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 $x \in [3, 5)$,
$\pi(x) = 3$ 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

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

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.