O distribuciji prostih brojeva

Definicija 1. *S $\pi(x)$ ćemo označavati broj prostih brojeva p takvih da je $p \leq x$.*

Godine 1896. Hadamard i de la Vallée Poussin su dokazali da je $\pi(x) \sim \frac{x}{\ln x}$ kad $x \to \infty$, tj. da je $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$. Mi ćemo dokazati nešto slabiju tvrdnju, koju je prvi dokazao Čebišev, 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 $x \geq 2$.

Naš će dokaz koristiti informacije o rastavu na proste faktore binomnih koeficijenata oblika $\binom{2n}{n}$. Tu će nam se prirodno pojaviti funkcija najveće cijelo, pa ćemo proučiti i neka njezina svojstva.

Podsjetimo se najprije definicije i najvažnijeg svojstva binomnih koeficijenata:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k},$$

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + y^n.$$

Definicija 2. *Neka je x realan broj. Najveći cijeli broj koji nije veći od x označavamo sa $\lfloor x \rfloor$ i zovemo* najveće cijelo od x *ili* strop od x. *Sa $\{x\} = x - \lfloor x \rfloor$ označavamo* razlomljeni dio od x.

Primjer 1. *Dokažimo da za svaki realan broj x vrijedi*

$$\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = \lfloor 2x \rfloor.$$

Rješenje:

$$\begin{aligned}
\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor &= \lfloor x \rfloor + \left\lfloor \lfloor x \rfloor + \{x\} + \frac{1}{2} \right\rfloor \\
&= \begin{cases} \lfloor x \rfloor + \lfloor x \rfloor, \text{ ako je } \{x\} + \frac{1}{2} < 1 \\ \lfloor x \rfloor + \lfloor x \rfloor + 1, \text{ ako je } \{x\} + \frac{1}{2} \geq 1 \end{cases} \\
&= \begin{cases} 2\lfloor x \rfloor, \text{ ako je } \{x\} < \frac{1}{2} \\ 2\lfloor x \rfloor + 1, \text{ ako je } \{x\} \geq \frac{1}{2} \end{cases}
\end{aligned}$$

$$\begin{aligned}
\lfloor 2x \rfloor &= \lfloor 2\lfloor x \rfloor + 2\{x\} \rfloor \\
&= \begin{cases} 2\lfloor x \rfloor, \text{ ako je } 2\{x\} < 1 \\ 2\lfloor x \rfloor + 1, \text{ ako je } 2\{x\} \geq 1 \end{cases} \\
&= \begin{cases} 2\lfloor x \rfloor, \text{ ako je } \{x\} < \frac{1}{2} \\ 2\lfloor x \rfloor + 1, \text{ ako je } \{x\} \geq \frac{1}{2} \end{cases}
\end{aligned}$$

$\diamondsuit$

Primjer 2. *Neka je n prirodan broj. Izračunajmo sumu*

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \cdots + \left\lfloor \frac{n+2^k}{2^{k+1}} \right\rfloor + \cdots .$$

Rješenje: Primjenimo formulu iz Primjera 1 na pribrojnike u promatranoj sumi, koji su oblika $\left\lfloor \frac{n}{2^{k+1}} + \frac{1}{2} \right\rfloor$. Dobivamo da je suma jednaka

$$\lfloor n \rfloor - \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor - \left\lfloor \frac{n}{8} \right\rfloor + \cdots = \lfloor n \rfloor = n.$$

$\diamondsuit$

Primjer 3. *Dokažimo da za svaki prirodan broj n vrijedi*

$$\left\lfloor \frac{n - \lfloor \frac{n}{3} \rfloor}{2} \right\rfloor = \left\lfloor \frac{n+1}{3} \right\rfloor .$$

Rješenje: Promotrimo tri slučaja u ovisnosti o ostatku kojeg pri dijeljenju s 3 daje broj n.

Ako je $n = 3k$, onda je $\left\lfloor \frac{n - \lfloor \frac{n}{3} \rfloor}{2} \right\rfloor = \left\lfloor \frac{3k-k}{2} \right\rfloor = k = \left\lfloor \frac{3k+1}{3} \right\rfloor$.

Ako je $n = 3k+1$, onda je $\left\lfloor \frac{n - \lfloor \frac{n}{3} \rfloor}{2} \right\rfloor = \left\lfloor \frac{3k+1-k}{2} \right\rfloor = k = \left\lfloor \frac{3k+2}{3} \right\rfloor$.

Ako je $n = 3k+2$, onda je $\left\lfloor \frac{n - \lfloor \frac{n}{3} \rfloor}{2} \right\rfloor = \left\lfloor \frac{3k+2-k}{2} \right\rfloor = k+1 = \left\lfloor \frac{3k+3}{3} \right\rfloor$. $\diamondsuit$

Teorem 1. *Potencija s kojoj zadani prosti broj p ulazi u rastav broja $n!$ na proste faktore jednaka je*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots .$$

Dokaz: U produktu $n! = 1 \cdot 2 \cdot 3 \cdots n$ ima $\lfloor \frac{n}{p} \rfloor$ faktora koji su višekratnici od p. Među njima je $\lfloor \frac{n}{p^2} \rfloor$ onih koji su višekratnici od p^2, $\lfloor \frac{n}{p^3} \rfloor$ onih koji su višekratnici od p^3, itd. Primijetimo da je u sumi iz teorema svaki faktor koji je višekratnik od p^m, ali nije od p^{m+1}, brojen točno m puta: kao višekratnik od $p, p^2, \ldots, p^m$. Primijetimo također da je ta suma konačna, jer za dovoljno veliki j vrijedi $p^j > n$, pa je $\lfloor \frac{n}{p^j} \rfloor = \lfloor \frac{n}{p^{j+1}} \rfloor = \cdots = 0$. □

Primjer 4. *U rastavu broja 40! na proste faktore, broj 3 se javlja s potencijom*

$$\lfloor \frac{40}{3} \rfloor + \lfloor \frac{40}{9} \rfloor + \lfloor \frac{40}{27} \rfloor = 13 + 4 + 1 = 18.$$

(Uočimo da je $\lfloor \frac{40}{3^j} \rfloor = 0$ za $j \geq 4$.)

♢

Primjer 5.

a) S koliko nula završava broj 562! ?

b) S koliko nula završava broj $\binom{101}{21}$?

Rješenje:

a) Trebamo naći najveći potenciju broja 10 koja dijeli 562!. Budući da su 2 i 5 prosti faktori broja 10, odredimo potenciju broja 2 i potenciju broja 5 u rastavu na proste faktore broja 562!:

$$\alpha = \left\lfloor \frac{562}{2} \right\rfloor + \left\lfloor \frac{562}{4} \right\rfloor + \left\lfloor \frac{562}{8} \right\rfloor + \cdots \left\lfloor \frac{562}{512} \right\rfloor = 558,$$

$$\beta = \left\lfloor \frac{562}{5} \right\rfloor + \left\lfloor \frac{562}{25} \right\rfloor + \left\lfloor \frac{562}{125} \right\rfloor = 112 + 22 + 4 = 138.$$

Sada tražimo minimum brojeva α i β. Zapravo nam je unaprijed trebalo biti jasno da će taj minimum biti β, pa je bilo dovoljno samo njega izračunati. Odgovor je da broj 562! završava sa 138 nula.

b) Uočimo da je $\binom{101}{21} = \frac{101!}{21! \cdot 80!}$, pa računamo potenciju broja 2 i potenciju broja 5 u rastavu broja $\binom{101}{21}$ na proste faktore:

$$\alpha = \left(\left\lfloor \frac{101}{2} \right\rfloor + \cdots + \left\lfloor \frac{101}{64} \right\rfloor \right) - \left(\left\lfloor \frac{21}{2} \right\rfloor + \cdots + \left\lfloor \frac{21}{16} \right\rfloor \right) - \left(\left\lfloor \frac{80}{2} \right\rfloor + \cdots + \left\lfloor \frac{80}{64} \right\rfloor \right)$$
$$= 97 - 18 - 78 = 1,$$

$$\beta = \left(\left\lfloor \frac{101}{5} \right\rfloor + \left\lfloor \frac{101}{25} \right\rfloor \right) - \left\lfloor \frac{21}{5} \right\rfloor - \left(\left\lfloor \frac{80}{5} \right\rfloor + \left\lfloor \frac{80}{25} \right\rfloor \right) = 24 - 4 - 19 = 1.$$

Traži se minimum brojeva α i β, a to je 1. Stoga broj $\binom{101}{21}$ završava s jednom nulom.

$\diamondsuit$

Sada ćemo vidjeti kako nam Teorem 1 može pomoći u dobivanju infomacija o distribuciji prostih brojeva.

Lema 1. *Neka je $n \in \mathbb{N}$. Vrijedi:*

(i) $2^n \leq \binom{2n}{n} < 2^{2n}$

(ii) $\displaystyle\prod_{n<p\leq 2n} p$ *dijeli* $\binom{2n}{n}$

(iii) Neka je $r(p) = \lfloor \log_p 2n \rfloor$*. Tada* $\binom{2n}{n}$ *dijeli* $\displaystyle\prod_{p\leq 2n} p^{r(p)}$.

(iv) Ako je $n > 2$ i $\frac{2n}{3} < p \leq n$, onda p ne dijeli $\binom{2n}{n}$.

(v) $\displaystyle\prod_{p\leq n} p < 4^n$

Dokaz:

(i) Zbog $2n - k \geq 2(n-k)$, imamo:

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} \geq 2^{2n}.$$

Nadalje,

$$2^{2n} = (1+1)^{2n} = 1 + \binom{2n}{1} + \cdots + \binom{2n}{n} + \cdots + 1 > \binom{2n}{n}.$$

(ii) Neka je $p \in \langle n, 2n]$ prost broj. Tada p dijeli $(2n)!$, ali ne dijeli $n!$. Stoga p dijeli $\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!}$.

(iii) Eksponent od p u rastavu broja $(2n)!$ na proste faktore je $\sum_{j=1}^{\infty} \left\lfloor \frac{2n}{p^j} \right\rfloor = \sum_{j=1}^{r(p)} \left\lfloor \frac{2n}{p^j} \right\rfloor$, a u rastavu broja $n!$ je $\sum_{j=1}^{r(p)} \left\lfloor \frac{n}{p^j} \right\rfloor$. Zato je eksponent od p u rastavu broja $\binom{2n}{n}$ jednak

$$\sum_{j=1}^{r(p)} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right) = \sum_{j=1}^{r(p)} \left(\left\lfloor \frac{n}{p^j} + \frac{1}{2} \right\rfloor - \left\lfloor \frac{n}{p^j} \right\rfloor \right) \leq \sum_{j=1}^{r(p)} 1 = r(p).$$

(Ovdje smo iskoristili formulu $\lfloor 2x \rfloor = \lfloor x + \frac{1}{2} \rfloor + \lfloor x \rfloor$ iz Primjera 1.)

(iv) Neka je $\frac{2n}{3} < p \leq n$. Tada je $2p > n$ i $3p > 2n$, pa se p pojavljuje u rastavu od $n!$ s potencijom $\lfloor \frac{n}{p} \rfloor = 1$, a u rastavu od $(2n)!$ s potencijom $\lfloor \frac{2n}{p} \rfloor = 2$. Stoga se p u rastavu od $\binom{2n}{n}$ pojavljuje s potencijom $2 - 1 - 1 = 0$, tj. p ne dijeli $\binom{2n}{n}$.

(v) Tvrdnju dokazujemo indukcijom po n. Za $n = 1, 2, 3$ direktnim uvrštavanjem provjerimo da tvrdnja vrijedi. Pretpostavimo sada da je $n \geq 4$, te da tvrdnja vrijedi za sve brojeve manje od n.

Ako je n paran, recimo $n = 2m$, onda n nije prost, pa imamo:

$$\prod_{p \leq 2m} p = \prod_{p \leq 2m-1} < 4^{2m-1} < 4^m.$$

Neka je n neparan, recimo $n = 2m + 1$ uz $m \geq 2$. Svaki prosti broj $p \in \langle m + 1, 2m + 1]$ dijeli $\binom{2m+1}{m+1} = \frac{(2m+1)!}{m! \cdot (m+1)!}$, pa imamo:

$$\prod_{p \leq 2m+1} p \leq \binom{2m+1}{m} \prod_{p \leq m+1} p < \binom{2m+1}{m} \cdot 4^{m+1}.$$

Koristeći činjenicu da su među binomnim koeficijentima $\binom{2m+1}{k}$ najveći $\binom{2m+1}{m}$ i $\binom{2m+1}{m+1}$ (koji su međusobno jednaki), zaključujemo da je

$$\begin{aligned} 2^{2m+1} &= (1+1)^{2m+1} = 1 + \cdots + \binom{2m+1}{m} + \binom{2m+1}{m+1} + \cdots + 1 \\ &> 2 \cdot \binom{2m+1}{m}, \end{aligned}$$

pa dobivamo

$$\prod_{p\le 2m+1} p < 4^m \cdot 4^{m+1} = 4^{2m+1}.$$

$\square$

Teorem 2. *Za $n \ge 2$ vrijedi*

$$\frac{n}{8\ln n} < \pi(n) < \frac{6n}{\ln n}.$$

Dokaz: Iz Lema 1 (ii) i (iii) slijedi

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\le 2n} p \le \binom{2n}{n} \le \prod_{p\le 2n} p^{r(p)} \le (2n)^{\pi(2n)},$$

pa Lema 1 povlači

$$n^{\pi(2n)-\pi(n)} < 2^{2n} \quad \text{i} \quad 2^{2n} \le (2n)^{\pi(2n)}. \tag{1}$$

Stavimo sada $n = 2^k$ u (1). Dobivamo:

$$k(\pi(2^{k+1} - \pi(2^k)) < 2^{k+1} \quad \text{i} \quad 2^k \le (k+1)\pi(2^{k+1}).$$

Jasno je da je $\pi(2^{k+1}) \le 2^k$ (parni brojevi veći od 2 nisu prosti), pa imamo:

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < \pi(2^{k+1}) + 2^{k+1} \le 3\cdot 2^{k+1}. \tag{2}$$

Zbrojimo relacije (2) za $k = m, m-1, \dots, 1, 0$, te nakon kraćenja ("teleskopiranja") dobivamo:

$$(m+1)\pi(2^{m+1}) \le 3(2^m + 2^{m-1} + \cdots + 2^1 + 2^0) < 3\cdot 2^{m+1}.$$

Odavde i iz (1), zaključujemo da vrijedi

$$\frac{2^m}{m+1} \le \pi(2^{m+1}) < \frac{3\cdot 2^{m+1}}{m+1}. \tag{3}$$

Neka je sada zadan prirodan broj $n \ge 2$, te neka je $m = \lfloor \log_2 n \rfloor - 1$. Tada je $2^{m+1} \le n < 2^{m+2}$. Uočimo još da za svaki $x > 0$ vrijedi $\ln 2^x = x\ln 2 < x$ i $\ln 2^x > \frac{x}{2}$. Konačno, iz (3) dobivamo

$$\pi(n) \le \pi(2^{m+2}) < \frac{3\cdot 2^{m+2}}{m+2} < \frac{6\cdot 2^{m+1}}{\ln(2^{m+2})} < \frac{6n}{\ln n};$$

$$\pi(n) \ge \pi(2^{m+1}) > \frac{2^m}{m+1} = \frac{2^{m+2}}{8\cdot\frac{m+1}{2}} > \frac{2^{m+2}}{8\ln(2^{m+1})} > \frac{n}{8\ln n}.$$

$\square$

Teorem 3 (Bertrand, Čebišev). *Za svaki prirodan broj n postoji prosti broj p takav da je $n < p \leq 2n$.*

Dokaz: Za $n = 1, 2, 3$ tvrdnja je očito točna: $1 < 2 \leq 2$, $2 < 3 \leq 4$, $3 < 5 \leq 6$. Pretpostavimo da tvrdnja ne vrijedi za neki $n > 3$. Iz Leme 1 (iv) slijedi za svi prosti faktori od $\binom{2n}{n}$ zadovoljavaju $p \leq \frac{2n}{3}$. Neka je $s(p)$ najveća potencija od p koja dijeli $\binom{2n}{n}$. Po Lemi 1 (iii) imamo da je $p^{s(p)} \leq p^{r(p)} \leq 2n$. Ako je $s(p) \geq 2$, onda je $p \leq \sqrt{2n}$, pa se stoga najviše $\lfloor\sqrt{2n}\rfloor$ prostoh brojeva pojavljuje u razvoju od $\binom{2n}{n}$ s potencijom ≥ 2. Zato je

$$\binom{2n}{n} \leq (2n)^{\lfloor\sqrt{2n}\rfloor} \cdot \prod_{p \leq \frac{2n}{3}} p.$$

Od svih binomnih koeficijenta $\binom{2n}{k}$, najveći je onaj srednji, tj. $\binom{2n}{n}$. Sada iz $2^{2n} = (1+1)^{2n} = 1 + \cdots + \binom{2n}{n} + \cdots + 1 < (2n+1)\binom{2n}{n}$, slijedi $\binom{2n}{n} > \frac{4^n}{2n+1}$. Dakle, po Lemi 1 (v),

$$\frac{4^n}{2n+1} < (2n)^{\lfloor\sqrt{2n}\rfloor} \cdot \prod_{p \leq \frac{2n}{3}} p < 4^{2n/3} \cdot (2n)^{\sqrt{2n}}.$$

No, $2n + 1 < (2n)^2$, pa dobivamo $4^{n/3} < (2n)^{2+\sqrt{2n}}$, tj.

$$\frac{n \ln 4}{3} < (2 + \sqrt{2n}) \ln 2n.$$

Funkcija $f(x) = \frac{x \ln 4}{3} - (2 + \sqrt{2x}) \ln 2x$ je za dovoljno velike x-eve rastuća i pozitivna ($f'(x) > 0$ za $x \geq 200$ i $f(507) > 0$ povlači da je $f(x) > 0$ za $x \geq 507$). Tako je teorem dokazan za $n \geq 507$. Tvrdnja teorema za $n < 507$ slijedi iz činjenice da je u sljedećem nizu prostih brojeva

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 631$$

svaki član manji od dvostrukog prethodnog člana. $\square$