20. □

Teorem 1.1.23. *[1] Ako je* $f(n) = \sum_{d|n} \mu(d)g(n/d)$ *za sve prirodne brojeve n, tada je* $g(n) = \sum_{d|n} f(d)$.

Dokaz. Prvo zapišimo

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

Budući da je k djelitelj od d, pišemo d/k, i zbog toga možemo zapisati

$$\sum_{d|n} \sum_{k|d} \mu(d/k)g(k).$$

$g(k)$ pojavljuje se za svaki mogući djelitelj k od n. Za svaki fiksni djelitelj k od n, imamo uvjete koji uključuju $g(k)$. Koeficijent je skupu svih $\mu(d/k)$, gdje je d/k djelitelj od n/k ili jednostavnije, skup svih $\mu(r)$, gdje je r djelitelj od n/k. Slijedi da se zadnji iznos može zapisati kao

$$\sum_{k|n} \sum_{r|(n/k)} \mu(r)g(k).$$

Iz teorema 1.1.19 vidimo da je koeficijent $g(k)$ jednak 0, osim ako $n/k = 1$, pa se cijeli zbroj reducira do $g(n)$. □

1.1.8 Möbiusova funkcija reda k

Definicija 1.1.24. *Za $k \geq 1$ definiramo μ_k, Möebiusovu funkciju reda k, ovako:*

$$\mu_k(n) = \begin{cases} 1; & za\ n = 1 \\ 0; & ako\ posto ji\ prost\ bro j\ p\ takav\ da\ p^{k+1}\ di jeli\ n \\ (-1)^r; & ako\ je\ n = p_1^k ... p_r^k \Pi_{i>r} p_i^{a_i}, 0 \leq a_i < k, \\ 1; & za\ ostale\ n. \end{cases}$$

Za Möbiusove funkcije reda k, vrijede sljedeća svojstva.

Teorem 1.1.25. *[3] Za $k \geq 1$ vrijedi da je $\mu_k(n^k) = \mu(n)$.*

Dokaz. Ako je $n = 1$, tada je $n^k = 1$ pa je $\mu_k(n^k) = \mu_k(1) = 1$, $\mu(n) = \mu(1) = 1$, te je očito $\mu_k(n^k) = \mu(n)$. Ako je n produkt različitih prostih brojeva, tj. n je oblika $n = p_1 p_2 ... p_r$, tada je $\mu(n) = (-1)^r$. No, tada je $n^k = p_1^k p_2^k ... p_r^k$ pa je $\mu_k(n^k) = (-1)^r$, te opet vrijedi $\mu_k(n^k) = \mu(n)$. Ako postoji prost broj p_1 koji se u faktorizaciji od n javlja više nego jedanput, tj. ako $p_1^2 \mid n$, tada je $\mu(n) = 0$. No tada i p_1^{2k} dijeli n^k, a budući da je $2k > k + 1$ slijedi da i p_1^{k+1} dijeli n^k, te je $\mu_k(n^k) = 0$, tj. opet je $\mu_k(n^k) = \mu(n)$. Time je dokaz gotov. □

Teorem 1.1.26. *[3] Funkcija μ_k je multiplikativna za svaki prirodni broj k.*

Dokaz. Neka su m i n relativno prosti brojevi. Ako je $m = 1$, tada je $\mu_k(m) = 1$ i $\mu_k(mn) = \mu_k(1 \cdot n) = \mu_k(n) = \mu_k(n) \cdot 1 = \mu_k(n) \cdot \mu_k(m)$. Analogno vrijedi ako je $n = 1$. Razmotrimo dalje opći slučaj kad su $m, n \neq 1$. Ako postoji prost broj p takav da p^{k+1} dijeli n, tada p^{k+1} dijeli i mn te je $\mu_k(n) = 0$ i $\mu_k(mn) = 0$. Stoga je $\mu_k(mn) = 0 = \mu_k(m) \cdot \mu_k(n)$. Ako je n oblika $n = p_1^k ... p_r^k \Pi_{i>r} p_i^{a_i}$, $0 \leq b_i \leq k$, a broj m je oblika $m = s_1^k ... s_t^k \Pi_{i>t} p_i^{b_i}$, $0 \leq b_i \leq k$, tada je

$$mn = p_1^k ... p_r^k s_1^k ... s_t^k \Pi_{i>r} p_i^{a_i} \Pi_{i>t} p_i^{b_i},$$

te je

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

Nakon analognog dokaza svih ostalih slučajeva dobivamo tvrdnju teorema. □

Teorem 1.1.27. *[3] Za $k \geq 2$ imamo*

$$\mu_k(n) = \sum_{d^k \mid n} \mu_{k-1}\left(\frac{n}{d^k}\right) \mu_{k-1}\left(\frac{n}{d}\right).$$

Teorem 1.1.28. *[3] Ako je $k \geq 1$ tada vrijedi*

$$|\mu_k(n)| = \textstyle\sum_{d^{k+1} \mid n} \mu(d).$$

1.1.9 Liouvilleova funkcija

Važan primjer potpuno multiplikativne funkcije je Liouvilleova funkcija λ.

Definicija 1.1.29. *Definiramo $\lambda(1) = 1$, a ako je $n = p_1^{a_1} \cdots p_k^{a_k}$ definiramo*

$$\lambda(n) = (-1)^{a_1+\cdots+a_k}.$$

Iz definicije je vidljivo da je λ potpuno multiplikativna.

Teorem 1.1.30. *[3] Za svaki $n \geq 1$ imamo*

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

Također, $\lambda^{-1}(n) = |\mu(n)|$ za sve n.

Dokaz. Neka je $g(n) = \sum_{d|n} \lambda(d)$. Tada je g multiplikativna, pa za izračunavanje $g(n)$ trebamo samo prebrojati $g(p^a)$ za proste brojeve. Imamo

$$g(p^a) = \sum_{d|p^a} \lambda(d) = 1 + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^a)$$

$$= 1 - 1 + 1 - \cdots + (-1)^a = \begin{cases} 0; & \textit{ako je a neparan} \\ 1; & \textit{ako je a paran.} \end{cases}$$

Stoga, ako je $n = \Pi_{i=1}^k p_i^{a_i}$ imamo $g(n) = \Pi_{i=1}^k g(p_i^{a_i})$. Ako je bilo koji eksponent od a_i neparan tada je $g(p_i^{a_i}) = 0$, odnosno $g(n) = 0$. Ako su svi eksponenti od a_i jednaki, tada je $g(p_i^{a_i}) = 1$ za sve i i $g(n) = 1$. To nam pokazuje da je $g(n) = 1$ ako je n kvadrat, inače je $g(n) = 0$. Također, $\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|$. □

1.2 Aditivne funkcije

Aritmetička funkcija f naziva se aditivna ako zadovoljava

$$f(n_1 n_2) = f(n_1) + f(n_2)$$

kad god je $(n_1, n_2) = 1$.

Istaknute aditivne funkcije su: ukupan broj prostih faktora Ω, broj različitih prostih faktora ω i funkcija ln definirana za prirodne brojeve.

1.2.1 Broj različitih prostih faktora

Definicija 1.2.1. *Broj različitih prostih faktora ω je funkcija definirana sa $\omega(1) = 0$ i $\omega(n) = k$ za $n \geq 2$ i $n = \Pi_{i=1}^{k} p_i^{\alpha_i}$, tj. $\omega(n) = \sum_{p|n} 1$.*

Primjer 1.2.2. *Za $n = 44100 = (3\cdot7)^2\cdot(2\cdot5)^2 = 2^2 3^2 5^2 7^2$ imamo $\omega(44100) = \omega(2^2 3^2 5^2 7^2) = 4$. Vrijedi $\omega(p) = 1$ jer broj p ima samo jedan prosti faktor u svojoj faktorizaciji.*

1.3 Von Mangoldtova funkcija

Definicija 1.3.1. *Von Mangoldtova funkcija Λ je funkcija koja prirodnom broju n pridružuje $\ln p$ ako je $n = p^m$ pri čemu je p prost broj ili 0 inače.*

Von Mangoldtova funkcija nije niti multiplikativna niti aditivna.

Teorem 1.3.2. *[2] Vrijedi*

$$\sum_{d|n} \Lambda(d) = \ln n \ (n \in N)$$

.

Dokaz. Za $n = 1$ identitet vrijedi jer je $\Lambda(1) = 0 = \ln 1$. Za $n \geq 2$ imamo, po definiciji Λ,

$$\sum_{d|n} \Lambda(d) = \sum_{p^m|n} \ln p = \ln n.$$

Za posljednji korak napominjemo da za svaki broj p^a koji dijeli n, svaki od izraza $p^1, p^2, ...p^a$ doprinosi izrazu $\ln p$ pa je ukupan doprinos jednak $a(\ln p) = \ln p^a$. □

Poglavlje 2

Dirichletov produkt aritmetičkih funkcija

Dvije očite operacije na skupu aritmetičkih funkcija su zbrajanje i množenje funkcija. Konstantne funkcije $f = 0$ i $f = 1$ su neutralni elementi s obzirom na te operacije. Aditivni i multiplikativni inverzi funkcije f su $-f$ i $\frac{1}{f}$ respektivno. Ovdje ćemo definirati novu operaciju na skupu aritmetičkih funkcija.

Definicija 2.0.1. *Dirichletov produkt aritmetičkih funkcija f i g je aritmetička funkcija $f * g$ definirana s*

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

Dirichletov produkt još nazivamo i Dirichletova konvolucija ili kraće, konvolucija.
Za konvoluciju vrijedi
(i) $(f * g)(1) = f(1)g(1)$.
(ii)$(f * g)(p) = f(1)g(p) + f(p)g(1)$ gdje je p prost broj.
(iii)Za prosti broj p i prirodni m vrijedi

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

Dokažimo te tvrdnje. Prva tvrdnja slijedi iz jednakosti $(f * g)(p^m) = \sum_{d|p^m} f(d)g\left(\frac{p^m}{d}\right) = \sum_{k=0}^{m} f(p^k)g(p^{m-k})$.

Dokažimo drugu tvrdnju. Jedini djelitelji prostog broja p su 1 i p, tj. u definiciji konvolucije sumira se po skupu $d \in \{1, p\}$. Imamo

$$(f * g)(p) = \sum_{d|p} f(d)g\left(\frac{p}{d}\right) = f(1)g(p) + f(p)g(1).$$

I konačno, ako je $n = p^m$, tada su njegovi djelitelji d oblika p^{m-k} pri čemu je $k = 0, 1, 2, ..., m$ pa imamo

$$(f * g)(p^m) = \sum_{d|p^m} f(d)g\left(\frac{p^m}{d}\right) = \sum_{k=0}^{m} f(p^k)g(p^{m-k}).$$

Ponekad je korisno napisati Dirichletovu konvoluciju u simetričnom obliku, tj. u obliku

$$(f * g)(n) = \sum_{ab=n} f(a)g(b)$$

gdje se sumira po svim parovima (a, b) brojeva čiji je produkt jednak n.

Jedan od razloga za uvođenje ovog produkta jest činjenica da mnogobrojne aritmetičke funkcije imaju oblik Dirichletovog produkta, te da se mogu napisati mnogi identiteti među aritmetičkim funkcijama koji uključuju Dirichletov produkt. Evo nekoliko primjera:

Primjer 2.0.2. *(i) Za funkciju τ vrijedi $\tau = 1 * 1$.*

Dokaz. Budući da je, po definiciji $\tau(n) = \sum_{d|n} 1$ zapišimo je ovako $\tau(n) = \sum_{d|n} 1 \cdot 1 = \sum_{d|n} 1(d) \cdot 1\left(\frac{n}{d}\right)$, gdje je 1 funckia koja svakom broju pridružuje 1. Dakle, τ je konvolucija dviju funkcija 1, to jest $\tau = 1 * 1$. □

(ii) Za zbroj djelitelja σ vrijedi $\sigma = id * 1$, pri čemu je id identiteta.

Dokaz. Budući da je, po definiciji,

$\sigma(n) = \sum_{d|n} d$ zapišimo je ovako $\sigma(n) = \sum_{d|n} d = \sum_{d|n} id(d) \cdot 1 = \sum_{d|n} id(d) \cdot 1(n/d)$.

Dakle, σ je konvolucija funkcije id i 1, to jest $\sigma = id * 1$. □

(iii) Za Möbiusovu funkciju vrijedi $\mu * 1 = I$.

Dokaz. $(\mu * 1)(n) = \sum_{d|n} \mu(d) \cdot 1(n) = \sum_{d|n} \mu(d) = I(n)$ pri čemu zadnja jednakost vrijedi prema teoremu 1.1.20. □

(iv) $\mu * id = \phi$.

Dokaz. Prema definiciji Eulerove funkcije vrijedi, $\phi(n) = \sum_{m\leq n,(m,n)=1} 1$. Uklanjanjem uvjeta $(m,n) = 1$ dobivamo $\phi(n) = \sum_{m\leq n}\sum_{d|(m,n)} \mu(d) = \sum_{d|n}\mu(d)\sum_{m\leq n,d|n} 1 = \sum_{d|n}\mu(d)(n/d)$, odakle slijedi tvrdnja. □

(v) $\phi * 1 = id$.

Dokaz. Ova tvrdnja slijedi iz jednakosti $\sum_{d|n}\phi(d) = n$. □

(vi) $\Lambda * 1 = log$.

Dokaz. Tvrdnja slijedi iz jednakosti $\sum_{d|n}\Lambda(d) = \ln n$. □

Dirichletov produkt ima lijepa algebarska svojstva koja su iskazana sljedećim teoremima.

Teorem 2.0.3. *[2] Funkcija I je neutralni element za $*$, to jest $f * I = I * f = f$ za sve aritmetičke funkcije f.*

Dokaz. Imamo

$$(f * I)(n) = \sum_{d|n} f(d)I\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\left[\frac{d}{n}\right] = f(n)$$

jer je $[d/n] = 0$ ako je $d < n$. □

Teorem 2.0.4. *[2] Operacija $*$ je komutativna, to jest $f * g = g * f$ za sve f i g.*

Dokaz. Kako bismo dokazali ovu tvrdnju potrebno je upotijebiti simetričnu inačicu Dirichletovog produkta, to jest $(f * g)(n) = \sum_{ab=n} f(a)g(b)$. Uočimo da komutativnost slijedi odmah iz tog prikaza. □

Teorem 2.0.5. *[2] Operacija $*$ je asocijativna, to jest $(f * g) * h = f * (g * h)$ za sve f, g, h.*

Dokaz. Kako bismo dokazali ovu tvrdnju potrebno je upotijebiti simetričnu inačicu Dirichletovog produkta, to jest $(f * g)(n) = \sum_{ab=n} f(a)g(b)$. Za dokazivanje asocijativnosti potrebno je dva puta primijeniti taj zapis kako bismo dobili

$$((f * g) * h)(n) = \sum_{dc=n} (f * g)(d)h(c) = \sum_{dc=n} \sum_{ab=d} f(a)g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c),$$

gdje posljednji izraz obuhvaća sve uređene trojke (a, b, c) prirodnih brojeva čiji je produkt jednak n. Zamjenimo li (f, g, h) s (g, h, f) dobivamo $(f * g) * h = (g * h) * f = f * (g * h)$, što dokazuje da je $*$ asocijativna. □

Teorem 2.0.6. *[2] Ako je $f(1) \neq 0$, tada f ima jedinstven Dirichletov inverz, to jest postoji jedinstvena funkcija g takva da vrijedi $f * g = I$.*

Dokaz. Neka je f aritmetička funkcija za koju vrijedi $f(1) \neq 0$. Prema definiciji, funkcija g je Dirihletov inverz funkcije f ako vrijedi $(f * g)(1) = I(1) = 1$ i $(f * g)(n) = I(n) = 0$ za sve $n \geq 2$. Vidimo da je jednako beskonačanom sustavu jednadžbi

(A_1)

$$f(1)g(1) = 1$$

(A_n)

$$\sum_{d|n} g(d)f(n/d) = 0 \ (n \geq 2)$$

Moramo dokazati da sustav $(A_n)_{n=1}^{\infty}$ ima jedinstveno rješenje. To ćemo učiniti induktivnim konstruiranjem vrijednosti $g(n)$ i pokazujući da su te vrijednosti jedinstveno određene.

Za $n = 1$, jednadžba (A_1) daje $g(1) = 1/f(1)$, što je dobro definirano za $f(1) \neq 0$. Dakle, $g(1)$ je jedinstveno definiran. Neka je $n \geq 2$, pretpostavimo da smo dokazali da postoje jedinstvene vrijednosti za $g(1), ...g(n-1)$ tako da jednadžbe $(A_1) - (A_{n-1})$ vrijede. Budući da je $f(1) \neq 0$, jednadžba (A_n) je ekvivalentna

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} g(d)f(n/d).$$

Budući da desna strana uključuje samo vrijednosti $g(d)$ za $d < n$, to jedinstveno određuje $g(n)$ i definiranjem $g(n)$ kao $g(n) := -\frac{1}{f(1)} \sum_{d|n, d<n} g(d)f(n/d)$ vidimo da (A_n) vrijedi. □

Primjer 2.0.7. *(1) Budući da je $\mu * 1 = I$, Möebiusova funkcija je Dirihletov inverz jedinične funkcije.*

(2) Množenje identiteta $\phi = \mu * id$ (dobivenog u zadnjem odjeljku) sa 1 daje $\phi * 1 = 1 * \phi = 1 * \mu * id = I * id = id$, te smo tako dobili identitet $\phi * 1 = id$.

Posljednji primjer je poseban slučaj važnog općeg načela, što ćemo navesti kao teorem.

Teorem 2.0.8. *[2] Ako je* $g(n) = \sum_{d|n} f(d)$ *za sve* $n \in \mathbf{N}$*, onda je* $f(n) = \sum_{d|n} g(d)\mu(n/d)$.

Dokaz. Navedeni odnos možemo zapisati kao $g = f * 1$. Djelujući Dirichletovim produktom sa svake strane ovog odnosa s funkcijom μ dobivamo $g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * I = f$, što je i trebalo dokazati. □

Napomenimo da smo se s ovim rezultatom već susreli u teoremu 1.1.22, ali ovdje smo dali malo drugačiji dokaz.

Koristeći teorem 2.0.8 koji se još i naziva Möbiusova inverzijska formula možemo dokazati sljedeću formulu za von Mangoldtovu funkciju.

Teorem 2.0.9. *[2] Za prirodni broj n vrijedi*

$$\Lambda(n) = \sum_{d|n} \mu(d) \ln\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d) \ln d.$$

Dokaz. Prema teoremu 1.1.2 imamo da je $\ln n = \sum_{d|n} \Lambda(d)$. Koristeći teorem 2.0.8 za funkcije $g = \ln$ i $f = 1$ dobivamo

$$\begin{aligned}\Lambda(n) = \sum_{d|n} \mu(d) \ln\left(\frac{n}{d}\right) &= \ln n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \ln d \\ &= I(n) \ln n - \textstyle\sum_{d|n} \mu(d) \ln d.\end{aligned}$$

Budući da je $I(n) \ln n = 0$ za sve n, tvrdnja je dokazana. □

Konačno, treća motivacija za definiciju Dirichletovog produkta je ta da čuva važna svojstava multiplikativnih funkcija, koja su prikazana u sljedećim teoremima.

Teorem 2.0.10. *[2]*

(i)Ako su f i g multiplikativne, tada je i $f * g$ multiplikativna.

(ii) Ako je f multiplikativna, onda je i Dirichletov inverz f^{-1} multiplikativan.

(iii) Ako je $f * g = h$ i f i h su multiplikativne, onda je i g multiplikativna.

(iv) (Distributivnost) Ako je h potpuno multiplikativna, onda vrijedi

$$h(f * g) = (hf) * (hg)$$

za svaku funkciju f i g.

Dokaz. (i) Neka su f i g multiplikativne i neka je $h = f * g$. Za relativno proste brojeve n_1 i n_2 moramo pokazati da je $h(n_1 n_2) = h(n_1)h(n_2)$. Koristimo činjenicu da svaki djelitelj d od umnoška $n_1 n_2$ može biti jedinstveno faktoriziran kao $d = d_1 d_2$ tako da je $d_1 \mid n_1$ i $d_2 \mid n_2$, te da za bilo koji par (d_1, d_2) s $d_1 | n_1$ i $d_2 \mid n_2$, produkt $d = d_1 d_2$ zadovoljava $d | n_1 n_2$. Stoga imamo

$$h(n_1, n_2) = \sum_{d | n_1 n_2} f(d) g\left(\frac{n_1 n_2}{d}\right) = \sum_{d_1 | n_1} \sum_{d_2 | n_2} f(d_1 d_2) g\left(\frac{n_1 n_2}{d_1 d_2}\right).$$

Budući da vrijedi $(n_1, n_2) = 1$, svaki djelitelji d_1 i d_2 takvi da je $d_1 | n_1$ i $d_2 | n_2$ zadovoljavaju $(d_1, d_2) = 1$ i $(n_1/d_1, n_2/d_2) = 1$. Dakle, u gornjoj dvostrukoj sumi možemo primijeniti multiplikativnost funkcija f i g te dobivamo

$$h(n_1 n_2) = \sum_{d_1 | n_1} \sum_{d_2 | n_2} f(d_1) g\left(\frac{n}{d_1}\right) f(d_2) g\left(\frac{n_2}{d_2}\right) = (f * g)(n_1)(f * g)(n_2) = h(n_1)h(n_2),$$

što smo trebali i dokazati.

(ii) Neka je f multiplikativna funkcija i neka je g Dirichletov inverz od f. Dokazujemo svojstvo multiplikativnosti

$$g(n_1 n_2) = g(n_1)g(n_2)$$

za relativno proste brojeve n_1 i n_2 indukcijom po produktu $n = n_1 n_2$. Za $n_1 n_2 = 1$, slijedi $n_1 = n_2 = 1$ i $g(n_1 n_2) = g(n_1)g(n_2)$ jer je $(n_1, n_2) = 1$ te tvrdnja vrijedi. Neka je $n \geq 2$ i pretpostavimo da $g(n_1 n_2) = g(n_1)g(n_2)$ vrijedi za $n_1 n_2 < n$ pri čemu je $/(n_1, n_2) = 1$. Koristeći multiplikativnost funkcija f i g za argument manji od n, primjenom identiteta (A_n) dobivamo

$$\begin{aligned}
0 &= \sum_{d | n_1 n_2} f(d) g(n_1 n_2 / d) \\
&= \sum_{d_1 | n_1} \sum_{d_2 | n_2} f(d_1) f(d_2) g(n_1/d_1) g(n_2/d_2) + (g(n_1 n_2) - g(n_1)g(n_2)) \\
&= (f * g)(n_1)(f * g)(n_2) + (g(n_1 n_2) - g(n_1)g(n_2)) \\
&= I(n_1)I(n_2) + (g(n_1 n_2) - g(n_1)g(n_2) \\
&= g(n_1 n_2) - g(n_1)g(n_2),
\end{aligned}$$

jer po našoj pretpostavci za $n = n_1 n_2 \geq 2$, barem jedan od n_1 i n_2 mora biti ≥ 2, pa je $I(n_1)I(n_2) = 0$. Stoga imamo $g(n_1 n_2) = g(n_1)g(n_2)$. Zime je indukcija dovršena.

(iii) Identitet $f*g = h$ podrazumijeva $g = f^{-1}*h$, gdje je f^{-1} Dirichletov inverz funkcije f. Budući da su f i h multiplikativne funkcije, po (ii) funkcija f^{-1} je isto multiplikativna, kao i $f^{-1} * h$ (po(i)). Stoga je funkcija g također multiplikativna.

(iv) Ako je h potpuno multiplikativna funkcija, tada za bilo koji djelitelj $d|n$ imamo $h(n) = h(d)h(n/d)$. Stoga, za sve n vrijedi

$$h(f * g)(n) = h(n) \sum_{d|n} f(d)g(n/d) = \sum_{d|n} h(d)f(d)h(n/d)g(n/d) = ((h/f) * (hg))(n).$$

□

Napomena: (i) Produkt dviju potpuno multiplikativnih funkcija je muliplikativan (po teoremu), ali ne nužno potpuno multiplikativan. Na primjer, τ može se izraziti kao produkt $1 * 1$ u kojem je svaki faktor 1 potpuno multiplikativan, ali τ nije potpuno multiplikativna. Isto vrijedi i za Dirichletov inverz: ako je f potpuno multiplikativna, onda i f^{-1} je multiplikativna.

(ii) Po teoremu 2.0.6. svaka funkcija f sa svojstvom $f \neq 0$ ima Dirichletov inverz. Budući da multiplikativna funkcija zadovoljava $f(1) = 1$ to znači da svaka multiplikativna funkcija ima Dirichletov inverz.

(iii) Imajmo na umu da distributivnost koja se tvrdi pod (iv) vrijedi samo kada je h potpuno multiplikativna. U stvari, može se pokazati da ovo svojstvo obilježava potpuno multiplikativne funkcije: ako je h funkcija različita od 0 za koju identitet u (iv) vrijedi za sve funkcije f i g, tada je h potpuno multiplikativna.

Teorem 2.0.11. *[2] Neka je f multiplikativna. Tada je f potpuno multiplikativna ako i samo ako je,*

$$f^{-1}(n) = \mu(n)f(n) \text{ za sve } n \geq 1.$$

Dokaz. Neka je $g(n) = \mu(n)f(n)$. Ako je f potpuno multiplikativna imamo

$$(g * f)(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = f(n) \sum_{d|n} \mu(d) = f(n)I(n) = I(n)$$

pošto je $f(1) = 1$ i $I(n) = 0$ za $n > 1$. Stoga je $g = f^{-1}$. Obrnuto, pretpostavimo da je $f^{-1}(n) = \mu(n)f(n)$. Kako bi pokazali da je f potpuno multiplikativna, dovoljno je dokazati da je $f(p^a) = f(p)^a$ za sve proste brojeve. Jednadžba $f^{-1}(n) = \mu(n)f(n)$ podrazumijeva da je

$$\textstyle\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0 \text{ za sve } n > 1.$$

Stoga, uvrštavajući $n = p^a$ dobivamo

$$\mu(1)f(1)f(p^a) + \mu(p)f(p)f(p^{a-1}) = 0,$$

odakle slijedi $f(p^a) = f(p)f(p^{a-1})$. To podrazumijeva $f(p^a) = f(p)^a$, stoga je f potpuno multiplikativna. □

Primjer 2.0.12. *Inverz Eulerove funkcije ϕ. Budući da vrijedi $\phi = \mu * id$ imamo $\phi^{-1} = \mu^{-1} * id^{-1}$. Znamo da je $id^{-1} = \mu id$ pošto je id potpuno multiplikativna, stoga*

$$\phi^{-1} = \mu^{-1} * \mu id = u * \mu id.$$

Tako je,

$$\phi^{-1}(n) = \sum_{d|n} d\mu(d).$$

Teorem 2.0.13. *[2] Ako je f multiplikativna, tada je*

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p)).$$

Dokaz. Neka je

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

Tada je g multiplikativna. Kako bi odredili $g(n)$ dovoljno je izračunati $g(p^a)$, ali

$$g(p^a) = \sum_{d|p^a} \mu(d)f(d) = \mu(1)f(1) + \mu(p)f(p) = 1 - f(p).$$

Stoga je,

$$g(n) = \prod_{p|n} g(p^a) = \prod_{p|n}(1 - f(p)).$$

□

Poglavlje 3

Generalizirana konvolucija

U ovom odjeljku F označava realnu ili kompleksnu funkciju definirane na pozitivnom dijelu x-osi, to jest na $(0, +\infty)$, takve da je $F(x) = 0$ za $0 < x < 1$.

Sume tog tipa

$$\sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

često nastaju u teoriji brojeva. Ovdje α označava bilo koju aritmetičku funkciju. Suma definira novu funkciju G na intervalu $(0, +\infty)$ za koju je također $G(x) = 0$ za $0 < x < 1$. Funkciju G označavamo kao $\alpha \circ F$. Tako je,

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Ako je $F(x) = 0$ za sve necjelobrojne x, restrikcija od F na skupu prirodnih brojeva je aritmetička funkcija definirana

$$(\alpha \circ F)(m) = (\alpha * F)(m)$$

za sve prirodne brojeve m takve da je $m \geq 1$, pa se operacija $\circ$ može smatrati generalizacijom konvolucije $*$.

Operacija $\circ$ generalno nije niti komutativna niti asocijativna. Međutim, sljedeći teorem služi kao korisna zamjena svojstva asocijativnosti.

Teorem 3.0.1. *[3] Za bilo koje aritmetičke funkcije α i β vrijedi*

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F.$$

Dokaz. Za $x > 0$ imamo

$$\Big(\alpha \circ (\beta \circ F)\Big)(x) = \sum_{n\le x} \alpha(n) \sum_{m\le x/n} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{mn\le x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right)$$

$$= \sum_{k\le x} \left(\sum_{n|k} \alpha(n)\beta\left(\frac{k}{n}\right)\right) F\left(\frac{x}{k}\right) = \sum_{k\le x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right)$$

$$= \Big(\alpha * \beta) \circ F)\Big)(x).$$

□

Nadalje, primjećujemo da je funkcija $I(n) = [1/n]$ jednaka lijevom neutralnom elementu za operaciju $\circ$. Odnosno, imamo

$$(I \circ F)(x) = \sum_{n\le x} \left[\frac{1}{n}\right] F\left(\frac{x}{n}\right) = F(x).$$

Koristeći tu činjenicu i svojstva asocijativnosti možemo dokazati sljedeći teorem.

Teorem 3.0.2. *[3] Ako je za funkciju α njezin Dirichletov inverz α^{-1}, tada jednadžba*

$$G(x) = \sum_{n\le x} \alpha(n) F\left(\frac{x}{n}\right) \tag{3.1}$$

podrazumijeva

$$F(x) = \sum_{n\le x} \alpha^{-1}(n) G\left(\frac{x}{n}\right). \tag{3.2}$$

Obrnuto, (3.2) povači (3.1).

Dokaz. Ako je $G = \alpha \circ F$ tada je

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F.$$

Obrat, se slično dokazuje. □

Posebno je važan sljedeći specijalan slučaj.

Teorem 3.0.3. *[3] Ako je α potpuno multiplikativna, tada je*

$$G(x) = \sum_{n\le x} \alpha(n) F\left(\frac{x}{n}\right),$$

ako i samo ako je $F(x) = \sum_{n\le x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right)$.

Dokaz. U ovom slučaju je $\alpha^{-1}(n) = \mu(n)\alpha(n)$. □

Poglavlje 4

Derivacija aritmetičke funkcije

Definicija 4.0.1. *Za svaku aritmetičku funkciju f možemo definirati njezinu derivaciju f', kao aritmetičku funkciju danu jednadžbom*

$$f'(n) = f(n) \ln n \text{ za } n \in \boldsymbol{N}.$$

Primjer 4.0.2. *Kako je $1(n) = 1$ za sve n tada vrijedi $1'(n) = \ln n$. Stoga, formulu $\sum_{d|n} \Lambda(d) = \ln n$ možemo zapisati kao $\Lambda * 1 = 1'$.*

Ovaj pojam deriviranja dijeli mnoga svojstava kao i deriviranje realnih funkcija. Na primjer, svojstvo derivacije zbroja i derivacije umnoška također vrijedi i za Dirichletov produkt.

Teorem 4.0.3. *[3] Ako su f i g multiplikativne funkcije, tada vrijedi:*
(i) $(f + g)' = f' + g'$,
(ii) $(f * g)' = f' * g + f * g'$,
(iii) $(f^{-1})' = -f' * (f * f)^{-1}$.

Dokaz. Dokaz za (i) je neposredan. Naime, vrijedi $(f + g)'(n) = (f + g)(n) \ln n = (f(n) + g(n)) \ln n = f(n) \ln n + g(n) \ln n = f'(n) + g'(n)$. Za dokaz tvrdnje (ii) koristimo identitet $\ln n = \ln d + \ln(n/d)$ te vrijedi

$$(f * g)'(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \ln n$$

$$= \sum_{d|n} f(d) \ln d \, g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \ln\left(\frac{n}{d}\right)$$

$$= (f' * g)(n) + (f * g')(n).$$

Za dokaz tvrdnje (iii) koristimo tvrdnju (ii) primjenjenu na izrazu $1 = f * f^{-1}$. To nam daje

$$0 = (f * f^{-1})' = f' * f^{-1} + f * (f^{-1})',$$

te slijedi

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

Množenjem s f^{-1} dobivamo

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

Ali znamo da vrijedi $f^{-1} * f^{-1} = (f * f)^{-1}$ i time je tvrdnja (iii) dokazana. □

4.0.1 Selbergov identitet

Koristeći koncept derivacije možemo elegantno dokazati Selbergov identitet koji opisuje sljedeći teorem.

Teorem 4.0.4. *[3] Za $n \geq 1$ imamo*

$$\Lambda(n) \ln n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \ln^2\left(\frac{n}{d}\right).$$

Dokaz. Derivacijom jednadžbe $\Lambda * 1 = 1'$ dobivamo

$$\Lambda' * 1 + \Lambda * 1' = (1')'.$$

Budući da je $\Lambda * 1 = 1'$ uvrštavanjem dobivamo

$$\Lambda' * 1 + \Lambda * (\Lambda * 1) = (1')'.$$

Množenjem obje strane jednadžbe s $\mu = 1^{-1}$ dobivamo

$$\Lambda' + \Lambda * \Lambda = (1')' * \mu.$$

Time smo dobili potreban identitet. □

Bibliografija

[1] I. Niven, H. S. Zuckerman, H. L. Montogomery, *An Introduction to the Theory of Numbers*, John Wiley and Sons,1991.

[2] A.J.Hildebrand, *Introduction to Analytic Number Theory*, Department of Mathematics, University od Illionis, 2013.,https://faculty.math.illinois.edu/ hildebr/ant/.

[3] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, Pasadena, 2000.

Sažetak

U ovom radu opisujemo aritmetičke funkcije teorije brojeva. Rad je podijeljen na četiri poglavlja. U prvom poglavlju donosimo definicije i pregled multiplikativnih funkcija, te aditivnih funkcija uz neka njihova svojstva. Funkcije koje obrađujemo su: Eulerova funkcija, zbroj djelitelja, broj djelitelja, Liouvilleova funkcija, Möbiusova funkcija, broj različitih prostih faktora, von Mangoldtova funkcija.

U drugom poglavlju donosimo definiciju i tvrdnje vezane za Dirichletov produkt aritmetičkih funkcija, dok se u trećem poglavlju bavimo generalizacijom konvolucije.

U posljednjem poglavlju definiramo derivaciju aritmetičke funkcije te opisujemo njezina svojstava i dokazujemo Selbergov identitet.

Summary

In this thesis, we describe some aritmetic functions of the theory of numbers. Thesis is divided into four chapters. In the first chapter, we provide basic definitions and properties of multiplicative functions and additive functions. We also describe particular functions such as: Euler function, sum of divisor function, divisor function, Liouville function, Möbius function, the number of distinct prime factors and the von Mangoldt function.

In the second chapter, we provide an overview of basic definition and claims related to the Dirichlet product of arithmetic functions, while in the third chapter we define the generalized convolutions.

In the last chapter, we define the derivation of arithmetic functions, describe its properties, and prove the Selberg identity.

Životopis

Rođena sam 13.2.1991. godine u Zagrebu. Školovanje sam započela 1997. godine u osnovnoj školi Dragutina Domjanić u Gajnicama u Zagrebu.. Godine 2005. upisala sam se u IX. gimnaziju u Zagrebu, opći smjer. Na Prirodoslovno-matematički fakultet, Matematički odsjek, nastavnički smjer, u Zagrebu upisala sam se 2009. godine. Prediplomski studij sam završila 2013. godine te iste godine sam upisala diplomski studij na Prirodoslovno-matematičkom fakultetu, Matematički odsjek, nastavnički smjer. Godine 2013. sam bila sudionik projekta Case Study Competition te sam zajedno sa svojim kolegama s temom projekta "Razvoj OTT tehnologija: Push notifikacije - nova budućnost SMS-a" izborila ulazak u finale prvog regionalnog Case Study Competitiona.