LUNDS UNIVERSITET

Matematikcentrum

Matematik NF

Bertrands postulat

Kjell Elfström

Bertrands postulat är satsen, som säger, att om $n > 3$ är ett heltal, så finns det ett primtal p, sådant att $n < p < 2n - 2$. Påståendet, som var ett förmodande från 1845 av den franske matematikern Joseph Bertrand, bevisades 1850 av den ryske matematikern Pafnutij Tjebysjov. Det bevis, som presenteras här, överensstämmer i allt väsentligt med det elementära bevis, som den ungerske matematikern Paul Erdős lät publicera 1932 [1].

Några olikheter

Lemma 1 Det gäller att

$$\frac{2^x}{x^2-1} > x^{\sqrt{x}} 2^{\frac{2x}{3}}, \quad x \geq 1024.$$

Bevis Det räcker att visa att

$$\frac{2^x}{x^2} > x^{\sqrt{x}} 2^{\frac{2x}{3}}, \quad x \geq 1024,$$

och denna olikhet är ekvivalent med

$$f(x) = x \ln 2 - 2 \ln x - \sqrt{x} \ln x - \frac{2x \ln 2}{3} > 0, \quad x \geq 1024.$$

Derivation ger att

$$f'(x) = \frac{\ln 2}{3} - \frac{2}{x} - \frac{2 + \ln x}{2\sqrt{x}},$$

och att

$$f''(x) = \frac{2}{x^2} + \frac{\ln x}{4x\sqrt{x}}.$$

Eftersom $f''(x) \geq 0$ då $x \geq 1$, är f' växande på intervallet $[1, \infty)$. Eftersom

$$f'(1024) = \frac{\ln 2}{3} - \frac{2}{1024} - \frac{2 + \ln 1024}{2\sqrt{1024}} = \frac{17 \ln 2}{96} - \frac{17}{512} = \frac{17}{96}\left(\ln 2 - \frac{3}{16}\right) \geq 0,$$

så är f växande på $[1024, \infty)$. Av att

$$f(1024) = 1024 \ln 2 - 2 \ln 1024 - \sqrt{1024} \ln 1024 - \frac{2048 \ln 2}{3} = \frac{4 \ln 2}{3} > 0$$

följer det slutligen att $f(x) > 0$ då $x \geq 1024$. ■

Sats 1 Det gäller att

$$\frac{4^n}{4n^2-1} > (2n)^{\sqrt{2n}} \cdot 4^{\frac{2n}{3}}, \quad n \geq 512.$$

Bevis Påståendet följer, om vi sätter $x = 2n$ i lemma 1. ■

Sats 2 Om $n > 5$, så gäller det att

$$\frac{2n}{3} > \sqrt{2n}.$$

Bevis Eftersom $n > 5$, så är $4n > 20 > 18$. Detta ger att $4n^2 > 18n$, varav

$$\frac{(2n)^2}{3^2} > 2n. ■$$

Den centrala binomialkoefficienten

Lemma 2 Om k och n är naturliga tal, och $0 \leq k \leq 2n$, så gäller det att

$$\binom{2n}{k} \leq \binom{2n}{n}.$$

Bevis På grund av symmetri räcker det att visa påståendet, då $0 \leq k \leq n$. Påståendet är då ekvivalent med

$$(n!)^2 \leq (2n-k)!\,k!,$$

vilket i sin tur är ekvivalent med

$$\frac{n!}{k!} \leq \frac{(2n-k)!}{n!}.$$

Denna olikhet kan skrivas

$$n(n-1)\cdots(n-(n-k-1)) \leq (2n-k)(2n-k-1)\cdots(2n-k-(n-k-1))$$

och är giltig, ty $(n-i) \leq (2n-k-i)$, då $i = 0, \ldots, n-k-1$. ■

Sats 3 Det gäller att

$$\binom{2n}{n} \geq \frac{4^n}{2n+1}, \quad n \in \mathbf{N}.$$

Bevis Det gäller enligt binomialsatsen och lemma 2, att

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

Exponenter

Definition 1 Om p är ett primtal och n ett positivt heltal, definierar vi exponenten $\ell_p(n)$ av p i n som det största naturliga tal k, för vilket $p^k \mid n$.

Lemma 3 Om m och n är positiva heltal, så gäller det att $\ell_p(mn) = \ell_p(m) + \ell_p(n)$, och om $m \mid n$, att $\ell_p(n/m) = \ell_p(n) - \ell_p(m)$.

Bevis Påståendet följer av aritmetikens fundamentalsats. ■

Följande sats bevisades 1808 av Adrien-Marie Legendre [2].

Sats 4 Om n är ett naturligt tal och p ett primtal, så är

$$\ell_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

Bevis Vi noterar att

$$\left\lfloor \frac{n}{p^k} \right\rfloor = |\{j \in \mathbf{Z};\ 1 \le j \le n,\ p^k \mid j\}|.$$

Definiera för $k \in \mathbf{Z}_+$ funktionen $f_k : \mathbf{Z}_+ \to \{0,1\}$ genom

$$f_k(j) = \begin{cases} 1 & \text{om } p^k \mid j, \\ 0 & \text{annars.} \end{cases}$$

Då är

$$\ell_p(j) = \sum_{k=1}^{\infty} f_k(j).$$

Vi kan nu genomföra beviset av satsen med induktion över n. Då $n = 0$, är påståendet trivialt sant. Antag att likheten gäller, då $n = m$. Då är, enligt lemma 3,

$$\begin{aligned} \ell_p((m+1)!) = \ell_p(m!) + \ell_p(m+1) &= \sum_{k=1}^{\infty} \left\lfloor \frac{m}{p^k} \right\rfloor + \sum_{k=1}^{\infty} f_k(m+1) \\ &= \sum_{k=1}^{\infty} \left(\left\lfloor \frac{m}{p^k} \right\rfloor + f_k(m+1) \right) \\ &= \sum_{k=1}^{\infty} \Big(|\{j \in \mathbf{Z};\ 1 \le j \le m,\ p^k \mid j\}| + f_k(m+1) \Big) \\ &= \sum_{k=1}^{\infty} |\{j \in \mathbf{Z};\ 1 \le j \le m+1,\ p^k \mid j\}| = \sum_{k=1}^{\infty} \left\lfloor \frac{m+1}{p^k} \right\rfloor . \ \blacksquare \end{aligned}$$

Summan i satsen innehåller bara ändligt många termer skilda från noll. Om $n \in \mathbf{Z}_+$, kan vi låta k löpa från 1 till $\lfloor \log_p n \rfloor$.

Lemma 4 Om n är ett naturligt tal och p ett primtal, så gäller det att

$$0 \le \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \le 1.$$

Bevis Det gäller enligt divisionsalgoritmen, att det finns ett heltal r, sådant att

$$n = \left\lfloor \frac{n}{p^k} \right\rfloor p^k + r, \quad 0 \le r < p^k.$$

Det följer att

$$2n = 2 \left\lfloor \frac{n}{p^k} \right\rfloor p^k + 2r, \quad 0 \le 2r < 2p^k,$$

varav

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor = \begin{cases} 0 & \text{om } 2r < p^k, \\ 1 & \text{om } 2r \ge p^k. \ \blacksquare \end{cases}$$

Sats 5 Om n är ett positivt heltal och p ett primtal, så är

$$\ell_p\left(\binom{2n}{n}\right) \le \log_p 2n.$$

Om $p > \sqrt{2n}$, så är

$$\ell_p\left(\binom{2n}{n}\right) = \left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor \le 1.$$

Bevis Enligt lemma 3, sats 4 och lemma 4 är

$$\begin{aligned}
\ell_p\left(\binom{2n}{n}\right) &= \ell_p((2n)!) - 2\ell_p(n!) = \sum_{k=1}^{\lfloor \log_p 2n \rfloor} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor \\
&= \sum_{k=1}^{\lfloor \log_p 2n \rfloor} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right) \le \lfloor \log_p 2n \rfloor \le \log_p 2n.
\end{aligned}$$

Det andra påståendet i satsen följer av lemma 4 och det faktum att

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor = 0,$$

om $k > 1$ och $p > \sqrt{2n}$. ■

Primultet

Definition 2 Om n är ett naturligt tal, definierar vi n-primultet som

$$n\# = \prod p,$$

där p genomlöper mängden av primtal, som är mindre än eller lika med n. Enligt de vanliga konventionerna för produkter är $0\# = 1\# = 1$.

Lemma 5 Om n är ett naturligt tal, så gäller det att

$$\prod_{n+2 \le p \le 2n+1} p \le \binom{2n+1}{n},$$

där produkten är över primtal p.

Bevis Om produkten är tom, är olikheten uppfylld. I annat fall delar vart och ett av de ingående primtalen högerledet, vilket därför också delas av deras produkt. ■

Lemma 6 Om n är ett naturligt tal, så gäller det att

$$\binom{2n+1}{n} \le 4^n.$$

Bevis Påståendet följer av att

$$2\binom{2n+1}{n} = \binom{2n+1}{n} + \binom{2n+1}{n+1} \le \sum_{k=0}^{2n+1} \binom{2n+1}{k} = 2^{2n+1} = 2 \cdot 4^n. \blacksquare$$

Sats 6 Om n är ett naturligt tal, så gäller det att

$$n\# \leq 4^n.$$

Bevis Vi bevisar påståendet med induktion över n. Då $0 \leq n \leq 2$, finner man att olikheten är uppfylld genom uträkning. Antag att $m \geq 3$, och att olikheten gäller, då $n < m$. Om m är ett jämnt tal, så är m inte ett primtal, och man får att

$$m\# = (m-1)\# \leq 4^{m-1} \leq 4^m$$

enligt induktionsantagandet. Antag att $m = 2k+1$ är udda. Då är

$$\begin{aligned} m\# = (2k+1)\# &= \prod_{p \leq 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right) = (k+1)\# \prod_{k+2 \leq p \leq 2k+1} p \\ &\leq 4^{k+1} \binom{2k+1}{k} \leq 4^{k+1} \cdot 4^k = 4^m \end{aligned}$$

enligt induktionsantagandet och lemma 5 och 6. ■

Bertrands postulat

Sats 7 Om $n > 3$ är ett heltal, så finns det ett primtal p, sådant att $n < p < 2n - 2$.

Bevis Vi bevisar först påståendet, då $n \geq 512$. Då gäller det enligt sats 2, att

$$\sqrt{2n} < \frac{2n}{3} < 2n - 1.$$

Om p är ett primtal, och

$$\frac{2n}{3} < p \leq n,$$

gäller det därför enligt sats 5, att

$$0 \leq \ell_p \left(\binom{2n}{n} \right) = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \leq 2 - 2 = 0.$$

Det följer att p inte delar

$$\binom{2n}{n}.$$

Om primtalet p delar denna centrala binomialkoefficient, så gäller det att $p \mid (2n)!$, och därför att $p \mid k$ för något heltal k, sådant att $1 \leq k \leq 2n$. Eftersom $2n$ inte är ett primtal, så gäller det att $p < 2n$.

Antag nu att det inte finns något primtal p, sådant att $n < p < 2n-2$. Om primtalet p delar binomialkoefficienten, så gäller det då att

$$p \leq \frac{2n}{3} \quad \text{eller} \quad p = 2n - 1,$$

eftersom inte heller $2n - 2$ är ett primtal. Om $p = 2n - 1$ är ett primtal, så är självklart

$$\ell_p \left(\binom{2n}{n} \right) \leq 1.$$

Vi får därför att

$$\binom{2n}{n} = \prod p^{\ell_p(\binom{2n}{n})} \leq \left(\prod_{p \leq \sqrt{2n}} p^{\ell_p(\binom{2n}{n})} \right) \left(\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\ell_p(\binom{2n}{n})} \right) (2n-1).$$

Enligt sats 5 är

$$\prod_{p \leq \sqrt{2n}} p^{\ell_p(\binom{2n}{n})} \leq \prod_{p \leq \sqrt{2n}} (2n) \leq (2n)^{\sqrt{2n}},$$

eftersom antalet primtal p, sådana att $p \leq \sqrt{2n}$, inte överstiger $\sqrt{2n}$. Enligt samma sats gäller det att

$$\ell_p\left(\binom{2n}{n}\right) \leq 1,$$

om $p > \sqrt{2n}$. Därför är

$$\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\ell_p(\binom{2n}{n})} \leq \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p \leq \prod_{p \leq \frac{2n}{3}} p = \left\lfloor \frac{2n}{3} \right\rfloor \# \leq 4^{\lfloor \frac{2n}{3} \rfloor} \leq 4^{\frac{2n}{3}}$$

enligt sats 6. Vi får alltså, att

$$\binom{2n}{n} \leq (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}} (2n-1),$$

och om vi kombinerar detta med sats 3, får vi

$$\frac{4^n}{4n^2-1} \leq (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}}.$$

Eftersom detta strider mot sats 1, har vi visat påståendet i satsen, då $n \geq 512$.

Det återstår att visa påståendet, då $4 \leq n \leq 511$. Betrakta följden

$$(p_k)_{k=0}^{10} = (4, 5, 7, 11, 19, 31, 59, 113, 223, 443, 883),$$

i vilken alla element utom p_0 är primtal. Det gäller att $p_{k+1} < 2p_k - 2$, då $k = 0, 1, \ldots, 9$. Om $4 \leq n \leq 511$, väljer vi k, så att $p_k \leq n < p_{k+1}$. Då är $2n - 2 \geq 2p_k - 2 > p_{k+1}$, och vi finner, att det för primtalet p_{k+1} gäller, att $n < p_{k+1} < 2n - 2$. ■

Det var i själva verket följande något mer eleganta men svagare sats, som bevisades av Erdős.

Korollarium 1 Låt n vara ett positivt heltal. Då finns det ett primtal p, sådant att $n < p \leq 2n$.

Bibliografi

[1] Erdős, P., Beweis eines Satzes von Tschebyschef, *Acta Sci. Math. (Szeged)* 5 (1930–1932), 194–198.

[2] Legendre, A. M., *Essai sur la théorie des nombres (2e éd.)*. Paris, 1808.