Test na prvočíselnost

Dáno přirozené číslo $N > 1$, o kterém jsme testem Millera a Rabina zjistili, že N je asi prvočíslo. Můžeme také předpokládat, že víme, že N není dělitelné malými prvočísly. Test na prvočíselnost má dokázat, že N skutečně prvočíslem je, anebo to vyvrátit.

Známe už $N - 1$ test Pocklingtona a Lehmera. Ten pracuje dobře, pokud jsme schopni dostatečně rozložit číslo $N - 1$. Pokud však neexistuje dost velký dělitel $F|N - 1$, který jsme schopni rozložit na prvočinitele, tato metoda neuspěje. Pak můžeme ještě zkusit $N + 1$ test, ten však vyžaduje rozložit dost velkého dělitele čísla $N + 1$, což se však často také nemusí podařit a skončíme nezdarem.

Řešení nabízí teorie eliptických křivek: je-li N skutečně prvočíslo, máme spoustu eliptických křivek nad $\mathbb{Z}_N$. Jejich řády jsou rovny přirozeným číslům v intervalu $(N + 1 - \sqrt{N}, N + 1 + \sqrt{N})$. Je pravděpodobné, že nezanedbatelnou část z těchto čísel budeme schopni rozložit na prvočinitele.

Síla metody eliptických křivek je v jejich počtu: pokud nevyhovuje několik konkrétních křivek, nevadí, vezmeme další.

Opakování $N-1$ testu Pocklingtona a Lehmera

Předpokládáme, že známe prvočíslo p dělící $N-1$, přitom p^{α_p} je nejvyšší mocnina p dělící $N-1$.
Dále označme d libovolné neznámé prvočíslo dělící N.
Máme homomorfismus okruhů $f : \mathbb{Z}_N \to \mathbb{Z}_d$, kde $f([a]_N) = [a]_d$ pro každé $a \in \mathbb{Z}$. Homomorfismus f je dobře definován, neboť $d \mid N$. Protože je d prvočíslo, je druhý okruh těleso $\mathbb{F}_d = \mathbb{Z}_d$.
Předpokládáme existenci $a_p \in \mathbb{Z}$, které splňuje

$$a_p^{N-1} \equiv 1 \pmod{N} \quad \text{a} \quad (a_p^{\frac{N-1}{p}} - 1, N) = 1.$$

Označme $b = f([a_p]_N) \in \mathbb{F}_d$. Pak $b^{N-1} = 1$, $b^{\frac{N-1}{p}} \neq 1$, a tedy řád prvku b je dělitelný p^{α_p}, odkud $p^{\alpha_p} \mid |\mathbb{F}_d^\times| = d-1$, tedy $d \equiv 1 \pmod{p^{\alpha_p}}$. Získali jsme tím informaci o neznámém d.

Klíčem k úspěchu zde byl homomorfismus $f : \mathbb{Z}_N \to \mathbb{Z}_d$.
Přestože jsme neznali d, a tedy nebyli schopni v $\mathbb{Z}_d$ pracovat, počítali jsme ve známém okruhu $\mathbb{Z}_N$ a výsledky výpočtů jsme do $\mathbb{Z}_d$ zobrazili homomorfismem f.

Test na prvočíselnost pomocí eliptických křivek

Přejděme k eliptickým křivkám, opět d značí libovolné neznámé prvočíslo dělící dané N, $(N, 6) = 1$. Zvolme libovolně $a, b \in \mathbb{Z}$ taková, že $(4a^3 + 27b^2, N) = 1$. Rovnice $y^2z = x^3 + axz^2 + bz^3$ nám dává „eliptickou křivku“ $\mathcal{E}_N$, na níž máme definovánu částečnou operaci, a eliptickou křivku $\mathcal{E}_d$, což je komutativní grupa. Z Hasseho věty víme, že $||\mathcal{E}_d| - d - 1| < 2\sqrt{d}$.
Přestože v $\mathcal{E}_d$ nejsme schopni počítat (vždyť neznáme d), máme částečný homomorfismus $f : \mathcal{E}_N \to \mathcal{E}_d$, kterým můžeme výpočet provedený v $\mathcal{E}_N$ zobrazit do $\mathcal{E}_d$. Víme, že $f([[0]_N, [1]_N, [0]_N]) = O$ a že pro libovolný $P = [[u]_N, [v]_N, [1]_N] \in \mathcal{E}_N$ platí $f(P) \neq O$.
Je-li q prvočíslo a bod $P = [[u]_N, [v]_N, [1]_N] \in \mathcal{E}_N$ takový, že máme definované $q \cdot P = P + P + \cdots + P = [[0]_N, [1]_N, [0]_N]$, pak řád bodu $f(P)$ v grupě $\mathcal{E}_d$ je q, a tedy $(\sqrt{d} + 1)^2 > |\mathcal{E}_d| \geq q$.
Najdeme-li takový bod P pro prvočíslo $q > (\sqrt[4]{N} + 1)^2$, plyne odtud $d > \sqrt{N}$, a tedy N je prvočíslo.

Problém je, jak volit čísla a, b a jak najít prvočíslo q a bod $P \in \mathcal{E}_N$ s potřebnými vlastnostmi...

Goldwasser - Kilian, 1986

Řešení navržené Goldwasserem a Kilianem má spíše teoretický význam; je možné dokázat, že platí-li jistá hypotéza o rozložení prvočísel v krátkých intervalech, pak očekávaný čas výpočtu je $O(\ln^{12} N)$, tedy polynomiální.

Existuje algoritmus Schoofa, který pro prvočíslo p počítá řád (tj. počet bodů) dané eliptické křivky nad $\mathbb{F}_p$ v čase $O(\ln^8 p)$.

Zvolíme náhodně a, $b \in \mathbb{Z}$ tak, aby $(4a^3 + 27b^2, N) = 1$. Pomocí Schoofova algoritmu určíme pro křivku $(\mathcal{E}, O)$ určenou rovnicí $y^2 = x^3 + ax + b$ a pro $p = N$ její řád m (jestliže N není prvočíslo, nemá m žádný význam). Získané m zkoušíme dělit malými prvočísly s nadějí, že poté, co odstraníme malé faktory, zůstane nám $q > (\sqrt[4]{N} + 1)^2$, $q < \frac{N}{2}$, o kterém test Millera a Rabina zjistí, že q je asi prvočíslo. Pokud se nám to nepodaří, začneme znovu s jinými a, $b \in \mathbb{Z}$.

Existuje algoritmus, který pro prvočíslo p a celé číslo e hledá v čase $O(\ln^4 p)$ řešení kongruence $x^2 \equiv e \pmod p$ a to, že takové řešení neexistuje, zjistí dokonce v čase $O(\ln^2 p)$.

Goldwasser - Kilian, 1986, pokračování

Najdeme bod P na křivce: náhodně zvolíme $c \in \mathbb{Z}_N$ a hledáme $d \in \mathbb{Z}_N$ tak, aby $d^2 = c^3 + ac + b$ (jde o kongruenci modulo N; d hledáme jako by bylo N prvočíslo, pak uděláme zkoušku, pokud nevyjde, nebylo N prvočíslo a jsme zcela hotovi). Neexistuje-li takové d, zkusíme jiné c. Pak za P zvolíme $\frac{m}{q}$-násobek bodu $[c, d, 1]$ v $(\mathcal{E}, +)$. Je-li $P = [0, 1, 0]$, zvolíme jiné c atd. Je-li $P \neq [0, 1, 0]$, pak platí $P = [x, y, 1]$ pro nějaké x, $y \in \mathbb{Z}_N$. Spočítáme q-násobek bodu P v $(\mathcal{E}, +)$. Není-li definován, našli jsme netriviálního dělitele čísla N. Jestliže nedostaneme $[0, 1, 0]$, není m řád křivky $(\mathcal{E}, O)$, Schoofův algoritmus tedy nedal správný výsledek a proto N není prvočíslo. Jestliže q-násobek bodu P je $[0, 1, 0]$, pak je N prvočíslo, pokud q je prvočíslo. To zjistíme rekurzívně ($N_0 = N$, N_1 je q pro N_0, N_2 je q pro N_1, ...). S rekurzí skončíme v okamžiku, kdy N_i je dost malé na to, abychom ověřili jeho prvočíselnost pokusným dělením (to nastane v $O(\ln N)$ krocích vzhledem k $N_{i+1} < \frac{1}{2} N_i$). Je třeba si uvědomit, že není-li N_i prvočíslo, skončíme jen v případě $i = 0$, pro $i < 0$ je třeba se vrátit k $i - 1$ a najít nové N_i.

Atkin, 1990

Tato metoda je založena na teoretických výsledcích, které bohužel notně převyšují možnosti naší přednášky. Nevolí křivky náhodně, ale volí speciální případ eliptických křivek, tzv. eliptické křivky s komplexním násobením. Výhoda metody je v tom, že je možné snadněji spočítat řád těchto křivek (vyhne se Schoofově algoritmu, který byl na předchozí metodě časově nejnáročnější).
Atkinův test byl implementován Atkinem a Morainem v roce 1990 a byl schopen dokazovat prvočíselnost čísel o zhruba 1000 dekadických cifrách v řádově týdnech strojového času na Sparc station (při tehdejší rychlosti počítačů, nyní by šlo o hodiny).
I v tomto případě je očekávaný čas výpočtu polynomiální (přesněji $O(\ln^6 N)$). Nejhorší možný čas výpočtu není možno stanovit, protože jde o pravděpodobnostní algoritmus.

Deterministický algoritmus AKS polynomiálního času objevili v roce 2002 pánové Agrawal, Kayal a Saxena z Kanpuru v Indii. Jejich algoritmus je založen na poměrně jednoduché myšlence a nepracuje s eliptickými křivkami. Avšak důkaz jeho polynomiálnosti vyžaduje výsledky analytické teorie čísel.

Funkce $\pi(x)$

Pro libovolné kladné reálné číslo x označme $\pi(x)$ počet prvočísel nepřevyšujících x. Je tedy
$\pi(x) = 0$ pro $x \in (0, 2)$,
$\pi(x) = 1$ pro $x \in [2, 3)$,
$\pi(x) = 2$ pro $x \in [3, 5)$, atd.
$\pi(x) = 3$ pro $x \in [5, 7)$, atd.

Následující důležitou, hlubokou a slavnou větu uvedeme bez důkazu. Její formulaci objevil Gauss v 18. století, avšak důkaz nenašel.
Byla dokázána až na konci 19. století (v roce 1896 objevili důkaz nezávisle na sobě Hadamard a de la Vallée Poussin).
Připomeňme, že $\ln x$ značí přirozený logaritmus.

Věta.

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Čebyševova věta

Pro účely důkazu polynomiálnosti algoritmu AKS bude stačit následující výsledek, který už budeme schopni dokázat.
Větu tohoto typu dokázal poprvé Čebyšev v roce 1852.

Věta 1. Pro libovolné celé číslo $N \geq 2$ platí

$$\frac{N}{\log_2 N} - 2 < \pi(N) < \frac{3N}{\log_2 N}.$$

Pro reálné číslo x značí $[x]$ jeho celou část, která je jednoznačně určena podmínkami $[x] \in \mathbb{Z}$, $0 \leq x - [x] < 1$.

Dále pro libovolné přirozené číslo n a libovolné prvočíslo p je $\nu_p(n)$ počet prvočinitelů v rozkladu čísla n, které jsou rovny p, neboli platí $p^{\nu_p(n)} \mid n$ a $p^{1+\nu_p(n)} \nmid n$.

Je zřejmé, že pro libovolné $m, n \in \mathbb{N}$ platí $\nu_p(mn) = \nu_p(m) + \nu_p(n)$.

Lemma 1. *Pro libovolné přirozené číslo n a libovolné prvočíslo p platí*

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Důkaz. Nejprve si všimněme, že suma na pravé straně je jen formálně nekonečná: je-li $p^k > n$, platí $\left[\frac{n}{p^k}\right] = 0$.

Dále je třeba si uvědomit, že $\left[\frac{n}{p^k}\right]$ značí počet těch čísel z množiny $\{1, 2, \ldots, n\}$, která jsou dělitelná číslem p^k.

A odtud plyne i důkaz: nejprve (pro $k = 1$) započítáme jednou všechny ty činitele v $n! = 1 \cdot 2 \cdot \cdots \cdot n$, kteří jsou dělitelní p.
Pak (pro $k = 2$) započítáme podruhé všechny ty činitele, kteří jsou dělitelní p^2.
Poté (pro $k = 3$) započítáme potřetí všechny ty činitele, kteří jsou dělitelní p^3 atd.
Libovolný činitel s součinu $n! = 1 \cdot 2 \cdot \cdots \cdot n$ je tedy započítán právě $\nu_p(s)$krát a tedy pravá strana dokazované rovnosti je rovna $\sum_{s=1}^{n} \nu_p(s) = \nu_p(n!)$.

Lemma 2. *Pro libovolné přirozené číslo n a libovolné prvočíslo p platí: je-li $\ell = \nu_p(\binom{2n}{n})$, pak $p^\ell \leq 2n$.*

Důkaz. Podle lemmatu 1 platí

$$\ell = \nu_p\Big(\frac{(2n)!}{(n!)^2}\Big) = \nu_p((2n)!) - 2\nu_p((n!)) = \sum_{k=1}^{\infty}\Big(\Big[\frac{2n}{p^k}\Big] - 2\Big[\frac{n}{p^k}\Big]\Big).$$

Pro libovolné reálné x takové, že $x - [x] < \frac{1}{2}$, platí $[2x] = 2[x]$. Je-li naopak $x - [x] \geq \frac{1}{2}$, platí $[2x] = 2[x] + 1$. Libovolný sčítanec v předchozí sumě je tedy 0 nebo 1. Přítom sčítance pro k takové, že $p^k > 2n$, jsou zřejmě nulové. Je tedy $\ell \leq \max\{k \in \mathbb{N};\, p^k \leq 2n\}$ a proto $p^\ell \leq 2n$.

Lemma 3. *Pro libovolná přirozená čísla n, k taková, že $1 \leq k \leq \frac{n}{2}$ platí $\binom{n}{k-1} < \binom{n}{k}$.*

Důkaz. Platí

$$\frac{\binom{n}{k}}{\binom{n}{k-1}} = \frac{n!}{k!(n-k)!}\cdot\frac{(k-1)!(n-k+1)!}{n!} = \frac{n-k+1}{k} \geq \frac{n/2+1}{n/2} > 1.$$

Lemma 4. *Pro libovolné přirozené číslo n platí $\binom{2n}{n} \leq (2n)^{\pi(2n)}$.*

Důkaz. Rozložme uvažovaný binomický koeficient na prvočinitele $\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = p_1^{k_1} \dots p_r^{k_r}$. Libovolné prvočíslo p_i, které se zde vyskytuje, dělí $(2n)!$ a je tedy menší než $2n$. Proto $r \leq \pi(2n)$ a podle lemmatu 2 každé $p_i^{k_i} \leq 2n$. Odtud plyne lemma.

Lemma 5. *Pro libovolné přirozené číslo n platí $\frac{2^{2n}}{2n} \leq \binom{2n}{n} < 2^{2n}$.*

Důkaz. Z binomické věty víme, že $\sum_{i=0}^{2n} \binom{2n}{i} = (1+1)^{2n} = 2^{2n}$, odkud plyne pravá nerovnost.
Ukážeme-li, že v tomto součtu je sčítanec $\binom{2n}{n}$ největší, dostaneme i levou nerovnost, neboť $\frac{2^{2n}}{2n}$ je aritmetický průměr $2n$ čísel $\binom{2n}{0} + \binom{2n}{2n} = 2, \binom{2n}{1}, \binom{2n}{2}, \dots, \binom{2n}{2n-1}$.
Ale to je snadné: platí $\binom{2n}{2n-i} = \binom{2n}{i}$ a pro libovolné $1 \leq i \leq n$ platí $\binom{2n}{i-1} < \binom{2n}{i}$ podle lemmatu 3.

Dolní odhad z věty 1: $\frac{N}{\log_2 N} - 2 < \pi(N)$

Z lemmat 4 a 5 plyne

$$(2n)^{\pi(2n)} \geq \binom{2n}{n} \geq \frac{2^{2n}}{2n},$$

odkud zlogaritmováním a vydělením $\log_2(2n)$ dostaneme

$$\pi(2n) \geq \frac{2n}{\log_2(2n)} - 1$$

a dolní odhad věty 1 je dokázán pro sudá $N = 2n$.
Je-li naopak $N = 2n + 1$ liché, užijeme odvozený odhad pro $\pi(2n)$:

$$\pi(2n+1) \geq \pi(2n) \geq \frac{2n}{\log_2(2n)} - 1 > \frac{2n}{\log_2(2n+1)} - 1 > \frac{2n+1}{\log_2(2n+1)} - 2,$$

což je dolní odhad věty 1 pro $N = 2n + 1$.

Lemma 6. *Pro libovolné přirozené číslo $N > 1$ platí*

$$\prod_{p \leq N} p < 4^{N-1},$$

kde v součinu p probíhá všechna prvočísla nepřevyšující N.

Důkaz. Pro přirozené číslo m označme
$b_m = \binom{2m+1}{m} = \frac{(2m+1)(2m)\ldots(m+2)}{m!}$. Je tedy b_m dělitelné všemi prvočísly p splňujícími $m + 2 \leq p \leq 2m + 1$, neboť tato prvočísla se vyskytují v čitateli a nedělí jmenovatele.
Proto $b_m \geq \prod_{m+2 \leq p \leq 2m+1} p$.
V součtu $\sum_{i=1}^{2m} \binom{2m+1}{i} = 2^{2m+1} - 2$ se sčítanec
$b_m = \binom{2m+1}{m} = \binom{2m+1}{m+1}$ objeví dvakrát, proto $b_m < 2^{2m}$.
Celkem tedy

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

Dokazujeme: $\prod_{p\leq N} p < 4^{N-1}$

Víme: $\prod_{m+2\leq p\leq 2m+1} p < 2^{2m}$.

Nyní můžeme lemma dokázat indukcí: lemma zřejmě platí pro $N = 2$. Předpokládejme tedy, že $N \geq 3$ a že lemma bylo dokázáno pro všechna $2 \leq m < N$. Je-li N sudé, není N prvočíslo a z indukčního předpokladu pro $m = N - 1$ plyne

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

Je-li naopak $N = 2m + 1$ liché, užijme indukční předpoklad pro $m + 1$ (vždyť $2 \leq m + 1 < N$) a odvozenou nerovnost

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

Lemma 7. *Nechť $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... je rostoucí posloupnost všech prvočísel. Pak pro každé $k \geq 9$ platí $p_1 \dots p_k \geq 2^k \cdot k!$.*

Důkaz. Přímým výpočtem lze ověřit, že $p_1 \dots p_9 = 2 \cdot 3 \cdot 5 \cdots 19 \cdot 23 = 233092870 > 185794560 = 2^9 \cdot 9!$. Pro $k > 9$ užijeme indukci: předpokládejme, že $k \geq 9$ a že pro k lemma platí. Zřejmě $p_{k+1} > 2(k+1)$, a tedy

$$p_1 \dots p_{k+1} > 2^k \cdot k! \cdot 2(k+1) = 2^{k+1} \cdot (k+1)!,$$

což jsme měli dokázat.

Lemma 8. *Pro libovolné přirozené číslo k platí $k! > (k/e)^k$.*

Důkaz. Vzpomeňme si z analýzy na Taylorův rozvoj funkce e^x v nule:

$$e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}.$$

Proto platí $\frac{k^k}{k!} < \sum_{i=0}^{\infty} \frac{k^i}{i!} = e^k$, odkud plyne lemma.

Horní odhad z věty 1: $\pi(N) < \frac{3N}{\log_2 N}$

Ukážeme nyní sporem, že $\pi(N) < 2N/\ln N$. Pak totiž $3/\log_2 N = 3\ln 2/\ln N > 2,07/\ln N > 2/\ln N > \pi(N)/N$, což chceme ukázat. Předpokládejme, že $N \geq 27$ (případ $2 \leq N \leq 26$ se rychle ověří výpočtem) a že platí $\pi(N) \geq 2N/\ln N$.
Nechť $k = \pi(N)$, pak $p_1, \ldots, p_k$ jsou právě všechna prvočísla nepřevyšující N. Lemmata 6, 7 a 8 dávají

$$4^N > \prod_{p \leq N} p = p_1 \ldots p_k \geq 2^k \cdot k! > 2^k \cdot (\tfrac{k}{e})^k.$$

Zlogaritmováním

$$(2\ln 2) \cdot N > k \cdot ((\ln k) + (\ln 2) - 1).$$

Dosazením předpokladu $k \geq 2N/\ln N$ do předchozí nerovnosti dostaneme

$$(2\ln 2) \cdot N > \frac{2N}{\ln N} \cdot ((\ln 2) + (\ln N) - (\ln\ln N) + (\ln 2) - 1),$$

a tedy

$$(1 - \ln 2)\ln N - (\ln\ln N) + (2\ln 2) - 1 < 0.$$

Dostali jsme

$$(1 - \ln 2) \ln N - (\ln \ln N) + (2 \ln 2) - 1 < 0.$$

přičemž $N \geq 27$.

Ovšem funkce $f(x) = (1 - \ln 2) \ln x - (\ln \ln x) + (2 \ln 2) - 1$, která je definovaná pro $x > 1$, splňuje $f(27) > \frac{1}{5}$ a má derivaci $f'(x) = \frac{1-\ln 2}{x} - \frac{1}{x \ln x}$. Zřejmě $f'(x_0) = 0$ jedině pro $x_0 = e^{1/(1-\ln 2)} \doteq 26,02$ a platí $f'(x) > 0$ pro $x > x_0$.
Platí tedy $f(N) > 0$, ale to je spor a věta 1 je dokázána:

Věta 1. Pro libovolné celé číslo $N \geq 2$ platí

$$\frac{N}{\log_2 N} - 2 < \pi(N) < \frac{3N}{\log_2 N}.$$

Další dolní odhad součinu několika nejmenších prvočísel

Dokázali jsme:

Lemma 7. *Nechť $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... je rostoucí posloupnost všech prvočísel. Pak pro každé $k \geq 9$ platí $p_1 \dots p_k \geq 2^k \cdot k!$.*

Věta 2. Pro libovolné přirozené číslo $n \geq 2$ platí $\prod_{p \leq 2n} p > 2^n$, kde v součinu p probíhá všechna prvočísla nepřevyšující $2n$.

Důkaz. Jako v důkaze lemmatu 4 rozložme binomický koeficient $\binom{2n}{n}$ na prvočinitele $\binom{2n}{n} = p_1^{k_1} \dots p_r^{k_r}$. Víme, že libovolné prvočíslo, které se zde vyskytuje, je menší než $2n$. Je-li $p_i \leq \sqrt{2n}$, užijeme odhad $p_i^{k_i} \leq 2n$ z lemmatu 2. Je-li naopak $p_i > \sqrt{2n}$, platí $p_i^2 > 2n$, a odhad $p_i^{k_i} \leq 2n$ z lemmatu 2 dává $k_i = 1$. Užitím lemmatu 5

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq 2n} p.$$

Označme $s_n = \prod_{p \le 2n} p$. Dokazujeme tedy $s_n > 2^n$. Předchozí nerovnost spolu s větou 1 dávají

$$\frac{2^{2n}}{2n} \le (2n)^{\pi(\sqrt{2n})} \cdot s_n < (2n)^{3\sqrt{2n}\big/\log_2 \sqrt{2n}} \cdot s_n.$$

Protože $(2n)^{1/\log_2 \sqrt{2n}} = (2n)^{2/\log_2 2n} = (2n)^{2\log_{2n} 2} = 2^2$,
z poslední nerovnosti plyne

$$s_n > 2^{2n}\big/(2n \cdot 2^{6\sqrt{2n}}).$$

Abychom dokázali lemma, musíme ukázat, že $2^n \ge 2n \cdot 2^{6\sqrt{2n}}$, neboli po zlogaritmování

$$n - 1 - \log_2 n - 6\sqrt{2n} \ge 0.$$

Uvažme funkci $f(x) = x - 1 - \log_2 x - 6\sqrt{2x}$. Platí $f(100) = 99 - \log_2 100 - 6\sqrt{200} > 7$ a derivace $f'(x) = 1 - \frac{1}{x \ln 2} - \frac{6}{\sqrt{2x}}$ je větší než $1 - \frac{1}{100 \ln 2} - \frac{6}{10\sqrt{2}} > 0$ pro $x \ge 100$. Tím jsme dokázali lemma pro $n \ge 100$. Nerovnost $s_n > 2^n$ pro hodnoty $2 \le n < 100$ je možné ověřit numericky.