Teorija sita

Matija Kazalicki

1 Problem sita

Jedan od klasičnih problema analitičke teorije brojeva je problem određivanja (broja) prostih brojeva u nekom intervalu. Povijesno prva metoda koja se koristila za rješavanje tog problema je Eratostenovi sito. Za ilustraciju, ako želimo odrediti proste brojeve u segmentu $[10, 100]$, iz tog segmenta trebamo "izbaciti" (prosijati) sve višekratnike brojeva $2, 3, 5$ i 7 (to su svi prosti brojevi manji od $\sqrt{100} = 10$). Ono što ostane su prosti brojevi. Lako je izračunati koliko ima višekratnika danih brojeva u tom segmentu - općenito višekratnika broja n u segmentu $[a, b]$ ima $\lfloor \frac{a}{n} \rfloor$-$\lfloor \frac{b}{n} \rfloor$. No ako zbrojimo te brojeve nećemo dobiti ukupan broj prosijanih elemenata jer smo neke od njih brojali više puta. Od tog zbroja moramo oduzeti broj višekratnika produkata $2\cdot 3, 2\cdot 5, 2\cdot 7, 3\cdot 4, \ldots$ pa onda (prema formuli uključivanja i isključivanja) tom zbroju dodati broj višekratnika brojeva $2 \cdot 3 \cdot 5, \ldots$. Ovu ideju možemo formalizirati na sljedeći način.

2 Eratostenovo sito

Koliko ima prostih brojeva manjih ili jednakih x (u oznaci $\pi(x)$)? Cilj analitičke teorije brojeva je odrediti kako se ta (i mnoge druge) funkcija ponaša za velike x.

Malo oznaka, kažemo da se funkcija $f(x)$ asimptotski ponaša kao funkcija $g(x)$, pišemo $f(x) \sim g(x)$, ako $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. Na primjer, prema teoremu o prostim brojevima (Prime number theorem) znamo da je $\pi(x) \sim \frac{x}{\ln x}$. Ako ne možemo odrediti asimptotsko ponašanje funkcije, možda možemo odrediti neku gornja među. Pišemo $f(x) = O(g(x))$ ili $f(x) << g(x)$ (za pozitivnu funkciju $g(x)$) ako postoji konstanta $C > 0$ takva da vrijedi $|f(x)| \leq C \cdot g(x)$ sve dovoljno velike x. Na primjer, ako je $f(x)$ ograničena funkcija, onda je $f(x) = O(1)$.

U ovom odjeljku ćemo vidjeti kakvu nam gornju ogradu za $\pi(x)$ daje Eratostenovo sito. Problem ćemo formulirati malo općenitije. Računat ćemo funkciju $\Phi(x,z) = \#\{n \leq x : \ n \text{ nije djeljiv s niti jednim } p < z\}$. Tada je $\pi(x) \leq \pi(z) + \Phi(x,z) \leq z + \Phi(x,z)$.

Označimo sa $\mathcal{A} = \{1, 2, \ldots, \lfloor x \rfloor\}$ i za $d \in \mathbb{N}$ sa $\mathcal{A}_d = \{n \in \mathcal{A} : d|n\}$ skup višekratnika od d u $\mathcal{A}$. Tada je $\Phi(x,z) = \#\mathcal{A} \setminus \bigcup_{p<z} \mathcal{A}_p$ (sa p odnosno p_i ćemo uvijek označavati prost broj). Prema formuli uključivanja i isključivanja

$$\Phi(x,z) = \mathcal{A} - \sum_{p_1|P_z} \#\mathcal{A}_{p_1} + \sum_{p_1,p_2|P_z} \#\mathcal{A}_{p_1p_2} - \sum_{p_1,p_2,p_3|P_z} \mathcal{A}_{p_1p_2p_3} + \cdots ,$$

gdje je $P_z = \prod_{p<z} p$, a p_i'ovi su međusobno različiti prosti brojevi. Koristeći Möbiusovu μ-funkciju

$$\mu(n) = \begin{cases} 0, \text{ ako } n \text{ nije kvadratno slobodan,} \\ (-1)^k, \text{ ako je } n \text{ produkt } k \text{ različitih prostih brojeva,} \end{cases}$$

taj izraz možemo elegantnije zapisati $\Phi(x,z) = \sum_{d|P_z} \mu(d)\#\mathcal{A}_d$. Očito je $\#\mathcal{A}_d = \left\lfloor \frac{x}{d} \right\rfloor = \frac{x}{d} + R_d$, gdje je $0 \leq R_d < 1$. Odnosno

$$\Phi(x,z) = x \sum_{d|P_z} \frac{\mu(d)}{d} + \sum_{d|P_z} \mu(d) R_d.$$

Na prvi dio ovog izraza gledamo kao na "glavni" član (main term), a na drugi dio kao na "grešku" (error term). Cilj nam je z odabrati (u ovisnosti o x) tako da to zbilja bude tako, tj. da asimptotski glavni član bude veći od greške.

2.1 Ocjena glavnog člana i greške - gornja ograda

Polazna točka naše analize je identitet (koji je jednostavna posljedica jedinstvene faktorizacije cijelih brojeva)

$$\sum_{d|P_z} \frac{\mu(d)}{d} = \prod_{p<z} \left(1 - \frac{1}{p}\right).$$

Zadatak 1. Dokažite da je za sve $x \in \mathbb{R}$

a) $e^{-x} \geq 1 - x$,

b) $e^{x} \leq 1 + xe^{x}$.

Iz prethodnog zadatka slijedi

$$\prod_{p<z} \left(1 - \frac{1}{p}\right) \leq \prod_{p<z} e^{-\frac{1}{p}} = e^{-\sum_{p<z} \frac{1}{p}}.$$

Kako je $\sum_{p<z} \frac{1}{p} > \ln\ln z + O(1)$ (za dokaz pogledajte skriptu iz Teorije brojeva), zaključujemo da je glavni dio $< e^{-\ln\ln z + O(1)} << \frac{1}{\ln z}$.

Za početak, kod ocjene greške ćemo koristiti trivijalnu nejednakost: $\mu(d)R_d \leq 1$ iz čega slijedi da je greška

$$\leq \sum_{d|P_z} 1 = 2^{\pi}(z) < 2^{z}.$$

Ako za proizvoljan (mali) $\epsilon > 0$ odaberemo $z = \ln x^{1-\epsilon} = (1-\epsilon)\ln x$ dobit ćemo da je glavni član veći od greške, odnosno

$$\Phi(x, (1-\epsilon)\ln x) << \frac{x}{\ln\ln x} + O(x^{1-\epsilon}),$$

odnosno

$$\Phi(x, \ln x) << \frac{x}{\ln\ln x}.$$

Proposition 2.1. *Vrijedi* $\pi(x) << \frac{x}{\ln\ln x}$.

Dokaz. Kako je $\pi(x) \leq \Phi(x,z) + \pi(z) \leq \Phi(x,z) + z$, tvrdnja slijedi iz prethodnog razmatranja ako odaberemo $z = \ln x$. □

2.2 Rankinov trik

Možemo li popraviti ovu gornju ogradu? Za razliku od prethodne analize, ovdje ćemo u ocjenama glavnog člana i greške iskoristiti činjenicu da je $d \leq x$.

Probajmo prvo bolje ocijeniti grešku. Neka je

$$\Psi(x,z) = \#\{n \leq x : n \text{ kvadratno slobodan i } \forall p, p|n \Rightarrow p < z\}.$$

Tada uz trivijalnu ocjenu $\mu(d)R_d < 1$ za kvadratno slobodan d imamo

$$\sum_{\substack{d|P_z \\ d \leq x}} \mu(d)R_d < \sum_{\substack{d|P_z \\ d \leq x}}{}' 1 = \Psi(x,z),$$

gdje $\sum{}'$ označava sumaciju po kvadratno slobodnim brojevima. Neka je $\delta > 0$ proizvoljan. Rankinov trik se bazira na nejednakosti $1 \leq \left(\frac{x}{n}\right)^{\delta}$ za $n \leq x$. Računamo

$$\Psi(x,z) = \sum_{\substack{n \leq x \\ p|n \Rightarrow p<z}}{}' 1 \leq \sum_{\substack{n \leq x \\ p|n \Rightarrow p<z}}{}' \left(\frac{x}{n}\right)^{\delta} \leq x^{\delta} \prod_{p<z} \left(1 + \frac{1}{p^{\delta}}\right).$$

Iz $1 + x \leq e^x$ dobivamo $\Psi(x,z) << \exp\left(\delta \ln x + \sum_{p<z} \frac{1}{p^{\delta}}\right)$. Odaberimo $\delta := 1 - \eta$ (u ovisnosti o z) tako da $\eta \to 0$ kad $z \to \infty$. Kako je $p^{-\delta} = p^{-1}p^{\eta} = p^{-1}e^{\eta \ln p}$, iz $e^x \leq 1 + xe^x$ dobivamo

$$\sum_{p<z} \frac{1}{p^{\delta}} \leq \sum_{p<z} \frac{1}{p} \left(1 + (\eta \ln p) z^{\eta}\right) (\text{ jer je } p < z).$$

Tada za $\eta = \frac{1}{\ln z}$ dobivamo,

Teorem 2.2.

$$\Psi(x,z) << x(\ln z)e^{-\frac{\ln x}{\ln z}} \quad \textit{kad } x \to \infty.$$

Dokaz. Imamo

$$\Psi(x,z) << \exp\left((1-\frac{1}{\ln z})\ln x + \sum_{p<z}\frac{1}{p}\left(1+\frac{1}{\ln z}(\ln p)z^{\frac{1}{\ln z}}\right)\right),$$

pa tvrdnja slijedi iz nejednakosti $\sum_{p<z}\frac{1}{p} = \ln\ln z + O(1)$ i $\sum_{p<z}\frac{\ln p}{p} = \ln z + O(1)$. □

Glavni član ponovno želimo ocijeniti s $x\prod_{p<z}\left(1-\frac{1}{p}\right)$, ali kako sada sumiramo samo po $d \leq x$ više ne vrijedi stroga nejednakost koristeći prethodni teorem izračunat ćemo grešku.

Teorem 2.3.

$$\sum_{\substack{d|P_z\\ d\leq x}}\frac{\mu(d)}{d} = \prod_{p<z}\left(1-\frac{1}{p}\right) + O((\ln z)^2 e^{-\frac{\ln x}{\ln z}}).$$

Dokaz. Imamo

$$\sum_{\substack{d|P_z\\ d\leq x}}\frac{\mu(d)}{d} = \prod_{p<z}\left(1-\frac{1}{p}\right) - \sum_{\substack{d|P_z\\ d>x}}\frac{\mu(d)}{d}.$$

Iz Propozicije 5.2 slijedi

$$\sum_{\substack{d|P_z\\ d>x}}\frac{1}{d} \leq -\frac{\Psi(x,z)}{x} + \int_x^\infty \frac{\Psi(t,z)}{t^2}dt.$$

Integral je odzgo ograničen s

$$\log z\int_x^\infty \exp\left(-\frac{\ln t}{\ln z}\right)\frac{dt}{t} = \log z\int_x^\infty \frac{dt}{t^{1+1/\ln z}} = (\log z)^2\exp\left(-\frac{\ln x}{\ln z}\right),$$

iz čega slijedi tvrdnja. □

Iz ovog teorema i prethodne analize direktno slijede dva sljedeće dvije tvrdnje.

Korolar 2.4.

$$\Psi(x,z) = x\prod_{p<z}\left(1-\frac{1}{p}\right) + O(x(\ln z)^2 e^{-\frac{\ln x}{\ln z}}).$$

Korolar 2.5.

$$\pi(x) << \frac{x}{\ln x}\ln\ln x.$$

Dokaz. Ako za mali $\epsilon > 0$ odaberemo $\ln z = \epsilon\frac{\ln x}{\ln\ln x}$, koristeći $\pi(x) \leq \Phi(x,z) + z$ dobivamo da je glavni član

$$x\prod_{p<z}\left(1-\frac{1}{p}\right) << x\frac{1}{\ln z} << \frac{x}{\ln x}\ln\ln x,$$

dok je greška manje od glavnog člana ($\epsilon > 0$ nam je trebao da bi član

$$x\ln z e^{-\frac{\ln x}{\ln z}} = x\left(\epsilon\cdot\frac{\ln x}{\ln\ln x}\right)^2(\ln x)^{-1/\epsilon}$$

učinili manjim od $\frac{x\ln\ln x}{\ln x}$ - što će vrijediti ako je $\epsilon < 1/3$). □

3 Brunovo sito

Eratostenovo sito možemo reformulirati na sljedeći način. Neka je $E(n)$ karakteristična funkcija jedinice.

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

Tada je

$$\Phi(x,z) = \sum_{n\leq x} E((n,P_z)) = \sum_{n\leq x}\sum_{\substack{d|n \\ d|P_z}}\mu(d) = \sum_{d|P_z}\mu(d)\left\lfloor\frac{x}{d}\right\rfloor.$$

Brunova ideja je bila funkciju $E(n)$ u gornjoj formuli za $\Phi(x,z)$ zamijeniti s nekom gornjom aproksimacijom i tako dobiti gornju ogradu za $\Phi(x,z)$ kod koje će se greška moći bolje aproksimirati.

Definicija 3.1. *Za $r \in \mathbb{Z}$, krnja Möbiusova funkcija je dana formulom*

$$\mu_r(n) = \begin{cases} \mu(d), & \text{ako je } \nu(d) \le r, \\ 0, & \text{inače,} \end{cases}$$

gdje $\nu(n)$ označava broj prostih djeljitelja od n. Označimo sa $\psi_r(n) = \sum_{d|n} \mu_r(d)$.

Vrijedi

$$\psi_r(n) = \sum_{d|n} \mu_r(d) = \sum_{\substack{d|n \\ \nu(d)\le r}} \mu(d) = \sum_{k \le r} (-1)^k \binom{\nu(n)-1}{r}.$$

Posljednja jednakost slijedi iz usporedbe koeficijenata uz x^r (pomoću binomne formule) u izrazu $(1-x)^{-1}(1-x)^{\nu} = (1-x)^{\nu-1}$.

Očito za prirodne brojeve n i k vrijedi

$$\psi_{2k+1}(n) \le \sum_{d|n} \mu(d) (= E(n)) \le \psi_{2k}(n).$$

Funkciju $E(n)$ ćemo ocijeniti s funkcijom $\psi_r(n)$ za paran broj r. Ovaj put dobivamo bolju ocjenu za grešku

$$\begin{aligned} \Phi(x,z) &\le \sum_{n \le x} \sum_{\substack{d|n \\ d|P_z}} \mu_r(d) = \sum_{d|P_z} \mu_r(d) \left\lfloor \frac{x}{d} \right\rfloor \\ &= x \sum_{d|P_z} \frac{\mu_r(d)}{d} + O(z^r), \end{aligned}$$

budući da je $\mu_r(d) = 0$ za $\nu(d) > r$.

Gornja ocjena se može i ovako (intuitivnije) kombinatorno opisati

$$\Phi(x,z) \le \mathcal{A} - \sum_{p_1|P_z} \#\mathcal{A}_{p_1} + \sum_{p_1,p_2|P_z} \#\mathcal{A}_{p_1p_2} - \cdots + \sum_{p_1,\ldots,p_r|P_z} \#\mathcal{A}_{p_1p_2\cdots p_r}.$$

3.1 Ocjena glavnog člana i gornja međa za $\pi(x)$

Formula Möbiusove inverzije nam daje

$$\mu_r(d) = \sum_{\delta|d} \mu(\frac{d}{\delta})\psi_r(\delta),$$

otkuda slijedi

$$\begin{aligned}\sum_{d|P_z} \frac{\mu_r(d)}{d} &= \sum_{d|P_z} \frac{1}{d} \sum_{\delta|d} \mu\left(\frac{d}{\delta}\right)\psi_r(\delta)\\ &= \sum_{\delta|P_z} \frac{\psi_r(\delta)}{\delta} \sum_{d|\frac{P_z}{\delta}} \frac{\mu(d)}{d}.\end{aligned}$$

Kako je $\sum_{d|n} \frac{\mu(d)}{d} = \prod\left(1 - \frac{1}{p}\right)$ i $\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$ slijedi

$$\sum_{d|P_z} \frac{\mu_r(d)}{d} = W(z) \sum_{\delta|P_z} \frac{\psi_r(\delta)}{\phi(\delta)},$$

gdje je $W(z) = \prod_{p<z}\left(1 - \frac{1}{p}\right)$ i $\phi(n)$ je Eulerova ϕ-funkcija.

Dakle, $\sum_{d|P_z} \frac{\mu_r(d)}{d} = W(z) + W(z)\sum_{\substack{\delta|P_z\\ \delta>1}} \frac{\psi_r(\delta)}{\phi(\delta)}$.

Kako je $\psi_r(\delta) \leq \binom{\nu(\delta)-1}{r}$, slijedi

$$
\begin{aligned}
\sum_{\substack{\delta | P_z \\ \delta > 1}} \frac{\psi_r(\delta)}{\phi(\delta)} &\leq \sum_{\substack{\delta | P_z \\ \delta > 1}} \binom{\nu(\delta)-1}{r} \frac{1}{\phi(\delta)} \leq \sum_{r+1 \leq m \leq \pi(z)} \binom{m-1}{r} \sum_{\substack{\delta | P_z \\ \delta > 1 \\ \nu(\delta) = m}} \frac{1}{\phi(\delta)} \\
&\leq \sum_{r+1 \leq m \leq \pi(z)} \binom{m-1}{r} \left(\sum_{p<z} \frac{1}{p-1} \right)^m \frac{1}{m!} \\
&\leq \frac{1}{r!} \sum_{m \geq r+1} \frac{1}{(m-r)!} (\ln \ln z + c_1)^m \\
&= \frac{\ln \ln z + c_1)^r}{r!} \sum_{m \geq r+1} \frac{1}{(m-r)!} (\ln \ln z + c_1)^{m-r} \\
&\leq \frac{(\ln \ln z + c_1)^r}{r!} \exp(\ln \ln z + c_1),
\end{aligned}
$$

gdje je c_1 neka pozitivna konstanta (znamo da takva postoji je je

$$
\lim_{z \to \infty} \left(\sum_{p<z} \frac{1}{p} - \ln \ln z = M \right),
$$

gdje je $M = 0.261497\ldots$ Meissel–Mertensova konstanta).

Iz $\frac{1}{r!} \leq \left(\frac{e}{r}\right)^r$, slijedi

$$
\sum_{\substack{\delta | P_z \\ \delta > 1}} \frac{\psi_r(\delta)}{\phi(\delta)} \leq c \exp(r - r \ln r + r \ln \Lambda) \ln z,
$$

gdje je $\Lambda = \ln \ln z + c_1$ i $c > 0$ neka konstanta.

Nije teško pokazati (ali je malo naporno, vidi 84. str. u [1]), da ako odaberemo za r najbliži paran broj broju $\eta \ln \ln z$ gdje je $\eta = \frac{\alpha \ln x}{(\ln z)(\ln \ln z)}$ za neki $\alpha < 1$ i ako uzmemo z takav da je $\ln z = O((\ln x)^{1-\epsilon})$ za bilo koji $0 < \epsilon < 1$, da ćemo dobiti ocjenu $\Phi(x,z) \leq xW(z) + O(x \exp(-(\ln x)^\epsilon))$, iz koje slijedi sljedeći teorem.

Teorem 3.2. $\pi(x) = O\left(\frac{x}{(\ln x)^{1-\epsilon}}\right)$.

Ako odaberemo z takav da je $\ln z = \frac{\alpha \ln x}{\ln \ln x}$, može se pokazati još i bolja ocjena.

Teorem 3.3. $\pi(x) = O\left(\frac{x \ln \ln x}{\ln x}\right)$.

Za ocjenu bolju od ove, trebat će nam Selbergovo sito.

4 Selbergovo sito

Kao i u Brunovom situ, Selbergova ideja je bila aproksimirati karakterističnu funkciju jedinice $E(n)$ nečim s čime je lakše računati. No dok je kod Brunovog sita tu aproksimaciju bilo moguće kombinatorno izinterpretirati, kod Selbergovog sita to nije slučaj.

Neka je $(\lambda_d)_{d\in\mathbb{N}}$ niz u $\mathbb{R}$ takav da je $\lambda_1 = 1$. Tada trivijalno vrijedi

$$E(n) = \sum_{d|n} \mu(d) \leq \left(\sum_{d|n} \lambda_d\right)^2.$$

Za pažljivo odabrani niz (λ_d), izraz s desne strane nejednakosti će biti naša aproksimacija funkcije $E(n)$. Vrijedi

$$\begin{aligned}
\Phi(x,z) &\leq \sum_{n\leq x}\left(\sum_{d|(n,P_z)} \lambda_d\right)^2 = \sum_{n\leq x}\left(\sum_{d_1,d_2|(n,P_z)} \lambda_{d_1}\lambda_{d_2}\right) \\
&= \sum_{d_1,d_2|P_z} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{n\leq x \\ [d_1,d_2]|n}} 1 = \sum_{d_1,d_2|P_z} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{n\leq x \\ [d_1,d_2]|n}} \left\lfloor \frac{x}{[d_1,d_2]} \right\rfloor \\
&\leq x \sum_{d_1,d_2|P_z} \frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]} + O\left(\sum_{d_1,d_2|P_z} |\lambda_{d_1}| \cdot |\lambda_{d_2}|\right).
\end{aligned}$$

Odabrat ćemo niz (λ_d) tako da je $\lambda_d = 0$ za $d > z$ i $|\lambda_d| \leq 1|$. Tada će vrijediti

$$\Phi(x,z) \leq x \sum_{d_1,d_2 \leq z} \frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]} + O(z^2).$$

Niz (λ_d) će mo odabrati tako da uz uvjet $\lambda_1 = 1$ minimiziramo kvadratnu formu

$$\sum_{d_1,d_2 \leq z} \frac{\lambda_{d_1}\lambda_{d_2}}{d_1 d_2} = \sum_{d_1,d_2 \leq z} \frac{\lambda_{d_1}}{d_1}\frac{\lambda_{d_2}}{d_2}(d_1,d_2),$$

jer je $[d_1,d_2](d_1,d_2) = d_1 d_2$.

Zadatak 2. Dokažite da je $\sum_{\delta|d} \phi(\delta) = d$.

Koristeći prethodni zadatak, ta forma

$$\sum_{\delta \leq z} \phi(\delta) \sum_{\substack{d_1,d_2 \leq z \\ \delta|(d_1,d_2)}} \frac{\lambda_{d_1}\lambda_{d_2}}{d_1 d_2} = \sum_{\delta \leq z} \phi(\delta) \left(\sum_{\substack{d \leq z \\ \delta|d}} \frac{\lambda_d}{d} \right)^2,$$

se dijagonalizira uz zamjenu varijabli $u_\delta = \sum_{\substack{d \leq z \\ \delta|d}} \frac{\lambda_d}{d}$ u formu

$$\sum_{\delta \leq z} \phi(\delta) u_\delta^2.$$

Zadatak 3. Dokažite da vrijedi

$$\frac{\lambda_\delta}{\delta} = \sum_{\delta|d} \mu(\frac{d}{\delta}) u_d.$$

Koristeći prethodni zadatak vidimo da je uvjet $\lambda_1 = 1$ ekvivalentan s $\sum_{\delta \leq z} \mu(\delta) u_\delta = 1$.

Za traženje minimuma kvadratne forme uz uvjet koristit ćemo metodu Lagrangeovog multiplikatora. Općenito, ako želimo minimizirati funkciju $f(x_1,\ldots,x_n)$ uz uvjet $g(x_1,\ldots,x_n) = 0$ možemo imamo sljedeći teorem.

Teorem 4.1. *Ako je $f(\underline{x})$ minumum onda postoji $\lambda \in \mathbb{R}^\times$ takav da je*
$$\nabla f(\underline{x}) = \lambda \nabla g(\underline{x}) \quad i \quad g(\underline{x}) = 0.$$

U našem slučaju iz $(2\phi(\delta)u_\delta)_{\delta \le z} = \lambda(\mu(\delta))_{\delta \le z}$ dobivamo da je $u_\delta = \frac{\mu(\delta)}{\phi(\delta)} \cdot \lambda$. Iz uvjeta slijedi $\sum_{\delta \le z} \frac{\mu(\delta)^2}{\phi(\delta)} = \frac{1}{\lambda}$. Ako definiramo $V(z) = \sum_{\delta \le z} \frac{\mu(\delta)^2}{\phi(\delta)}$, slijedi da je minimum jednak $\sum_{\delta \le z} \phi(\delta) \frac{\mu(\delta)^2}{\phi(\delta)^2} \frac{1}{V(z)^2} = \frac{1}{V(z)}$, odnosno
$$\lambda_\delta = \delta \sum_{\substack{d \le z \\ \delta | d}} \frac{\mu(d/\delta)\mu(d)}{\phi(d)V(z)}.$$

Dokazali smo sljedeći teorem.

Teorem 4.2. $\Phi(x,z) \le \frac{x}{V(z)} + O(\sum_{d_1,d_2 \le z} |\lambda_{d_1}\lambda_{d_2}|)$.

Pokažimo sada da za svaki δ vrijedi $|\lambda_\delta| \le 1$. Računamo
$$\begin{aligned}
V(z)\lambda_\delta &= \delta \sum_{\substack{d \le z \\ \delta | d}} \frac{\mu(d/\delta)\mu(d)}{\phi(d)} = \delta \sum_{t \le \frac{z}{\delta}} \frac{\mu(t)\mu(\delta t)}{\phi(\delta t)} \\
&= \delta \sum_{\substack{t \le \frac{z}{\delta} \\ (t,\delta)=1}} \frac{\mu(t)^2 \mu(\delta)}{\phi(d)\phi(t)} = \mu(d) \prod_{p|\delta} (1 - \frac{1}{p})^{-1} \sum_{\substack{t \le \frac{z}{\delta} \\ (t,\delta)=1}} \frac{\mu(t)^2}{\phi(t)} \\
&= \mu(d) \prod_{p|\delta} (1 + \frac{1}{\phi(p)}) \sum_{\substack{t \le \frac{z}{\delta} \\ (t,\delta)=1}} \frac{\mu(t)^2}{\phi(t)} \\
&= \mu(d) \sum_{\substack{u|\delta \\ u \text{ squarefree}}} \sum_{\substack{t \le \frac{z}{\delta} \\ (t,\delta)=1}} \frac{\mu(ut)^2}{\phi(ut)}.
\end{aligned}$$

Sada slijedi da je $|V(z)| \cdot |\lambda_\delta| \le |V(z)|$, odnosno $|\lambda_d| \le 1$.

Korolar 4.3. $\pi(x) << \frac{x}{\ln x}$.

Dokaz. Kako je $V(z) = \sum_{d \le z} \frac{\mu(d)^2}{\phi(d)} >> \ln z$ (vidi primjer u dodatku), iz $\pi(x) \le \Phi(x,z) + z$ slijedi da je $\pi(x) << \frac{x}{\ln z} + z^2$. Tvrdnja sada slijedi ako odaberemo $z = \left(\frac{x}{\ln x}\right)^{1/2}$. $\square$

5 Dodatak - metoda parcijalne sumacije

Teorem 5.1. *Neka je $c_1, c_2, \ldots$ niz kompleksnih brojeva i neka je*

$$S(x) = \sum_{n \leq x} c_n.$$

Neka je n_0 fiksan prirodan broj. Ako je $c_j = 0$ za $j < n_0$ i $f : [n_0, \infty) \to (C)$ je klase $C^1([n_0, \infty))$, tada za cijeli broj $x > n_0$ imamo

$$\sum_{n \leq x} c_n f(n) = S(x) f(x) - \int_{n_0}^{x} S(t) f'(t) dt.$$

Dokaz. Lijevu stranu jednakosti možemo ovako napisati

$$\begin{aligned} \sum_{n \leq x} \left(S(n) - S(n-1)\right) f(n) &= \sum_{n \leq x} S(n) f(n) - \sum_{n \leq x-1} S(n) f(n+1) \\ &= S(x) f(x) - \sum_{n \leq x-1} S(n) \int_{n}^{n+1} f'(t) dt \\ &= S(x) f(x) - \int_{n_0}^{x} S(t) f'(t) dt, \end{aligned}$$

jer je $S(t)$ po dijelovima konstantna funkcija na intervalima oblika $[n, n+1)$. $\square$

Primjer. Neka je $c_n = 1$ za kvadratno slobodan n, a $c_n = 0$ inače te neka je $f(x) = \frac{1}{x}$. Tada iz prethodnog teorema za $n_0 = 1$ $x \in \mathbb{N}$ slijedi

$$\sum_{n \leq x} c_n \cdot \frac{1}{n} = \frac{1}{x} S(x) + \int_{1}^{x} S(t) \frac{1}{t^2} dt.$$

Budući da kvadratno slobodni brojevi imaju pozitivnu gustoću (vidi odjeljak sa zadacima), slijedi da je postoji $\alpha > 0$ tako da je $S(t) > \alpha t$ za svaki $t > 0$ pa zaključujemo

$$\sum_{\substack{n \leq x \\ \mu(n)^2 = 1}} \frac{1}{n} > \alpha + \alpha \int_{1}^{x} \frac{1}{t} dt >> \ln x.$$

Posebno, budući da je $\phi(d) < d$ slijedi

$$\sum_{n\leq x} \frac{\mu(n)^2}{n} >> \ln(x).$$

Proposition 5.2. *Neka je* $S(x) = \sum_{n\leq x} c_n$ *i neka je* $f(t)$ *funkcija klase* C^1*. Pretpostavimo*

$$\lim_{Y\to\infty} S(Y)f(Y) = 0$$

i

$$\int_1^\infty S(t)f'(t)dt < \infty.$$

Tada je

$$\sum_{n>x} c_n f(n) = -S(x)f(x) - \int_x^\infty S(t)f'(t)dt.$$

Dokaz. Kad pustimo da x teži u beskonačnost u izrazu (koji slijedi iz prethodnog teorema)

$$\sum_{n\leq x} c_n f(n) = S(x)f(x) - \int_1^x S(t)f'(t)dt$$

dobit ćemo

$$\sum_{n\geq 1} c_n f(n) = -\int_1^\infty S(t)f'(t)dt.$$

Tvrdnja slijedi oduzimanjem prve jednakosti od druge. □

Napomena. Izlaganje u ovom članku prati odličnu knjigu [1].

6 Zadaci

Svaki zadatak nosi dva boda. Potrebno je skupiti četiri boda. Molim vas da mi javite ako pronađete neku grešku ili nejasnoću u tekstu.

1.) Označimo sa $\Xi(x) = \#\{n \leq x : n \text{ je kvadratno slobodan}\}$. Koristeći neko sito dokažite da je

$$\Xi(x) = \frac{6}{\pi^2}x + O(\sqrt{x}).$$

Napomena: možda vam pomogne činjenica da je

$$\sum_{d^2|n} \mu(d) = \begin{cases} 1, & \text{ako je } n \text{ kvadratno slobodan} \\ 0, & \text{inače.} \end{cases}$$

2.) Dokažite sami (koristeći npr. Eratostenovo sito) ili negdje pronađite i raspišite (npr. u knjizi [1]) dokaz tvrdnje da je broj prostih brojeva blizanaca

$$<< \frac{x(\ln \ln x)^2}{(\ln x)^2}.$$

Iz te tvrdnje koristeći metodu parcijalne sumacije dokažite da suma

$$\sum_p \frac{1}{p},$$

konvergira, gdje sumiramo po prostim brojevima p za koje je $p+2$ također prost broj.

3.) Koristeći neko sito, pronađite neku (netrivijalnu) gornju među za broj prostih brojeva u nizu n^2+1 gdje je $n \leq x$. Npr. pomoću Brunovog sita se može dokazati $<< \frac{x}{\ln x}$.

4.) Pretpostavimo da je $\mathcal{P}$ podskup skupa prostih brojeva sa svojstvom da suma $\sum_{p \in \mathcal{P}} \frac{1}{p}$ divergira. Dokažite da je broj prirodnih brojeva $n \leq x$ koji nisu djeljivi niti s jednim prostim brojem $p \in \mathcal{P}$ jednak o(x). (Kažemo da je funkcija $f(x) = o(x)$ ako $\lim_{x \to \infty} \frac{f(x)}{x} = 0$.)

5.) Dokažite da je broj rješenja (u prirodnim brojevima) nejednadžbe $[d_1, d_2] \leq z$ jednak $O(z(\ln z)^3)$.

Literatura

[1] A. C. Cojocaru and M. Ram Murty, *An introduction to sieve methods and their applications*, London Mathematical Society Student Texts, 66, Cambridge University Press, Cambridge, 2006, xii+224 pp., ISBN 978-0-521-64275-3