Teorija brojeva

Filip Najman

8. predavanje

17.5.2021.

Aritmetičke funkcije

Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako je $f(1) = 1$, te ako je $f(mn) = f(m)f(n)$ za $(m, n) = 1$.

Jedan primjer multiplikativne funkcije je Eulerova funkcija za koju je ranije dokazano da zadovoljava ovo svojstvo.

Često uz multiplikativnu funkciju f vežemo funkciju $g(n) = \sum_{d|n} f(d)$.

Pokažimo da je g također multiplikativna. Neka je $(m, n) = 1$. Tada je

$$\begin{aligned} g(mn) &= \sum_{d|m} \sum_{d'|n} f(dd') = \sum_{d|m} \sum_{d'|n} f(d)f(d') \\ &= \left(\sum_{d|m} f(d) \right) \left(\sum_{d'|n} f(d') \right) = g(m)g(n). \end{aligned}$$

Često ćemo koristiti i da za proizvoljnu funkciju f vrijedi

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

Na primjer za $n = 6$ vrijedi

$$f(1) + f(2) + f(3) + f(6) = f(6/1) + f(6/2) + f(6/3) + f(6/6).$$

Također često mijenjamo redoslijed sumacije, pa imamo

$$\sum_{d} \sum_{d'} f(d, d') = \sum_{d'} \sum_{d} f(d, d'),$$

s tim da moramo paziti po čemu idu d i d' tako da se s obje strane pojavljuju isti $f(d, d')$.

Definicija

Möbiusova funkcija $\mu(n)$, $n \in \mathbb{N}$ je definirana sa

$$\mu(n) = \begin{cases} 0, & \text{ako } n \text{ nije kvadratno slobodan} \\ (-1)^k, & \text{ako je } n = p_1 p_2 \cdots p_k,\ p_i \text{ različiti prosti brojevi.} \end{cases}$$

Očito je funkcija μ multiplikativna, pa je i funkcija $\nu(n) = \sum_{d|n} \mu(d)$ također multiplikativna.

Dakle, $\nu(1) = 1$, dok za $n > 1$ vrijedi

$$\nu(n) = \nu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \nu(p_1^{\alpha_1}) \cdots \nu(p_k^{\alpha_k})$$

$$= (\mu(1) + \mu(p_1) + \mu(p_1^2) + \cdots) \cdots (\mu(1) + \mu(p_k) + \mu(p_k^2) + \cdots)$$

$$= (1 - 1 + 0 + \cdots) \cdots (1 - 1 + 0 + \cdots) = 0.$$

Teorem (Möbiusova formula inverzije)

Neka je $f : \mathbb{N} \to \mathbb{C}$ proizvoljna funkcija, te neka je $F(n) = \sum_{d|n} f(d)$, $n \in \mathbb{N}$. Tada je $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$. Obrnuto, ako je $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ za svaki $n \in \mathbb{Z}$, onda je $F(n) = \sum_{d|n} f(d)$.

Dokaz: Imamo:

$$
\begin{aligned}
\sum_{d|n} \mu(d) F(\frac{n}{d}) &= \sum_{d|n} \mu(d) \sum_{d' | \frac{n}{d}} f(d') = \sum_{d'|n} f(d') \sum_{d | \frac{n}{d'}} \mu(d) \\
&= \sum_{d'|n} f(d') \nu(\frac{n}{d'}) = f(n).
\end{aligned}
$$

Da bi dokazali obrat, zapišimo jednakost $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ u obliku $f(n) = \sum_{d'|n} \mu(\frac{n}{d'}) F(d')$. Sada je

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

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

$\square$

Primjenimo li Möbiusovu formulu inverzije na relaciju $\sum_{d|n} \varphi(d) = n = id(n)$, dobivamo

$$\varphi(n) = \sum_{d|n} \mu(d) id\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{1}$$

Definicija

Neka je n prirodan broj. S $\tau(n)$ ćemo označavati broj pozitivnih djelitelja broja n, a sa $\sigma(n)$ sumu svih pozitivnih djelitelja broja n.

Jasno je da vrijedi $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$.

Pošto su konstantna funkcija i identita multiplikativna, slijedi da su funkcije τ i σ također multiplikativne.

Budući da je $\tau(p^j) = j+1$, $\sigma(p^j) = 1 + p + p^2 + \cdots p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

$$\begin{aligned}
\tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} (\alpha_i + 1), \\
\sigma(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.
\end{aligned}$$

Često ćemo aproksimirati sumu integralima. Za rastuću integrabilnu funkciju f vrijedi

$$\int_{a-1}^{b} f(x)dx \leq \sum_{k=a}^{b} f(k) \leq \int_{a}^{b+1} f(x)dx.$$

Posebno

$$\int_{k-1}^{k} f(x)dx \leq f(k) \leq \int_{k}^{k+1} f(x)dx.$$

Propozicija

1) $\sigma(n) < n(1+\ln n)$ *za* $n \geq 2$.

2) $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$ *za* $n \geq 2$.

Dokaz:

1) Imamo:

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

$$< n\left(1 + \sum_{d=1}^{n-1} \frac{1}{d}\right) \leq n \cdot \left(1 + \int_1^n \frac{1}{x}\,dx\right) = n(1+\ln n).$$

2) Funkcija $f(n) = \frac{\sigma(n)\varphi(n)}{n^2}$ je multiplikativna. Nadalje,

$$f(p^j) = \frac{(p^{j+1}-1)p^{j-1}(p-1)}{(p-1)p^{2j}} = 1 - \frac{1}{p^{j+1}} \geq 1 - \frac{1}{p^2},$$

pa je

$$f(n) \geq \prod_{p|n}(1 - \frac{1}{p^2}) \geq \prod_{m=2}^{\infty}(1 - \frac{1}{m^2}) = \frac{1\cdot 3}{2\cdot 2} \cdot \frac{2\cdot 4}{3\cdot 3} \cdot \frac{3\cdot 5}{4\cdot 4} \cdot \frac{4\cdot 6}{5\cdot 5} \cdots = \frac{1}{2}.$$

Prema tome, $\sigma(n)\varphi(n) \geq \frac{1}{2}n^2$. Iz 1) slijedi $\sigma(n) < 2n \ln n$ za $n > 2$, odakle je $\varphi(n) > \frac{1}{4} \cdot \frac{n}{\ln n}$. Za $n = 2$ ekplicitno provjerimo. $\square$

Često je od interesa ispitati asimptotsko ponašanje aritmetičkih funkcija, tj. ocijeniti sume oblika $\sum_{n \leq x} f(n)$, gdje je x dovoljno velik realan broj.

Mi ćemo to učiniti za funkcije τ, σ i φ. Pritom ćemo rabiti sljedeću oznaku: $f(x) = O(g(x))$ ako postoji konstanta C takva da je $|f(x)| \leq Cg(x)$ za sve x.

Na primjer, budući da je $\lfloor x \rfloor = x - \{x\}$, a $\{x\}$ je omeđena funkcija, možemo pisati: $\lfloor x \rfloor = x + O(1)$.

Također, zbog

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

tj. $\ln \lfloor x \rfloor \leq \sum_{n \leq x} \frac{1}{n} < 1 + \ln x$, možemo pisati:

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

Sljedeću lemu ostavljamo bez dokaza.

Lema

Vrijedi: $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Propozicija

1) $\sum_{n\le x} \tau(n) = x\ln x + O(x)$
2) $\sum_{n\le x} \sigma(n) = \frac{1}{12}\pi^2 x^2 + O(x\ln x)$
3) $\sum_{n\le x} \varphi(n) = \frac{3}{\pi^2}\cdot x^2 + O(x\ln x)$

Dokaz:

1)

$$\begin{aligned}\sum_{n\le x} \tau(n) &= \sum_{n\le x}\sum_{d\mid n} 1 = \sum_{d\le x}\sum_{m\le \frac{x}{d}} 1 = \sum_{d\le x}\left\lfloor \frac{x}{d}\right\rfloor = \sum_{d\le x}\left(\frac{x}{d} + O(1)\right) \\ &= x\sum_{d\le x}\left(\frac{1}{d} + O(1)\right) = x\ln x + O(x)\end{aligned}$$

2) Primijetimo da je

$$\sum_{n\leq x}\sigma(n)=\sum_{n\leq x}\sum_{d|n}d=\sum_{n\leq x}\sum_{d|n}\frac{n}{d}=\sum_{d\leq x}\sum_{n=md\leq x}\frac{md}{d}=\sum_{d\leq x}\sum_{m\leq\frac{x}{d}}m.$$

Nadalje je

$$\sum_{m\leq\frac{x}{d}}m=\frac{1}{2}\left\lfloor\frac{x}{d}\right\rfloor\Big(\left\lfloor\frac{x}{d}\right\rfloor+1\Big)=\frac{1}{2}\Big(\frac{x}{d}\Big)^2+O\Big(\frac{x}{d}\Big).$$

Sada je

$$\sum_{d\leq x}\frac{1}{d^2}-\sum_{d=1}^{\infty}\frac{1}{d^2}=O\Big(\int_x^{\infty}\frac{1}{t^2}\,dt\Big)=O\Big(\frac{1}{x}\Big).$$

Konačno je, po Lemi koju nismo dokazivali $\sum_{d=1}^{\infty}\frac{1}{d^2}=\frac{\pi^2}{6}$. Slijedi

$$\begin{aligned}\sum_{n\leq x}\sigma(n)= &\ \textstyle\sum_{d\leq x}\left[\frac{1}{2}\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right)\right]=\frac{x^2}{2}\sum_{d\leq x}\left(\frac{1}{d}\right)^2+x\sum_{d\leq x}O\left(\frac{1}{d}\right)\\ = &\ \left[\tfrac{\pi^2}{12}x^2+O(x)\right]+xO(\ln x)=\tfrac{\pi^2}{12}x^2+O(x\ln x).\end{aligned}$$

3) Prema (1), imamo:

$$\sum_{n\leq x}\varphi(n)=\sum_{n\leq x}\sum_{d|n}\mu(d)\cdot\frac{n}{d}=\sum_{d\leq x}\mu(d)\sum_{m\leq\frac{x}{d}}m.$$

Već smo vidjeli da je zadnja suma jednaka $\frac{1}{2}(\frac{x}{d})^2+O(\frac{x}{d})$. Nadalje

$$\sum_{d\leq x}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O\Big(\frac{1}{x}\Big).$$

Da bi izračunali $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$, pomnožimo je s $\sum_{d=1}^{\infty}\frac{1}{d^2}$. Dobivamo:

$$\Big(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}\Big)\Big(\sum_{d=1}^{\infty}\frac{1}{d^2}\Big)=\sum_{m=1}^{\infty}\frac{1}{m^2}\sum_{dd'=m}1\cdot\mu(d)=\sum_{m=1}^{\infty}\frac{1}{m^2}\sum_{d|m}\mu(d)$$

$$=\sum_{m=1}^{\infty}\frac{\nu(m)}{m^2}=1.$$

Prema tome, dobili smo da je $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}$, pa konačno imamo:

$$\sum_{n\leq x}\varphi(n)=\sum_{d\leq x}\mu(d)\Big[\frac{1}{2}\Big(\frac{x}{d}\Big)^2+O\Big(\frac{x}{d}\Big)\Big]=\frac{x^2}{2}\sum_{d\leq x}\Big(\frac{\mu(d)}{d^2}\Big)+\sum_{d\leq x}O\Big(\frac{x}{d}\Big)$$

$$= \frac{3}{\pi^2}x^2 + O(x \ln x).$$

$\square$

Budući da je $\sum_{n\le x}\varphi(n) \sim \frac{3}{\pi^2}x^2$, $\sum_{n\le x} n \sim \frac{1}{2}x^2$, rezultat iz Propozicije 3) može se interpretirati i tako da kažemo da je vjerojatnost da su dva nasumce izabrana cijela broja relativno prosta jednaka $\frac{6}{\pi^2} \approx 0.6079$.

Sada ćemo promotriti neke funkcije koje su povezane s distribucijom prostih brojeva.

Definicija

S $\pi(x)$ ćemo označavati broj prostih brojeva p takvih da je $p \le x$. Von Mangoldtova funkcija $\Lambda(n)$, $n \in \mathbb{N}$ je definirana s $\Lambda(n) = \ln p$ ako je $n = p^k$, $\Lambda(n) = 0$ inače. Stavimo nadalje

$$\psi(x) = \sum_{n\le x}\Lambda(n), \quad \vartheta(x) = \sum_{p\le x}\ln p, \quad T(x) = \sum_{n\le x}\ln n.$$

Godine 1896. Hadamard i de la Vallée Poussin su dokazali da je $\pi(x) \sim \frac{x}{\ln x}$ kad $x \to \infty$.

Mi ćemo dokazati nešto slabiju tvrdnju. Naime pokazat ćemo da postoje pozitivni realni brojevi a i b takvi da je

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}$$

za dovoljno velike x.

Teorem

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

Dokaz: Neka je $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Tada je $\ln n = \sum_{i=1}^{k} \alpha_i \ln p_i$. No, $p_i^{\alpha_i} \parallel n$, pa $p_i^e \mid n$ ako i samo ako je e jedan od brojeva $1, 2, \ldots, \alpha_i$. Stoga je

$$\sum_{i=1}^{k} \alpha_i \ln p_i = \sum_{i=1}^{k} \sum_{p_i^e|n} \ln p_i = \sum_{d|n} \Lambda(d).$$

$\square$

Sljedeći teorem ostavljamo bez dokaza, koji se može naći u skripti.

Teorem

Neka je $a_0 = \frac{1}{3}\ln 2 + \frac{1}{2}\ln 3 \approx 0.7804$, $b_0 = \frac{3}{2}a_0 \approx 1.1705$. *Ako je* $a < a_0$ *i* $b > b_0$, *onda postoji realan broj* x_0 *(koji ovisi o a i b) takav da je*

$$ax < \psi(x) < bx$$

za sve $x > x_0$.

Teorem

Za $x \geq 1$ vrijedi: $\vartheta(x) = \psi(x) + O(\sqrt{x})$.

Dokaz: Iz definicije je $\vartheta(x) \leq \psi(x)$ za sve x. Dakle, moramo još naći donju ogradu za razliku $\psi(x) - \vartheta(x)$.

Imamo:

$$\psi(x) = \sum_{n \leq x} \Lambda(x) = \sum_{p^k \leq x} \ln p = \sum_k \sum_{p \leq \sqrt[k]{x}} \ln p = \sum_k \vartheta(\sqrt[k]{x}).$$

Stavimo $K = \lfloor \frac{\ln x}{\ln 2} \rfloor$. Imamo

$$k > K \Longrightarrow k > \frac{\ln x}{\ln 2} \Longrightarrow \ln 2 > \frac{1}{k} \ln x \Longrightarrow 2 > \sqrt[k]{x},$$

pa je $\vartheta(\sqrt[k]{x}) = 0$.

Stoga je

$$\psi(x) - \vartheta(x) = \sum_{2 \leq k \leq K} \vartheta(\sqrt[k]{x}) \leq \sum_{2 \leq k \leq K} \psi(\sqrt[k]{x}) = \sum_{2 \leq k \leq K} O(\sqrt[k]{x}),$$

po prethodnom Teoremu. Konstanta u O ne ovisi o k, a članovi u sumi padaju.

Zato je

$$\psi(x) - \vartheta(x) = O(\sqrt{x} + \sum_{3 \le k \le K} \sqrt[k]{x}) =$$

$$O(\sqrt{x} + K\sqrt[3]{x}) = O(\sqrt{x} + \sqrt[3]{x}\ln x) = O(\sqrt{x}).$$

$\square$

Teorem

Za $x \ge 2$ vrijedi:

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big).$$

Dokaz: Pokažimo najprije da za $x \ge 2$ vrijedi

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + \int_2^x \frac{\vartheta(u)}{u \ln^2 u}\, du. \tag{2}$$

Zaista,

$$\int_2^x \frac{\vartheta(u)}{u \ln^2 u}\, du = \int_2^x (\sum_{p \le u} \ln p) u^{-1} \ln^{-2} u\, du$$

$$= \sum_{p \le x} \ln p \int_p^x u^{-1} \ln^{-2} u \, du = \sum_{p \le x} \ln p \Big(\frac{1}{\ln p} - \frac{1}{\ln x} \Big) =$$

$$\pi(x) - \frac{\vartheta(x)}{\ln x}.$$

Budući da je $0 \le \vartheta(x) \le \psi(x)$, iz Teorema kojeg smo ostavili bez dokaza slijedi da je $\vartheta(x) = O(x)$. Zato je integral u (2) $O(\int_2^x \ln^{-2} u \, du)$.

Rastavimo područje integracije ovog integrala na dva dijela: $2 \le u \le \sqrt{x}$ i $\sqrt{x} \le u \le x$.

Na prvom dijelu, podintegralna funkcija je omeđena, pa je doprinos tog dijela $O(\sqrt{x})$.

Na drugom dijelu, podintegralna funkcija je $\le \frac{4}{\ln^2 x}$, pa je doprinos drugog dijela $O(\frac{x}{\ln^2 x})$. $\square$

Teorem

Neka su brojevi a_0 i b_0 kao u Teoremu prije. Ako je $a < a_0$ i $b > b_0$, onda nejednakost

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x} \tag{3}$$

vrijedi za sve dovoljno velike x.

Dokaz: Koristeći ranije dokazane rezultate, imamo:

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big) = \frac{\psi(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big) \le b_0\frac{x}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big).$$

To daje gornju ogradu u (3) za dovoljno velike x ako je $b > b_0$.

Slično se dobiva

$$\pi(x) \ge a_0\frac{x}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big),$$

što daje donju ogradu u (3) za dovoljno velike x. $\square$