

## Jedan neobičan dokaz

Petra Jambriško, Mladen Vuković

Pojam najmanjeg zajedničkog višekratnika uči se još u osnovnoj školi. Za prirodne brojeve  $m, n \in \mathbb{N}$  označimo sa  $nzv(m, n)$  njihov najmanji zajednički višekratnik. Primjerice,  $nzv(5, 6) = 30$ , a  $nzv(10, 32) = 160$ . U ovom članku baviti ćemo se najmanjim zajedničkim višekratnicima skupova oblika  $\{1, 2, \dots, n\}$ , gdje je  $n$  neki prirodan broj. Radi kratkoće zapisa označimo sa  $L_n$  broj  $nzv(1, 2, \dots, n)$ . Primjerice,  $L_1 = 1$ ,  $L_2 = 2$ ,  $L_3 = 6$ ,  $L_4 = 12$ ,  $L_5 = 60$  i  $L_6 = 60$ . Nije teško izračunati da je najmanji zajednički višekratnik skupa  $\{1, 2, \dots, 7\}$  jednak 420, tj.  $L_7 = 420$ , te  $L_8 = 840$ . Mi ćemo se zapravo baviti dokazom jedne nejednakosti u vezi brojeva  $L_n$ . U tu svrhu primijetimo da redom vrijedi:

$$\begin{array}{ll} L_1 = 1 < 2^1 & L_4 = 12 < 2^4 \\ L_2 = 2 < 2^2 & L_5 = 60 > 2^5 \\ L_3 = 6 < 2^3 & L_6 = 60 < 2^6 \end{array}$$

No,  $L_7 = 420 > 2^7 = 128$ , te  $L_8 = 840 > 2^8 = 256$ . Glavni cilj ovog članka je izložiti dokaz da za svaki  $n \geq 7$  vrijedi  $L_n \geq 2^n$ . Na samom kraju članka komentirat ćemo zašto je navedena nejednakost jako važna. No, smatramo da je dokaz te nejednakosti posebno zanimljiv jer se tvrdnja iz teorije brojeva dokazuje primjenom integrala.

Prisjetimo se prvo binomne formule: za sve  $a, b \in \mathbb{R}$  i  $n \in \mathbb{N}$  vrijedi sljedeća formula

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k, \quad \text{gdje je } \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Budući da ćemo u dokazu koristiti integrale, sada ćemo istaknuti neke činjenice o integralima koje su nam važne. Neka su  $f$  i  $g$  integrabilne funkcije na segmentu  $[0, 1]$ , te  $A \in \mathbb{R}$  i  $p \in \mathbb{N}$  proizvoljni. Tada vrijedi:

$$\int_0^1 (f(x) + g(x)) dx = \int_0^1 f(x) dx + \int_0^1 g(x) dx \quad (\text{svojstvo aditivnosti integrala})$$

$$\int_0^1 A \cdot f(x) dx = A \int_0^1 f(x) dx \quad (\text{svojstvo linearnosti integrala})$$

$$\int_0^1 x^p dx = \frac{1}{p+1} x^{p+1} \Big|_0^1 = \frac{1}{p+1} (1^{p+1} - 0^{p+1}) = \frac{1}{p+1} \quad (\text{formula } (*))$$

Sada dokazujemo da za svaki  $n \geq 7$  vrijedi  $L_n \geq 2^n$ .

U svrhu dokaza prvo razmatramo integral  $\int_0^1 x^{m-1}(1-x)^{n-m} dx$ , gdje su  $n \in \mathbb{N}$  i  $m \in \{1, \dots, n\}$  proizvoljni. Taj integral označimo sa  $I_{m,n}$ . Tada redom vrijedi:

$$\begin{aligned}
 I_{m,n} &= \int_0^1 x^{m-1}(1-x)^{n-m} dx = (\text{primjena binomne formule}) \\
 &= \int_0^1 x^{m-1} \sum_{k=0}^{n-m} \binom{n-m}{k} 1^{n-m-k} (-x)^k dx = \int_0^1 x^{m-1} \sum_{k=0}^{n-m} (-1)^k \binom{n-m}{k} x^k dx \\
 &= \int_0^1 \sum_{k=0}^{n-m} (-1)^k \binom{n-m}{k} x^{m+k-1} dx = (\text{svojstvo aditivnosti integrala}) \\
 &= \sum_{k=0}^{n-m} \int_0^1 (-1)^k \binom{n-m}{k} x^{m+k-1} dx = (\text{svojstvo linearnosti integrala}) \\
 &= \sum_{k=0}^{n-m} (-1)^k \binom{n-m}{k} \int_0^1 x^{m+k-1} dx = (\text{formula } (*)) \\
 &= \sum_{k=0}^{n-m} (-1)^k \binom{n-m}{k} \frac{1}{m+k}
 \end{aligned}$$

Pokažimo da vrijedi:

$$L_n \cdot I_{m,n} \in \mathbb{Z} \tag{1}$$

(sa  $\mathbb{Z}$  smo označili skup svih cijelih brojeva). Kako je  $1 \leq m \leq n$  i  $0 \leq k \leq n-m$ , tada je očito  $1 \leq m+k \leq n$ . Budući da je  $L_n$  višekratnik svih brojeva od 1 do  $n$ , tada je posebno  $L_n$  višekratnik svakog broja  $m+k$  (za  $k \in \{0, \dots, n-m\}$ ). Zbog toga je  $L_n \cdot \frac{1}{m+k} \in \mathbb{N}$  za svaki  $k \in \{0, \dots, n-m\}$ . Znamo da za svaki  $k \leq n-m$  vrijedi  $\binom{n-m}{k} \in \mathbb{N}$  (znate li to dokazati?). Time imamo  $L_n \cdot \sum_{k=0}^{n-m} (-1)^k \binom{n-m}{k} \frac{1}{m+k} \in \mathbb{Z}$ .

U sljedećom dijelu dokaza koristit ćemo formulu za parcijalnu integraciju:

$$\int_0^1 f(x) \cdot g'(x) dx = f(x) \cdot g(x) \Big|_0^1 - \int_0^1 f'(x) \cdot g(x) dx$$

Sada dokazujemo da vrijedi jednakost  $I_{m,n} = 1/(m \binom{n}{m})$ .

$$\begin{aligned} I_{m,n} &= \int_0^1 x^{m-1} (1-x)^{n-m} dx = \left\{ \begin{array}{l} f(x) = x^{m-1} \Rightarrow f'(x) = (m-1)x^{m-2} \\ g'(x) = (1-x)^{n-m} \Rightarrow g(x) = \frac{-1}{n-m+1} (1-x)^{n-m+1} \end{array} \right\} \\ &= (\text{formula za parcijalnu integraciju}) = \frac{m-1}{n-m+1} \int_0^1 x^{m-2} (1-x)^{n-m+1} dx \\ &= \left\{ \begin{array}{l} f(x) = x^{m-2} \Rightarrow f'(x) = (m-2)x^{m-3} \\ g'(x) = (1-x)^{n-m+1} \Rightarrow g(x) = \frac{-1}{n-m+2} (1-x)^{n-m+2} \end{array} \right\} \\ &= \frac{(m-1)(m-2)}{(n-m+1)(n-m+2)} \int_0^1 x^{m-3} (1-x)^{n-m+2} dx \\ &\quad \vdots \\ &= (\text{još } m-3 \text{ puta primijenimo parcijalnu integraciju}) \\ &\quad \vdots \\ &= \frac{(m-1)(m-2) \cdots 2 \cdot 1}{(n-m+1)(n-m+2) \cdots (n-1)} \int_0^1 (1-x)^{n-1} dx \\ &= (\text{supstitucija } t = 1-x, \text{ pa primjena formule } (*)) \\ &= \frac{(m-1)!}{(n-m+1) \cdots (n-1)} \cdot \frac{1}{n} = \frac{(m-1)!}{(n-m+1) \cdots (n-1) \cdot n} \cdot \frac{m}{m} \end{aligned}$$

$$\begin{aligned}
&= \frac{m!}{(n-m+1) \cdots (n-1) \cdot n} \cdot \frac{1}{m} = \frac{1}{m} \cdot \frac{m!}{(n-m+1) \cdots (n-1) \cdot n} \\
&= \frac{1}{m} \cdot \frac{m!}{(n-m+1) \cdots (n-1) \cdot n} \cdot \frac{1 \cdot 2 \cdots (n-m)}{1 \cdot 2 \cdots (n-m)} = \frac{1}{m} \cdot \frac{m! \cdot (n-m)!}{n!} \\
&= \frac{1}{m \binom{n}{m}}
\end{aligned}$$

Time smo dokazali da za svaki  $n \in \mathbb{N}$  i svaki  $m \in \{1, \dots, n\}$  vrijedi sljedeća jednakost:

$$I_{m,n} = \frac{1}{m \binom{n}{m}} \quad (2)$$

Bili smo dokazali da vrijedi  $L_n \cdot I_{m,n} \in \mathbb{Z}$ . Iz dokazane jednakosti (2) slijedi posebno  $I_{m,n} > 0$ . Budući da je očito  $L_n > 0$ , tada dobivamo da za svaki  $n \in \mathbb{N}$  i svaki  $m \in \{1, \dots, n\}$  vrijedi  $L_n \cdot I_{m,n} \in \mathbb{N}$ . Tada posebno imamo:

$$m \binom{n}{m} \mid L_n. \quad (3)$$

Uvrstimo li  $2n$  umjesto  $n$ , te  $n$  umjesto  $m$  u (3) dobivamo sljedeće:

$$n \binom{2n}{n} \mid L_{2n}. \quad (4)$$

Isto tako, iz (3) posebno slijedi i

$$(n+1) \binom{2n+1}{n+1} \mid L_{2n+1}. \quad (5)$$

Lako je vidjeti da redom vrijede sljedeće jednakosti:

$$(2n+1) \binom{2n}{n} = (2n+1) \frac{(2n)!}{n!n!} \cdot \frac{n+1}{n+1} = (n+1) \frac{(2n+1)!}{(n+1)!n!} = (n+1) \binom{2n+1}{n+1}$$

Iz prethodnog slijedi da vrijedi  $(n+1) \binom{2n+1}{n+1} = (2n+1) \binom{2n}{n}$ , a onda primjenom (5) slijedi

$$(2n+1) \binom{2n}{n} \mid L_{2n+1}. \quad (6)$$

Očito vrijedi  $nzd(n, 2n + 1) = 1$ , te  $L_{2n} | L_{2n+1}$ . Tada (4) i (6) povlače da vrijedi:

$$n(2n + 1) \binom{2n}{n} | L_{2n+1} \quad (7)$$

(Probajte iskazati općenitu tvrdnju o djeljivosti koja se koristi za posljednji zaključak, te je probajte dokazati; možete i dokaz potražiti u knjizi [4].) Kako je djeliteľ broja sigurno manji ili jednak tom broju (sve su to prirodni brojevi!), tada iz (7) imamo:

$$L_{2n+1} \geq n(2n + 1) \binom{2n}{n} \quad (8)$$

Najveći binomi koeficijent izraza  $(1 + x)^{2n}$  je  $\binom{2n}{n}$  (to je "srednji" binomni koeficijent; možete li to dokazati?). Odnosno, za svaki  $k \in \{0, \dots, 2n\}$  vrijedi  $\binom{2n}{n} \geq \binom{2n}{k}$ . Posebno, tada za  $x = 1$  imamo redom sljedeće:

$$4^n = 2^{2n} = (1 + 1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} 1^{n-k} 1^k = \sum_{k=0}^{2n} \binom{2n}{k} \leq \sum_{k=0}^{2n} \binom{2n}{n} = (2n + 1) \binom{2n}{n},$$

tj. za svaki  $n \in \mathbb{N}$  vrijedi  $(2n + 1) \binom{2n}{n} \geq 4^n$ . Množenjem sa  $n$  posljednje nejednakosti dobivamo:

$$n(2n + 1) \binom{2n}{n} \geq n \cdot 4^n \quad (9)$$

Očito za svaki  $n \geq 4$  vrijedi  $n \cdot 4^n \geq 2^2 \cdot 2^{2n} = 2^{2n+2}$ . Ovo posljednje, te (8) i (9) povlače da za svaki  $n \geq 4$  vrijedi  $L_{2n+1} \geq 2^{2n+2}$ , a onda očito i sljedeće:

$$L_{2n+2} \geq L_{2n+1} \geq 2^{2n+2} \geq 2^{2n+1} \quad (10)$$

Označimo  $k = 2n + 2$ . Tada  $n \geq 4$  povlači  $k \geq 10$ , a iz (10) slijedi  $L_k \geq 2^k$  za svaki parni broj  $k \geq 10$ . Uzmemo li  $k = 2n + 1$ , tada  $n \geq 4$  povlači  $k \geq 9$ , a (10) povlači  $L_k \geq 2^k$ , za svaki neparni  $k \geq 9$ .

Time smo dokazali da vrijedi  $L_n \geq 2^n$  za svaki  $n \geq 9$ . No, na samom početku ovog članka bili smo primijetili da vrijedi  $L_7 \geq 2^7$  i  $L_8 \geq 2^8$ . Na taj način je završen dokaz da za svaki  $n \geq 7$  vrijedi  $L_n \geq 2^n$ .

Malo pažljivijem čitanjem dokaza može se vidjeti da smo mi zapravo dokazali  $L_n > 2^n$ . Probajte sami pronaći mjesto u dokazu gdje možemo staviti strogu nejednakost. Može se postaviti pitanje gornje međe za brojeve  $L_n$ . U članku [6] je dokazano da vrijedi  $L_n < 4^n$ .

Kao što smo na početku bili i najavili, istaknimo ovdje na samom kraju važnost upravo dokazane tvrdnje. Algoritmi za ispitivanje je li neki prirodan broj prost jako su važni. Godine 2004. trojica indijskih matematičara su u članku [1] dokazali da postoji efikasan algoritam za ispitivanje prostosti. U tom je dokazu činjenica  $L_n \geq 2^n$  jako važna. Više informacija o tome možete čitati u [3], odnosno [1].

Zatim, brojevi  $L_n$  povezani su sa Čebiševljevom funkcijom  $\psi$  koja se često koristi u dokazima u vezi prostih brojeva. Funkciju  $\psi$  nećemo ovdje definirati. Pokušat ćemo objasniti vezu funkcije  $\psi$  i brojeva  $L_n$ . Prilikom proučavanja distribucije prostih brojeva razmatra se funkcija  $\pi : \langle 0, +\infty \rangle \rightarrow \mathbb{N}_0$  koja je definirana ovako:

$$\pi(x) = \text{broj prostih brojeva } p \in \mathbb{N} \text{ takvih da je } p \leq x.$$

Primjerice, vrijedi  $\pi(10) = 4$  i  $\pi(100) = 25$ . Možete li odrediti  $\pi(150)$ ? A  $\pi(1000)$ ? Teorem o prostim brojevima tvrdi da vrijedi  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1$ . Iz toga slijedi da je za velike prirodne brojeve  $x$  vrijednost  $\pi(x)$  približno jednaka  $x/\ln x$ . Probajte primjenom teorema o prostim brojevima procijeniti  $\pi(1000)$ . Pokazalo se da je u teoriji brojeva jednostavnije raditi s funkcijom  $\psi$  nego s funkcijom  $\pi$ . Može se pokazati da je teorem o prostim brojevima ekvivalentan sa  $\lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1$ . Funkcija  $\psi$  je povezana s brojevima  $L_n$  preko jednakosti  $e^\psi(n) = L_n$ . Stoga iz teorema o prostim brojevima zaključujemo da se brojevi  $L_n$  asimptotski ponašaju kao  $e^n$  (što je skladu s navedenim nejednakostima  $2^n < L_n < 4^n$ ). Više detalja o svemu ovome možete pronaći u knjizi [4].

Zanimljivo je još istaknuti da je prošle godine u jednom američkom časopisu objavljen članak s nešto drugačijim dokazom od ovog koji smo ovdje dali (vidi [6]).

## Literatura

- [1] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Annals of Mathematics, (2) 160 (2004), 781–793
- [2] A. Dujella, *Uvod u teoriju brojeva (skripta)*, PMF–Matematički odsjek, Sveučilište u Zagrebu, 2006. <http://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf>
- [3] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.
- [4] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.
- [5] M. Nair, *On Chebyshev-type inequalities for primes*, American Mathematical Monthly 89:2(1982), 126–129
- [6] B. Sury, *Lower Bound for the Least Common Multiple*, American Mathematical Monthly 126:10(2019), 940–942