1. Stručná historie algoritmů pro prvočísla

Problémy týkající se prvočíselnosti fascinovaly matematiky od starověku. Mezi těmito problémy hraje klíčovou roli následující problém

Problém. *PRIME:*
Vstup: přirozené číslo $p > 1$;
Výstup: ano, když p je prvočíslo.

Nejstarší známý korektní algoritmus pro tento problém je Eratosthenovo síto, které vzniklo někdy kolem roku 240 před naším letopočtem. Tento algoritmus vyžaduje čas $O(p)$, kde p je vstupní číslo. Protože délka vstupu je $\log p$, je tento algoritmus exponenciální. Protože exponenciální algoritmy nejsou použitelné pro velká čísla, motivuje to snahu nalézt efektivnější, tj. rychlejší algoritmus. Fermat v 17. století dokázal tzv. Malou Fermatovu větu, která tvoří základ většiny nových algoritmů pro $PRIME$.

Malá Fermatova věta. *Když p je prvočíslo a n je číslo nesoudělné s p, pak* $n^{p-1} \equiv 1 \bmod p$.

Bohužel Malá Fermatova věta není charakteristika prvočísel. Řekneme, že přirozené číslo n je Carmichaelovo číslo [10,11], když n není prvočíslo a pro každé přirozené číslo a, které je nesoudělné s n, platí $a^{n-1} \equiv 1 \bmod n$. Nejmenší Carmichaelovo číslo je 561 a existuje 8241 Carmichaelových čísel menších než 10^{12}. Nedávno bylo dokázáno [6], že existuje nekonečně mnoho Carmichaelových čísel. Další fakta o Carmichaelových číslech jsou v sekci Pravděpodobnostní algoritmy pro $PRIME$.

V devatenáctém století a v první polovině dvacátého století se problémy o prvočíslech zabývali matematici, kteří studovali teorii čísel. Z nich je třeba jmenovat Kraitchika (1926) [25] a Lehmera (1927) [27], kteří navrhli nezávisle na sobě stejný algoritmus pro $PRIME$. Tento algoritmus vylepšil J. L. Selfridge (1967) [10]. K. Gödel v dopise von Neumannovi v roce 1956 se ptal na výpočetní složitost problému $PRIME$. Pozornost na složitost problému $PRIME$ však inicioval až výsledek V. Pratta (1975) [33], který ukázal, že $PRIME \in \mathbf{NP}$. Protože je zřejmé, že $PRIME \in \mathbf{coNP}$ (stačí uhodnout dělitele p a pak ověřit dělením, že byl uhodnut správně), tak až do roku 2002 byl problém $PRIME$ jediný přirozený problém takový, že $PRIME \in \mathbf{NP} \cap \mathbf{co} - \mathbf{NP}$, ale nevědělo se, zda bez dalších předpokladů patří do $\mathbf{P}$. G. Miller (1976) [31] navrhl deterministický algoritmus pro řešení problému $PRIME$, který za předpokladu rozšířené Riemanovy hypotézy (ERH) vyžadoval polynomiální čas. Tento algoritmus modifikoval M. O. Rabin (1976,1980) [34,35] na pravděpodobnostní polynomiální algoritmus pro $PRIME$ typu Monte Carlo. R. Solovay a V. Strassen (1977) [37] navrhli jiný pravděpodobnostní polynomiální algoritmus pro $PRIME$ typu Monte Carlo, který byl založen na kvadratických residuích. Oba algoritmy jsou popsány v kapitole Pravděpodobnostní algoritmy pro $PRIME$.

L. M. Adelman, C. Pomerance a R. S. Rumely (1983) [2] navrhli deterministický algoritmus pro $PRIME$ vyžadující čas $\log^{O(\log\log\log n)} n$ za hypotézy, která je slabší než zobecněná Riemanova hypotéza. S. Goldwasser a J. Kilian (1986) [19] a nezávisle A. O. L. Atkin [8] navrhli deterministický algoritmus, který má očekávaný polynomiální čas a za platnosti velmi slabé hypotézy má i čas v nejhorším případě polynomiální. C. Pomerance (1987) [32] navrhl nedeterministický algoritmus pro $PRIME$ pracující v lineárním čase (tím vylepšil výsledek V. Pratta).

Analogický výsledek ukázali R. K. Guy, C. B. Lacampagne a J. L. Selfridge (1987) [20]. Překvapivý výsledek tohoto typu ukázali J. P. Jones, D. Sato, H. Wada a D. Wiens (1976) [22]. Ukázali, že pro prvočíslo p existuje důkaz, že p je prvočíslo, který vyžaduje pouze 87 sčítání a násobení (celých čísel). To znamená, že existuje nedeterministický algoritmus, který ověří, že p je prvočíslo, a použije pouze 87 sčítání a násobení. Algoritmus S. Goldwassera a J. Kiliana vylepšili L. M. Adleman a M.-D. Huang (1992) [1] a navrhli pravděpodobnostní algoritmus pro $PRIME$ typu Las Vegas, který pracuje v polynomiálním čase.

M. Agrawal, N. Kayal a N. Saxena (2002) [4] navrhli deterministický algoritmus pro $PRIME$ vyžadující čas $O(\log^{12} n \log^{O(1)} \log n)$ a tím ukázali, že $PRIME \in \mathbf{P}$. Tento algoritmus je založen na stejné idei jako pravděpodobnostní algoritmus navržený M. Agrawalem a S. Biswasem (1999) [3] a je to vlastně jeho vylepšení. Za předpokladu platnosti hypotézy Sophie Germainové o hustotě prvočísel tento algoritmus vyžaduje jen $O(\log^6 n \log^{O(1)} \log n)$ času. Algoritmus je popsán v kapitole Deterministický algoritmus pro $PRIME$. Velký exponent u polynomu omezujícího čas, který spotřebuje algoritmus, vedl k pokusům o další zlepšení. Nejprve Lenstra (2004) vylepšil algoritmus tak, že vyžaduje jen čas $O(\log^{7.5} n)$, a pak Lenstra a Pomerance (2005) [29] navrhli další zlepšní. Jejich algoritmus spotřebuje už jen $O(\log^6 n \log^{O(1)} \log n)$ času. Tato zlepšení deterministického algoritmu pro řešení $PRIME$ jsou založena na hlubokých teoreticko-číselných výsledcích na rozdíl od původního algoritmu, který lze dobře prezentovat. Kvůli stupni polynomu však stále nejsou tyto algoritmy prakticky použitelné. Podle informací v praxi se hlavně používají pravděpodobnostní algoritmy Solovay-Strassena a Rabin- Millera. Nejpoužívanější má být Rabin-Millerův algoritmus, je rychlejší než Solovay-Strassenův algoritmus (asymptoticky jsou oba algoritmy stejně rychlé – $O(\log^3 n)$, ale Rabin-Millerův algoritmus je v jistém smyslu jen část Solovay-Strassenova algoritmu, proto má reálně menší multiplikativní konstantu), a také pravděpodobnost chyby je menší. Solovay-Strassenův algoritmus se zřejmě hodně používá z konzervativních důvodů, byl to první prakticky použitelný algoritmus pro řešení problému $PRIME$.

2. Pravděpodobnostní algoritmy

Pravděpodobnostní algoritmus je jakási kombinace deterministického a nedeterministického algoritmu. Nedeterministický krok má jen volbu z dvou možných pokračování a navíc má kromě standardního vstupu ještě náhodný vstup z 0 a 1, který pro konkrétní výpočet určuje, kterou volbu má použít (to znamená, že náhodný vstup musí být tak dlouhý jako je doba nejdelšího výpočtu nad daným vstupem). Přitom stejně jako nedeterministický algoritmus nemusí vždy počítat korektně. Přesně řečeno pravděpodobnostní algoritmus A řeší problém P s chybou $\chi(x)$ (kde x je vstup pro problém P), která je pro vstup x rovna podílu korektních výpočtů nad x a všech náhodných vstupů pro x. Formálně řečeno, když délka náhodného vstupu pro x je k, pak

$$\chi(x) = \frac{|\{y \mid y \text{ je náhodný vstup a } A(x,y) \text{ dává korektní výsledek}\}|}{2^k}.$$

Dále budeme vždy předpokládat, že délka výpočtu A je shora omezena polynomem vzhledem k délce vstupu (to plyne z předpokladu, že v praxi jsou použitelné jen algoritmy pracující v polynomiálním čase). Řekneme, že jazyk L je přijímán

pravděpodobnostním algoritmem A v čase f, kde f je polynom, když

$$L = \{x \in \{0,1\}^*; |\{y \in \{0,1\}^{f(|x|)}; A(x,y) \text{ přijímá}\}| > 2^{f(|x|)-1}\}.$$

Třída těchto jazyků se značí **PP** a platí $\mathbf{NP} \cup \mathbf{coNP} \subseteq \mathbf{PP} \subseteq \mathbf{PSPACE}$. Ukazuje se, že třída **PP** je příliš velká a obsahuje mnoho problémů, které jsou pravděpodobně prakticky neřešitelné. To vedlo k její restrikci. Pravděpodobnostní algoritmus A pracující v polynomiálním čase je typu Atlantic City, když existuje $0 \leq \epsilon < \frac{1}{2}$ takové, že pro každé x je $\chi(x) < \epsilon$. Pak **BPP** značí třídu jazyků přijímaných algoritmy typu Atlantic City. Zřejmě $\mathbf{BPP} \subseteq \mathbf{PP}$, ale vztah **NP** a **BPP** je otevřený problém. Pravděpodobnostní algoritmus A pracující v polynomiálním čase je algoritmus typu Monte Carlo pro jazyk L, když existuje $0 \leq \epsilon < 1$ takové, že platí:

(1) když $x \in L$, pak $A(x,y)$ přijímá pro každý náhodný vstup y (tj. $\chi(x) = 0$);
(2) když $x \notin L$, pak $\chi(x) < \epsilon$.

Pravděpodobnostní algoritmus A pracující v polynomiálním čase f je algoritmus typu Las Vegas přijímající jazyk L, když A má tři výstupy – přijímá, odmítá a neví a existuje $0 \leq \epsilon < 1$ tak, že platí

(1) když $x \in L$, pak výstup $A(x,y)$ je buď přijímá nebo neví pro každý náhodný vstup y;
(2) když $x \notin L$, pak výstup $A(x,y)$ je buď odmítá nebo neví pro každý náhodný vstup y;
(3) pro každé x platí $|\{y \in \{0,1\}^{f(|x|)}; \text{výstup } A(x,y) \text{ je neví}\}| < \epsilon 2^{f(|x|)}$.

Jazyky přijímané algoritmy typu Monte Carlo tvoří třídu **RP** a jazyky přijímané algoritmy typu Las Vegas tvoří třídu **ZPP**.

Následující věta ukazuje význam těchto tříd.

Věta 2.1. *Když $L \in \mathbf{BPP}$, pak pro každý polynom g existuje algoritmus typu Atlantic City přijímající L s chybou $\chi(x) \leq 2^{-g(|x|)}$. Když $L \in \mathbf{RP}$, pak pro každý polynom g existuje algoritmus typu Monte Carlo přijímající L s chybou $\chi(x) < 2^{-g(|x|)}$. Když $L \in \mathbf{ZPP}$, pak pro každý polynom g existuje algoritmus typu Las Vegas přijímající L a*

$$|\{y \in \{0,1\}^{f(|x|)}; \textit{výstup } A(x,y) \textit{ je neví}\}| < 2^{-g(|x|)}.$$

Důkaz. Nejprve dokážeme druhé a třetí tvrzení. Mějme jazyk $L \in \mathbf{RP}$ nebo $L \in \mathbf{ZPP}$, pak existuje algoritmus A typu Monte Carlo nebo Las Vegas přijímající L a existuje $0 \leq \epsilon < 1$ takové, že $\chi(x) < \epsilon$ nebo

$$|\{y \in \{0,1\}^{f(|x|)}; \text{výstup } A(x,y) \text{ je neví}\}| < \epsilon 2^{f(|x|)},$$

kde f je polynom omezující dobu výpočtu A. Protože $\epsilon < 1$, tak existuje k takové, že $\epsilon^k < \frac{1}{2}$. Nechť g je libovolný polynom. V obou případech použijme následující algoritmus:

Algoritmus B
Vstup: x
$i = 0$
while $i \leq kg(x)$ **do**
zvol náhodně $y \in \{0,1\}^{f(|x|)}$

(pro **RP**){ **if** $A(x,y)$ odmítne **then** odmítne, stop **endif**
(pro **ZPP**){ if $A(x,y)$ odmítne then odmítne, stop else
if $A(x,y)$ přijme then přijme, stop endif endif
$i := i + 1$
enddo
(pro **RP**) přijme
(pro **ZPP**) neví

Všimněme si, že v případě **RP**, když $x \in L$, pak algoritmus B vždy přijímá, v případě **ZPP**, když $x \in L$, pak algoritmus B neskončí s odmítnutím a když $x \notin L$, pak algoritmus B neskončí s přijmutím. Protože f a g jsou polynomy, tak algoritmus pracuje v polynomiálním čase. V případě **RP**, když $x \notin L$, pak A přijímá s pravděpodobností menší než ϵ. Aby B přijmul, musel cyklus běžet $kg(x)$-krát a ve všech bězích musel A přijmout. Protože běhy cyklů jsou nezávislé, tak pravděpodobnost, že se to stane, je menší než $\epsilon^{kg(|x|)} \leq 2^{g(|x|)}$. V případě **ZPP** je pravděpodobnost, že algoritmus odpověděl, že neví, menší než ϵ. Aby B odpověděl, že neví, musel cyklus běžet $kg(x)$-krát a ve všech bězích musel A odpovědět, že neví. Proto pravděpodobnost, že B odpověděl, že neví, je menší než $2^{g(|x|)}$.

Nyní dokážeme první tvrzení. Nechť $L \in \mathbf{BPP}$ a nechť A je algoritmus typu Atlantic City přijímající L s chybou menší než ϵ pro $0 \leq \epsilon < \frac{1}{2}$. Nechť A pracuje v čase f, kde f je polynom. Nechť g je polynom. Pak $4\epsilon(1-\epsilon) < 1$, a tedy existuje k takové, že $\big(4\epsilon(1-\epsilon)\big)^k \leq \frac{1}{2}$. Uvažujme následující algoritmus:

Algoritmus B_1
Vstup x
$i := 0$, $c := 0$
while $i \leq 2kg(|x|)$ **do**
zvol náhodně $y \in \{0,1\}^{f(|x|)}$
if $A(x,y)$ přijímá **then** $c := c + 1$ **endif**
$i := i + 1$
enddo
if $c > kg(|x|)$ **then** přijmi **else** odmítni **endif**

Protože f a g jsou polynomy, tak B_1 pracuje v polynomiálním čase. Předpokládejme, že pro vstup x je pravděpodobnost chyby ϵ_1, pak $0 \leq \epsilon_1 < \epsilon$, a proto $4\epsilon_1(1-\epsilon_1) < 4\epsilon(1-\epsilon)$, a tedy $\big(4\epsilon_1(1-\epsilon_1)\big)^k < \big(4\epsilon(1-\epsilon)\big)^k \leq \frac{1}{2}$. Protože běhy cyklu jsou nezávislé a A dává pro x nekorektní odpověď s pravděpodobností ϵ_1, tak pravděpodobnost, že A dá nekorektní odpověď na fixované j-tici běhů cyklu, je $\epsilon_1^j(1-\epsilon_1)^{2k(g(|x|)+1-j}$. Tedy pravděpodobnost, že B_1 dal nesprávnou odpověď právě v j bězích cyklu, je nejvýše $\binom{2kg(|x|)+1}{j}\epsilon_1^j(1-\epsilon_1)^{2kg(x)+1-j}$. Tedy pravděpodobnost, že B_1 odpověděl nekorektně, je nejvýše

$$\sum_{j=0}^{kg(|x|)} \binom{2kg(|x|)+1}{j} \epsilon_1^j (1-\epsilon_1)^{2kg(|x|)+1-j} \leq$$

$$\big(\epsilon_1(1-\epsilon_1)\big)^{kg(|x|)+1/2} \sum_{j=0}^{kq(x)} \binom{2kg(|x|)+1}{j} \leq$$

$$\big(\epsilon_1(1-\epsilon_1)\big)^{kg(|x|)+1/2} 2^{2kg(|x|)+1} = \big(4\epsilon_1(1-\epsilon_1)\big)^{kg(|x|)+1/2} \leq$$

$$\Big(\big(4\epsilon_1(1-\epsilon_2)\big)^k\Big)^{g(|x|)} \leq 2^{-g(|x|)}.$$

Tím je důkaz kompletní. □

Z toho okamžitě dostáváme, že $\mathbf{P} \subseteq \mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$ a $\mathbf{RP} \subseteq \mathbf{NP} \cap \mathbf{BPP}$, $\mathbf{coRP} \subseteq \mathbf{coNP} \cap \mathbf{BPP}$, ale zda jsou inkluse ostré, se neví. Na druhou stranu na základě této věty je třída **BPP** považována za největší třídu problémů prakticky řešitelných.

3. Pravděpodobnostní algoritmy pro *PRIME*.

Nejprve si připomeneme pár základních pojmů z teorie čísel a teorie grup.

Pro přirozené číslo $n > 1$ označme $\mathbb{Z}_n^*$ množinu všech celých čísel mezi 0 a $n-1$, která jsou nesoudělná s n, spolu s operací násobení modulo n. Pak $\mathbb{Z}_n^*$ je grupa a říká se jí multiplikativní grupa modulo n. Nechť $\lambda(n)$ je řád grupy $\mathbb{Z}_n^*$, tj. $\lambda(n)$ je nejmenší přirozené číslo p takové, že $i^p \equiv 1 \bmod n$ pro každé $i \in \mathbb{Z}_n^*$. Protože $\mathbb{Z}_n^*$ je konečná grupa, tak pro každé $i \in \mathbb{Z}_n^*$ existuje p takové, že $i^p \equiv 1 \bmod n$ (1 je jednotkový prvek $\mathbb{Z}_n^*$), a pak $i^{kp} \equiv 1 \bmod n$ pro každé celé číslo $k > 1$. Nyní z konečnosti $\mathbb{Z}_n^*$ plyne existence λ. Dále si připomeneme Čínskou větu o zbytcích.

Věta 3.1. *(Čínská věta o zbytcích). Nechť $m_1, m_2, \ldots, m_n$ jsou navzájem nesoudělná přirozená čísla větší než 1. Pak pro každou n-tici čísel $x_1, x_2, \ldots x_n$ existuje právě jedno číslo x takové, že $0 \leq x < \prod_{i=1}^n m_i$ a $x \equiv x_i \bmod m_i$ pro každé $i = 1, 2, \ldots, n$. Pro celá čísla x a y a pro $m = \prod_{i=1}^n m_i$ platí $x \equiv y \bmod m$, právě když $x \equiv y \bmod m_i$ pro každé $i = 1, 2, \ldots, n$.*

Důkaz. Zvolme $i \in \{1, 2, \ldots, n\}$ a všimněme si, že pro $f_i = \frac{m}{m_i}$ platí $f_i \equiv 0 \bmod m_j$ pro každé $j = 1, 2, \ldots, n$, $j \neq i$, a f_i je nesoudělné s m_i. Proto existuje $g_i \in \{1, 2, \ldots, m_i - 1\}$ takové, že $f_i g_i \equiv 1 \bmod m_i$. Položme $e_i = f_i g_i$, pak $e_i \equiv 1 \bmod m_i$ a $e_i \equiv 0 \bmod m_j$ pro každé $j = 1, 2, \ldots, n$, $j \neq i$. Odtud pro $x = \sum_{i=1}^n x_i e_i$ platí $x \equiv x_i \bmod m_i$ pro každé $i = 1, 2, \ldots, n$.

Nyní mějme dvě celá čísla x a y taková, že $x \equiv y \bmod m$. Protože $m = \prod_{i=1}^n m_i$, dostáváme, že $x \equiv y \bmod m_i$ pro každé $i = 1, 2, \ldots, n$. Naopak, když $x \equiv y \bmod m_i$ pro každé $i = 1, 2, \ldots, n$, pak pro každé i existuje celé číslo k_i takové, že $x = y + k_i m_i$. Odtud plyne, že $x - y$ je násobkem m_i pro každé $i = 1, 2, \ldots, n$, a protože m_i a m_j jsou nesoudělná pro všechna různá čísla $i, j \in \{1, 2, \ldots, n\}$, dostáváme, že $x - y$ je násobkem m, neboli $x \equiv y \bmod m$. Tedy platí druhé tvrzení věty.

První tvrzení dostaneme kombinací první části důkazu a druhého tvrzení. □

Odtud dostaneme

Tvrzení 3.2. *Když $n = \prod_{i=1}^j p_i^{m_i}$ je prvočíselný rozklad n, pak $\lambda(n)$ je nejmenší společný násobek čísel $\lambda(p_i^{m_i})$ pro $i = 1, 2, \ldots, j$.*

Důkaz. Nechť k je nejmenší společný násobek čísel $\lambda(p_i^{m_i})$ pro $i = 1, 2, \ldots, j$. Pak pro každé $i = 1, 2, \ldots, j$ a každé $a \in \mathbb{Z}_{p_i^{m_i}}^*$ platí $a^k \equiv 1 \bmod p_i^{m_i}$, protože k je násobek $\lambda(p_i^{m_i})$. Z Čínské věty o zbytcích plyne, že k je násobek $\lambda(n)$.

Naopak, pro každé $i = 1, 2, \ldots, j$ existuje $a_i \in \mathbb{Z}_{p_i^{m_i}}^*$ takové, že řád a_i je $\lambda(p_i^{m_i})$ (to plyne z konečnosti $\mathbb{Z}_{p_i^{m_i}}$). Z Čínské věty o zbytcích plyne existence a jednoznačnost čísla $a \in \{1, 2, \ldots, n\}$ takového, že $a \equiv a_i \bmod p_i^{m_i}$ pro každé $i = 1, 2, \ldots, j$. Pro každé $l < k$ existuje $i = 1, 2, \ldots, j$ takové, že $a_i^l \not\equiv 1 \bmod p_i^{m_i}$, a z Čínské věty o zbytcích plyne $a^l \not\equiv 1 \bmod n$. Na druhé straně $a_i^k \equiv 1 \bmod p_i^{m_i}$ pro každé $i = 1, 2, \ldots, j$, a proto $a^k \equiv 1 \bmod n$. Odtud plyne, že $\lambda(n) \geq k$, a proto $k = \lambda(n)$. □

Pro liché prvočíslo p a pro každé celé kladné číslo i je $\mathbb{Z}_{p^i}^*$ cyklická grupa a protože $|\mathbb{Z}_{p^i}^*| = \phi(p^i) = (p-1)p^{i-1}$ (ϕ je Eulerova funkce), dostáváme $\lambda(p^i) = (p-1)p^{i-1}$. Pro mocniny 2 je situace komplikovanější, $\mathbb{Z}_2^*$ a $\mathbb{Z}_4^*$ jsou cyklické grupy, a $\mathbb{Z}_{2^i}^*$ pro $i > 2$ je isomorfní se součinem cyklické grupy řádu 2^{i-2} s cyklickou grupou řádu 2, proto $\lambda(2) = 1$, $\lambda(4) = 2$ a $\lambda(2^i) = 2^{i-2}$ pro $i \geq 3$.

Základní výsledek, který položil základy k hledání pravděpodobnostních algoritmů pro řešení problému $PRIME$, je Malá Fermatova věta.

Věta 3.3. *Když n je provočíslo a a je celé číslo nesoudělné s n, pak $a^{n-1} \equiv 1 \bmod n$.* □

Kdyby toto byla charakterizace prvočísel a kdyby pro kladné číslo n, které není prvočíslo, existovalo 'hodně' celých čísel a v intervalu $< 1, n-1 >$ takových, že $a^{n-1} \not\equiv 1 \bmod n$, pak bychom mohli navrhnout pravděpodobnostní algoritmus, který by pro vstup n náhodně zvolil celé číslo $a \in < 1, n-1 >$ a spočítal by $a^{n-1} \bmod n$. Kdyby $a^{n-1} \equiv 1 \bmod n$, pak by odpověď byla, že n je prvočíslo, a kdyby součin byl různý od 1, pak by odpověď byla, že n není prvočíslo. Protože a^{n-1} lze spočítat v polynomiálním čase (vzhledem k $\log n$), tak pokud by 'hodně' znamenalo proporcionálně vzhledem k n, měli bychom algoritmus typu Monte Carlo pro problém $PRIME$.

Bohužel tato vlastnost není charakteristická pro prvočísla. Číslo, které není prvočíslo, ale přesto pro každé celé číslo a, které je nesoudělné s n, platí, že $a^{n-1} \equiv 1 \bmod n$, se nazývá Carmichaelovým číslem. Existenci a jejich vlastnosti dokázal Carmichael [11,12] a nezávisle na něm to oznámil Korselt [24]. Je známo, že nejmenší Carmichaelovo číslo je 561 a počet Carmichaelových čísel menších než 10^{12} je 8241. Na druhé straně pro všechna dostatečně velká čísla x je počet Carmichaelových čísel menších než x větší než $x^{\frac{2}{7}}$. To dokázali Alford, Granville a Pomerance (1994) [6]. To motivuje hledání charakteristik pro prvočísla podobných Malé Fermatově větě. Než se vydáme tímto směrem, dokážeme si některé základní vlastnosti Carmichaelových čísel. Platí

Lemma 3.4. [11,12,24]*Když n je Carmichaelovo číslo, pak*

(1) *$\lambda(n)$ dělí $n-1$;*
(2) *n je liché;*
(3) *neexistuje přirozené číslo $a > 1$ takové, že a^2 dělí n;*
(4) *n není součinem dvou prvočísel.*

Důkaz. Protože n je Carmichaelovo číslo, tak $a^{n-1} \equiv 1 \bmod n$ pro každé $a \in \mathbb{Z}_n^*$, a proto $\lambda(n)$ dělí $n-1$. Protože $-1^2 \equiv 1 \bmod n$, dostáváme, že $\lambda(n)$ je sudé pro každé n, a proto každé Carmichaelovo číslo n je liché. Když pro přirozené číslo $a > 1$ platí, že a^2 dělí n, pak můžeme předpokládat, že a je prvočíslo. Pak $\lambda(a^2) = a(a-1)$ podle Tvrzení 3.2 dělí $\lambda(n)$. Odtud plyne, že a dělí $n-1$ i n, a proto $a = 1$, spor. Proto neexistuje přirozené číslo $a > 1$ takové, že a^2 dělí n. Když n je součinem dvou prvočísel p a q, pak podle (3) $p \neq q$ a podle (2) p a q jsou lichá čísla. Podle Tvrzení 3.2 $p-1$ dělí $\lambda(n)$, a tedy dělí i $n-1$. Proto $n-1 \equiv 0 \bmod p-1$, a tedy $n \equiv 1 \bmod p-1$. Protože $p \equiv 1 \bmod p-1$, dostaváme, že $q \equiv 1 \bmod p-1$. Proto $q \geq p$. Ze symetrie dostaneme, že $q \leq p$, a tedy $q = p$, a to je spor. □

Abychom specifikovali pojem 'hodně', bylo by vhodné, aby množina

$$\{a \in \mathbb{Z}_n^* \mid a \text{ splňuje uvažovanou charakteristiku prvočísel}\}$$

byla vlastní podgrupa $\mathbb{Z}_n^*$, když n není prvočíslo. Této množině se říká množina lhářů vzhledem k uvažované charakteristice. Zřejmě chyba algoritmu je majorizována poměrem velikosti grupy lhářů vzhledem k velikosti $\mathbb{Z}_n^*$. Když grupa lhářů je vlastní podgrupa, pak nutně $\frac{1}{2}$ majorizuje tento poměr a tedy i chybu. Všimněme si, že když n není prvočíslo, pak $F_n = \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \bmod n\}$ je podgrupa $\mathbb{Z}_n^*$. Říká se jí grupa Fermatových lhářů a n je Carmichaelovo číslo, právě když n není prvočíslo, ale $F_n = \mathbb{Z}_n^*$.

Solovay-Strassenův algoritmus

První pravděpodobnostní algoritmus je založen na Eulerově charakterizaci prvočísel, která používá Legendreovy a Jacobiho symboly. Než zavedeme tyto symboly, budeme definovat pojem residuum. Pro kladná celá čísla m a n a pro celé číslo a nesoudělné s n řekneme, že a je m-té residuum $\bmod n$, když existuje celé číslo x takové, že $x^m \equiv a \bmod n$. Když $m = 2$, pak říkáme, že a je kvadratické residuum $\bmod n$. Když a je nesoudělné s n a není kvadratické residuum $\bmod n$, pak říkáme, že a je kvadratické non-residuum $\bmod n$. Připomeňme si definici Eulerovy funkce ϕ. Eulerova funkce ϕ je zobrazení z přirozených čísel do sebe takové, že $\phi(n)$ je počet kladných celých čísel, která jsou v intervalu $< 1, n >$ a jsou nesoudělná s n, tj. $\phi(n)$ je počet prvků v grupě $\mathbb{Z}_n^*$.

Lemma 3.5. *Mějme kladné přirozené číslo n takové, že $\mathbb{Z}_n^*$ je cyklická grupa. Pak $a \in \mathbb{Z}_n^*$ je m-té residuum vzhledem k* $\bmod n$*, kde m je kladné celé číslo, právě když $a^{\frac{\phi(n)}{d}} \equiv 1 \bmod n$, kde d je největší společný dělitel m a $\phi(n)$.*

Důkaz. Nechť g je generátor $\mathbb{Z}_n^*$ a nechť a je m-té residuum vzhledem k mod$n$. Pak existuje celé číslo x takové, že $x^m \equiv a \bmod n$. Tedy existují kladná celá čísla u a v taková, že $g^u \equiv a \bmod n$ a $g^v \equiv x \bmod n$. Odtud $g^{mv} \equiv g^u \bmod n$ a to znamená, že $mv \equiv u \bmod \phi(n)$ (protože $\mathbb{Z}_n^*$ je cyklická, tak $\lambda(n) = |\mathbb{Z}_n^*| = \phi(n)$). Nyní použijeme pomocné lemma.

Pomocné lemma 3.6. *Mějme celá čísla a, b a kladné celé číslo n. Označme d největšího společného dělitele n a a. Pak existuje celé číslo x takové, že $ax \equiv b \bmod n$, právě když d dělí b, a v tom případě je x určeno jednoznačně* $\bmod \frac{n}{d}$.

Důkaz. Předpokládejme, že existuje celé číslo x takové, že $ax \equiv b \bmod n$, pak existuje celé číslo k takové, že $ax - kn = b$. Odtud plyne, že největší společný dělitel d čísel a a n musí dělit b. Naopak předpokládejme, že d dělí b. Pak z vlastností největšího společného dělitele (a Euklidova algoritmu pro jeho nalezení) existují celá čísla x_0 a y_0 taková, že $d = x_0 a + y_0 n$. Pak pro $c = \frac{b}{d}$ platí $ax_0 c + ny_0 c = dc = b$ a stačí položit $x = x_0 c$ a dostaneme, že $ax \equiv b \bmod n$.

Abychom dokázali druhé tvrzení, předpokládejme, že x_0 a x_1 jsou celá čísla taková, že $ax_0 \equiv b \equiv ax_1 \bmod n$. Protože d dělí n a a, dostáváme $\frac{a}{d}x_0 \equiv \frac{a}{d}x_1 \bmod \frac{n}{d}$. Z vlastností největšího společného dělitele plyne, že $\frac{a}{d}$ a $\frac{n}{d}$ jsou nesoudělná celá čísla, a tedy můžeme rovnici vydělit číslem $\frac{a}{d}$ a dostaneme, že $x_0 \equiv x_1 \bmod \frac{n}{d}$, a tedy druhé tvrzení platí. □

Položme d rovno největšímu společnému děliteli m a $\phi(n)$, pak $mv \equiv u \bmod \phi(n)$ implikuje, že d dělí u, a tedy $a^{\frac{\phi(n)}{d}} \equiv g^{\frac{u\phi(n)}{d}} \equiv 1 \bmod n$, protože $\phi(n) = \lambda(n)$. Naopak předpokládejme, že $a^{\frac{\phi(n)}{d}} \equiv 1 \bmod n$. Když $a = g^u$ pro generátor g cyklické grupy $\mathbb{Z}_n^*$, pak $g^{\frac{u\phi(n)}{d}} \equiv 1 \bmod n$. Odtud plyne, že $\frac{u}{d}$ je celé číslo (opět používáme

$\lambda(n) = \phi(n)$). Pak podle Pomocného lemmatu 3.6 existuje celé číslo k takové, že $mk \equiv u \bmod \phi(n)$. Odtud plyne, že $(g^k)^m \equiv g^u \equiv a \bmod n$, a tedy stačí položit $x \equiv g^k \bmod n$ a dostaneme, že $x^m \equiv a \bmod n$. □

Jako důsledek dostaneme Eulerovo kriterium.

Důsledek 3.7. [18]*Nechť p je liché prvočíslo. Pak*

(1) *a je kvadratické residuum* $\bmod p$*, právě když $a^{\frac{p-1}{2}} \equiv 1 \bmod p$;*
(2) *a je kvadratické non-residuum* $\bmod p$*, právě když $a^{\frac{p-1}{2}} \equiv -1 \bmod p$;*
(3) *existuje $\frac{p-1}{2}$ kvadratických residuií $a \in < 1, p-1 >$ a $\frac{p-1}{2}$ kvadratických non-residuií $a \in < 1, p-1 >$.*

Důkaz. Z Malé Fermatovy věty (Věta 3.3) plyne, že $a^{p-1} \equiv 1 \bmod p$. Protože celá čísla modulo prvočíslo tvoří těleso a protože v každém tělese platí základní věta algebry, tak rovnice $x^2 \equiv 1 \mod p$ má jen dvě řešení, $x = 1$ nebo $x = -1$. Proto $a^{\frac{p-1}{2}} \equiv 1 \mod p$ nebo $a^{\frac{p-1}{2}} \equiv -1 \mod p$ a odtud plyne (1) a (2). Podle stejného argumentu rovnice $x^{\frac{p-1}{2}} \equiv 1 \bmod p$ a $x^{\frac{p-1}{2}} \equiv -1 \bmod p$ mají v $\mathbb{Z}_p^*$ nejvýše $\frac{p-1}{2}$ řešení. Jak bylo řečeno, rovnice $x^2 \equiv 1 \bmod p$ má v $\mathbb{Z}_p^*$ jen dvě řešení, a to 1 a -1, ptoto z Malé Fermatovy věty plyne, že každé $a \in \mathbb{Z}_p^*$ je buď řešením rovnice $x^{\frac{p-1}{2}} \equiv 1 \bmod p$ nebo $x^{\frac{p-1}{2}} \equiv -1 \bmod p$. Nyní z toho, že $\mathbb{Z}_p^*$ má právě $p-1$ prvků, dostáváme (3). □

Nyní budeme definovat Legendreův symbol. Mějme celé číslo a a liché prvočíslo p. Pak Legendreův symbol $\left(\frac{a}{p}\right)$ [26] je definován takto

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{když } a \text{ je kvadratické residuum } \bmod p, \\ -1 & \text{když } a \text{ je kvadratické non-residuum } \bmod p, \\ 0 & \text{když } p \text{ dělí } a. \end{cases}$$

Nejprve uvedeme základní vlastnosti Legendreova symbolu, a pak ho zobecníme na Jacobiho symbol.

Lemma 3.8. *Nechť p a q jsou lichá prvočísla. Pak pro celá čísla a a b platí*

(1) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$*, speciálně* $\left(\frac{-1}{p}\right) = 1$*, právě když* $p \equiv 1 \bmod 4$ *a* $\left(\frac{-1}{p}\right) = -1$*, právě když* $p \equiv 3 \bmod 4$*;*
(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$*;*
(3) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*, když* $a \equiv b \bmod p$*;*
(4) $\left(\frac{a^2}{p}\right) = 1$*, když p nedělí a;*
(5) $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$*, tedy* $\left(\frac{2}{p}\right) = 1$*, právě když* $p \equiv 1 \bmod 8$ *nebo* $p \equiv 7 \bmod 8$ *a* $\left(\frac{2}{p}\right) = -1$*, právě když* $p \equiv 3 \bmod 8$ *nebo* $p \equiv 5 \bmod 8$*;*
(6) *když $p \neq q$, pak* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$*, neboli* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$*, právě když* $p \equiv q \equiv 3 \bmod 4$*, jinak* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Důkaz. (1) plyne z Důsledku 3.7. Protože $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \bmod p$, tak (2) je důsledkem (1). (3) plyne přímo z definice. Z Malé Fermatovy věty plyne (4). (5) plyne z Gaussova lemmatu:

pro $a \in \mathbb{Z}_n^*$ označme $\mu(a)$ počet záporných čísel b z množiny

$$\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$$

takových, že $b \equiv c \bmod p$ pro nějaké $c \in \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. Pak $\left(\frac{a}{p}\right) = (-1)^{\mu(a)}$.

(6) se nazývá zákon kvadratické reciprocity a byl dokázán Gaussem. Opírá se o fakta z abstraktní algebry, pomocí nichž se pro dvě lichá prvočísla p a q ukáže ekvivalence tvrzení:

p je kvadratické residuum $\bmod q$;
vynásobení číslem p v $\mathbb{Z}_q^*$ je sudá permutace;
$(-1)^{\frac{q-1}{2}}q$ je kvadratické residuum $\bmod p$.

Z toho pak dostaneme (6). □

Jacobiho symbol je zobecněním Legendreova symbolu a je označován stejně jako Legendreův symbol. Jacobiho symbol je definován pro celé číslo a pro liché přirozené číslo n. Když n je prvočíslo, tak jeho hodnota se shoduje s hodnotou Legendreova symbolu, takže nedochází k žádným nesrovnalostem. Mějme celé číslo a a liché přirozené číslo $n > 1$ a nechť $p_1^{i_1}, p_2^{i_2}, \ldots, p_k^{i_k}$ je prvočíselný rozklad čísla n. Pak Jacobiho symbol je [21] $\left(\frac{a}{n}\right) = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right)^{i_j}$, kde v součinu na pravé straně je Legendreův symbol. Když $n = 1$, pak $\left(\frac{a}{1}\right) = 1$. Nejprve uvedeme základní vlastnosti Jacobiho symbolu, které jsou zobecněním Lemmatu 3.8 pro Legendreův symbol, a pak popíšeme algoritmus pro nalezení hodnoty Jacobiho symbolu.

Lemma 3.9. *Nechť n a m jsou lichá přirozená čísla a nechť a a b jsou celá čísla. Pak platí:*

(1) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$;
(2) $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$;
(3) $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$, *když* $a \equiv b \bmod n$;
(4) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$;
(5) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$;
(6) *když n a m jsou nesoudělná, pak* $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$.

Důkaz. Vlastnosti (1), (2) a (3) plynou z definice. Vlastnosti (4), (5) a (6) plynou z Lemmatu 3.8, když se použije, že pro lichá čísla $n_1, n_2, \ldots, n_k$ platí:

$$\sum_{i=1}^{k}\left(\frac{n_i - 1}{2}\right) \equiv \frac{\prod_{i=1}^{k} n_i - 1}{2} \bmod 2,$$

$$\sum_{i=1}^{k}\left(\frac{n_i^2 - 1}{8}\right) \equiv \frac{\prod_{i=1}^{k} n_i^2 - 1}{8} \bmod 2. \quad \square$$

Následující algoritmus pro výpočet Jacobiho symbolu je založen na kombinaci Lemmatu 3.9 a idejích Euklidova algoritmu pro nalezení největšího společného dělitele.

Algoritmus 3.10. [15,40]
Vstup: celé číslo a a liché přirozené číslo n.
if $a < 0$ nebo $a \geq n$ **then** $a := a \bmod n$ **endif** (tj. $0 \leq a < n$)
$t := 1$
while $a \neq 0$ **do**

while $a \equiv 2 \bmod 2$ **do**
$a := \frac{a}{2}$
if $n \equiv 3 \bmod 8$ nebo $n \equiv 5 \bmod 8$ **then** $t := -t$ **endif**
enddo
vyměňme a a n
if $a \equiv n \equiv 3 \bmod 4$ **then** $t := -t$ **endif**
$a := a \bmod n$ (tj. $0 \leq a < n$)
enddo
if $n = 1$ **then Výstup**: t **else Výstup**: 0 **endif**
Konec

Korektnost algoritmu plyne z následujícího invariantu, který je důsledkem Lemmatu 3.9:

> když a' a n' jsou hodnoty a a n po ukončení běhu některého **while**-cyklu, pak platí $\left(\frac{a}{n}\right) = t\left(\frac{a'}{n'}\right)$ (zde a a n jsou vstupy algoritmu).

Tedy dostáváme

Věta 3.11. *Algoritmus 3.10 korektně spočítá hodnotu Jacobiho symbolu* $\left(\frac{a}{n}\right)$ *a spotřebuje* $O((1 + \log|a|)\log n)$ *času.*

Důkaz. Korektnost algoritmu plyne z popsaného invariantu a z Lemmatu 3.9, a tedy zbývá odhadnout časovou složitost algoritmu. První krok algoritmu, výpočet $a \bmod n$, vyžaduje čas $O(\log n(1 + \log|a|))$ (použijeme klasický školní algoritmus pro celočíselné dělení se zbytkem). Po jeho provedení můžeme předpokládat, že $0 \leq a < n$. Nyní budeme rekurzivně definovat celá čísla a_i a n_i pro $i = 0, 1, \ldots$. Tato čísla popisují práci algoritmu. Položme $a_0 = a$ a $n_0 = n$. Když a_i a n_i jsou definovány a $a_i > 0$, pak rekurzivně definujme $a_i = 2^{e_{i+1}} n_{i+1}$, kde e_{i+1} je maximální přirozené číslo takové, že $2^{e_{i+1}}$ dělí a_i, $n_i = q_{i+1}n_{i+1} + a_{i+1}$, kde q_{i+1} a a_{i+1} jsou přirozená čísla a $a_{i+1} < n_{i+1}$. Když $a_i = 0$, pak končíme. Zřejmě n_i je liché pro každé i, pro které je definováno. Platí

$$n_0 > a_0 \geq n_1 > a_1 \geq \cdots \geq n_k > a_k.$$

Odhadneme velikost k. Když q_i je liché, pak a_i je sudé a $n_{i+1} \leq \frac{a_i}{2}$, když q_i je sudé, pak $q_i \geq 2$ a tedy $n_i \leq \frac{n_{i-1}}{2}$. Tedy můžeme shrnout, že $n_{i+1} \leq \frac{n_{i-1}}{2}$, a odtud plyne, že $k = O(\log n)$. Všimněme si, že vnější **while**-cyklus začíná s hodnotami a_0 a n_0 a i-tý běh vnějšího **while**-cyklu vypočítá hodnoty a_i a n_i, proto vnější **while**-cyklus běží k-krát. Dále i-tý běh vnějšího **while**-cyklu vyžaduje čas $(e_i + 1)\log a_{i-1} + \log q_i \log n_i$. Tedy algoritmus vyžaduje čas

$$O(\log a \log n + \sum_{i=1}^{k} \left[(e_i + 1)\log a_{i-1} + \log q_i \log n_i\right]).$$

Indukcí lehce dostaneme, že pro každé $i = 0, 1, \ldots, k-1$ platí $n_i \geq \prod_{j=i+1}^{k} q_j$, a proto $n \geq \prod_{j=1}^{k} q_j$. Z toho plyne

$$\sum_{i=1}^{k} \log q_i \log n_i \leq \log n_1 (k + \log \prod_{i=1}^{k} q_i) = O((1 + \log|a|)\log n)$$

(použili jsme, že $\log n_1 \leq \log a_0 \leq 1 + \log |a|$). Protože $2^{\sum_{i=1}^{k} e_i} \leq a_0$, dostáváme

$$\sum_{i=1}^{k}(e_i + 1)\log a_{i-1} \leq \log a_1(k + \sum_{i=1}^{k} e_i) \leq k \log a_1 + \log n_0 \log a_0 = O(\log n(1 + \log(1 + |a|))).$$

Tím je důkaz úplný. □

K charakterizaci prvočísel použijeme Lemma 3.8(1): když n je prvočíslo a a je nesoudělné s n, pak $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$. To vede k tomu, že pro liché přirozené číslo n definujeme

$$E_n = \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n\}.$$

Z Lemmatu 3.9(1) a z faktu, že $a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} = (ab)^{\frac{n-1}{2}}$, plyne, že E_n je podgrupa $\mathbb{Z}_n^*$. Když n není prvočíslo, tak se E_n nazývá grupou Eulerových lhářů. Solovay-Strassenův algoritmus je založen na následujícím tvrzení.

Tvrzení 3.12. [28,37]*Liché číslo $n \geq 3$ je prvočíslo, právě když $E_n = \mathbb{Z}_n^*$.*

Důkaz. Z Lemmatu 3.8(1) plyne, že když n je prvočíslo, pak $E_n = \mathbb{Z}_n^*$. Předpokládejme, že $E_n = \mathbb{Z}_n^*$ a n není prvočíslo. Pak pro každé $a \in \mathbb{Z}_n^*$ platí $a^{n-1} \equiv \left(\frac{a}{n}\right)^2 \equiv 1 \bmod n$, a proto n je Carmichaelovo číslo. Z Lemmatu 3.4 plyne, že existuje prvočíslo p a číslo r nesoudělné s p takové, že $n = pr$. Podle Důsledku 3.7(3) existuje kvadratické non-residuum q pro $\bmod p$. Podle Věty 3.1 existuje celé číslo a takové, že $0 \leq a < n$, $a \equiv q \bmod p$ a $a \equiv 1 \bmod r$. Podle Lemmatu 3.9(2) a (3) je

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{r}\right) = \left(\frac{q}{p}\right)\left(\frac{1}{r}\right) = (-1)(1) = -1$$

a protože $E_n = \mathbb{Z}_n^*$, dostáváme, že

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \equiv -1 \bmod n.$$

Protože r dělí n, tak také platí $a^{\frac{n-1}{2}} \equiv -1 \bmod r$, ale to je spor, protože $a \equiv 1 \bmod r$ implikuje $a^{\frac{n-1}{2}} \equiv 1 \bmod r$. Proto když n je liché a není prvočíslo, pak $E_n \neq \mathbb{Z}_n^*$. □

Tvrzení 3.12 vede k návrhu následujícího algoritmu.

Algoritmus 3.13. [28](Solovay-Strassenův algoritmus)
Vstup: přirozené číslo n
if $n = 2$ **then Výstup**: n je prvočíslo, **konec endif**
if $n < 2$ nebo n je sudé a $n > 2$ **then**
  Výstup: n není prvočíslo, **konec**
endif
zvolme náhodně přirozené číslo $a \in \{1, 2, \ldots, n-1\}$
if a a n jsou soudělná **then**
  Výstup: n není prvočíslo
else
  if $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ **then**

Výstup: n je prvočíslo
else
Výstup: n není prvočíslo
endif
endif
Konec

Pro zjištění, zda a a n jsou soudělná, použijeme Euklidův algoritmus, pro výpočet $\left(\frac{a}{n}\right)$ použijeme Algoritmus 3.10 a pro výpočet $a^{\frac{n-1}{2}} \bmod n$ použijeme následující rekursivní podproceduru

Power(x, a, R)
Vstup: číslo x, přirozené číslo a a okruh R, v kterém se realizuje násobení
if $a = 0$ **then**
Výstup: $x^a = 1$
else
if a je sudé **then**
$b := \frac{a}{2}$, $t :=$ **Power**(x, b, R), $t := t^2$
else
$b := a - 1$, $t :=$ **Power**(x, b, R), $t := tx$
endif
Výstup: $x^a = t$
endif
Konec

Korektnost podprocedury je zřejmá. Odtud plyne

Věta 3.14. *Solovay-Strassenův algoritmus je pravděpodobnostní algoritmus typu Monte Carlo řešící problém $PRIME(n)$ v čase $O(\log^3 n)$ s chybou $\leq \frac{1}{2}$.*

Důkaz. Z předchozích argumentů plyne, že Solovay-Strassenův algoritmus je pravděpodobnostní algoritmus typu Monte Carlo řešící problém $PRIME(n)$ s chybou $\leq \frac{1}{2}$. Euklidův algoritmus zjišťující, zda a a n jsou soudělná, vyžaduje čas $O(\log^2 n)$, algoritmus pro výpočet $\left(\frac{a}{n}\right)$ podle Věty 3.11 vyžaduje čas $O(\log^2 n)$. Musíme odhadnout čas rekursivní podprocedury **Power**. Označme $\mu(R)$ čas potřebný pro násobení v okruhu R, pak podprocedura **Power** bez rekursivních volání vyžaduje $O(\mu(R))$ času. Protože každé místo v binárním zápise čísla a odpovídá nejvýše dvěma rekurzivním voláním podprocedury **Power** (přesněji, když je na i-tém místě zleva 1, pak to odpovídá dvěma voláním, první změní 1 na 0 a druhé odstraní 0, když je na i-tém místě 0, tak to odpovídá jednomu volání), dostáváme, že procedura **Power** vyžaduje $O(\mu(R) \log a)$ času. Protože násobení v $\mathbb{Z}_n^*$ vyžaduje čas $O(\log^2 n)$ (standardní školní algoritmus), tak podprocedura **Power** vyžaduje čas $O(\log^3 n)$. Tedy Solovay-Strassenův algoritmus pracuje v čase $O(\log^3 n)$. Když bychom použili 'chytrý' algoritmus na násobení čísel, tak algoritmus bude pracovat v čase $O(\log^2 n \log\log n \log\log\log n)$. □

Rabin-Millerův algoritmus

V této části popíšeme pravděpodobnostní algoritmus navržený Rabinem na základě Millerova algoritmu. Tento algoritmus je založen na tomto postřehu. Když přirozené číslo n má k prvočíselných dělitelů, pak 1 má 2^k různých druhých odmocnin

z 1 v $\mathbb{Z}_n^*$. Tento fakt vede k definici S_n – předpokládejme, že $n-1 = 2^s d$, kde d je liché číslo, pak $S_n = \{a \in \mathbb{Z}_n^* \mid$ buď $a^d \equiv 1 \bmod n$ nebo $a^{2^r d} \equiv -1 \bmod n$ pro $0 \leq r < s\}$. Když n není prvočíslo, pak prvky v S_n se nazývají silní lháři. Následující lemma ukazuje korektnost tohoto pojmu. Důkaz je podle H. W. Lenstra a byl publikován v [9]

Lemma 3.15. [9]*Nechť $n \geq 3$ je liché přirozené číslo. Pak n je prvočíslo, právě když $\mathbb{Z}_n^* = S_n$. Když n není prvočíslo, pak $|S_n| \leq \frac{n-1}{4}$.*

Důkaz. Předpokládejme, že n je prvočíslo a $a \in \mathbb{Z}_n^*$. Podle Malé Fermatovy věty (Věta 3.3) $a^{n-1} \equiv 1 \bmod n$. Pak $a^{\frac{n-1}{2}} \equiv 1 \bmod n$ nebo $a^{\frac{n-1}{2}} \equiv -1 \bmod n$, protože existují přesně dva prvky $x \in \mathbb{Z}_n^*$ takové, že $x^2 \equiv 1 \bmod n$, a to $x \equiv 1 \bmod n$ nebo $x \equiv -1 \bmod n$. V druhém případě $a \in S_n$, v prvém případě buď $s = 1$ a $a \in S_n$, nebo $s \geq 2$ a pak buď $a^{\frac{n-1}{4}} \equiv 1 \bmod n$ nebo $a^{\frac{n-1}{4}} \equiv -1 \bmod n$. V druhém případě $a \in S_n$, v prvém případě buď $s = 2$ a $a \in S_n$ a v opačném případě, tedy když $s > 2$, můžeme celý postup zopakovat. Tedy indukcí podle velikosti s dostaneme, že $S_n = \mathbb{Z}_n^*$.

Předpokládejme, že $n \geq 3$ je liché, ale není prvočíslo. Nechť $p_1^{e_1}, p_2^{e_2}, \ldots, p_k^{e_k}$ je prvočíselný rozklad n. Předpokládejme, že $n - 1 = 2^s d$, kde d je liché. Nechť j je takové největší přirozené číslo, že existuje alespoň jedno $b \in \mathbb{Z}_n^*$, pro něž platí $b^{2^j} \equiv -1 \bmod n$. Protože $(-1)^{2^0} \equiv -1 \bmod n$, je j korektně definováno a zřejmě platí $0 \leq j < s$. Položme $m = 2^j d$ a definujme

$$\begin{aligned} J &= \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \bmod n\} \\ K &= \{a \in \mathbb{Z}_n^* \mid a^m \equiv \pm 1 \bmod p_i^{e_i}\ \forall i\} \\ L &= \{a \in \mathbb{Z}_n^* \mid a^m \equiv \pm 1 \bmod n\} \\ M &= \{a \in \mathbb{Z}_n^* \mid a^m \equiv 1 \bmod n\} \end{aligned}$$

Zřejmě $M \subseteq L \subseteq K \subseteq J \subseteq \mathbb{Z}_n^*$ a M, L, K a J jsou podgrupy $\mathbb{Z}_n^*$. Nejprve si ukážeme, že $S_n \subseteq L$. Skutečně, když $a \in S_n$, pak buď $a^d \equiv 1 \bmod n$, ale pak $a^m \equiv 1 \bmod n$, a tedy $a \in L$ nebo $a^{2^r d} \equiv -1 \bmod n$ pro $0 \leq r < s$. Z definice j plyne, že $r \leq j$, a tedy $a^m \equiv \pm 1 \bmod n$, a proto $a \in L$. Dále z definice j plyne $L \setminus M \neq \emptyset$ (když $b^{2^j} \equiv -1 \bmod n$, pak $b^m \equiv b^{2^j d} \equiv (b^{2^j})^d \equiv (-1)^d \equiv -1 \bmod n$, protože d je liché). Když $a \in L$ takové, že $a^m \equiv -1 \bmod n$ pak pro $x \in L$ platí $x^m \equiv -1 \bmod n$, právě když $ax \in M$. Skutečně, když $x^m \equiv -1 \bmod n$, pak $(ax)^m \equiv a^m x^m \equiv (-1)(-1) \equiv 1 \bmod n$, a tedy $ax \in M$. Když $ax \in M$, pak

$$x^m \equiv (a^{-1}ax)^m \equiv (a^{-1})^m (ax)^m \equiv (a^{-1})^m 1 \equiv (a^{-1})^m \bmod n.$$

Ale platí $1 \equiv (aa^{-1})^m \equiv a^m (a^{-1})^m \equiv (-1)(a^{-1})^m \bmod n$, a proto $(a^{-1})^m \equiv -1 \bmod n$, a tedy $x^m \equiv -1 \bmod n$. Z toho plyne, že $L = M \cup a^{-1}M$, ale $|M| = |a^{-1}M|$ a $M \cap a^{-1}M = \emptyset$. Proto $\frac{|L|}{|M|} = 2$. Protože $b^{2^j} \equiv -1 \bmod n$ implikuje, že $b^{2^j} \equiv -1 \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$, a tedy $b^m \equiv -1 \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$, dostaneme z Čínské věty o zbytcích (Věta 3.1), že pro každou posloupnost čísel $c = \{c_i\}_{i=1}^k$ takovou, že $c_i \in \{-1, 1\}$ pro každé $i = 1, 2, \ldots, k$, existuje $x_c \in K$ takové, že $x_c^m \equiv -1 \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$. Stačí vzít $x_c \in \mathbb{Z}_n$ takové, že $x_c \equiv b \bmod p_i^{e_i}$, když $c_i = -1$, a $x_c \equiv 1 \bmod p_i^{e_i}$, když $c_i = 1$. Pak x_c je nesoudělné s n, tedy patří do $\mathbb{Z}_n^*$, a $x_c^m \equiv b^m \equiv c_i \bmod p_i^{e_i}$,

když $c_i = -1$, a $x_c^m \equiv 1^m \equiv 1 \equiv c_i \bmod p_i^{e_i}$, když $c_i = 1$. Všimněme si, že pak $1 \equiv (x_c^{-1}x_c)^m \equiv (x_c^{-1})^m(x_c)^m \equiv (x_c^{-1})^m c_i \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$. Z toho plyne, že $(x_c^{-1})^m \equiv c_i \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$. Protože $x^m \equiv 1 \bmod n$ implikuje, že $x^m \equiv 1 \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots k$, tak dostáváme, že M je podgrupou K. Nyní ukážeme pro $x \in K$ a pro posloupnost $c = \{c_i\}_{i=0}^k$ složenou z -1 a 1, že $x^m \equiv c_i \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$, právě když $(x_c x) \in M$. Skutečně, když $x^m \equiv c_i \bmod p_i^{e_i}$, pak $(x_c x)^m \equiv (x_c)^m x^m \equiv c_i c_i \equiv 1 \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$ a z Čínské věty o zbytcích (Věta 3.1) dostáváme, že $(x_c x)^m \equiv 1 \bmod n$, a tedy $x_c x \in M$. Naopak, když $x_c x \in M$, pak $(x_c x)^m \equiv 1 \bmod p_i^{e_i}$ implikuje, že $(x_c x)^m \equiv 1 \bmod p_i^{e_i}$ pro každé $i = 1, 2, \ldots, k$. Nyní

$$x^m \equiv (x_c^{-1}x_c x)^m \equiv (x_c^{-1})^m (x_c x)^m \equiv (x_c^{-1})^m 1 \equiv c_i \bmod p_i^{e_i}$$

pro každé $i = 1, 2, \ldots, k$. Odtud plyne, že $K = \bigcup x_c M$, kde sjednocení se bere přes všechny posloupnosti $c = \{c_i\}_{i=1}^k$ složené z -1 a 1. Protože $|M| = |x_c M|$ pro každou takovou posloupnost c z -1 a 1 a protože pro dvě různé posloupnosti c a c' složené z -1 a 1 platí $x_c M \cap x_{c'} M = \emptyset$, dostáváme, že $|K| = 2^k |M|$, protože posloupností c složených z -1 a 1 je 2^k. Tedy $\frac{|K|}{|M|} = 2^k$, a odtud $\frac{|K|}{|L|} = 2^{k-1}$. Protože

$$\frac{n-1}{|S_n|} \geq \frac{|\mathbb{Z}_n^*|}{|S_n|} \geq \frac{|\mathbb{Z}_n^*|}{|L|} \geq \frac{|\mathbb{Z}_n^*|}{|J|}\frac{|K|}{|L|},$$

dostáváme, že když $k > 2$, pak $\frac{n-1}{|S_n|} \geq 4$. Když $k = 2$, pak podle Lemmatu 3.4 n není Carmichaelovo číslo, a tedy $\frac{|\mathbb{Z}_n^*|}{|J|} \geq 2$, a odtud $\frac{n-1}{|S_n|} \geq 4$, protože $\frac{|K|}{|L|} = 2^{k-1} = 2$. Uvažme případ, že $k = 1$ a $p_1 \neq 3$ nebo $e_1 \neq 2$ (tj. $n \neq 9$). Pak $|\mathbb{Z}_n^*| = p_1^{e_1-1}(p_1 - 1)$ a $\mathbb{Z}_n^*$ je cyklická grupa. Když g je generátor $\mathbb{Z}_n^*$, pak pro $a \in \mathbb{Z}_n^*$ máme $a \in J$, právě když $a = g^{ip_1^{e_1-1}}$. Skutečně, když $a = g^l$ a $a^{n-1} \equiv 1 \bmod n$, pak $g^{l(n-1)} \equiv 1 \bmod n$, a to je právě když $(p_1 - 1)p_1^{e_1-1}$ dělí $l(n-1) = l(p_1^{e_1} - 1)$. To nastane právě když $p_1^{e_1-1}$ dělí l, protože p_1 a $n - 1 = p_1^{e_1} - 1$ jsou nesoudělná. Z toho plyne, že $|J| = (p_1 - 1)$, takže $\frac{|\mathbb{Z}_n^*|}{|J|} \geq 4$, a proto $\frac{n-1}{S_n} \geq 4$. Ve všech těchto případech $\frac{|\mathbb{Z}_n^*|}{|L|} \geq 4$, a tedy $\mathbb{Z}_n^* \neq S_n$ protože $S_n \subseteq L$. Přímým ověřením zjistíme, že pro $n = 9$ platí $S_9 = \{1, 8\}$, a tedy $\frac{8}{|S_9|} = 4$ a $\mathbb{Z}_9^* \neq S_9$ (platí $|\mathbb{Z}_9^*| = 6$). Důkaz je hotov, protože $\frac{n-1}{|S_n|} \geq 4$ implikuje $\frac{n-1}{4} \geq |S_n|$. □

Poznámka. Všimněme si, že jsme dokázali, že když n není prvočíslo, pak existuje vlastní podgrupa G grupy $\mathbb{Z}_n^*$ taková, že $S_n \subseteq G$. Když n je součinem aspoň dvou prvočísel, pak stačí vzít $G = L$, a když n je mocnina prvočísla, pak podle Lemmatu 3.4 n není Carmichaelovo číslo, a tedy $S_n \subseteq J$ a J je vlastní podgrupa $\mathbb{Z}_n^*$.

Lemma 3.15 vede k návrhu následujícího pravděpodobnostního algoritmu

Algoritmus 3.16. [34,35](Rabin-Millerův algoritmus)
Vstup: přirozené číslo n
if $n = 2$ **then Výstup**: n je prvočíslo, **konec endif**
if $n < 2$ nebo n je sudé a $n > 2$ **then**
  Výstup: n není prvočíslo, **konec**
endif
nalezněme s a liché přirozené číslo d takové, že $n - 1 = 2^s d$
zvolme náhodně přirozené číslo $a \in \{1, 2, \ldots, n-1\}$
$a := a^d$

if $a \equiv 1 \bmod n$ **then Výstup**: n je prvočíslo. **konec endif**
$i = 0$
while $i < s$ a $a \not\equiv -1 \bmod n$ **do**
  $i := i + 1$, $a := a^2$
enddo
if $a \equiv -1 \bmod n$ **then**
  Výstup: n je prvočíslo
else
  Výstup: n není prvočíslo
endif
Konec

Pro výpočet a^d použijeme proceduru **Power** ze Solovay-Strassenova algoritmu. Nalezení d a s, když n je v binárním zápise, znamená provádět jen posuny.

Věta 3.17. *Rabin-Millerův algoritmus je pravděpodobnostní Monte Carlo algoritmus řešící problém $PRIME(n)$ v čase $O(\log^3 n)$ s chybou $\leq \frac{1}{4}$.*

Důkaz. Z předchozích argumentů plyne, že Rabin-Millerův algoritmus je pravděpodobnostní algoritmus typu Monte Carlo řešící problém $PRIME(n)$ s chybou $\leq \frac{1}{4}$, viz Lemma 3.15. Nalezení s a d vyžaduje čas $O(\log n)$. Protože výpočet **while-**cyklu představuje vlastně výpočet a^{n-1} procedurou **Power**, tak algoritmus spotřebuje $O(\log^3 n)$ času. □

Poznámka. Zde také platí stejně jako pro algoritmus Solovay-Strassena, že když se použije 'chytrý' algoritmus pro násobení čísel, tak Rabin-Millerů algoritmus bude také vyžadovat čas $O(\log^2 n \log\log n \log\log\log n)$.

Důsledky a souvislosti

Jednou ze základních otázek je rozdělení prvočísel. Jednu z možných odpovědí dává následující věta.

Věta 3.18. [9]*Nechť $p_1, p_2, \ldots$ je rostoucí posloupnost všech prvočísel. Pak $p_i \geq i \ln i$ pro každé přirozené číslo $i \geq 1$ a $p_i \leq i(\ln i + \ln\ln i)$ pro každé přirozené číslo $i \geq 6$.*

Jiný pohled je, když definujeme $\pi(n)$ jako počet prvočísel menších nebo rovných n a chceme znát průběh této funkce. Už Čebyšev [13,14] dokázal, že $\pi(n) = \Theta(\frac{x}{\ln x})$. Souvislost s řešením tohoto problému má Riemannova hypotéza [36], která tvrdí, že reálná část kořenů Riemannovy zeta funkce je $\frac{1}{2}$. Platí

Věta 3.19. [23]*Riemannova hypotéza je ekvivalentní s tvrzením, že*

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + O(x^{\frac{1}{2}+\varepsilon}) \quad \textit{pro každé } \varepsilon > 0.$$

Dále se ukázalo, že

Věta 3.20. [23]*Za předpokladu Riemannovy hypotézy platí*

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + O(\sqrt{x}\ln x).$$

Pro náš problém hraje podstatnou roli její rozšíření motivované Dirichletovým výsledkem

Věta 3.21. [16,17]*Když a je nesoudělné s n, pak existuje nekonečně mnoho prvočísel p takových, že $p \equiv a \bmod n$.*

Toto vedlo k definici $\pi(x, n, a)$ jako počtu prvočísel p takových, že $p \leq x$ a zároveň platí $p \equiv a \bmod n$. La Vellée Poussin [39] ukázal analogii Čebyševova odhadu, když pro nesoudělná a a n ukázal, že $\pi(x, a, n) = \Theta(\frac{x}{\phi(n) \ln x})$, kde ϕ je Eulerova funkce (tj. $\phi(n) = |\mathbb{Z}_n^*|$). To vedlo k rozšíření Riemannovy hypotézy. Tzv. Rozšířená Riemannova hypotéza (krátce ERH) říká, že všechny kořeny Dirichletový L-funkce s reálnou částí mezi 0 a 1 mají reálnou část rovnou $\frac{1}{2}$. Pak platí

Věta 3.22. [38]*Když a a n jsou nesoudělná přirozená čísla, pak EHR je ekvivalentní s tvrzením, že pro každé $\varepsilon > 0$ platí*

$$\pi(x, n, a) = \frac{\int_2^x \frac{dt}{\ln t}}{\phi(n)} + O(x^{\frac{1}{2}+\varepsilon}).$$

Lze také odvodit následující tvrzení o hustotě prvočísel

Věta 3.23. [38]*Za předpokladu ERH, když a a n jsou nesoudělná přirozená čísla, pak*

$$\pi(x, n, a) = \frac{\int_2^x \frac{dt}{\ln t}}{\phi(n)} + O(\sqrt{x}(\ln x + \ln n)).$$

Pro nás hraje důležitou roli následující výsledek od Ankeny

Věta 3.24. [7]*Za předpokladu ERH existuje číslo c takové, že pro každé liché n každá vlastní podgrupa grupy $\mathbb{Z}_n^*$ neobsahuje nějaké číslo $a \in \mathbb{Z}_n^*$ menší než $c \ln^2 n$.*

Tento výsledek umožňuje za předpokladu ERH determinizovat Solovay-Strassenův algoritmus. Místo náhodné volby a systematicky prohledáme všechna a menší než $c \ln^2 n$ a pokud test vždy projde, pak n je prvočíslo, v opačném případě n není prvočíslo. Tento algoritmus vyžaduje čas $O(\log^5 n)$, tedy lepší čas než vyžadují známé deterministické algoritmy pro problém $PRIME$ bez předpokladu ERH. Je zajímavé, že takto jednoduše nelze determinizovat Rabin-Millerův algoritmus, protože S_n není podgrupa. Na druhé straně podle poznámky za Lemmatem 3.15, když n není prvočíslo, pak existuje vlastní podgrupa L grupy $\mathbb{Z}_n^*$ obsahující S_n a podle Věty 3.24 stačí testovat jen $c \ln^2 n$ čísel, když zvolené číslo a neleží v podgrupě L, pak není silný lhář, a tedy Rabin-Millerův algoritmus lze determinizovat. První verze Rabin-Millerova algoritmu prezentovaná Millerem [31] byla deterministická a pokud platí ERH, tak algoritmus pracuje v polynomiálním čase (byl navržen přímo bez determinizace). Na tuto pravděpodobnostní podobu upravil tento algoritmus až Rabin.

Na závěr srovnáme Solovay-Strassenův a Rabin-Millerův algoritmus. Rabin-Millerův algoritmus je rychlejší, protože kromě posunů v binárním zápise $n - 1$ počítá prakticky jen $a^{\frac{n-1}{2}}$. Solovay-Strassenův algoritmus navíc používá Euklidův algoritmus a počítá $\left(\frac{a}{n}\right)$.

Rabin-Millerův algoritmus také počítá s menší chybou, protože každý silný lhář pro liché n, které není prvočíslo, je také Eulerův lhář. Tedy lepší odhad ve Větě 3.17 než ve Větě 3.14 není způsoben nepřesným počítáním.

Tato část byla napsána podle prezentace v knize od Bacha a Shallita [9].

Deterministický algoritmus pro $PRIME$

Cílem této kapitoly bude prezentovat polynomiální algoritmus, který pro přirozené číslo n rozhodne, zda n je prvočíslo. Algoritmus je založen na počítání s polynomy v okruzích $\mathbb{Z}_n$, proto každý uvažovaný polynom bude s celočíselnými koeficienty. Nejprve rozvedeme teorii těchto polynomů. Protože naším cílem je polynomiální algoritmus, kde vstup bude mít délku $\log n$ vzhledem k velikosti čísla n, budou všechny uvažované logaritmy o základu 2. Idea algoritmu vychází z následující charakterizace prvočísel. Začneme s několika konvencemi pro zápis polynomů, které budeme dále používat.

Budeme psát $p \equiv q \bmod n$ pro polynomy p a q a přirozené číslo $n > 1$, když pro každé celé číslo x bude platit $p(x) \equiv q(x) \bmod n$ (neboli $p = q$ v okruhu $\mathbb{Z}_n$). Když p, q a r jsou polynomy, pak budeme psát $p \equiv q \bmod r$, když $p = q + kr$ nebo $q = p + kr$ pro nějaký polynom k. Proto $p \bmod q$ bude polynom, který je zbytkem při dělení polynomu p polynomem q. Tedy stupeň $p \bmod q$ je nejvýše roven stupni polynomu p a je ostře menší než stupeň polynomu q. Speciálně $\big(p \equiv q \bmod r\big) \bmod n$ pro polynomy p, q a r a pro přirozené číslo n znamená, že pro každé přirozené číslo m platí: když $m_1 = \big(p \bmod r\big)(m)$ a $m_2 = \big(q \bmod r\big)(m)$, pak $m_1 \equiv m_2 \bmod n$.

Věta 4.1. *Nechť $p > 1$ je přirozené liché číslo. Pak následující tvrzení jsou ekvivalentní:*

(1) *p je prvočíslo;*
(2) *existuje přirozené číslo a nesoudělné s p takové, že $(x-a)^p \equiv (x^p-a) \bmod p$;*
(3) *pro každé přirozené číslo a nesoudělné s p platí $(x-a)^p \equiv (x^p-a) \bmod p$.*

Důkaz. Dokážeme 1) $\implies$ 3). Podle binomické věty koeficient polynomu $(x-a)^p$ u x^i pro $0 \le i \le p$ je $(-1)^{p-i}\binom{p}{i}a^{p-i}$. Když p je prvočíslo a $0 < i < p$, pak p dělí $\binom{p}{i}$, a tedy koeficient u x^i v polynomu $(x-a)^p$ je 0 modulo p. Pro $i = 0$ podle Malé Fermatovy věty platí $(-1)^{p-0}\binom{p}{0}a^{p-0} = (-a)^p \equiv -a \bmod p$. Pro $i = p$ platí $(-1)^{p-p}\binom{p}{p}a^{p-p} = 1$, a tedy $(x-a)^p \equiv x^p - a \bmod p$. Dokázali jsme implikaci 1) $\implies$ 3). Implikace 3) $\implies$ 2) je zřejmá.

Ukážeme implikaci 2) $\implies$ 1). Předpokládejme, že p není prvočíslo. Pak existuje prvočíslo q, které dělí p, a nechť k je největší přirozené číslo takové, že q^k dělí p. Pak q^k nedělí $\binom{p}{q}$. Skutečně,

$$\binom{p}{q} = \frac{\prod_{i=0}^{q-1}(p-i)}{q!},$$

a protože q je provočíslo a dělí p, tak q nedělí $p-i$ pro $i = 1, 2, \ldots, q-1$. Pak q^k nedělí $\frac{p}{q}$, a tedy ani $\binom{p}{q}$. Protože a je nesoudělné s p, je také nesoudělné s q, a proto a^{p-q} je nesoudělné s q. Odtud q^k nedělí $\binom{p}{q}a^{p-q}$, a tedy ani p nedělí $(-1)^{p-q}\binom{p}{q}a^{p-q}$. Proto koeficient u x^q v polynomu $(x-a)^p$ je různý od 0 modulo p a protože $0 < q < p$, dostáváme, že $(x-a)^p \not\equiv (x^p - a) \bmod p$ (polynom $(x-a)^p - x^p + a$ je polynom stupně alespoň q, a tedy je různý od nulového polynomu). Odtud dostáváme implikaci 2) $\implies$ 1). $\square$

Když budeme chtít použít přímo tuto vlastnost pro algoritmus řešící $PRIME$, pak musíme spočítat všechny koeficienty polynomu $(x-a)^p \bmod p$. Těchto koeficientů je $p+1$, a proto to vyžaduje čas $\Theta(p)$. Takže tuto větu nemůžeme použít

přímo. Naším cílem bude ukázat, že za jistých okolností stačí počítat jen koeficienty polynomu $(x-a)^p \bmod (x^r-1)$, kde r bude proti n malé číslo. Abychom to dokázali, budeme potřebovat několik technických lemmat. Začneme s odhadem velikosti speciálních nejmenších společných násobků.

Lemma 4.2. *Pro každé $m \geq 7$ je velikost nejmenšího společného násobku čísel $2, 3, \ldots, m$ aspoň 2^m.*

Důkaz. Nechť $m > 1$ je přirozené číslo. Označme n_m nejmenší násobek čísel $2, 3, \ldots, m$ a pro $k = 1, 2, \ldots, m$ definujme

$$I_k = \int_0^1 x^{k-1}(1-x)^{m-k}\mathrm{d}x.$$

Podle binomické věty dostáváme

$$(1-x)^{m-k} = \sum_{i=0}^{m-k} \binom{m-k}{i}(-x)^i 1^{m-k} = \sum_{i=0}^{m-k} \binom{m-k}{i}(-x)^i,$$

a tedy

$$I_k = \int_0^1 x^{k-1}(1-x)^{m-k}\mathrm{d}x = \int_0^1 x^{k-1} \sum_{i=0}^{m-k} \binom{m-k}{i}(-x)^i \mathrm{d}x =$$
$$\sum_{i=0}^{m-k}(-1)^i \binom{m-k}{i} \int_0^1 x^{k+i-1}\mathrm{d}x = \sum_{i=0}^{m-k}(-1)^i \binom{m-k}{i}\frac{1}{k+i}.$$

Protože $k \leq k+i \leq m$ pro $i = 0, 1, \ldots, m-k$, dostáváme, že $k+i$ dělí n_m, a proto $n_m I_k$ je celé číslo pro každé $k = 1, 2, \ldots, m$.

Nyní zintegrujeme per partes I_k a dostaneme

$$I_k = [\frac{x^k}{k}(1-x)^{m-k}]_0^1 + \frac{m-k}{k}\int_0^1 x^k(1-x)^{m-k-1}\mathrm{d}x = \frac{m-k}{k}I_{k+1}.$$

Rekurzivním dosazováním dostaneme

$$I_k = \frac{m-k}{k}I_{k+1} = \frac{m-k}{k}\frac{m-k-1}{k+1}I_{k+2} = \cdots = \frac{(m-k)!(k-1)!}{(m-1)!}I_m.$$

Protože

$$I_m = \int_0^1 x^{m-1}(1-x)^{m-m}\mathrm{d}x = \int_0^1 x^{m-1}\mathrm{d}x = \frac{1}{m},$$

platí

$$I_k = \frac{(m-k)!(k-1)!}{m!} = \frac{1}{k}\frac{(m-k)!k!}{m!} = \frac{1}{k\binom{m}{k}}.$$

Protože $I_k n_m = \frac{n_m}{k\binom{m}{k}}$ je celé číslo, tak $k\binom{m}{k}$ dělí n_m pro všechna přirozená čísla $m \geq 2$ a $1 \leq k \leq m$. Speciálně $m\binom{2m}{m}$ dělí n_{2m} a $(m+1)\binom{2m+1}{m+1}$ dělí n_{2m+1} pro každé přirozené číslo $m \geq 2$. Z definice binomiálních čísel plyne

$$(m+1)\binom{2m+1}{m+1} = (m+1)\frac{(2m+1)!}{(m+1)!m!} = \frac{(2m+1)!}{(m!)^2} =$$
$$(2m+1)\frac{(2m)!}{(m!)^2} = (2m+1)\binom{2m}{m},$$

takže $(2m+1)\binom{2m}{m}$ dělí n_{2m+1}. Protože $m\binom{2m}{m}$ dělí n_{2m} a n_{2m} dělí n_{2m+1}, dostáváme, že $m\binom{2m}{m}$ dělí n_{2m+1}, a protože m a $2m+1$ jsou nesoudělné čísla, tak dostáváme, že $m(2m+1)\binom{2m}{m}$ dělí n_{2m+1}. Z

$$4^m = 2^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} \leq (2m+1)\binom{2m}{m}$$

plyne $n_{2m+1} \geq m(2m+1)\binom{2m}{m} \geq m4^m$. Odtud pro $m \geq 2$ plyne

$$n_{2m+1} \geq 24^m = 2^{2m+1}$$

a pro $m \geq 4$ plyne

$$n_{2m+2} \geq n_{2m+1} \geq 44^m = 2^{2m+2}.$$

Protože $2^8 = 512$, ale nejmenší společný násobek čísel 2,3,4,5,6,7,8 je $8 \cdot 7 \cdot 5 \cdot 3 = 840$, dostáváme, že pro $m \geq 7$ platí $n_m \geq 2^m$. □

Na základě tohoto lemmatu dokážeme další technické lemma, které nám umožní nalézt polynom h malého stupně a rovnost $(x-a)^p \equiv x^p - a \bmod p$ redukovat na rovnost $(x-a)^p \equiv x^p - a \bmod h \bmod p$ (to značí, že pro každé $x \in \mathbb{Z}_p^*$ platí $[(x-a)^p \bmod h](x) \equiv [(x^p - a) \mod h](x) \bmod p$).

Lemma 4.3. *Pro liché $n \geq 1$ existuje r takové, že $1 < r \leq \lceil \log^5 n \rceil$ a buď r dělí s n nebo r a n jsou nesoudělné a $o_r(n) > \log^2 n$.*

Důkaz. Protože $3 \leq \log^5 3$ a $5 \leq \log^5 5$, tak stačí vyšetřovat $n \geq 7$ a můžeme použít Lemma 4.2. Dále můžeme předpokládat, že všechna přirozená čísla $2, 3, \ldots, \lceil \log^5 n \rceil$ jsou nesoudělná s n, protože jinak existuje $r = 2, 3, \ldots, \lceil \log^5 n \rceil$ takové, že dělí n a tvrzení platí. Nechť $a_1, a_2, \ldots, a_t$ je prostá posloupnost všech přirozených čísel z množiny $\{2, 3, \ldots, \lceil \log^5 n \rceil\}$ takových, že $o_{a_i}(n) \leq \log^2 n$ (protože a_i je nesoudělné s n, tak platí $n \bmod a_i \in \mathbb{Z}_{a_i}^*$, a tedy $o_{a_i}(n)$ je definováno). Podle definice pro každé $i = 1, 2, \ldots, t$ existuje $j_i \leq \log^2 n$ takové, že $n^{j_i} \equiv 1 \bmod a_i$, a proto a_i dělí $n^{j_i} - 1$. Položme

$$b = \prod_{i=1}^{\lceil \log^2 n \rceil} (n^i - 1),$$

pak $n^{j_i} - 1$ je dělitel b a tedy a_i dělí b. Proto nejmenší společný násobek čísel $a_1, a_2, \ldots, a_t$ dělí b. Protože platí

$$\sum_{i=1}^{\lceil \log^2 n \rceil} i \leq \frac{(1+\log^2 n)(2+\log^2 n)}{2} = \frac{\log^4 n + 3\log^2 n + 2}{2}$$

a protože pro $n \geq 5$ platí

$$\log^4 n - \frac{\log^4 n + 3\log^2 n + 2}{2} = \frac{\log^4 n - 3\log^2 n - 2}{2} =$$
$$\frac{\log^2 n(\log^2 n - 3) - 2}{2} \geq \frac{\log^2 n - 2}{2} > 0,$$

tak dostávéme

$$b = \prod_{i=1}^{\lceil \log^2 n \rceil} (n^i - 1) < \prod_{i=1}^{\lceil \log^2 n \rceil} n^i = n^{\sum_{i=1}^{\lceil \log^2 n \rceil} i} < n^{\log^4 n} = 2^{\log^5 n},$$

protože $n = 2^{\log n}$. Kdyby $\{a_1, a_2, \ldots, a_t\}$ byla posloupnost všech přirozených čísel z intervalu $< 2, \lceil \log^5 \rceil >$, pak podle Lemmatu 4.2 je jejich nejmenší společný násobek alespoň $2^{\log^5 n}$, a to je spor. Proto buď existuje v intervalu $< 2, \lceil \log^5 n \rceil >$ přirozené číslo r, které dělí n nebo přirozené číslo r nesoudělné s n a $o_r(n) > \log^2 n$. □

V další části textu předpokládáme, že je dané liché přirozené číslo n, přirozené číslo r takové, že je nesoudělné s n a $r \leq \lceil \log^5 n \rceil$ a $o_r(n) > \log^2 n$, a prvočíslo p, které dělí n, $o_r(p) > 1$ a $p > r$ (může platit i $n = p$). Všimněme si, že pro dostatečně velké přirozené číslo n takové r existuje, a podle Věty 4.1, když n je prvočíslo, pak pro každé přirozené a z intervalu $< 1, n >$ platí

$$\big((x-a)^n \equiv (x^n - a) \bmod (x^r - 1)\big) \bmod n.$$

Protože $o_r(n) > \log^2 n$, tak existuje prvočíslo p', které dělí n a $o_r(p') > 1$, takže podstatný předpoklad je, že $r < p$. Protože p dělí n a n a r jsou nesoudělná, tak i p a r jsou nesoudělná. Položme $\ell = \sqrt{\phi(r)} \log n$, kde ϕ je Eulerova funkce (tj. $\phi(n)$ je počet přirozených čísel a takových, že $0 < a < n$ a a a n jsou nesoudělná čísla).

Nechť I je množina všech přirozených čísel m takových, že pro každé přirozené čšlo a takové, že $0 < a \leq \ell$, platí

$$\big((x-a)^m \equiv x^m - a \bmod (x^r - 1)\big) \bmod p.$$

Následující lemmata ukazují důležité vlastnosti množiny I.

Lemma 4.4. *I je uzavřená vůči násobení.*

Důkaz. Zvolme přirozené číslo a takové, že $0 < a \leq \ell$. Mějme $m_1, m_2 \in I_g$. Pak platí $\big((x-a)^{m_2} \equiv x^{m_2} - a \bmod (x^r - 1)\big) \bmod p$ a použitím substituce $y = x^{m_1}$ dostaneme, že $\big((x^{m_1} - a)^{m_2} \equiv x^{m_1 m_2} - a \bmod (x^{m_1 r} - 1)\big) \bmod p$. Protože $(x^r - 1) \sum_{i=0}^{m_1 - 1} x^{ir} = x^{m_1 r} - 1$, tak dostáváme $\big((x^{m_1} - a)^{m_2} \equiv x^{m_1 m_2} - a \bmod (x^r - 1)\big) \bmod p$. Nyní z $\big((x-a)^{m_1} \equiv x^{m_1} - a \bmod (x^r - 1)\big) \bmod p$ plyne

$$\big((x-a)^{m_1 m_2} \equiv (x^{m_1} - a)^{m_2} \equiv x^{m_1 m_2} - a \bmod (x^r - 1)\big) \bmod p,$$

a tedy $m_1 m_2 \in I_g$. □

Ze zobecnění Malé Fermatovy věty víme, že $n^{\phi(r)} \equiv 1 \bmod r$, kde $\phi(r)$ je Eulerova funkce. Protože $o_r(n) > \log^2 n$, dostáváme $o_r(n)$ dělí $\phi(r)$, odtud plyne

$$\log^2 n < o_r(n) \leq \phi(r) \leq r - 1,$$

a tedy

$$\ell = \sqrt{\phi}(r) \log n < \sqrt{r}\sqrt{r} = r < p.$$

Toto využije následující lemma.

Lemma 4.5. *Když $n \in I$, pak $p, \frac{n}{p} \in I$.*

Důkaz. Položme $q = \frac{n}{p}$. Z předpokladu plyne, že pro každé přirozené číslo a takové, že $0 < a \leq \ell$, platí

$$\big((x-a)^n \equiv x^n - a \bmod (x^r - 1)\big) \bmod p.$$

Z Věty 4.1 plyne, že pro každé $a \in \mathbb{Z}_p^*$ platí

$$(x-a)^p \equiv x^p - a \bmod p$$

a protože $\ell < p$, tak $p \in I$. Dále

$$\big((x^p-a)^q \equiv (x-a)^{pq} \equiv (x-a)^n \equiv x^n - a \bmod (x^r-1)\big) \bmod p.$$

Když $q \notin I$, pak

$$\big((x-a)^q \equiv x^q + \sum_{i=0}^{q-1} \alpha_i x^i \bmod (x^r-1)\big) \bmod p,$$

kde $\alpha_i \neq 0$ pro nějaké $i = 1, 2, \ldots, r-1$. Pak ale

$$\big((x^n - a) \equiv (x^p-a)^q \equiv x^{pq} + \sum_{i=0}^{q-1} \alpha_i x^{ip} \bmod (x^r-1)\big) \bmod p,$$

a to je spor s tím, že $n \in I$, protože $\alpha_i \neq 0$ pro nějaké $i = 1, 2, \ldots, r-1$. □

Lemma 4.6. *Když f a g jsou polynomy a $m > 1$ je přirozené číslo takové, že $(f(x))^m \equiv f(x^m) \bmod p$ a $(g(x))^m \equiv g(x^m) \bmod p$, pak $(f \cdot g(x))^m \equiv f \cdot g(x^m) \bmod p$.*

Důkaz. Zřejmě platí $(f \cdot g(x))^m \equiv (f(x))^m \cdot (g(x))^m \equiv f(x^m) \cdot g(x^m) \equiv (f \cdot g(x^m)) \bmod p$. □

Nyní si připomeneme některá fakta o cyklotomických polynomech, která lze najít na internetu nebo v monografii [30]. Je známé, že kořeny polynomu $x^m - 1$ pro přirozené číslo $m > 1$ v tělese komplexních čísel jsou komplexní čísla $e^{2\pi i \frac{k}{m}}$ pro $k = 0, 1, \ldots, m-1$. Tato čísla spolu s násobením tvoří cyklickou grupu a $e^{2\pi i \frac{k}{m}}$ je generátorem této grupy, právě když k je nesoudělné s m. Když k je nesoudělné s m, pak $e^{2\pi i \frac{k}{m}}$ se se nazýva m-tou primitivní odmocninou z 1 a hraje důležitou roli v rychlé diskrétní Fourierové transformaci. Polynom

$$\Phi_m(x) = \prod \{(x - e^{2\pi i \frac{k}{m}}) \mid k = 1, 2, \ldots, m-1,\ k \text{ a } m \text{ jsou nesoudělná}\}$$

se nazývá m-tý cyklotomický polynom. Koeficienty Φ_m jsou celá čísla a jeho stupeň je $\phi(m)$ a Φ_m dělí polynom $x^m - 1$. Když a je vícenásobný kořen polynomu f, pak a je kořen i jeho derivace, ale žádný kořen polynomu $x^m - 1$ není kořenem mx^{m-1}. Proto všechny kořeny polynomu $x^m - 1$ jsou jednonásobné (v každém tělese). Tedy Φ_m má v každém tělese jen jednonásobné kořeny. Dále $\Phi_m = \frac{x^m-1}{f}$, kde f je polynom, který je nejmenším společným násobkem polynomů $x^d - 1$, kde d dělí m.

Připomínáme, že polynom h is irreducibilní v okruhu O, když neexistují polynomy f a g stupně menšího než stupeň h takové, že $f \cdot g = h$ v okruhu O. Když polynom h je irreducibilní faktor polynomu Φ_m v $\mathbb{Z}_q$, kde q je prvočíslo, pak stupeň h je $o_m(q)$. Tato fakta dále použijeme, ale nejprve si připomeneme základní výsledky o podílových tělesech.

Lemma 4.7. [30]*Nechť q je prvočíslo a h je irreducibilní polynom v $\mathbb{Z}_q$ stupně d, kde $d \geq 2$. Pak podílové těleso $\mathbb{Z}_q[x]/h$ je konečné těleso o velikosti q^d s cyklickou multiplikativní grupou, které je extenzí $\mathbb{Z}_p$ o polynom h.* □

Zafixujme si některý irreducibilní faktor h polynomu Φ_r v $\mathbb{Z}_p$ a uvažujme těleso $\mathbb{Z}_p[x]/h$. Dále nechť $q = \frac{n}{p}$, nechť P je množina polynomů

$$\prod\{(x-a)^{m_a} \mid a \in \{0,1,\ldots,\ell\},\, m_a \geq 0 \text{ je přirozené číslo}\}$$

a nechť $G = \{(f \bmod h) \bmod p \mid f \in P\}$. Pak G je podgrupa multiplikativní grupy $\mathbb{Z}_p[x]/h$. Připomínáme, že dva polynomy f a g nad $\mathbb{Z}_p$ odpovídají stejnému polynomu v $\mathbb{Z}_p[x]/h$, právě když $f \equiv g \bmod h$. Protože p i q jsou nesoudělná s r, tak $H = \{p^i q^j \bmod r \mid i,j \geq 0\}$ tvoří podgrupu $\mathbb{Z}_r^*$. Označme t velikost H. Všimněme si, že $H \subseteq I$.

Nyní nalezneme horní a dolní odhad na velikost grupy G. Z toho nám vyplyne, že když n nebude prvočíslo a když nalezneme r a p požadovaných vlastností, pak n bude mocnina prvočísla p. Nejprve si všimněme, že polynom h dělí Φ_r a Φ_r dělí polynom $x^r - 1$, proto $x^r \equiv 1 \mod h$, a tedy x je r-tá odmocnina 1 v $\mathbb{Z}_p^*/h$.

Lemma 4.8. *Když $f, g \in P$ jsou dva různé polynomy, které mají stupeň menší než t, pak $f \bmod h$ a $g \bmod h$ jsou různé polynomy v grupě G.*

Důkaz. Předpokládejme opak. Nechť $f, g \in P$ jsou polynomy, které nesplňují tvrzení lemmatu, tedy stupně f i g jsou menší než t a $f \equiv g \bmod h$. Pak $f(x)^m \equiv g(x)^m \bmod h$ pro každé přirozené číslo m. Podle Lemmatu 4.6 pro každé $m \in I$ platí $\big(f(x)^m \equiv f(x^m) \bmod (x^r-1)\big) \bmod p$ a $\big(g(x)^m \equiv g(x^m) \bmod (x^r-1)\big) \bmod p$. Protože h dělí $x^r - 1$, dostáváme, že $\big(f(x^m) \equiv g(x^m) \mod h\big) \bmod p$. Definujme polynom $k = f - g$, pak polynom k má stupeň menší než t, ale x^m je kořen k v tělese $\mathbb{Z}_p^*/h$ pro každé $m \in I$. Když $n \in I$, pak podle Lemmatu 4.5 $p, q = \frac{n}{p} \in I$ a podle Lemmatu 4.4 $p^i q^j \in I$ pro každé $i,j \geq 0$. Tedy $x^{p^i q^j}$ je kořen polynomu k v tělese $\mathbb{Z}_p^*/h$. Všimněme si, že když ukážeme, že $x^{p^i q^j}$ a $x^{p^{i'} q^{j'}}$ jsou různé prvky $\mathbb{Z}_p^*/h$, jakmile $p^i q^j$ a $p^{i'} q^{j'}$ jsou různé prvky v grupě H, pak dostáváme spor se Základní větou algebry, protože stupeň k je menší než t, ale má alespoň t kořenů v $\mathbb{Z}_p^*/h$. Odtud plyne, že $f \not\equiv g \bmod h$, a tedy $f \bmod h$ a $g \bmod h$ jsou různé prvky v G. To bude spor a důkaz bude hotov.

Z definice grupy H plyne,že $p^i q^j$ a $p^{i'} q^{j'}$ jsou stejné prvky v grupě H, právě když $p^i q^j \equiv p^{i'} q^{j'} \bmod r$. Dále $x^{p^i q^j}$ a $x^{p^{i'} q^{j'}}$ jsou stejné prvky $\mathbb{Z}_p^*/h$, právě když $x^{p^i q^j} \equiv x^{p^{i'} q^{j'}} \bmod h$, a to je právě když h dělí $x^{p^i q^j} - x^{p^{i'} q^{j'}}$. Bez újmy na obecnosti můžeme předpokládat, že $m_1 = p^i q^j > m_2 = p^{i'} q^{j'}$ a že $x^{p^i q^j} \equiv x^{p^{i'} q^{j'}} \bmod h$. Proto h dělí $x^{m_2}(x^{m_1 - m_2} - 1)$. Protože 0 není kořen h, tak z toho plyne, že h dělí $x^{m_1 - m_2} - 1$. Když h dělí $x^m - 1$ a také dělí $x^{m'} - 1$ pro $m' < m$, pak h také dělí $x^m - 1 - x^{m'} + 1 = x^{m'}(x^{m-m'} - 1)$ a stejným obratem dostáváme, že h dělí $x^{m-m'} - 1$. Z definice h víme, že h dělí $x^r - 1$. Ukážeme, že neexistuje s takové, že $1 \leq s < r$ takové, že h dělí $x^s - 1$. Z toho dostaneme, že $m_1 - m_2$ je násobek r neboli $m_1 \equiv m_2 \bmod r$. Předpokládejme, že existuje s takové, že $1 \leq s < r$ takové, že h dělí $x^s - 1$ a nechť s je nejmenší takové, že h dělí $x^s - 1$ a $1 \leq s < r$. Opakovaním předchozího postupu dostaneme postupně, že h dělí $x^{r-s} - 1$, $x^{r-2s} - 1$, $x^{r-3s} - 1$, atd. Tedy buď nalezneme $1 \leq s' < s$ takové, že h dělí

$x^{s'} - 1$, a to bude spor s definicí s, nebo r je násobkem s. Ale to je spor s definicí h, h je faktor cyklotomického polynomu Φ_r, všechny kořeny Φ_r jsou jednonásobné a navíc $\Phi_r = \frac{x^r-1}{f}$, kde f je polynom, který je nejmenším společným násobkem polynomů $x^d - 1$, kde d dělí r. Proto když d dělí r, pak $x^d - 1$ a Φ_r jsou nesoudělné, a tedy také h a $x^d - 1$ jsou nesoudělné. Tedy takové s neexistuje a $m_1 \equiv m_2 \bmod r$ a důkaz je kompletní. □

Důsledek 4.9. *Když $n \in I$, pak $|G| \geq \binom{t+l}{t-1}$.*

Důkaz. Z Lemmatu 4.8 plyne, že když $f, g \in P$ jsou dva různé polynomy, které mají stupeň menší než t, pak $f \bmod h$ a $g \bmod h$ jsou různé polynomy v grupě G. Protože $i \neq j$ v $\mathbb{Z}_p$ pro $0 \leq i \neq j \leq \ell$ (platí $\ell = \sqrt{\phi(r)} \log n \leq \sqrt{r} \log n \leq r < p$), tak $x - a$ pro $a = 0, 1, \ldots \ell$ jsou navzájem různé polynomy v $\mathbb{Z}_p^*$ stupně 1. Pak polynomů stupně menšího než t v množině P je tolik, kolik je podmnožin s násobností velikosti t z ℓ prvků (množina s násobností je množina, kde každému prvku je přiřazené kladné celé číslo, jeho násobnost, a velikost množiny je součet násobností prvků v množině). Proto podle počtu kombinací s opakováním dostáváme $|G| \geq \binom{t+l}{t-1}$. □

Lemma 4.10. *Když n není mocnina p a $n \in I$, pak $|G| \leq n^{\sqrt{t}}$.*

Důkaz. Uvažujme množinu $J = \{p^i q^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor\}$. Když n není mocninou p, pak $|J| = (\lfloor \sqrt{t} \rfloor + 1)^2 > t$ a protože $|H| = t$, existují dva různé prvky $m_1, m_2 \in J$ takové, že $m_1 \equiv m_2 \bmod r$. Předpokládejme, že $m_2 = m_1 + kr$ pro přirozené číslo k. Protože polynom $x^r - 1$ dělí polynom $x^{kr} - 1$ pro každé přirozené číslo k, dostáváme, že $x^{kr} \equiv 1 \bmod (x^r - 1)$, a odtud plyne $x^{m_2} \equiv x^{m_1 + kr} \equiv x^{m_1} x^{kr} \equiv x^{m_1} \bmod (x^r - 1)$. Protože h dělí $x^r - 1$, tak i $x^{m_2} \equiv x^{m_1} \bmod h$. Uvažujme polynom $f \in P$, pak $f \bmod h \in G$. Podle Lemmat 4.4, 4.5 a 4.6 dostáváme

$$\big(f(x)^{m_1} \equiv f(x^{m_1}) \equiv f(x^{m_2}) \equiv f(x)^{m_2} \bmod (x^r - 1)\big) \bmod p.$$

Uvažujme polynom $g = x^{m_1} - x^{m_2}$, pak stupeň g je menší než $q^{\sqrt{t}} p^{\sqrt{t}} = n^{\sqrt{t}}$. Protože pro každý prvek $f \in G$ a každé $x \in \mathbb{Z}_p$ platí

$$\big(g(f(x)) \equiv f(x)^{m_1} - f(x)^{m_2} \equiv f(x^{m_1}) - f(x^{m_2}) \equiv 0 \bmod (x^r - 1)\big) \bmod p,$$

tak dostáváme, že každé $f \in G$ je kořenem polynomu g v tělese $\mathbb{Z}_p^* / \bmod h$ (protože h dělí $x^r - 1$). Ze Základní věty algebry pak plyne, že $|G| \leq n^{\sqrt{t}}$. □

Lemma 4.11. *Když $n \in I$, pak n je mocnina p.*

Důkaz. Podle Lemmatu 4.9 platí $|G| \geq \binom{t+l}{t-1}$ a podle Lemmatu 4.10, když n není mocnina p, pak platí $|G| \leq n^{\sqrt{t}}$. Protože n a r jsou nesoudělná čísla, $o_r(n) > \log^2 n$ a $t = |H| = \{p^i q^j \bmod r \mid 0 \leq i, j\}$, tak dostáváme, že $t > \log^2 n$, protože $p^i q^i = n^i$, a tedy $t - 1 \geq \lfloor \sqrt{t} \log n \rfloor$. Z nerovnosti $t \leq \phi(r)$ (každé $p_i q^j$ je nesoudělné s n), plyne, že $\ell = \sqrt{\phi(r)} \log n \geq \sqrt{t} \log n$. Dále použijeme, že pro přirozená čísla $a \geq b > c$ platí $\frac{a!}{b!} \geq \frac{(a-c)!}{(b-c)!}$ a odtud plyne $\binom{a}{b} \geq \binom{a-c}{b-c}$. Z těchto vztahů dostaváme

$$\binom{t+\ell}{t-1} \geq \binom{\ell+1+t-1}{t-1} \geq \binom{\ell+1+\lfloor \sqrt{t} \log n \rfloor}{\lfloor \sqrt{t} \log n \rfloor} \geq \binom{2\lfloor \sqrt{t} \log n \rfloor + 1}{\lfloor \sqrt{t} \log n \rfloor} =$$

$$\prod_{i=1}^{\lfloor \sqrt{r} \log n \rfloor} \frac{\lfloor \sqrt{t} \log n \rfloor + 1 + i}{i} > 2^{\sqrt{t} \log n} = n^{\sqrt{t}},$$

a proto n je mocnina prvočísla. □

Shrneme dokázané výsledky. Když ověříme, že neexistují přirozená čísla a a b taková, že $b > 1$ a $a^b = n$, pak můžeme postupně prohledávat přirozená čísla r od 2 v rostoucím pořadí a testovat, zda r dělí n nebo zda $o_r(n) > \log^2 n$. Podle Lemmatu 4.3 víme, že existuje $r < \log^5 n$ a buď r dělí n nebo každé prvočíslo, které dělí n je větší než r a $o_r(n) > \log^2 n$. Když $n \leq r$, pak $n \leq \log^5 n$, a tedy není problém přímo ověřit, zda n není prvočíslo (např. Eratosthenovým sítem). Teď jsou splněné předpoklady Lemmatu 4.11, a tedy n je prvočíslo, právě když pro každé $a = 1, 2, \ldots, \ell$ platí $\big((x-a)^n \equiv x^n - a \bmod (x^r - 1)\big) \bmod n$. Už jsme připraveni zformulovat algoritmus.

Algoritmus 4.12. Vstup: přirozené číslo $n \geq 1$
if $n = 2$ **then** n je prvočíslo, **konec endif**
if $n = 1$ nebo $n > 2$ je sudé **then** n není prvočíslo **konec endif**
if $n = a^b$ pro přirozená čísla a, b, $b > 1$ **then** n není prvočíslo **konec endif**
najdi nejmenší $r > 1$ takové, že $o_r(n) > \log^2 n$ nebo r dělí n
if $r < n$ a dělí n **then** n není prvočíslo **konec endif**
if $n \leq r$ **then** ověř, zda je n prvočíslo a podle toho přijmi **konec endif**
for every $a \in \{1, 2, \ldots, \sqrt{\phi(r)} \log n$ **do**
  if $\big((x-a)^n \not\equiv x^n - a \bmod (x^r - 1)\big) \bmod n$ **then** n není prvočíslo **konec endif**
enddo
n je prvočíslo
konec

Věta 4.13. *Algoritmus 4.12 dává korektní výsledek.*

Důkaz. Když jedna z prvních tří podmínek **if** je splněna, pak výstup je korektní. V dalším příkazu hledáme vhodné r a podle Lemma 4.5, když $n \geq 3$, pak buď takové r existuje a je menší než $\log^5 n$, nebo nějaké číslo menší než $\log^5 n$ dělí n. Když nastane druhý případ a nalezené číslo je menší než n, pak n není prvočíslo a následující příkaz **if** je korektní. Další příkaz **if** také dává korektní výsledek a aplikuje se jen v konečně mnoha vstupech (když $n \leq \log^5 n$). Všimněme si, že když máme provádět cyklus, tak žádné přirozené číslo a takové, že $2 \leq a \leq r$, nedělí n, a protože $\ell = \sqrt{\phi(r)} \log n < r$, tak všechna přirozená čísla a taková, že $1 \leq a \leq \ell$, jsou nesoudělná s n. Podle Věty 4.1 příkaz **if** v cyklu dává korektní výsledek. Zbývá jen ověřit, že když n není prvočíslo, tak nejsou splněny příkazy **if** v cyklu pro všechna $a \in \{1, 2, \ldots, \ell\}$. Když se to stane, pak $n \in I$, a podle Lemmatu 4.11 $n = p^e$ pro vhodné přirozené číslo $e \geq 1$. Když $e > 1$, pak třetí příkaz **if** ukončí běh algoritmu s korektním výsledkem a když $e = 1$, pak $n = p$ je prvočíslo. □

Zbývá popsat provedení jednotlivých příkazů a provést časovou analýzu algoritmu. V časové analýze symbol $f = \tilde{O}(g)$ znamená, že $f = O(g \log^{O(1)} g)$.

V následující analýze pro násobení nebo dělení dvou n-ciferných čísel použijeme Schönhage-Strassenův algoritmus [5], a tedy násobení a dělení v $\mathbb{Z}_n$ vyžaduje čas $\tilde{O}(\log n)$ a pro násobení a dělení polynomů stupně k v $\mathbb{Z}_n$ použijeme kombinaci rychlé diskrétní Fourierovy transformace s Schönhage-Strassenovým algoritmem [5], a tedy bude vyžadovat čas $\tilde{O}(k \log k \log n)$. V závorce budeme uvádět výsledek analýzy, když se místo těchto algoritmu použijí standardní školní algoritmy (násobení a dělení v $\mathbb{Z}_n$, pak vyžaduje čas $O(\log^2 n)$ a násobení a dělení polynomů stupně nejvýše k vyžaduje čas $O(k^2 \log k \log^2 n)$).

Podle Lemmatu 4.3, když $n \geq 3$, pak pro nějaké $r \leq \log^5 n$ platí, že buď r dělí n nebo $o_r(n) > \log^2 n$. Proto můžeme použít hrubou sílu pro nalezení r. Procedura může mít tvar:

$r := 2$, $m := n$, $e := 1$
while $e \leq \log^2 n$ **do**
  if r dělí $m - 1$ **then**
    $m := n$, $r := r + 1$, $e := 1$
    if r dělí n **then** exit z cyklu **endif**
  else
    $m := m \cdot n \bmod r$, $e := e + 1$
  endif
enddo
r je hledané číslo

Protože n je liché, tak platí invariant 'buď $e = 1$ nebo žádné k takové, že $1 < k \leq r$ nedělí n' (a v tom případě r a n jsou nesoudělná). První příkaz **if** v cyklu testuje, zda $o_r(n) = e < \log^2 n$. Když toto zjistí tak pokračuje na následujícím r a otestuje, zda toto r nedělí n. Podle Lemmatu 4.3 se cyklus v této podproceduře provádí jen pro $r \leq \log^5 n$ a pro každé r se provádí nejvýše $(2 + \log^2 n)$-krát. Proto tato procedura vyžaduje čas $\tilde{O}(\log^8 n)$ (nebo $O(\log^9 n)$).

Když $n \leq r$, pak lze použít Eratosthenevo síto, a to vyžaduje sice čas $O(n)$, protože se však používá jen v případě, že $n \leq r < \log^5 n$, tak se použije jen v konečně mnoha případech a nemá vliv na časovou analýzu.

Vynásobení dvou polynomů stupně nejvýše r v $\mathbb{Z}_n$ vyžaduje čas $\tilde{O}(r \log r \log n)$ (nebo $\tilde{O}(r^2 \log^2 n)$) Když pro umocňování použijeme algoritmus z předchozí sekce, tak výpočet $\big((x-a)^n \bmod (x^r-1)\big) \bmod n$ vyžaduje čas $\tilde{O}(\log^7 n)$ (nebo $\tilde{O}(\log^{13} n)$), protože $r < \log^5 n$. Protože $x^r \equiv 1 \bmod (x^r - 1)$, dostáváme $(x^n - a) \equiv x^{n \bmod r} - a \bmod (x^r - 1)$, a tedy pro dané a zjistit, zda

$$\big((x - a)^n \equiv x^n - a \bmod (x^r - 1)\big) \bmod n,$$

vyžaduje čas $\tilde{O} \log^7 n)$ (nebo $\tilde{O}(\log^{13} n)$). Tedy test pro všechny hodnoty $a = 1, 2, \ldots, \ell$ vyžaduje celkově čas $\tilde{O}(\log^{10.5} n)$ (nebo $\tilde{O}(\log^{16.5} n)$, protože $\sqrt{\phi(r)} < \log^{2.5} n$.

Zbývá popsat proceduru, která pro dané přirozené číslo n zjistí, zda existují přirozená čísla a a b taková, že $b > 1$ a $n = a^b$. Nejprve si všimněme, že binární zápis čísla n má délku $\lfloor \log n \rfloor + 1$, a dále když $n > 1$ a délka binárního zápisu čísla n je k, pak neexistuje přirozené číslo a takové, že $a^k = n$ (skutečně, když a existuje, pak $a \geq 2$, a tedy $\log a \geq 1$ a $\log a^k = k \log a \geq k > \log n$). Nejprve popíšeme proceduru, která v polynomiálním čase pro daná přirozená čísla n a k taková, že $n, k > 1$ a $k < \log n$ rozhodne, zda existuje přirozené číslo a takové, že $a^k = n$, a pokud takové a existuje nalezne ho. Vyjdeme z triviální nerovnosti $1^k = 1 < n < n^k$.

$u := 1$, $v := n$
while $u + 1 < v$ **do**
  $w := \lceil \frac{u+v}{2} \rceil$, spočítej w^k
  if $w^k = n$ **then** $a := w$ **konec endif**
  if $w^k < n$ **then** $u := w$ **else** $v := w$ **endif**

enddo
neexistuje a takové, že $a^k = n$
Konec

Korektnost algoritmu plyne z invariantu, že pokud algoritmus běží, tak platí $u^k < n < v^k$. Když použijeme algoritmus pro výpočet mocniny popsaný v předchozí sekci, pak výpočet w^k vyžaduje čas $\tilde{O}(\log^2 n)$ (nebo $O(\log^3 n)$). Protože w^k se počítá nejvýše pro $\log n$ hodnot w, celá procedura vyžaduje čas $\tilde{O}(\log^3 n)$ (nebo $O(\log^4 n)$). Nyní se vrátíme k našemu problému. Jak už jsme poznamenali, stačí vyzkoušet nejvýše $1+\log n$ hodnot b, zda pro ně neexistuje přirozené číslo a takové, že $a^b = n$. Proto tento test vyžaduje čas $\tilde{O}(\log^4 n)$ (nebo $O(\log^5 n)$).

Závěrečné poznámky. Číslo $1 + \lfloor \log n \rfloor$ je délka binárního zápisu čísla n a proto není problém pracovat s $\log n$. Hodnotu $\phi(r)$ můžeme zjistit prohledáním všech čísel $1, 2, \ldots, r-1$ a zjištěním, zda jsou nesoudělná s r. Protože $r < \log^5 n$ tak to vyžaduje čas $\tilde{O}(\log^5 n)$. Druhá alternativa je provádět test $\big((x-a)^n \equiv x^n - a \bmod (x^r - 1)\big)n$ pro všechna $a = 1, 2, \ldots, \lceil \log^{3.5} n \rceil$. V obou případech uvedená časová analýza dává stejný odhad. Na závěr si všimněte, že poslední algoritmus vlastně nalezne nejmenší přirozené číslo a, že $a^k \geq n$, tedy $a = \lceil \sqrt[k]{n} \rceil$. Tím je časová analýza algoritmu ukončena.

Tedy můžeme shrnout

Věta 4.14. *Algoritmus 4.12 bude vyžadovat čas $\tilde{O}(\log^{\frac{21}{2}} n)$ (nebo $\tilde{O}(\log^{\frac{33}{2}} n)$.)* □

Na závěr uvedeme několik hypotéz, jejichž platnost by vedla k zrychlení algoritmu.

Artinova hypotéza. Pro přirozené číslo n, které není perfektní čtverec, je počet prvočísel $q \leq m$, pro která platí $o_q(n) = q - 1$, asympoticky nejvýše $A(n)\frac{m}{\ln m}$, kde $A(n)$ je Artinova konstanta taková, že $A(n) > 0.35$.

Hypotéza Sophie Germainové o hustotě prvočísel. Počet prvočísel $q \leq m$ takových, že $2q + 1$ je také prvočíslo, je asymptoticky $\frac{2Cm}{\ln^2 m}$, kde C je konstanta prvočíselných dvojčat a odhaduje se na 0.6601618.

Když Artinova hypotéza platí pro $m = O(\log^2 n)$, pak $r = O(\log^2 n)$. Ví se, že když platí zobecněná Riemannova hypotéza, pak Artinova hypotéza platí. Když platí hypotéza Sophie Germainové, pak $r = \tilde{O}(\log^2 n)$. V obou případech by pak časová složitost Algoritmu 4.12 byla $\tilde{O}(\log^6 n)$ (to znamená, že za rozšířené Riemannovy hypotézy by derandomizace Solovay-Strassenova algoritmu i Rabin-Millerova algoritmu byly rychlejší).

References

1. L. Adleman and M-D. A. Huang, *Primality Testing and Two Dimensional Abelian Varieties over Finite Fields*, Verlag-Springer, Lesture in Mathematics 1512, Heidelberg, Berlin, New York, 1992.
2. L. M. Adleman, C. Pomerance and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. **117** (1983), 173–206.
3. M. Agrawal and S. Biwas, *Primality and Identity testing via Chinese Remaindering*, FOCS'99, 1999, pp. 202–209.
4. M. Agrawal, N. Kayal and N. Saxena, *PRIME is in* **P**, Ann. Math. **160** (2004), 781–793.
5. A. Aho, J. Hocroft and J. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Massachusetts, 1974.

6. W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **140** (1994), 703-722.
7. N. C. Ankeny, *The least quadratic non-residue*, Ann. Math. **55** (1952), 65–72.
8. A. O. L. Atkin, *Lecture notes on conference*, manuscript (1986).
9. E. Bach and J. Shallit, *Algorithmic Number Theory Vol 1 Efficient algorithms*, MIT Press, Cambridge, Massachusetts, 1996.
10. J. Brillhart and J. L. Selfridge, *Some factorizations of* $2^n \pm 1$ *and related results*, Math. Comp **21** (1967), 87–96, Oprava v Math. Comp. 21(1967), 751.
11. R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), 232–238.
12. R. D. Carmichael, *On composite numbers P which satisfy the Fermat congruence* $a^{P-1} \equiv 1 \mod P$, Amer. Math. Monthly **19** (1912), 22–27.
13. P. L. Chebyshev, *Sur la fonction qui détermine la totalité des nombres premiers inférieus à une limite donnée*, Mem. Imp. Acad. Sci. St.-Pétersbourgh **6** (1951), 141–157, in Ocuvres Vol. I, 29–48.
14. P. L. Chebyshev, *Mémoire sur les nombres premiers*, J. Math. Pures Appl. **17** (1852), 366–390, In Ocuvres Vol. I 51–70.
15. A. Cobham, *The recognition problem for the set of perfect squares*, Proc. 7th Ann Symp. Switching and Automata Theory, IEEE Press, 1966, pp. 24–30.
16. P. G. L. Dirichlet, *Beweis eine Satzes über die arithmetische Progression*, Bericht. Ak. Wiss Berlin (1837), 108–110, in Werke Vol. 1, 307–312.
17. P. G. L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhand Ak. Wiss. Berlin (1837), 45–81, in Werke Vol 1. 313–342.
18. L. Euler, *Theoremata circa residua ex divisione potestatum relicta*, Novi Comm. Acad. Sci. Petrop. **7** (1761), 49–82.
19. S. Goldwasser and J. Kilian, *Almost all primes can be quickly certificated*, STOC'86, ACM, 1986, pp. 316–329.
20. R. K. Guy, C. B. Lacampagne and J. L. Selfridge, *Primes at glance*, Math. Comp. **48** (1987), 183–202.
21. C. G. Jacobi, *Über die Kriestheilung und ihre Anwendung auf die Zahlentheorie*, Bericht Ak. Wiss. Berlin (1837), 127–136, in J. Reine Angew. Math. 30(1846), 166–182.
22. J. P. Jones, D. Sato, H. Wada and D.Wiens, *Diophantine representationof the set prime numbers*, Amer. Math. Monthly **83** (1976), 449–464.
23. H. von Koch, *Sur la distribution des nombres premiers*, Acta Math. **24** (1901), 159–182.
24. A. Korselt, *Problème chinois*, L'Intermédiaire Math. **6** (1899), 143.
25. M. Kraitchik, *Théorie des Nombres II*, Gauthier–Villars, Paris, 1926.
26. A.-M. Legendre, *Théorie des Numbres*, Firmin Didot Frères, Paris, 1830.
27. D. H. Lehmer, *Tests for primality by the converse of Fermat's theorem*, Bull. Amer. Math. Soc. **33** (1927), 327–340, Oprava v Math. Comp. 23 (1969), 217.
28. D. H. Lehmer, *Strong Carmichael numbers*, J. Austral. Math. Soc. Ser. A **21** (1976), 508–510.
29. H. W. Lenstra and C. Pomerance, *Primality testing with Gaussian periods*, preprint (2005), Revise 2009 a 2011.
30. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986.
31. G. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci **13** (1976), 300-317.
32. C. Pomerance, *Very short primality proofs*, Math. Comp. **48** (1987), 315–322.
33. V. R. Pratt, *Every prime has a succinct certificate*, SIAM J. Comput. **4** (1975), 214–220.
34. M. O. Rabin, *Probabilistic algorithms*, Algorithms and Complexity: New Directions and Recent Results, Academic Press, New York, 1976, pp. 21–39.
35. M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), 128-138.
36. B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grosse*, Monats. der Königlichen Prussischen Ak. Wiss. Berlin (1860), 671–680, in Gessammelte Werke 2.dn edit. 145–153.
37. R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), 84–85, Oprava v SIAM J. Comput. 7(1978), 118.

38. E. C. Titmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo **54** (1930), 414–429.
39. C.-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Ann. Soc. Sci. Bruxelles **20** (1986), 183–256, 281–397.
40. H. Williams, *A modification of the RSA public-key encryption procedure*, IEEE Trans. Inform. Theory **IT-26** (1980), 726–729.