

Testy prvočíselnosti

19. a 20. přednáška z kryptografie

Obsah

- 1 Testy prvočíselnosti**
 - Deterministické testy
 - Pravděpodobnostní testy
 - Millerův-Rabinův test

- 2 Generování náhodných prvočísel**
 - IsPrime jako Millerův-Rabinův test
 - IsPrime jako Millerův-Rabinův test s dělením malými prvočísly

Testy prvočíselnosti

V předchozí kapitole jsme používali algoritmus $IsPrime(n)$, který testoval, zda je n prvočíslo, jako "černou skříňku". V této kapitole se seznámíme s některými testy prvočíselnosti, z nichž nejdůležitější bude Millerův-Rabinův test.

V druhé části spočteme časovou složitost generování náhodného prvočísla, pokud se prvočíselnost bude testovat Millerovým - Rabinovým testem, vylepšeným případně o dělení prvočíslu do jisté meze.

Deterministické testy prvočíselnosti

Test prvočíselnosti hrubou silou

Tvrzení: Přirozené číslo $n > 1$ je prvočíslo, právě když není dělitelné žádným prvočíslem $p \leq \sqrt{n}$.

Test prvočíselnosti hrubou silou: Dělit n všemi (prvo)čísly do \sqrt{n} .

Časová náročnost je exponenciální: $O(2^{\frac{1}{2} \text{len}(n)} \text{len}(n)^2)$

Výhoda - pokud je n složené číslo, tak nalezneme jeho dělitele.

Deterministické testy prvočíselnosti

Deterministický polynomiální test prvočíselnosti

Existuje deterministický algoritmus na testování prvočíselnosti pracující v polynomiálním čase, autoři Agrawal, Kayal a Saxena, publikovaný 2004.

Algoritmus využívá vlastností polynomů na okruhem \mathbb{Z}_n , resp. polynomů nad tělesem, pokud n je prvočíslo.

Algoritmus pracuje v čase $O(\text{len}(n)^{16,5})$.

S použitím rychlejších algoritmů pro celočíselnou a polynomiální aritmetiku pracuje v čase $O(\text{len}(n)^{10,5+o(1)})$.

Poznámka

Přestože je tento algoritmus důležitým teoretickým výsledkem, nemá v praxi žádný význam - mocnina polynomu je příliš vysoká.

Deterministické testy prvočíselnosti

Poznámka

Pokud by počítač vykonal miliardu ($= 10^9$) dělení za sekundu, pak by otestování prvočíselnosti stomístného čísla (330-bitového)

$n = 10^{100} \doteq 2^{330}$ trvalo

- hrubou silou přibližně 10^{33} let,
- deterministickým AKS algoritmem přibližně 10^7 let,
- pravděpodobnostním Millerovým-Rabinovým algoritmem jednu sekundu, s pravděpodobností omylu menší než 2^{-100} , což je pravděpodobnost téměř nulová.

Pravděpodobnostní testy prvočíselnosti

Pravděpodobnostní testy s jednostrannou chybou

Pravděpodobnostní testy prvočíselnosti využívají vlastností, které v případě, že n je prvočíslo, platí pro všechna $a \in \mathbb{Z}_n^*$ (všechny prvky v \mathbb{Z}_p^* pravdivě dosvědčují prvočíselnost p), zatímco při n složeném čísle vlastnost platí jen pro některá $a \in \mathbb{Z}_n^*$ (tyto prvky jsou pak falešnými svědky prvočíselnosti ve skutečnosti složeného čísla n).

V testu k -krát náhodně zvolíme nějaké $a \in \mathbb{Z}_n^*$ a ověříme danou vlastnost. Pokud všechna zvolená $a \in \mathbb{Z}_n^*$ vlastnost mají, prohlásíme n za prvočíslo. Na množství falešných svědků závisí pravděpodobnost, se kterou se můžeme zmýlit a prohlásit složené číslo n za prvočíslo. Test je tedy zatížen jednostrannou chybou.

Pravděpodobnostní testy prvočíselnosti

Představíme Fermatův test a Millerův-Rabinův test prvočíselnosti. Nejdříve se vždy podíváme se na vlastnosti, které používají, a odhadneme počet falešných svědků prvočíselnosti u složených čísel.

Zjistíme také, že dané vlastnosti prvočísla nemusí charakterizovat, aneb existují pseudoprvočísla.

Fermatův test

Malá Fermatova věta

Nechť p je prvočíslo. Pro každé $a \in \mathbb{Z}_p^*$ platí: $a^{p-1} = 1$ v \mathbb{Z}_p

Svědkové prvočíslnosti pro Fermatův test

Nechť $n > 1$. Označme $K_n = \{a \in \mathbb{Z}_n^*, a^{n-1} = 1\}$.

Mohli jsme definovat $K_n = \{a \in \mathbb{Z}_n, a^{n-1} = 1\}$, i tak $K_n \subseteq \mathbb{Z}_n^*$.
Pokud totiž $a^{n-1} = 1$, pak má a inverzi $a^{-1} = a^{n-2}$ a je v \mathbb{Z}_n^* .

Je tedy jedno, zda volíme náhodný prvek ze \mathbb{Z}_n nebo ze \mathbb{Z}_n^* , počet svědků prvočíslnosti je stále stejný.

Fermatův test

Věta

Je-li n prvočíslo, pak $K_n = \mathbb{Z}_n^* = \mathbb{Z}_n^+$.

Je-li n složené číslo, pro něž $K_n \neq \mathbb{Z}_n^*$, pak $|K_n| \leq \frac{1}{2}|\mathbb{Z}_n^*| < \frac{1}{2}|\mathbb{Z}_n^+|$.

Důkaz se opírá o fakt, že K_n je podgrupa grupy \mathbb{Z}_n^* .

Situace, že $K_n = \mathbb{Z}_n^*$, může nastat pro tzv. Carmichaelova čísla.

Fermatův test

Otestování, zda $a \in K_n$ (booleovská procedura)

Vstup: $n > 1$, $a \in \mathbb{Z}_n^*$ (nebo jen $a \in \mathbb{Z}_n^+$)

Výstup: *True* či *false*

- $b \leftarrow a^{n-1} \text{ v } \mathbb{Z}_n$
- if $b = 1$ then return *true*
else return *false*

Časová náročnost $O(\text{len}(n)^3)$ (algoritmus opakovaných čtverců).

Fermatův test

Fermatův test prvočíselnosti - algoritmus $F(\cdot, k)$

Vstup: $n > 1$; (testuje, zda je n prvočíslo)
parametr $k \geq 1$ (počet náhodných svědků)

Výstup: *True* či *false*

- repeat k times
 - $a \stackrel{\$}{\leftarrow} \mathbb{Z}_n^+$ (nebo $a \stackrel{\$}{\leftarrow} \mathbb{Z}_n^*$)
 - if $a \notin K_n$ then return *false* endif enddo
- return *true*

Časová náročnost je v nejhorším případě $O(k \text{len}(n)^3)$.

Očekávaný čas pro složené n (ne Carmichaelovo) je $O(2 \text{len}(n)^3)$.

Fermatův test

Pravděpodobnost omylu

Pokud je n prvočíslo, pak Fermatův test odpoví vždy správně *true*.

Pokud je n složené číslo, ale nikoli Carmichaelovo, pak pravděpodobnost omylu (test odpoví *true*) je nejvýše $\epsilon = \frac{1}{2^k}$, kde k je počet nezávisle náhodně zvolených svědků $a \in \mathbb{Z}_n^+$.

Pro Carmichaelova čísla je pravděpodobnost omylu větší (při volbě $a \stackrel{\not\leftarrow}{\in} \mathbb{Z}_n^*$ je Fermatovým testem od prvočísel nerozeznáme vůbec).

Poznámka

Náhodná volba $a \in \mathbb{Z}_n^+ \setminus \mathbb{Z}_n^*$ umožňuje najít faktor čísla n , je jím $d = \gcd(a, n) > 1$.

Carmichaelova čísla

Definice

Carmichaelovo číslo je takové složené číslo n ,
že pro každé $a \in \mathbb{Z}_n^*$ platí $a^{n-1} = 1$ v \mathbb{Z}_n .

Carmichaelova čísla jsou řídká, přesto jich je nekonečně mnoho.
 $561 = 3 \cdot 11 \cdot 17$ je jediné Carmichaelovo číslo menší než 1000,
další jsou $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$.
Do 10^{16} je zhruba $2,7 \cdot 10^{14}$ prvočísel a jen $2,4 \cdot 10^5$
Carmichaelových čísel.

Carmichaelova čísla

Tvrzení

Složené číslo n je Carmichaelovo, právě když $\lambda(n) \mid n - 1$, kde $\lambda(n) = \exp(\mathbb{Z}_n^*)$ je Carmichaelova funkce.

Tvrzení

Každé Carmichaelovo číslo n je tvaru $n = p_1 \cdot \dots \cdot p_r$, kde

- p_i jsou různá lichá prvočísla (aneb n je liché a square free),
- $r \geq 3$,
- $p_i - 1 \mid n - 1$ pro každé $1 \leq i \leq r$.

Millerův-Rabinův test

Tvrzení

Nechť $p > 2$ je prvočíslo.

Rovnice $x^2 = 1$ má v grupě \mathbb{Z}_p^* právě dvě řešení a to $x = \pm 1$, (tj. v \mathbb{Z}_p^* nejsou netriviální druhé odmocniny z 1).

Svědkové prvočíslnosti pro Millerův-Rabinův test

Bud' $n > 1$ liché číslo, $n - 1 = t 2^h$ pro t liché číslo.

$L_n = \{a \in \mathbb{Z}_n^*, a^{n-1} = 1$ a dále, když $a^{t 2^j} = 1$, pak $a^{t 2^{j-1}} = \pm 1$
pro všechna $1 \leq j \leq h\}$

Opět jsme mohli definovat L_n jako podmnožinu \mathbb{Z}_n a vymezili bychom tím tutéž množinu L_n . Zřejmě též $L_n \subseteq K_n$.

Millerův-Rabinův test

Poznámka

Vlastnost, že rovnice $x^2 = 1$ má právě dvě řešení $x = \pm 1$ v \mathbb{Z}_n^* , prvočísla necharakterizuje. Tato vlastnost platí v každé cyklické grupě \mathbb{Z}_n^* , tedy i pro $n = p^e$, kde $p > 2$ je prvočíslu, $e \geq 1$.

(A ještě pro $n = 2$, $n = 4$, $n = 2p^e$, kde $p > 2$ je prvočíslu, ale sudá n nás teď nezajímají.)

Pro takováto n bude platit $L_n = K_n$ (Millerův-Rabinův test má stejně falešných svědků prvočíslnosti jako Fermatův test).

Millerův-Rabinův test

Věta

Nechť n je liché číslo. Je-li n prvočíslo, pak je $L_n = \mathbb{Z}_n^* = \mathbb{Z}_n^+$.
Je-li n složené číslo, pak je $|L_n| \leq \frac{1}{4}|\mathbb{Z}_n^*| < \frac{1}{4}|\mathbb{Z}_n^+|$.

Poznámky k důkazu:

- Pro $n = p^e$, $e \geq 2$, p liché prvočíslo, je $L_n = K_n$ a díky cykličnosti grupy \mathbb{Z}_n^* lze spočítat $|K_n| = p - 1 = \frac{1}{p^{e-1}}|\mathbb{Z}_n^*|$.
- Pro $n = \prod_{i=1}^r p_i^{e_i}$, $r \geq 2$, p_i lichá prvočísla, lze odvodit $|L_n| \leq \frac{2}{2^r} |\text{Ker } \rho_{t2^g}| \leq \frac{1}{2^{r-1}} |K_n|$, kde $\rho_{t2^g} : x \mapsto x^{t2^g}$,
 $g = \min\{h, h_1, \dots, h_r\}$, $n - 1 = t2^h$, $\varphi(p_i^{e_i}) = t_i 2^{h_i}$, t, t_i lichá.
Pokud n není Carmichaelovo číslo, tak $|L_n| \leq \frac{1}{2}|K_n| \leq \frac{1}{4}|\mathbb{Z}_n^*|$.
Pokud n je Carmichaelovo číslo, tak víme, že $r \geq 3$, tudíž $|L_n| \leq \frac{1}{4}|K_n| = \frac{1}{4}|\mathbb{Z}_n^*|$.

Millerův-Rabinův test

Otestování, zda $a \in L_n$ (booleovská procedura)

Vstup: $n > 1$ liché, kde $n - 1 = t 2^h$ pro t liché;
 $a \in \mathbb{Z}_n^*$ (nebo jen $a \in \mathbb{Z}_n^+$)

Výstup: *True* či *false*

- $b \leftarrow a^t \text{ v } \mathbb{Z}_n$
- if $b = 1$ then return *true* endif
- for $j \leftarrow 0$ to $h - 1$ do
 - if $b = -1$ then return *true* endif
 - if $b = 1$ then return *false* endif
 - $b \leftarrow b^2 \text{ v } \mathbb{Z}_n$ enddo
- return *false*

Časová náročnost je $O(\text{len}(n)^3)$. Algoritmus postupně spočítá a^{n-1} v \mathbb{Z}_n metodou opakovaných čtverců.

Millerův-Rabinův test

Millerův-Rabinův test prvočíslnosti - algoritmus $MR(\cdot, k)$

Vstup: $n > 1$ (testuje, zda je n prvočíslo),
parametr $k \geq 1$ (počet náhodných svědků)

Výstup: *True* či *false*

- if $n = 2$ then return *true* endif
- if n is even (sudé) then return *false* endif
- repeat k times (nyní je n liché)
 - $a \xleftarrow{\$} \mathbb{Z}_n^+$ (nebo $a \xleftarrow{\$} \mathbb{Z}_n^*$)
 - if $a \notin L_n$ then return *false* enddo
- return *true*

Časová složitost je v nejhorším případě $O(k \text{len}(n)^3)$.
Očekávaný čas pro libovolné složené n je $O(\frac{4}{3} \text{len}(n)^3)$.

Millerův-Rabinův test

Pravděpodobnost omylu

Pokud je n prvočíslo, pak Millerův-Rabinův test odpoví vždy *true*.

Pokud je n složené číslo, pak pravděpodobnost omylu (tj. $MR(\cdot, k)$ přesto odpoví *true*) je nejvýše $\epsilon = \frac{1}{4^k}$.

Poznámka

Náhodná volba $a \in K_n \setminus L_n$ umožní číslo n částečně faktorizovat. Prvek a ve svých mocninách vygeneruje netriviální druhou odmocninu z 1 (tj. $c \neq \pm 1$, ale $c^2 = 1 \vee \mathbb{Z}_n$), proto $d = \gcd(c - 1, n) > 1$ je faktor n .

Generování náhodných prvočísel

Algoritmus RP (=Random Prime)

Vstup: přirozené číslo $m \geq 2$, (označme $l = \text{len}(m)$)

Výstup: náhodné prvočíslo mezi 2 a m

- repeat $n \xleftarrow{\$} \{2, \dots, m\}$
- until $\text{IsPrime}(n)$
- output n

$\text{IsPrime}(\cdot)$ bude nyní implementován jako Millerův-Rabinův test $\text{MR}(\cdot, k)$ s parametrem k .

Generování náhodných prvočísel

Analýza algoritmu RP používajícího $MR(\cdot, k)$ - OUTPUT

$MR(\cdot, k)$ je pravděpodobnostní test s jednostrannou chybou, pro n složené je pravděpodobnost omylu nejvýše $\epsilon = \frac{1}{4^k}$.

Od minule víme:

- Každé prvočíslo do $m \doteq 2^l$ může být nalezeno se stejnou pravděpodobností.
- Pravděpodobnost, že výstup je složené číslo do $m \doteq 2^l$, je $O(\epsilon l) = O(\frac{1}{4^k} l)$.

Chceme-li najít náhodné 1024-bitové prvočíslo s pravděpodobností omylu nejvýše $\frac{1}{2^{100}}$, budeme volit $k = 55$.

Generování náhodných prvočísel

Poznámka

Ve skutečnosti je pravděpodobnost omylu ještě menší, zvláště při generování velkých prvočísel.

Počet falešných svědků prvočíselnosti v Millerově-Rabinově testu jsme odhadli: $|L_n| \leq \frac{2}{2^r} |K_n| \leq \frac{1}{2^r} |\mathbb{Z}_n^*|$ (není-li n Carmichaelovo), kde r je počet prvočísel ve faktorizaci čísla n .

Aneb "většina" složených čísel má falešných svědků prvočíselnosti velmi málo.

Označme $\gamma(m, k)$ pravděpodobnost, že výstup je složené číslo. Pro velká m je už $\gamma(m, 1)$ (jeden svědek) velmi malé:

$$\gamma(2^{200}, 1) \leq \frac{1}{8}, \quad \gamma(2^{300}, 1) \leq \frac{1}{2^{19}}, \quad \gamma(2^{500}, 1) \leq \frac{1}{2^{55}}$$

Pro vygenerování 512-bitového prvočísla s pravděpodobností omylu nejvýše $\frac{1}{2^{100}}$ stačí volit $k = 2$.

Generování náhodných prvočísel

Časová analýza algoritmu RP používajícího $MR(\cdot, k)$

Od minule víme:

- Očekávaný počet cyklů je $O(l)$, kde $l = \text{len}(m)$, neboť *LOOPS* má geometrické rozdělení s parametrem $p > \frac{\pi(m)}{m-1} \in O(\frac{1}{l})$ (Čebyševova věta).
Aneb budeme muset otestovat průměrně l čísel do $m = 2^l$, než najdeme jedno prvočíslo.
- Algoritmus $MR(\cdot, k)$ pracuje v (nejhorším) čase $O(kl^3)$.
- Očekávaný čas je $E(\text{TIME}) \in O(kl^4)$.

Generování náhodných prvočísel

Časová analýza algoritmu RP používajícího $MR(\cdot, k)$

Tento časový odhad je ale velmi pesimistický, protože je-li n složené, pak pravděpodobnost, že najdeme svědka složenosti, je aspoň $\frac{3}{4}$. Veličina $LOOPS$ v Millerově-Rabinově testu má "skoro geometrické" rozdělení, lze tedy očekávat $E(LOOPS) = \frac{4}{3}$ testů.

Složená n rozpoznají většinou jeden či dva Millerovy-Rabinovy svědci, pouze pro prvočíslo najdeme (pro jistotu) k svědků.

Odtud plyne:

- Očekávaný čas je $E(TIME) \in O(l^4 + kl^3)$.

Zhruba l složených čísel otestujeme každé v čase $O(l^3)$ než najdeme jedno prvočíslo, které otestujeme v čase $O(kl^3)$.

Millerův-Rabinův test - vylepšení

Millerův-Rabinův test s dělením malými prvočísly - - algoritmus $MRS(\cdot, k)$

Většina složených čísel bude dělitelná malými prvočísly (každé druhé dvojkou, každé třetí trojkou, atd.).

Ověřit dělitelnost čísla n malými prvočísly lze v čase $O(\text{len}(n))$, zatímco Millerův-Rabinův test vezme čas $O(\text{len}(n)^3)$.

Testování prvočíselnosti urychlíme, pokud do Millerova-Rabinova testu pustíme jen čísla, která nejsou dělitelná žádným prvočíslem do jisté meze s .

Millerův-Rabinův test - vylepšení

Millerův-Rabinův test s dělením malými prvočísky - - algoritmus $MRS(\cdot, k)$

Vstup: $n > 1$ (testuje, zda je n prvočíslo),
parametr $k \geq 1$ (počet Millerových-Rabinových svědků)
parametr $s > 1$ (dělíme prvočísky do meze s)

Výstup: *True* či *false*

- for each prime $p \leq s$ do
 - if $p \mid n$ then if $p = n$ then return *true*
else return *false* endif enddo
- repeat k times
 - $a \xleftarrow{\$} \mathbb{Z}_n^+$ (nebo $a \xleftarrow{\$} \mathbb{Z}_n^*$)
 - if $a \notin L_n$ then return *false* endif enddo
- return *true*

Generování náhodných prvočísel

Časová analýza algoritmu RP používajícího $\text{MRS}(\cdot, k)$

Odhadneme, kolik čísel půjde do Millerova-Rabinova testu.

Víme, že každé p -té číslo je dělitelné prvočíslem p .

Pravděpodobnost, že náhodné číslo n není dělitelné prvočíslem p je tedy $(1 - \frac{1}{p})$. Budeme předpokládat, že nedělitelnost různými prvočísly jsou nezávislé jevy (heuristický argument).

Označme \tilde{p} pravděpodobnost, že náhodné n není dělitelné žádným prvočíslem $p \leq s$, pak platí:

$$\tilde{p} = \prod_{p \leq s} (1 - \frac{1}{p}) \in O\left(\frac{1}{\ln(s)}\right)$$

Mertonova věta

Součin přes všechna prvočísla $\prod_{p \leq s} (1 - \frac{1}{p}) \in \Theta\left(\frac{1}{\ln(s)}\right)$.

Generování náhodných prvočísel

Časová analýza algoritmu RP používajícího $MRS(\cdot, k)$

Lze tedy očekávat, že než nalezneme prvočíslo $\leq m$, budeme testovat zhruba $l = \text{len}(m)$ čísel, z nichž

- $\frac{1}{\text{len}(s)}$ l čísel půjde do Millerova-Rabinova testu a jeden či dva svědkové prokážou jejich složenost (v čase $O(l^3)$);
- ostatní složená čísla (těch je nejvýše l) budou dělitelná nějakým prvočíslem do s , což u každého zjistíme v čase $O(\pi(s) l) = O(\frac{s}{\text{len}(s)} l)$;
- jedno prvočíslo bude v Millerově-Rabinově testu otestováno všemi k svědky v čase $O(kl^3)$;
- Očekávaný čas je $E(\text{TIME}) \in O(\frac{1}{\text{len}(s)} l^4 + \frac{s}{\text{len}(s)} l^2 + kl^3)$.

Generování náhodných prvočísel

Časová analýza algoritmu RP používajícího $MRS(\cdot, k)$

- Volí se mez s tak, aby $l \leq s \leq l^2$, resp. $s \doteq l$, potom je očekávaný čas pro nalezení náhodného prvočísla do 2^l s použitím algoritmu $MRS(\cdot, k)$:

$$E(\text{TIME}) \in O\left(\frac{1}{\text{len}(l)} l^4 + kl^3\right)$$

Například pro hledání náhodného 1024-bitového prvočísla budeme dělit prvočíslu do meze $s = 1024$. Pro $k = 55 < 2^6$ lze očekávat čas $c\left(\frac{1}{10}2^{40} + k2^{30}\right) \doteq c2^{37}$ pro malou konstantu $c \doteq 1$.

Superpočítače pracující s rychlostí 1000 miliard ($= 10^{12} \doteq 2^{40}$) operací za sekundu najdou 1024-bitové prvočíslu za jednu sekundu s pravděpodobností omylu téměř nulovou. Počítačům s rychlostí jedna miliarda operací za sekundu by to trvalo 15 minut.

Eratosthenovo síto

Uvedeme ještě algoritmus, jak najít všechna prvočísla do meze s .

Algoritmus Eratosthenovo síto

Vstup: $s > 1$

Výstup: pole $A[2, \dots, s]$, kde $A[i] = 1$, právě když i je prvočíslo

- for $i \leftarrow 2$ to s do $A[i] \leftarrow 1$ enddo
- for $i \leftarrow 2$ to $\lfloor \sqrt{s} \rfloor$ do
 - if $A[i] = 1$ then
 - $j \leftarrow i + i$
 - while $j \leq s$ do $A[j] \leftarrow 0, j \leftarrow j + i$ enddo
 - endif
- enddo

Eratosthenovo síto

Analýza algoritmu Eratosthenovo síto

Prostorová náročnost je exponenciální $O(s) = O(2^{\text{len}(s)})!$

Časová náročnost:

Pro každé prvočíslo $p \leq \sqrt{s}$ provádíme $\frac{s}{p}$ jednoduchých operací.

$$TIME = \sum_{p \leq \sqrt{s}} \frac{s}{p} < s \int_1^{\sqrt{s}} \frac{1}{y} dy = \frac{1}{2}s \ln(s) \in O(s \ln(s))$$

Přesnější odhad: $TIME \in O(s \ln(\ln(s)))$, díky následující větě.

Věta

Součet přes všechna prvočísla $\sum_{p \leq \sqrt{s}} \frac{1}{p} = \ln(\ln(s)) + O(1)$.

Millerův-Rabinův test

Poznámka

Platí-li zobecněná Riemannova hypotéza, pak pro každé složené číslo n existuje svědek neprvočíselnosti, tj. $a \in \mathbb{Z}_n \setminus L_n$, velikosti $a \leq 2 \ln(n)^2$.

Je-li tomu tak, pak by Millerův-Rabinův test mohl být deterministický a pracoval by v čase $O(\ln(n)^5)$.

Algoritmus RP by pak našel prvočíslo do $m = 2^l$ neomylně v čase $O\left(\frac{1}{\ln(l)} l^6\right)$ (při dělení prvočísly do meze $s \doteq l$).

Testy prvočíselnosti

Literatura

- Shoup: A Computational Introduction to Number Theory and Algebra. Kapitola 10.
<http://shoup.net/ntb/>