Subexponenciální algoritmus pro diskrétní logaritmus

22. a 23. přednáška z kryptografie

Obsah

1. **Využívaná fakta**
   - y-hladká čísla
   - Lineární algebra nad tělesem
2. **Subexponenciální algoritmus pro diskrétní logaritmus**
3. **Analýza algoritmu SEDL**

Subexponenciální složitost

Subexponenciální algoritmus pro diskrétní logaritmus (SEDL) používá $y-$hladkost čísel a lineární algebru nad tělesem $\mathbb{Z}_p$. Funguje tedy pro podgrupy grupy $\mathbb{Z}_p^*$.

- Exponenciální složitost: $O(n) = O(2^{\text{len}(n)})$
- Subexponenciální složitost: $O(2^{f(\text{len}(n))})$, kde $f(x) \in o(x)$, tj. $\lim_{x\to\infty} \frac{f(x)}{x} = 0$.
  Algoritmus SEDL bude mít složitost $O(2^{c\sqrt{\text{len}(n)\,\text{len}(\text{len}(n))}})$.
  Například pro $n = 2^{256}$ vychází čas $O(2^{\sqrt{256\cdot 8}}) \doteq O(2^{47})$.

y-hladká čísla

Definice

Buď $y \geq 0$ reálné číslo. Přirozené číslo $m \geq 1$ je *$y-$hladké*, jestliže každé prvočíslo, které dělí m, je menší rovno y.

Nechť $0 \leq y \leq x$ jsou reálná čísla. Označme $\Psi(y, x)$ počet všech $y-$hladkých čísel do x (včetně).

Příklady

Čísla $4, 27, 24, 9216 = 3^2 \cdot 2^{10}$ jsou $3-$hladká.

$\Psi(2, 10) = 4$, neboť $2-$hladká čísla do 10 jsou 1, 2, 4 a 8.
$\Psi(3, 10) = 7$, neboť $3-$hladká čísla do 10 jsou 1, 2, 3, 4, 6, 8 a 9.

Zřejmě $\Psi(n, n) = n$ pro $n \in \mathbb{N}$.

y-hladká čísla

Věta 1

Pokud $y = y(x)$ splňuje $\lim_{x\to\infty} \frac{\ln(x)}{y} = 0$ a $\lim_{x\to\infty} \frac{\ln(y)}{\ln(x)} = 0$, pak platí:

$$\Psi(y, x) \geq x\, e^{(-1+o(1))\frac{\ln(x)}{\ln(y)}\ln(\ln(x))}$$

Poznámka

Připomeňme, že $f \in o(g)$, když $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.
Symbol $o(1)$ representuje nějakou funkci $f(x)$, pro níž $\lim_{x\to\infty} f(x) = 0$.

y-hladká čísla

Věta 2

Pokud $y = y(x)$ splňuje $y \in \Omega(\ln(x)^{1+\epsilon})$ pro nějaké $\epsilon > 0$ a $\lim_{x\to\infty} \frac{\ln(y)}{\ln(x)} = 0$, pak platí

$$\Psi(y, x) = x\, e^{(-1+o(1))\frac{\ln(x)}{\ln(y)}\ln(\frac{\ln(x)}{\ln(y)})}$$

Poznámka

$y-$hladká čísla hrají významnou roli v následujících subexponenciálních algoritmech. Tyto odhady jejich počtu budeme potřebovat při určování očekávaného času běhu algoritmů.

Lineární algebra nad tělesem

Nad tělesem (nad $\mathbb{Z}_p$) lze dělat lineární algebru stejně jako nad $\mathbb{R}$.

Lineární prostor nad tělesem

Lineární prostor nad tělesem $(T, +, \cdot)$ je množina L spolu s operací sčítání $\oplus : L \times L \to L$ a akcí číselného násobku $\boxdot : T \times L \to L$, pro které platí:

- $(L, \oplus)$ je komutativní grupa s neutrálním prvkem $\bar{o}$;
- Pro všechny $\alpha, \beta \in T$ a všechny $\bar{u}, \bar{v} \in L$:
  - $\alpha \boxdot (\bar{u} \oplus \bar{v}) = (\alpha \boxdot \bar{u}) \oplus (\alpha \boxdot \bar{v})$
  - $(\alpha + \beta) \boxdot \bar{u} = (\alpha \boxdot \bar{u}) \oplus (\beta \boxdot \bar{u})$
  - $(\alpha \cdot \beta) \boxdot \bar{u} = \alpha \boxdot (\beta \boxdot \bar{u})$
  - $1 \boxdot \bar{u} = \bar{u}$

Prvky z L se nazývají vektory, prvky z T jsou skaláry.

Lineární algebra nad tělesem

Lineární prostory nad tělesem

- *Podprostor* lineárního prostoru L je neprázdná podmnožina $P \subseteq L$, která je uzavřená na sčítání a číselné násobky.
- *Báze* lineárního podprostoru P je jeho lineárně nezávislá podmnožina $B = \{\bar{b}_1, \ldots, \bar{b}_n\}$, která generuje podprostor P, tj. $\bar{u} \in P$, právě když $\bar{u} = \sum_{i=1}^{n} a_i \bar{b}_i$, přičemž n-tice koeficientů $(a_1 \ldots a_n) \in T^{\times n}$ je určena jednoznačně.
- Tato n-tice koeficientů se nazývá *souřadnice* vektoru $\bar{u}$ vzhledem k (uspořádané) bázi B.
- Počet prvků libovolné báze podprostoru P se nazývá *dimenze* podprostoru P, zde $\dim P = n$.

Lineární algebra nad tělesem

Lineární prostory nad tělesem

- Vektory $\bar{u}_1, \ldots, \bar{u}_m$ jsou *lineárně závislé*, pokud existují koeficienty $c_1, \ldots, c_m \in T$, kde aspoň jedno $c_i \neq 0$, takové, že $c_1\bar{u}_1 + \ldots c_m\bar{u}_m = \bar{o}$,
  (existuje jejich netriviální kombinace rovná nulovému vektoru).
- V lineárním prostoru dimenze n je libovolných $m > n$ vektorů lineárně závislých.
- Speciálně množina $T^{\times n}$ všech $n-$tic nad tělesem T tvoří lineární prostor dimenze n, tudíž libovolných $n+1$ vektorů v něm tvoří lineárně závislou množinu.

Lineární algebra nad tělesem

Soustavy lineárních rovnic nad tělesem

- Nad tělesem T funguje *Gaussova eliminační metoda*. Místo dělení rovnice vedoucím pivotem používá násobení k němu inverzním prvkem. (V tělese T má každé nenulové číslo inverzní prvek.)
- Poznámka: Nad okruhem (nad $\mathbb{Z}_n$, kde n není prvočíslo) obecně Gaussova eliminace nefunguje, protože vedoucí pivoty nemusí být invertibilní.
- Soustava může mít jedno řešení, žádné řešení, nebo $|T|^k$ různých řešení, kde k je počet proměnných, které smíme volit libovolně v T.

Lineární algebra nad tělesem

Soustavy lineárních rovnic nad tělesem

Struktura množiny všech řešení soustavy $\mathbb{A}\bar{x}^T = \bar{b}^T$ pro n neznámých nad tělesem T:

- Všechna řešení homogenní soustavy $\mathbb{A}\bar{x}^T = \bar{o}^T$ tvoří podprostor v $T^{\times n}$ dimenze k, kde k je počet proměnných, které smíme volit libovolně v T.
- Každé řešení (ne)homogenní soustavy rovnic $\mathbb{A}\bar{x}^T = \bar{b}^T$ je součtem partikulárního řešení této soustavy a nějakého řešení přidružené homogenní soustavy.

Lineární algebra nad tělesem

Maticový počet nad tělesem

- Maticový počet nad tělesem T funguje jako nad $\mathbb{R}$ - lze analogicky definovat determinant i hodnost, či počítat inverzní matice.
- Maticový počet nad okruhem lze dělat s jistými zvláštnostmi - např. řádková hodnost se nemusí rovnat sloupcové hodnosti (neboť nefunguje Gaussova eliminace).
  Determinant definovat lze, invertibilní matice jsou právě ty matice, které mají invertibilní determinant.

Algoritmus SEDL

Representace prvku v grupě

Nechť G je cyklická grupa řádu n s generátorem a, prvek $b \in G$.
Representace prvku $g \in G$ vzhledem ke generátoru a a prvku b je každá dvojice $(s, t) \in \mathbb{Z}_n \times \mathbb{Z}_n$ taková, že $g = a^s b^t$ v G.
Je-li navíc $t \in \mathbb{Z}_n^*$, pak mluvíme o netriviální representaci.

Tvrzení

1. Pro každé $t \in \mathbb{Z}_n$ existuje právě jedno $s \in \mathbb{Z}_n$ tak, že (s, t) je representace prvku g vzhledem ke generátoru a a prvku b.
2. Známe-li netriviální representaci (s, t) prvku 1 vzhledem ke generátoru a a prvku b, pak umíme spočítat diskrétní logaritmus: $\mathrm{dlog}_a(b) = -st^{-1}$ v $\mathbb{Z}_n$.

Algoritmus SEDL

Subexponenciální algoritmus pro diskrétní logaritmus (SEDL)

Vstup: p, q, a, b,
kde $G = \langle a \rangle$ je podgrupa řádu q v grupě $\mathbb{Z}_p^*$,
p, q jsou prvočísla,
a je generátor grupy G, $b \in G$.

Předpokládejme navíc, že $|\mathbb{Z}_p^*| = p - 1 = qm$, kde $q \nmid m$.
(Jak postupovat bez tohoto předpokladu, si řekneme později.)

Výstup: $x = \mathrm{dlog}_a(b)$, nebo hláška "neúspěch".

Algoritmus SEDL hledá netriviální representaci prvku 1 vzhledem ke generátoru a a prvku b. Pokud ji nalezne, spočte z ní diskrétní logaritmus.

Algoritmus SEDL

Tvrzení

Nechť $|\mathbb{Z}_p^*| = qm$, kde p, q jsou prvočísla a $q \nmid m$, a nechť G je podgrupa řádu q a H je podgrupa řádu m v grupě $\mathbb{Z}_p^*$.
Pak $\mathbb{Z}_p^* = G \dot{\times} H$ je vnitřní direktní součin podgrup G a H, tj.

- $G \cap H = \{1\}$
- $GH = \mathbb{Z}_p^*$

Aneb $G \times H \simeq \mathbb{Z}_p^*$ a každý prvek $z \in \mathbb{Z}_p^*$ lze jednoznačně napsat ve tvaru $z = gh$, kde $g \in G$ a $h \in H$.

Tvrzení

Nechť $|\mathbb{Z}_p^*| = qm$, kde p je prvočíslo, a nechť H je podgrupa řádu m v grupě $\mathbb{Z}_p^*$. Pak pro libovolný prvek $z \in \mathbb{Z}_p^*$ je $z^q \in H$.

Algoritmus SEDL

1. fáze algoritmu SEDL

Budeme používat $y-$hladkost, vhodnou volbu parametru $y < p$ budeme diskutovat později.

Nechť $p_1, \ldots, p_k$ jsou všechna prvočísla do y, je jich tedy k.

Náhodnou volbou nalezneme $(k+1)$ $y-$hladkých čísel ze $\mathbb{Z}_p^*$ tvaru $a^{s_i} b^{t_i} h_i$, kde $a^{s_i} b^{t_i} = g_i \in G$, $h_i \in H$.

Provedeme to pro každé $1 \leq i \leq k+1$ takto:

- zvol náhodně $s_i, t_i \in \mathbb{Z}_q$ a $\tilde{h}_i \in \mathbb{Z}_p^*$, spočti $h_i = \tilde{h}_i^q \in H$
- ověř prostým dělením, zda $a^{s_i} b^{t_i} h_i = z_i$ v $\mathbb{Z}_p^*$ je $y-$hladké, tj. zda $z_i = p_1^{e_{i_1}} \cdot \ldots \cdot p_k^{e_{i_k}}$ v $\mathbb{Z}$, kde $0 < z_i < p$; pak $a^{s_i} b^{t_i} h_i = p_1^{e_{i_1}} \cdot \ldots \cdot p_k^{e_{i_k}}$ v $\mathbb{Z}_p^*$
- dokud ne, tak opakuj náhodnou volbu

Algoritmus SEDL

1. fáze algoritmu SEDL

Poznámka:
Pro fungování algoritmu by stačilo najít $(k+1)$ $y-$hladkých čísel z podgrupy G tvaru $a^{s_i} b^{t_i}$, ale neuměli bychom odhadnout očekávaný čas hledání (očekávaný počet cyklů pro každé i), protože nevíme, kolik je $y-$hladkých čísel v podgrupě G.

Umíme odhadnout jen počet $y-$hladkých čísel do p, tedy v $\mathbb{Z}_p^*$, proto volíme náhodná čísla tvaru $a^{s_i} b^{t_i} h_i = g_i h_i \in \mathbb{Z}_p^*$.

Algoritmus SEDL

2. fáze algoritmu SEDL

Budeme používat lineární algebru nad tělesem $\mathbb{Z}_q$, kde $q = |G|$. Víme, že q je prvočíslo, proto $\mathbb{Z}_q$ je těleso.

V 1. fázi jsme nalezli $(k+1)$ rovností tvaru:

$$a^{s_i} b^{t_i} h_i = p_1^{e_{i_1}} \cdot \ldots \cdot p_k^{e_{i_k}} \text{ v } \mathbb{Z}_p^*$$

Pro $1 \leq i \leq k+1$ uvažujme $k-$tice exponentů $\bar{v}_i = (e_{i_1}, \ldots, e_{i_k})$ jakožto vektory nad $\mathbb{Z}_q$.

Množina $\mathbb{Z}_q^{\times k}$ všech $k-$tic nad $\mathbb{Z}_q$ tvoří lineární prostor dimenze k. Našich $(k+1)$ vektorů tedy musí být lineárně závislých, aneb existuje jejich netriviální kombinace rovná nulovému vektoru.

Algoritmus SEDL

2. fáze algoritmu SEDL

Existují koeficienty $c_1, \ldots, c_{k+1} \in \mathbb{Z}_q$, ne všechny nulové, tak, že

$$c_1 \bar{v}_1 + \ldots + c_{k+1} \bar{v}_{k+1} = \bar{o} = (0, \ldots, 0) \text{ v } \mathbb{Z}_q^{\times k}.$$

Podíváme-li se na tuto kombinaci nad $\mathbb{Z}$, pak všechny složky výsledného vektoru jsou dělitelné číslem q:

$$c_1 \bar{v}_1 + \ldots + c_{k+1} \bar{v}_{k+1} = (e_1, \ldots, e_k) \text{ v } \mathbb{Z}^{\times k},\ q \mid e_i \text{ pro každé } i.$$

Koeficienty $c_1, \ldots, c_{k+1}$ nalezneme pomocí Gaussovy eliminace, která nad tělesem $\mathbb{Z}_q$ funguje.
(Budeme řešit homogenní soustavu k rovnic pro $(k+1)$ neznámých nad $\mathbb{Z}_q$. Stačí najít jedno netriviální řešení.)

Algoritmus SEDL

2. fáze algoritmu SEDL

Uvažujme opět $(k+1)$ rovností tvaru $a^{s_i} b^{t_i} h_i = p_1^{e_{i_1}} \cdot \ldots \cdot p_k^{e_{i_k}}$ v $\mathbb{Z}_p^*$. Pokud každou $i-$tou rovnost umocníme na příslušné c_i a všechny rovnosti navzájem vynásobíme, získáme rovnost:

$$a^s b^t h = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} \text{ v } \mathbb{Z}_p^*,$$

kde $s = \sum_{i=1}^{k+1} c_i s_i$, $t = \sum_{i=1}^{k+1} c_i t_i$ v Z_q, $h = \prod_{i=1}^{k+1} h_i^{c_i}$ v $\mathbb{Z}_p^*$.

Přitom ne všechna c_i jsou nulová, tedy může vyjít $s \neq 0$, $t \neq 0$.

Navíc víme, že $q \mid e_i$ pro každé i, tudíž $p_i^{e_i} \in H$ pro každé i.

Algoritmus SEDL

2. fáze algoritmu SEDL

Nyní máme rovnost

$$a^s b^t = h^{-1} p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} \text{ v } \mathbb{Z}_p^*,$$

kde prvek nalevo je z podgrupy G a prvek napravo z podgrupy H.

Jelikož ale $G \cap H = \{1\}$ (viz náš předpoklad navíc), tak musí být tento prvek roven 1. Našli jsme representaci prvku 1 vzhledem ke generátoru a a prvku b,

$$a^s b^t = 1 \text{ v } G \subseteq \mathbb{Z}_p^*.$$

Pokud je $t \neq 0$, spočteme $\mathrm{dlog}_a(b) = -st^{-1}$ v $\mathbb{Z}_q$.
Pokud je $t = 0$, tak ohlásíme neúspěch.

Algoritmus SEDL

- for $i \leftarrow 1$ to $k+1$ do
  - repeat
    - choose $s_i, t_i \overset{q}{\leftarrow} \mathbb{Z}_q$, $\tilde{h}_i \overset{q}{\leftarrow} \mathbb{Z}_p^*$ at random
    - $h_i \leftarrow \tilde{h}_i^q$, $z_i \leftarrow a^{s_i} b^{t_i} h_i$ in $\mathbb{Z}_p$
    - test if z_i is $y-$smooth (trial division)
  - until $z_i = p_1^{e_{i_1}} \cdot \ldots \cdot p_k^{e_{i_k}}$ for some $e_{i_1}, \ldots, e_{i_k} \in \mathbb{Z}$
  - $\bar{v}_i \leftarrow (e_{i_1}, \ldots, e_{i_k})$ in $\mathbb{Z}^{\times k}$ enddo
- apply Gaussian elimination over $\mathbb{Z}_q$ to find $c_1, \ldots, c_{k+1} \in \mathbb{Z}_q$, not all zero, such that $c_1 \bar{v}_1 + \ldots + c_{k+1} \bar{v}_{k+1} = (0, \ldots, 0)$ in $\mathbb{Z}_q^{\times k}$
- $s \leftarrow \sum_{i=1}^{k+1} c_i s_i$, $t \leftarrow \sum_{i=1}^{k+1} c_i t_i$ in $\mathbb{Z}_q$
- if $t = 0$ in $\mathbb{Z}_q$
  - then output "failure"
  - else $x \leftarrow (-st^{-1})$ in $\mathbb{Z}_q$ and output x endif

Algoritmus SEDL

Příklad

$G = \langle 4 \rangle$ je podgrupa řádu 11 v grupě $\mathbb{Z}_{23}^*$, $|\mathbb{Z}_{23}^*| = 2 \cdot 11$,
tedy $H = \{\pm 1\}$.
Spočtěte $\mathrm{dlog}_4(12)$ v $\mathbb{Z}_{23}^*$ a zvolte parametr hladkosti $y = 4$.
(Pozn.: $12^{11} = 1$ v $\mathbb{Z}_{23}^*$, tedy $12 \in G$ a $\mathrm{dlog}_4(12)$ je definován.)

- 1.fáze - počítáme v $\mathbb{Z}_{23}^*$, náhodnou volbou získáme rovnosti:
  R_1: $4^5 \cdot 12^7 \cdot 1 = 8 = 2^3$, odtud $\bar{v}_1 = (3, 0)$.
  R_2: $4^4 \cdot 12^9 \cdot 1 = 12 = 2^2 \cdot 3^1$, odtud $\bar{v}_2 = (2, 1)$.
  R_3: $4^3 \cdot 12^5 \cdot 1 = 2 = 2^1$, odtud $\bar{v}_3 = (1, 0)$.

  Pozn.: Volba $4^3 \cdot 12^5 \cdot (-1) = 21 = 3 \cdot 7$ byla neúspěšná.

Algoritmus SEDL

Příklad - pokračování

- 2.fáze - počítáme nad $\mathbb{Z}_{11}$, Gaussovou eliminací získáme pro $c_1(3,0) + c_2(2,1) + c_3(1,0) = (0,0)$ netriviální řešení $c_1 = 1$, $c_2 = 0$, $c_3 = -3 = 8$.
- kompletování výpočtů - $R_1^1 \cdot R_2^0 \cdot R_3^8$ dává rovnost:
  $4^{29} \cdot 12^{47} \cdot 1 = 2^{11} = 1$ v $\mathbb{Z}_{23}^*$,
  přitom $4, 12 \in G$, tedy v exponentu počítáme modulo 11:
  $4^7 \cdot 12^3 = 1$ v $\mathbb{Z}_{23}^*$ je netriviální representace 1.
- Odtud $3x + 7 = 0$ v $\mathbb{Z}_{11}$, $x = -7 \cdot 3^{-1} = 5$.
  Diskrétní logaritmus $\mathrm{dlog}_4(12) = 5$.

Algoritmus SEDL

Zobecnění algoritmu SEDL

Algoritmus SEDL lze upravit tak, aby počítal diskrétní logaritmus v podgrupě G řádu q^e grupy $\mathbb{Z}_p^*$, kde p, q jsou prvočísla, $|\mathbb{Z}_p^*| = q^e m$, $q \nmid m$. Buď H podgrupa řádu m v $\mathbb{Z}_p^*$.

Algoritmus bude fungovat, protože i teď je $\mathbb{Z}_p^* = G \dot{\times} H$.
První fáze proběhne stejně, ve druhé fázi budeme řešit homogenní soustavu rovnic nad okruhem $\mathbb{Z}_{q^e}$.

Gaussova eliminace nad okruhem obecně nefunguje, ale v tomto případě ji lze upravit tak, abychom pomocí ní nakonec našli netriviální řešení, tj. koeficienty $c_1, \ldots, c_{k+1} \in \mathbb{Z}_{q^e}$, které nejsou všechny nulové, dokonce ani nejsou všechny dělitelné číslem q. Pak může vyjít t invertibilní v $\mathbb{Z}_{q^e}$, tj. $q \nmid t$, tedy SEDL může najít netriviální representaci prvku 1, ze které dopočte diskrétní logaritmus.

Algoritmus SEDL

Cvičení

Předpokládejme, že umíme pomocí algoritmu SEDL spočítat diskrétní logaritmus v podgrupě G' řádu q^e grupy $\mathbb{Z}_p^*$, kde $|\mathbb{Z}_p^*| = p - 1 = q^e m$, $q \nmid m$. Navrhněte algoritmus, který vždy spočte diskrétní logaritmus v podgrupě G řádu q grupy $\mathbb{Z}_p^*$, kde $q \mid p - 1$ (bez dalších předpokladů pro q).

Vstup: generátor a grupy G, prvek $b \in G$, prvočísla p, q.
Výstup: $x = \mathrm{dlog}_a(b)$ v G.

Nápověda: Uvědomte si, že $G \subseteq G'$. Nalezněte generátor c grupy G', spočtěte $\mathrm{dlog}_c(a)$, $\mathrm{dlog}_c(b)$ v grupě G' a z nich dopočtěte x.

Analýza algoritmu SEDL

Vraťme se k základní variantě algoritmu SEDL. Počítáme diskrétní logaritmus z prvku b v podgrupě $G = \langle a \rangle$ řádu q grupy $\mathbb{Z}_p^*$, kde p, q jsou prvočísla, $|\mathbb{Z}_p^*| = p - 1 = qm$, $q \nmid m$.
Chceme analyzovat výstup algoritmu a očekávaný čas jeho běhu.

Tvrzení

Pravděpodobnost, že algoritmus SEDL ohlásí neúspěch, je $\frac{1}{q}$.

Lze dokázat, že každé $t \in \mathbb{Z}_q$ může být nalezeno algoritmem SEDL se stejnou pravděpodobností. Pak $P[\text{neúspěch}] = \frac{1}{q}$.

Analýza algoritmu SEDL

Očekávaný čas algoritmu SEDL

- 1. fáze SEDL: Označme σ pravděpodobnost, že náhodný prvek ze $\mathbb{Z}_p^*$ je $y-$hladký. Pak očekávaný počet cyklů pro nalezení jednoho $y-$hladkého prvku tvaru $a^{s_i} b^{t_i} h_i \in \mathbb{Z}_p^*$ je $\frac{1}{\sigma}$. V každém cyklu dělíme všemi k prvočísly do y $(y < p)$. Těchto $y-$hladkých prvků potřebujeme najít $(k+1)$. $E(TIME1) = O(\frac{k^2}{\sigma} \operatorname{len}(p)^2)$
- 2. fáze SEDL: Gaussova eliminace na matici typu $(k, k+1)$ vyžaduje zhruba k^3 operací v $\mathbb{Z}_q$ a její čas bude dominantní pro druhou fázi. $TIME2 = O(k^3 \operatorname{len}(p)^2)$
- Očekávaný čas pro SEDL: $E(TIME) = O((\frac{k^2}{\sigma} + k^3) \operatorname{len}(p)^2)$

Analýza algoritmu SEDL

Očekávaný čas algoritmu SEDL

Odhadneme k a σ pomocí y.
Předpokládejme, že $y = e^{\ln(p)^{\lambda+o(1)}}$, $0 < \lambda < 1$, abychom mohli použít větu odhadující počet $y-$hladkých čísel do p.

- $\sigma = \frac{\Psi(y,p-1)}{p-1} \geq \frac{\Psi(y,p)}{p} \geq e^{(-1+o(1))\frac{\ln(p)}{\ln(y)}\ln(\ln(p))}$
- Podle Čebyševovy věty je $k = \pi(y) = \Theta(\frac{y}{\ln(y)})$. Odtud lze odvodit (pro jakékoli y), že $k = e^{(1+o(1))\ln(y)}$.
- $\mathrm{len}(p)^2 = e^{o(1)\ln(y)}$ díky našemu předpokladu pro y.

Analýza algoritmu SEDL

Očekávaný čas algoritmu SEDL

Dosadíme do $E(TIME) = O((\frac{k^2}{\sigma} + k^3)\,\mathrm{len}(p)^2)$ a získáme odhad:

$$E(TIME) \leq e^{(1+o(1))\max\{\frac{\ln(p)}{\ln(y)}\ \ln(\ln(p))+2\ln(y);3\ln(y)\}}$$

Nyní chceme zvolit parametr hladkosti y tak, aby byl odhad očekávaného času minimální.

Označme $\mu = \ln(y)$, $A = \ln(p)\ln(\ln(p))$.
Chceme najít minimim pro funkci $f(\mu) = \max\{\frac{A}{\mu} + 2\mu; 3\mu\}$, použijeme základní kalkulus (nulová první derivace).

Analýza algoritmu SEDL

Očekávaný čas algoritmu SEDL

Funkce $f_1(\mu) = \frac{A}{\mu} + 2\mu$ má $f_1'(\mu) = -\frac{A}{\mu^2} + 2 = 0$ pro $\mu = \pm\sqrt{\frac{A}{2}}$.

Lokální minimum je v bodě $\mu = \sqrt{\frac{A}{2}}$, hodnota minima je $4\sqrt{\frac{A}{2}}$.

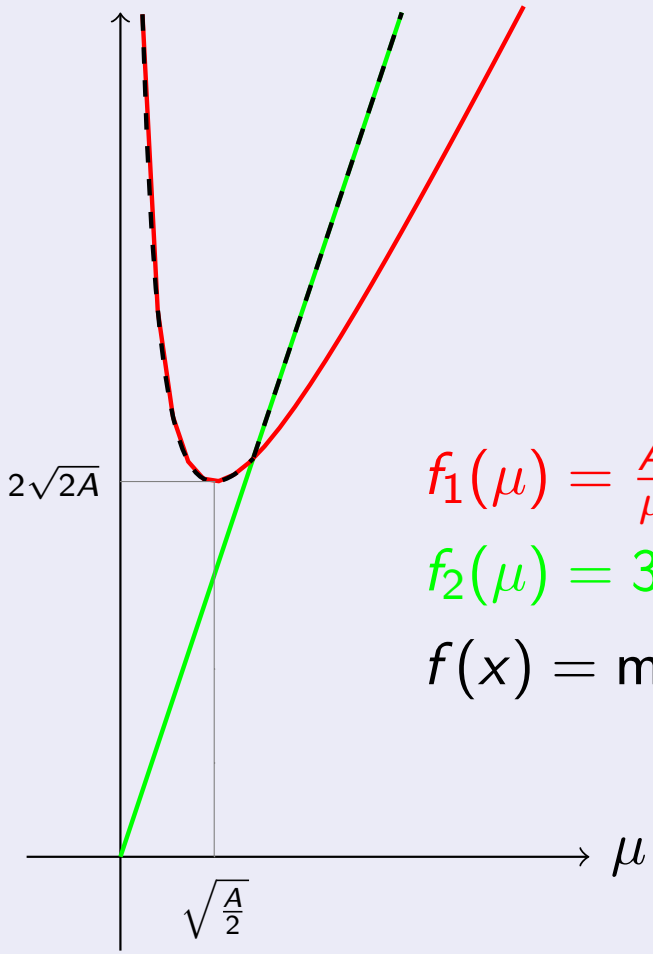
Funkce $f_2(\mu) = 3\mu$ nabývá v tomto bobě hodnoty $3\sqrt{\frac{A}{2}}$.

Tudíž $\mu = \sqrt{\frac{A}{2}}$ je bodem minima pro $f(\mu) = \max\{f_1(\mu); f_2(\mu)\}$

a hodnota minima je $4\sqrt{\frac{A}{2}} = 2\sqrt{2A}$.

Analýza algoritmu SEDL

Očekávaný čas algoritmu SEDL



$$f_1(\mu) = \frac{A}{\mu} + 2\mu,$$

$$f_2(\mu) = 3\mu$$

$$f(x) = \max\{f_1(\mu), f_2(\mu)\}$$

Analýza algoritmu SEDL

Očekávaný čas algoritmu SEDL

Volíme parametr hladkosti $y = e^{\sqrt{\frac{A}{2}}} = e^{\frac{1}{\sqrt{2}}\sqrt{\ln(p)\ln(\ln(p))}}$
(všimněme si, že splňuje předpoklady našeho výpočtu).

Při tomto y bude očekávaný čas algoritmu SEDL

$$E(TIME) \leq e^{(2\sqrt{2}+o(1))\sqrt{\ln(p)\ln(\ln(p))}},$$

tedy subexponenciální s konstantou $2\sqrt{2} \doteq 2,828$ v exponentu.

Poznámka

Konstantu v exponentu je možné zmenšit na $2,0$, použijeme-li přesnější odhad počtu $y-$hladných čísel (viz věta 2).

Algoritmus SEDL

Literatura

- Shoup: A Computational Introduction to Number Theory and Algebra. Kapitola 15.
- Lineární prostory nad tělesem najdete tamtéž v kapitole 13. http://shoup.net/ntb/