Algoritmy teorie čísel - aktualizace učebního textu

Deterministický test na prvočíselnost polynomiální časové náročnosti

V létě roku 2002, přestože byly prázdniny, oběhla rychle světem zpráva, že byl konečně objeven dlouho hledaný algorimus, který v polynomiálním čase rozhodne, zda dané přirozené číslo je prvočíslem. Jde o významný pokrok, přestože se zdá, že jeho využití je jen na teoretické úrovni – dříve známé nedeterministické algoritmy totiž pracují rychleji. Zjednodušeně řečeno, pokud se nedeterministický algoritmus zastaví a dá nám výsledek (včetně certifikátu, což je důkaz, že dané číslo je prvočíslo, nebo důkaz, že je složené), nemusí nám vadit, že jsme k výsledku došli nedeterministickou cestou. Kromě toho o dříve známých deterministických algoritmech (například o původním Millerově deterministickém algoritmu, který později Rabin upravil do známého nedeterministického testu, nebo o deterministické verzi testu Solovaye a Strassena) je známo, že jsou polynomiální, pokud platí zobecněná Riemannova hypotéza (což je tvrzení, o němž je všeobecně věřeno, že je pravdivé, avšak neumí to nikdo dokázat). Na druhou stranu pro teoretickou informatiku je důležité vědět, že nedeterministický algoritmus polynomiálního času skutečně existuje.

Ve zmiňovaném článku pánové Agarval, Kayal a Saxena z Indie dokázali, že následující algoritmus je polynomiálního času a pro každé přirozené číslo n dává správný výsledek.

Algoritmus (Agarval, Kayal, Saxena). *Pro dané přirozené číslo $n > 2$ algoritmus rozhodne, zda je n prvočíslo nebo složené.*

1. *[Mocniny] Je-li n sudé nebo pokud je $n = a^b$, kde $a, b \in \mathbb{N}$, $b > 1$, vytiskni, že n je složené a skonči. Jinak polož $r \leftarrow 2$.*
2. *[První cyklus] Nejmenší prvočíslo větší než r ulož do r. Jestliže $r|n$, pak vytiskni, že n je složené a skonči. Jinak do q ulož největší prvočíslo dělící číslo $r-1$. Jestliže platí $q \geq 4\sqrt{r}\log n$ a současně $n^{(r-1)/q} \not\equiv 1 \pmod r$, jdi na 3, jinak opakuj 2.*
3. *[Druhý cyklus] Pro a od 1 do $2\sqrt{r}\log n$ prováděj: jestliže*

$$(x-a)^n \not\equiv (x^n - a) \pmod{(x^r - 1, n)},$$

pak vytiskni, že n je složené a skonči.

4. *[Závěr] Vytiskni, že n je prvočíslo a skonči.*

Kongruence užitá v bodě 2 je kongruencí mezi celými čísly a je ověřována tak, že levá strana je počítána binárním umocňováním, přičemž po každém násobení je výsledek zmenšován dělením celým číslem r se zbytkem. Kongruence v bodě 3 je však kongruencí mezi polynomy. Je opět ověřována tak, že levá strana je počítána binárním umocňováním, přitom však po každém násobení polynomů je nejprve stupeň jejich součinu eliminován pomocí dělení se zbytkem polynomem $x^r - 1$ (jinými slovy, koeficient u mocniny x^s pro $s \geq r$ se přesune, tj. přičte ke koeficientu u mocniny x^{s-r}), poté se všechny koeficienty vzniklého polynomu nahradí svými zbytky po dělení číslem n.

V důkaze správnosti algoritmu je třeba ověřit dvě věci:

- „malých" prvočísel r s „velkým" prvočíselným dělitelem čísla $r - 1$ je hodně, a tedy první cyklus je „brzy" přerušen s „poměrně malým" r;
- případná složenost čísla n se projeví v průběhu výpočtu druhého cyklu.

Celý důkaz využívá řady dřívějších výsledků, které svou hloubkou přesahují možnosti této přednášky. Jen pro představu o tom, jak je asi důkaz veden, zde tyto výsledky analytické teorie čísel uvádím:

Věta 1. *Nechť $P(n)$ značí největší prvočíslo dělící přirozené číslo n. Pak existují konstanty $c > 0$ a n_0 tak, že pro všechna $x > n_0$ platí*

$$|\{p;\ p \text{ je prvočíslo},\ p \leq x,\ P(p-1) > x^{\frac{2}{3}}\}| \geq \frac{cx}{\log x}.$$

Věta 2. *Nechť $\pi(n)$ značí počet prvočísel $p \leq n$. Pak pro libovolné $n \geq 1$ platí*

$$\frac{n}{6 \log n} \leq \pi(n) \leq \frac{8n}{\log n}.$$

V článku je dokázáno, že časová náročnost uvedeného algoritmu je řádu $O(\log^{12} n \cdot f(\log \log n))$ pro nějaký polynom f, je tedy například řádu $o(\log^{13} n)$ a tedy jde opravdu o polynomiální algoritmus.