Tšebõšovi teoreem

Kes poleks kuulnud Eukleidese teoreemi algarvude hulga lõpmatusest? See sätestab, et kui tahes suure algarvu me arvteljel ka ei märgiks, kindlasti on veelgi kaugemal olemas veelgi suurem algarv. Aga kui kaugel?

Hinnanguid algarvude esinemistihedusele otsisid matemaatikud juba aegade hämarusest. Eukleidese teoreemi tõestus annab ühe, väga jämeda hinnangu. Praktika näitab, et algarvud esinevad palju tihedamalt kui Eukleidese teoreemi tõestuse põhjal tingimata vaja. Aastal 1845 püstitas prantsuse matemaatik Joseph Bertrand (1822–1900) hüpoteesi, mis hiljem leidis ka kinnitust: positiivsete arvude n ja $2n$ vahel on alati vähemalt üks algarv, kui tahes suur n ka ei oleks. Seda väidet tuntakse tänapäeval Bertrand'i postulaadi nime all või siis esmatõestaja, vene matemaatiku Pafnuti Tšebõšovi (1821–1894) järgi Tšebõšovi teoreemina.

Tšebõšovi teoreem iseenesest tänapäeval palju huvi ei paku, kuna leitud on palju tugevamaid ja täpsemaid algarvude esinemistiheduse hinnanguid. Selle teoreemi tõestus on aga väärt läbitöötamist kui üks matemaatiku kavaluse musternäide. Pärast hüpoteesi püstitamist ja algse komplitseeritud tõestuse publitseerimist Tšebõšovi poolt oli möödunud üle 80 aasta, kui äkki avastati sellele teoreemile elementaarne tõestus. Kuidas on võimalik, et see üsna lihtne mõttekäik jäi nii kauaks matemaatikute silme eest varjatuks?

Lugege ja püüdke teiste vigadest õppida!

Esmased jämedad hinnangud

Alustuseks püstitame ülal viidatud jämeda hinnangu, mis tuletatakse sarnaselt Eukleidese tõestusega algarvude hulga lõpmatusele. Selles tõestuses moodustatakse olemasolevate algarvude korrutis ja näidatakse, et tema naaberarv peab jaguma mõne algarvuga, mida tegurite seas pole.

Korrutise ainus roll on jaguda kõigi vaadeldavate algarvudega, seega võib tema asemel kasutada nende algarvude suvalist ühiskordset. Kui algarvudeks on suuruselt mingi etteantud naturaalarvuga n tõkestatud algarvud, on selleks valikuks mitu käepärast valikut.

- Arvude 1 kuni n korrutis sisaldab teguritena kõik vaadeldavad algarvud ja on seega nende ühiskordne. Seda korrutist nimetatakse arvu n **faktoriaaliks** ja tähistatakse $n!$.

- Arvude 1 kuni n vähim ühiskordne $\operatorname{lcm}(1, 2, \ldots, n)$ on muuhulgas kõigi vaadeldavate algarvude ühiskordne.
- Suuruselt arvuga n tõkestatud algarvude korrutis jagub kõigi nende algarvudega ja on ühtlasi nende vähim ühiskordne, sest erinevad algarvud on ühistegurita. Seda korrutist nimetatakse arvu n **primoriaaliks** ja tähistatakse $n\sharp$.

Nende kolme funktsiooni väärtused väikestel positiivsetel täisarvudel on näidatud tabelis. Lihtsuse mõttes võtame $\operatorname{lcm}(1, 2, \ldots, n)$ jaoks kasutusele tähistuse n^*.

n	1	2	3	4	5	6	7
$n!$	1	2	6	24	120	720	5040
n^*	1	2	6	12	60	60	420
$n\sharp$	1	2	6	6	30	30	210

Ilmselt $n\sharp \mid n^*$ ja $n^* \mid n!$, millest järeldub ka $n\sharp \leqslant n^* \leqslant n!$. Seega piisab tõestada algarvude esinemistiheduse hinnang primoriaali suhtes, nagu kohe teemegi. Analoogilise hinnangu näiteks faktoriaali kaudu saab vajadusel vahetult järeldada. Hinnangud nende funktsioonidega on muidugi kõik äärmiselt jämedad ja sellisena ühtviisi praktiliselt kasutud.

Teoreem 1 *Olgu n positiivne täisarv, $n > 2$. Siis leidub algarv p, nii et $n < p < n\sharp$.*

Tõestus. Kuna $n \geqslant 3$ ja 3 on algarv, siis $3 \mid n\sharp$, kust $n\sharp \geqslant 3$. Seega arv $n\sharp - 1$ on suurem 1-st ja jagub mingi algarvuga p. Kui oleks $p \leqslant n$, siis jaguks algarvuga p ka arv $n\sharp$. See aga tähendaks, et $p \mid n\sharp - (n\sharp - 1) = 1$, mis pole võimalik. Järelikult $p > n$. Samas $p \mid n\sharp - 1$ annab $p \leqslant n\sharp - 1 < n\sharp$. Kokkuvõttes $n < p < n\sharp$. ■

Funktsiooni n^* väärtused erinevad primoriaalidest selle poolest, et iga algarv 1 ja n vahel esineb n^* kanoonilises esituses maksimaalsel astmel, milles see algarv esineb arvudes 1 kuni n. Primoriaalis on kõik need algarvud astmel 1. Teine võimalus arvu n^* avaldamiseks on korrutisena üle kõigi 1 ja n vahele jäävate algarvude astmete, kus teguriteks on vastavad algarvud. Sellises korrutises esineb iga algarv tegurina täpselt niimitu korda, milline on tema maksimaalne aste 1 ja n vahel, sest 1 ja n vahele jäävad ka selle algarvu kõik madalamad astmed. Näiteks $9^* = 2\cdot 3\cdot 2\cdot 5\cdot 7\cdot 2\cdot 3$, kus tegurid vastavad algarvude astmetele $2^1, 3^1, 2^2, 5^1, 7^1, 2^3, 3^2$ (nende esitamise järjestuses). Selle analoogia tõttu primoriaaliga ning tulenevalt asjaolust, et arvus n^* on rohkem tegureid kui primoriaalis, nimetame siin edaspidi arvu n^* arvu n **superprimoriaaliks** (aga see pole standardmõiste).

Eelteadmised binoomkordajatest

Tähistagu $\mathbb{N}$ kõigi naturaalarvude hulka (kuhu kuulub ka 0) ning $\mathbb{P}$ kõigi algarvude hulka. Kõigi positiivsete täisarvude hulka tähistagu $\mathbb{N}^+$.

Tšebõšovi teoreemi elegantne tõestus kasutab binoomkordajate omadusi. Nn **binoomkordajad** $\binom{n}{k}$, kus $n \in \mathbb{N}$ ja $k \in \mathbb{N}$, $k \leqslant n$, võib defineerida järgmiste tingimustega.

- Iga $n \in \mathbb{N}$ korral $\binom{n}{0} = \binom{n}{n} = 1$.
- Iga $n \in \mathbb{N}$ ja $k \in \mathbb{N}$, $0 < k < n$, korral
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Binoomkordajad moodustavad nn **Pascali kolmnurga**

$$\begin{array}{c}
1\\
1 \quad 1\\
1 \quad 2 \quad 1\\
1 \quad 3 \quad 3 \quad 1\\
1 \quad 4 \quad 6 \quad 4 \quad 1\\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1\\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1\\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1\\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1\\
1 \quad 9 \quad 36 \quad 84 \quad 126 \quad 126 \quad 84 \quad 36 \quad 9 \quad 1\\
1 \quad 10 \quad 45 \quad 120 \quad 210 \quad 252 \quad 210 \quad 120 \quad 45 \quad 10 \quad 1\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}$$

Järgmised kaks binoomkordajate põhiomadust on üldtuntud ja lihtsasti tõestatavad faktid.

Omadus 1 *Iga $n \in \mathbb{N}$ ja $k \in \mathbb{N}$, $k \leqslant n$, korral*
$$\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!}.$$

Tõestus. Väide kehtib $k = 0$ ja $k = n$ korral, ükskõik milline on n, sest $\binom{n}{0} = 1 = \frac{n!}{0!\cdot n!}$ ja $\binom{n}{n} = 1 = \frac{n!}{n!\cdot 0!}$. Ülejäänud juhud ($0 < k < n$) näitame induktsiooniga. Eeldades väite kehtivust $n-1$ korral, saame
$$\begin{aligned}
\binom{n}{k} &= \binom{n-1}{k-1} + \binom{n-1}{k}\\
&= \frac{(n-1)!}{(k-1)!\cdot(n-k)!} + \frac{(n-1)!}{k!\cdot(n-1-k)!}\\
&= \frac{(n-1)!\cdot k + (n-1)!\cdot(n-k)}{k!\cdot(n-k)!}\\
&= \frac{(n-1)!\cdot n}{k!\cdot(n-k)!}\\
&= \frac{n!}{k!\cdot(n-k)!}.
\end{aligned}$$
■

Omadus 2 *Iga $n \in \mathbb{N}$ ja $k \in \mathbb{N}$, $k \leqslant n$ korral*
$$\binom{n}{k} = \binom{n}{n-k}.$$

Tõestus. Et $k!\cdot(n-k)! = (n-k)!\cdot k!$, tuleneb väide omadusest 1. ■

Binoomkordaja esituse algarvude astmete korrutisena paneb paika Kummeri teoreem, mis omakorda põhineb Legendre'i valemil. Mõlemad on üldtuntud standardfaktid, tõestame järgmiseks ka need. Tähistagu $p \triangleright m$ algarvu p astendajat positiivse täisarvu m esituses algarvude astmete korrutisena, $n \bmod m$ jääki arvu n jagamisel arvuga m ning $|X|$ hulga X elementide arvu.

Teoreem 2 (Legendre'i valem) *Olgu n positiivne täisarv ja p algarv. Siis*
$$p \triangleright n! = \sum_{i\in\mathbb{N}^+} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Vormiliselt lõpmatu summa on sisuliselt lõplik, sest juhul $p^i > n$ on $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$ ja sellised on mingist kohast alates kõik liidetavad.

Tõestus. Ilmselt

$$p \triangleright n! = \sum_{\substack{k \in \mathbb{N} \\ 0 < k \leqslant n}} p \triangleright k.$$

Rühmitades liidetavad algarvu p astendajate kaupa (tähistame seda astendajat j-ga), saame

$$p \triangleright n! = \sum_{j \in \mathbb{N}} \sum_{\substack{k \in \mathbb{N} \\ 0 < k \leqslant n \\ p \triangleright k = j}} j = \sum_{j \in \mathbb{N}} j \cdot |\{k \in \mathbb{N} \;:\; 0 < k \leqslant n, p \triangleright k = j\}|.$$

Korrutamise j-ga võib samaväärselt asendada sama suuruse j-kordse liitmisega. Indekseerides selle asendussumma liidetavad arvudega $i = 1, \ldots, j$, võime kogusummat vaadelda kui suuruste $|\{k \in \mathbb{N} \;:\; 0 < k \leqslant n, p \triangleright k = j\}|$ liitmist kõigi selliste naturaalarvupaaride (i, j) jaoks, kus $0 < i \leqslant j$. Vahetades sobivalt liidetavate järjekorda, saame

$$\begin{aligned} p \triangleright n! &= \sum_{j \in \mathbb{N}} \sum_{\substack{i \in \mathbb{N}^+ \\ i \leqslant j}} |\{k \in \mathbb{N} \;:\; 0 < k \leqslant n, p \triangleright k = j\}| \\ &= \sum_{i \in \mathbb{N}^+} \sum_{\substack{j \in \mathbb{N} \\ j \geqslant i}} |\{k \in \mathbb{N} \;:\; 0 < k \leqslant n, p \triangleright k = j\}|. \end{aligned}$$

Et

$$\begin{aligned} \sum_{\substack{j \in \mathbb{N} \\ j \geqslant i}} |\{k \in \mathbb{N} \;:\; 0 < k \leqslant n, p \triangleright k = j\}| &= |\{k \in \mathbb{N} \;:\; 0 < k \leqslant n, p \triangleright k \geqslant i\}| \\ &= |\{k \in \mathbb{N} \;:\; 0 < k \leqslant n, p^i \mid k\}| \\ &= \left\lfloor \frac{n}{p^i} \right\rfloor, \end{aligned}$$

siis saamegi kokkuvõttes

$$p \triangleright n! = \sum_{i \in \mathbb{N}^+} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

■

Teoreem 3 (Kummeri teoreem) *Olgu n ja k naturaalarvud, $k \leqslant n$. Siis*

$$p \triangleright \binom{n}{k} = \left|\left\{i \in \mathbb{N}^+ \;:\; k \bmod p^i + (n-k) \bmod p^i \geqslant p^i\right\}\right|.$$

Sarnaselt Legendre'i valemile on ka siin tegu lõpliku astendajate hulgaga, sest kui $p^i > n$, siis $k \bmod p^i + (n-k) \bmod p^i = k + (n-k) = n < p^i$ ehk i ei kuulu vaadeldavasse hulka.

Tõestus. Omaduse 1 ja Legendre'i valemi põhjal

$$\begin{aligned} p \triangleright \binom{n}{k} &= p \triangleright \frac{n!}{k! \cdot (n-k)!} \\ &= p \triangleright n! - (p \triangleright k! + p \triangleright (n-k)!) \\ &= \sum_{i \in \mathbb{N}^+} \left\lfloor \frac{n}{p^i} \right\rfloor - \left(\sum_{i \in \mathbb{N}^+} \left\lfloor \frac{k}{p^i} \right\rfloor + \sum_{i \in \mathbb{N}^+} \left\lfloor \frac{n-k}{p^i} \right\rfloor \right) \\ &= \sum_{i \in \mathbb{N}^+} \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left(\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \right) \right). \end{aligned}$$

Iga $i \in \mathbb{N}^+$ korral

$$\begin{aligned} & p^i \cdot \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left(\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \right) \right) \\ &\quad = (n - n \bmod p^i) - ((k - k \bmod p^i) + ((n-k) - (n-k) \bmod p^i)) \\ &\quad = k \bmod p^i + (n-k) \bmod p^i - n \bmod p^i. \end{aligned}$$

Teame, et $0 \leqslant k \bmod p^i < p^i$ ja $0 \leqslant (n-k) \bmod p^i < p^i$, seega kehtivad võrratused $0 \leqslant k \bmod p^i + (n-k) \bmod p^i < 2p^i$, samas kui $0 \leqslant n \bmod p^i < p^i$.

Juhul, kui $0 \leqslant k \bmod p^i + (n-k) \bmod p^i < p^i$, kehtivad võrratused $-p^i < k \bmod p^i + (n-k) \bmod p^i - n \bmod p^i < p^i$, mistõttu ainsa võimalusena $p^i \cdot \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left(\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \right) \right) = 0$. Teisel juhul, kui selle asemel hoopis $p^i \leqslant k \bmod p^i + (n-k) \bmod p^i < 2p^i$, siis saame analoogiliselt võrratused $0 < k \bmod p^i + (n-k) \bmod p^i - n \bmod p^i < 2p^i$ ning ainsa võimalusena

$p^i \cdot \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left(\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \right) \right) = p^i$. Liidetav $\left\lfloor \frac{n}{p^i} \right\rfloor - \left(\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \right)$ on vastavalt kas 0 või 1. Nullide ja ühtede summa võrdub aga ühtede arvuga summas. Kokkuvõttes

$$\begin{aligned} p \triangleright \binom{n}{k} &= \sum_{i \in \mathbb{N}^+} \left\{ \begin{matrix} 1 & \text{kui } k \bmod p^i + (n-k) \bmod p^i \geqslant p^i \\ 0 & \text{kui } k \bmod p^i + (n-k) \bmod p^i < p^i \end{matrix} \right\} \\ &= \left| \{ i \in \mathbb{N}^+ \ : \ k \bmod p^i + (n-k) \bmod p^i \geqslant p^i \} \right| . \end{aligned}$$

■

Kummeri teoreemi sõnastatakse tihti siin toodust erinevalt: $p \triangleright \binom{n}{k}$ võrdub ülekannete arvuga k ja $n-k$ liitmisel arvusüsteemis alusel p. See sõnastus on ülaltooduga samaväärne, sest liitmisel tekib ülekanne parajasti neisse järguühikutesse, kus madalamatest järkudest moodustatud arvude (aga need on parajasti liidetavate jäägid jagamisel jooksva järguühikuga p^i) summa on vähemalt niisama suur kui jooksev järguühik (ehk p^i).

Kui seni esitatud faktid on kõik standardteadmised, siis järgnevalt tõestame mitte nii tuntud lemma, mis sätestab alumise ja ülemise suurushinnangu binoomkordajale $\binom{2n}{n}$.

Lemma 1 *Iga naturaalarvu $n \geqslant 5$ korral $\frac{4^n}{n} < \binom{2n}{n} < 4^{n-1}$.*

Tõestus. Juhul $n = 5$ saame võrratused $\frac{4^5}{5} < 252 < 4^4$, mis kehtivad. Valime suvalise n ja eeldame väite kehtivust $n-1$ jaoks. Omaduse 1 põhjal $\binom{2n}{n} = \binom{2(n-1)}{n-1} \cdot \frac{(2n-1)\cdot 2n}{n \cdot n} = \binom{2(n-1)}{n-1} \cdot 4 \cdot \frac{n-\frac{1}{2}}{n}$. Seega

$$\binom{2n}{n} > \frac{4^{n-1}}{n-1} \cdot 4 \cdot \frac{n-\frac{1}{2}}{n} = \frac{4^n}{n} \cdot \frac{n-\frac{1}{2}}{n-1} > \frac{4^n}{n}$$

ja

$$\binom{2n}{n} < 4^{n-2} \cdot 4 \cdot \frac{n-\frac{1}{2}}{n} = 4^{n-1} \cdot \frac{n-\frac{1}{2}}{n} < 4^{n-1}.$$

■

Superprimoriaali omadused

Sissejuhatuses sai mainitud faktoriaali, primoriaali ja superprimoriaali, samuti nende omavahelist suurusvahekorda: superprimoriaal kasvab kiiremini kui primoriaal ja faktoriaal omakorda superprimoriaalist kiiremini. Tšebõšovi teoreemi tõestamisel mängib tähtsat rolli superprimoriaali kasvukiirus, täpsemalt selle ülemine hinnang.

Mõneti üllatavalt osutub superprimoriaal väga oluliselt aeglasemalt kasvavaks funktsiooniks kui faktoriaal. Faktoriaali jaoks on lihtne tõestada induktsiooniga hinnang $n! > \left(\frac{n}{4}\right)^n$, mõninga kõrgema matemaatika kaasabil ka tugevam hinnang $n! > \left(\frac{n}{\mathrm{e}}\right)^n$. See näitab, et faktoriaal kasvab kiiremini igast eksponentfunktsioonist (sulgude avamisel tuleb lugejasse n^n). Kuid leidub eksponentfunktsioone, mis kasvavad superprimoriaalist kiiremini.

Teoreem 4 *Iga $n \in \mathbb{N}^+$ korral $n^* < \frac{4^n}{n}$.*

Tõestus. Läbivaatus näitab, et väide kehtib, kui $n \in \{1, 3, 5, 7\}$, millest saame induktsiooni baasi. Tõestame nüüd väite suvalise muu n jaoks.

Olgu algul $n = 2k$, $k \geqslant 1$, ja eeldame väite kehtivust $n-1$ korral. Kui n ei ole algarvu aste, siis $n^* = (n-1)^*$. Vastasel korral saab n olla ainult 2 aste, mistõttu $n^* = 2 \cdot (n-1)^*$. Igal juhul saame

$$n^* \leqslant 2 \cdot (n-1)^* < 2 \cdot \frac{4^{n-1}}{n-1} = \frac{4^n}{2(n-1)} \leqslant \frac{4^n}{n},$$

kus viimane võrratus kehtib seetõttu, et $n \geqslant 2 \Rightarrow 2(n-1) \geqslant n$.

Olgu nüüd $n = 2k-1$, $k \geqslant 5$, ja eeldame väite kehtivust k korral. Superprimoriaali omadustest

$$(2k-1)^* = k^* \cdot \prod_{\substack{p \in \mathbb{P} \\ i \in \mathbb{N}^+ \\ k < p^i \leqslant 2k-1}} p.$$

Kummeri teoreemist järeldub, et kui $k < p^i \leqslant 2k-1$, siis $p \mid \binom{2k-1}{k}$, sest $k \bmod p^i + (k-1) \bmod p^i = k + (k-1) = 2k-1 \geqslant p^i$, mistõttu p astmete hulk teoreemi väites on mittetühi. Et hulk $\{k+1,\ldots,2k-1\}$ sisaldab iga algarvu p jaoks ülimalt ühe tema astme, siis ka

$$\prod_{\substack{p\in\mathbb{P}\\ i\in\mathbb{N}^+\\ k<p^i\leqslant 2k-1}} p \mid \binom{2k-1}{k}.$$

Arvestades, et omaduse 2 põhjal $\binom{2k-1}{k}=\binom{2k-1}{k-1}$, saame

$$\binom{2k-1}{k}=\frac{\binom{2k-1}{k-1}+\binom{2k-1}{k}}{2}=\frac{\binom{2k}{k}}{2}.$$

Induktsiooni eelduse ja lemma 1 põhjal järelikult

$$n^*\leqslant k^*\cdot\frac{\binom{2k}{k}}{2}<\frac{4^k}{k}\cdot\frac{4^{k-1}}{2}=\frac{4^n}{2k}<\frac{4^n}{n}.$$

■

Äsja nähtud tõestuses mängis olulist rolli superprimoriaali tegurite n-ö ülemise poole osav ja nutikas hindamine läbi binoomkordaja. Kuid superprimoriaali seob binoomkordajaga ka otseselt järgmine fakt algarvude astendajate suurusvahekorrast.

Teoreem 5 *Olgu n ja k naturaalarvud, $n\geqslant k$. Siis iga algarvu p korral $p\rhd\binom{n}{k}\leqslant p\rhd n^*$.*

Tõestus. Kummeri teoreemi põhjal

$$\begin{aligned}
p\rhd\binom{n}{k} &= |\{i\in\mathbb{N}^+ \;:\; k \bmod p^i+(n-k)\bmod p^i\geqslant p^i\}|\\
&\leqslant |\{i\in\mathbb{N}^+ \;:\; p^i\leqslant n\}|\\
&= \max\nolimits_{\substack{i\in\mathbb{N}^+\\ p^i\leqslant n}} i\\
&= p\rhd n^*.
\end{aligned}$$

■

Selle teoreemi väitest järeldub otseselt fakt, et algarvude astmed binoomkordaja kanoonilises esituses on tõkestatud binoomkordaja ülemise arvuga, st $p^{p\rhd\binom{n}{k}}\leqslant n$. Veel saab seda väidet samaväärselt väljendada jaguvusega $\binom{n}{k}\mid n^*$. Siit tuleneb ka superprimoriaali alumine suurushinnang keskmise (Pascali kolmnurga rea suurima) binoomkordaja kaudu: $n^*\geqslant\binom{n}{\lfloor\frac{n}{2}\rfloor}$. Neid toredaid fakte aga Tšebõševi teoreemi tõestamisel otseselt vaja ei ole.

Tšebõšovi teoreem

Tšebõšovi teoreemi tõestamiseks kombineeritakse jälle kord superprimoriaali ja binoomkordajate omadusi. Väitevastasest oletusest järeldatakse võrratus, mis kehtib ainult lõpliku arvu väikeste arvude korral, nende jaoks aga tõestatakse teoreem vahetu läbivaatusega.

Teoreem 6 (Tšebõšovi teoreem) *Iga $n\in\mathbb{N}^+$ korral leidub algarv p, nii et $n<p\leqslant 2n$.*

Tõestus. Kummeri teoreemist saame, et kui $n>2$ ja algarv p rahuldab võrratusi $\frac{2n}{3}<p\leqslant n$, siis $p\rhd\binom{2n}{n}=0$. Tõepoolest, sellisel juhul $n\geqslant p$, kuid $n-p\leqslant n-\frac{2n}{3}=\frac{n}{3}\leqslant\frac{1}{2}\cdot\frac{2n}{3}<\frac{p}{2}<p$, mistõttu $n \bmod p=n-p<\frac{p}{2}$, kust saame $n \bmod p+n \bmod p<p$ ehk p^1 ei panusta arvu $p\rhd\binom{2n}{n}$. Algarvu p kõrgemad astmed on aga suuremad kui $2n$ ega panusta samuti arvu $p\rhd\binom{2n}{n}$.

Oletame väitevastaselt, et ei leidu algarvu p, mille korral $n<p\leqslant 2n$. Eelneva põhjal jagub $\binom{2n}{n}$ ainult algarvudega, mis pole suuremad kui $\left\lfloor\frac{2n}{3}\right\rfloor$. Iga sellise algarvu $p\geqslant 3$ korral $p\rhd(2n)^*\leqslant p\rhd\left\lfloor\frac{2n}{3}\right\rfloor^*+1$, sest vahemikus $\left\lfloor\frac{2n}{3}\right\rfloor+1,\ldots,2n$ leidub ülimalt üks algarvu p aste. Analoogiliselt saame $2\rhd(2n)^*\leqslant 2\rhd\left\lfloor\frac{2n}{3}\right\rfloor^*+2$. Kui aga $p>\sqrt{2n}$, siis $p\rhd(2n)^*=p\rhd\left\lfloor\frac{2n}{3}\right\rfloor^*$, sest sellise algarvu p astmeid vahemikus $\left\lfloor\frac{2n}{3}\right\rfloor+1,\ldots,2n$ ei ole. Kasutades teoreemi 5, saame kokkuvõttes

$$\binom{2n}{n} = \prod_{\substack{p\in\mathbb{P}\\ p\leqslant\left\lfloor\frac{2n}{3}\right\rfloor}} p^{p\triangleright\binom{2n}{n}} \leqslant \prod_{\substack{p\in\mathbb{P}\\ p\leqslant\left\lfloor\frac{2n}{3}\right\rfloor}} p^{p\triangleright(2n)^*} \leqslant \left\lfloor\frac{2n}{3}\right\rfloor^* \cdot \left\lfloor\sqrt{2n}\right\rfloor\sharp\cdot 2.$$

Teoreemi 4 põhjal (millega saab mõistagi hinnata ka primoriaali) aga $\left\lfloor\frac{2n}{3}\right\rfloor^* < \frac{4^{\left\lfloor\frac{2n}{3}\right\rfloor}}{\left\lfloor\frac{2n}{3}\right\rfloor}$ ja $\left\lfloor\sqrt{2n}\right\rfloor\sharp < \frac{4^{\left\lfloor\sqrt{2n}\right\rfloor}}{\left\lfloor\sqrt{2n}\right\rfloor}$, samas kui lemmast 1 järeldub $n\geqslant 5$ jaoks $\frac{4^n}{n} < \binom{2n}{n}$. Kokkuvõttes

$$\frac{4^n}{n} < \binom{2n}{n} < \frac{4^{\left\lfloor\frac{2n}{3}\right\rfloor}}{\left\lfloor\frac{2n}{3}\right\rfloor}\cdot\frac{4^{\left\lfloor\sqrt{2n}\right\rfloor}}{\left\lfloor\sqrt{2n}\right\rfloor}\cdot 2,$$

kust $4^n\cdot\frac{\left\lfloor\frac{2n}{3}\right\rfloor\cdot\left\lfloor\sqrt{2n}\right\rfloor}{2n} < 4^{\left\lfloor\frac{2n}{3}\right\rfloor+\left\lfloor\sqrt{2n}\right\rfloor}$.

Kui $n\geqslant 8$, siis $\left\lfloor\sqrt{2n}\right\rfloor \geqslant 4 > 3\cdot\frac{n}{n-1} = \frac{2n}{\frac{2n-2}{3}} > \frac{2n}{\left\lfloor\frac{2n}{3}\right\rfloor}$. Seetõttu $\frac{\left\lfloor\frac{2n}{3}\right\rfloor\cdot\left\lfloor\sqrt{2n}\right\rfloor}{2n} > 1$ ja eelneva põhjal $4^n < 4^{\left\lfloor\frac{2n}{3}\right\rfloor+\left\lfloor\sqrt{2n}\right\rfloor}$ ehk kehtib võrratus $n < \left\lfloor\frac{2n}{3}\right\rfloor + \left\lfloor\sqrt{2n}\right\rfloor$.

Kuid juhul $n\geqslant 18$ kehtib võrratus $\frac{2n}{\left\lfloor\sqrt{2n}\right\rfloor}\geqslant\left\lfloor\sqrt{2n}\right\rfloor\geqslant 6$, mille tõttu $n-\left\lfloor\frac{2n}{3}\right\rfloor\geqslant\frac{n}{3}\geqslant\left\lfloor\sqrt{2n}\right\rfloor$. See on vastuolus võrratusega $n < \left\lfloor\frac{2n}{3}\right\rfloor + \left\lfloor\sqrt{2n}\right\rfloor$. Sellega on näidatud Tšebõšovi teoreemi väite kehtivus $n\geqslant 18$ korral. Arvude $n < 18$ jaoks nähtub väite kehtivus tabelist.

n	Algarv p, $n<p\leqslant 2n$	n	Algarv p, $n<p\leqslant 2n$	n	Algarv p, $n<p\leqslant 2n$
1	2	7	11, 13	13	17, 19, 23
2	3	8	11, 13	14	17, 19, 23
3	5	9	11, 13, 17	15	17, 19, 23, 29
4	5, 7	10	11, 13, 17, 19	16	17, 19, 23, 29, 31
5	7	11	13, 17, 19	17	19, 23, 29, 31
6	7, 11	12	13, 17, 19, 23		

■

Järelsõna

Siin esitatuga sarnane tõestus ilmus esmakordselt ungari matemaatiku Paul Erdősi (1913–1996) sensatsioonilises artiklis aastal 1932. Noor Erdős, ise siis vaid 19-aastane, oli suutnud kummutada peaaegu sajandi püsinud eksiarvamuse, et sel teoreemil puudub elementaarne tõestus. Niisiis isegi võrdlemisi lihtsad tõestused võivad teinekord aastasadade suurimate matemaatikute ees peitu jääda, et saada avastatud mõne nutika noore poolt. Lootust on!