

Hledání generátoru v \mathbb{Z}_p^*

Udělejme, že prvek a je generátor cyklické grupy \mathbb{Z}_n^* rádu n , právě když $a^n \neq 1$
a to každého vlastního dělítelého čísla n . Bude tedy sloučit jen maximální
dělítelé čísla n . Tj. na nášem generátoru počítáme snad faktorizaci n .

Algoritmus 1: p je prvočíslo, $p-1 = \prod_{i=1}^k q_i^{e_i}$ je faktorizace pro \mathbb{Z}_p^*
všechny násobky jsou v \mathbb{Z}_p^* .
while true:

$a = \text{náhodný prvek ze } \mathbb{Z}_p^*$
 $\text{is_gen} = \text{TRUE}$

$i = 1$

while is_gen and $i < k$:

if $a^{q_i^{e_i}} = 1$:

$\text{is_gen} = \text{False}$

$i + 1$

if is_gen :

return a

- kolik prvků v \mathbb{Z}_p^* je generátorem? Je jich $\varphi(p-1)$, takže pravděpodobnost, že nějaký generátor bude, je: $\frac{\varphi(p-1)}{p-1} = \frac{\prod_{i=1}^k (q_i^{e_i} - q_i^{e_i-1})}{\prod_{i=1}^k q_i^{e_i}} = \prod_{i=1}^k \frac{q_i-1}{q_i} > \prod_{i=1}^{k+1} \frac{i-1}{i} = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdots \frac{k}{k+1} = \frac{1}{k+1}$
- celkem musíme udělat $k+1$ cyklot, v každém z nich k -krát počítat $\text{len}(p^3)$. Celková složitost je tedy $O((k+1) \cdot k \cdot \text{len}(p^3)) = O(k^2 \text{len}(p^3)) = O(\text{len}(p)^5)$, protože $k < \text{len}(p)$

Algoritmus 2:

for i in range $(1, k+1)$:

do:

$b = \text{náhodný prvek ze } \mathbb{Z}_p^*$

$b_i = b^{\frac{p-1}{q_i}}$

while $b_i = 1$

$a_i = b^{\frac{p-1}{q_i^{e_i}}}$

$a = \prod_{i=1}^k a_i$

$P[b_i \neq 1] = \frac{q_i-1}{q_i} > \frac{1}{2}$, pro velká p to jde k 1 $\Rightarrow b_i$ mají často napovídají výslednému výsledku.

- jak délko bude hledat minimální smyčka? volá se 2x a po každém pokusu se počítají opakovány čtvrtce, tj. $O(\text{len}(p)^3)$

- jak délko hledá nejčastější smyčku? volá se k-krať, pokudže se volá minimální smyčka ($2 \cdot \text{len}(p^2)$), a pak jednou opakovány čtvrtce. Celková náročnost je tedy $O(2k \cdot \text{len}(p)^3)$.

$a_i = b^{\frac{p-1}{q_i^{e_i}}}$, $r(a_i) = q_i^{e_i}$, neboť $a_i^{(q_i^{e_i})} = b^{p-1} = 1$, ale $a_i^{(q_i^{e_i-1})} = b^{\frac{p-1}{q_i}} \neq 1$ když odčteme všechny různé a_i jsou nesoudělné, pak $a = \prod a_i$, $r(a) = p-1$, a je generátor.
Počítaný výsledek jsme použili, v důkladu hledaném prvku, aby má ráčit jako exponent grupy

Příklad: $\mathbb{Z}_{26}^* = \mathbb{Z}_{2^3}^*$ je cyklická. Najděte její generátor. $|\mathbb{Z}_{26}^*| = 1 \cdot 12 = 12 = 2^2 \cdot 3$

Udělejme to algoritmem 2: $q_1 = 2, q_2 = 3, e_1 = 2, e_2 = 1$

$i = 1$:

$$b = 3, b_1 = 3^{\frac{12}{2}} = 3^6 = 1 \times$$

$$b = 5, b_1 = 5^{\frac{12}{2}} = 125 \neq -1 \checkmark$$

$$a_1 = b_1^{\frac{p-1}{q_1}} = 5^{\frac{12}{2}} = 5^6 = 5^3 = -5$$

$i = 2$:

$$b = 3, b_2 = 3^{\frac{12}{3}} = 3^4 = 3$$

$$a_2 = 3^{\frac{12}{3}} = 3^4 = 3$$

$$a = \prod a_i = a_1 \cdot a_2 = (-5) \cdot 3 = -15 = 11$$

$$r(a) = 3 \cdot 4 = 12, \text{ tedy } a \text{ je generátor}$$

| Přavděpodobnostní algoritmy
| = algoritmy, které používají náhodu

RAND: funkce, která generuje náhodný bit
 $y = \text{RAND}()$ $\rightarrow P[y=1] = P[y=0] = \frac{1}{2}$

- | - výsledek funkce RAND je nezávislý na předchozích voláních funkce RAND
- funkce RAND má složitost $O(1)$.

Algoritmy, které fungují pomocí náhodnosti jsou nazývány deterministické.

Náhodné veličiny pro pravděpodobnostní algoritmus

- LOOPS: počet spuštění cyklu
- LOOPTIME: čas běhu jednoho cyklu
- TIME: celkový čas běhu algoritmu
- OUTPUT: hodnota výstupu

Práce během algoritmu: posloupnost náhodných bitů.

Euklidova věta: Existuje neboničné mnoho prvočísel.

Dk: Uvorem: Nechtě p_1, \dots, p_k jsou všechna prvočísla. Uvažme $m = \prod_{i=1}^k p_i + 1$, pak m nejdé vyjádřit jako součin prvočísel, tedy je to taky prvočíslo.

Dovolení: Meri prvočísky jsou libovolné větší "číny". Tj. n je dělitelné n jeho souběžných složených čísel.

| Dk: Vezmeme čísla $(n+1)!+2, (n+1)!+3, \dots, (n+1)!+(n+1)$. Uvažka $(n+1)!$ je dělitelná všemi číslůmi až do $n+1$, a když je každá hodnota v posloupnosti jde např. jako součes $(n+1)!$ a nějakého čísla m , $m \leq n+1$, sedy bylo dělitelná stejně, a tímže i m prvočíslo. Máme tedy n po sobě jeho souběžných složených čísel.

| Čelyševova věta: Označme $T(m)$ počet prvočísel v intervalu $[1, m]$. Pro každé párce čísel $m \geq 2$ platí $T(m) \in \Theta\left(\frac{\ln(m)}{m}\right)$

Prvočíslo do 1000 je celkem 168, Čelyševův odhad je $\frac{1000}{\ln(1000)} \approx 145$.

Bertrandův postulát: Prvočíslo mezi m a $2m$ je $\Omega\left(\frac{m}{\ln(m)}\right)$.

Přednáška Algoritmus RP (random prime), vždy náhodné prvočíslo mezi 2 a m .
18.4.2019

Označme $l = \ln(m)$. Předpokládáme, že algoritmus IsPrime pracuje v čase $O(g(e))$, kde $g(e) > l$.

Počet volání cyklu vycházející z Čelyševovy a Bertrandovy věty. Celkový očekávaný čas práce algoritmu je $O(l \cdot g(e))$.

do:
 $n = \text{RAND}(2, m)$
 while not isPrime(n)
 return n

$$P[\text{isPrime}(n) / n \text{ je prvočíslo}] = 1$$
$$P[\text{isPrime}(n) / n \text{ je složené}] = \epsilon, \epsilon \ll \frac{1}{2}$$

Chceme odhadnout: $P[n \text{ je složené} / \text{isPrime}(n)]$

$$P[\text{isPrime}] \Rightarrow p > \frac{\pi(m)}{m} = \frac{c}{l}, \text{ kde } l = \ln(m)$$

| Vyhrajeme následkem: $P[A / B] = \frac{P[A \cap B]}{P[B]} = \frac{P[B / A] \cdot P[A]}{P[B]}$

$$P[m \text{ je složené} / \text{isPrime}(n)] = \frac{P[\text{isPrime}(n) / m \text{ je složené}] \cdot P[m \text{ je složené}]}{P[\text{isPrime}(n)]} <$$

$$< \frac{\epsilon \cdot \frac{1}{l}}{\frac{c}{l}} = \frac{\epsilon l}{c}, \text{ takže to je } O(\epsilon \cdot l)$$

lze tedy říci, že je to $O(\epsilon \cdot l)$

Deterministické testy prvočiselnosti:

- Brunou silou: dělíme n načni (prvočísl) čísla až do \sqrt{n} a zkontrolujeme dělitelnost.
- Agrawal, Kayal, Saxena: polynomický, ale $\tilde{O}(\text{len}(n)^{10.5 + o(1)})$

Pravděpodobnostní testy

- mají jednoduchou logiku
- odpovídá "šložné" je vždy správné
- odpovídá "prvočíslo" je správné aspoň v polovině případů

Fermatův test

- Svědkové prvočiselnosti pro Fermatův test

$$K_n = \{a \in \mathbb{Z}_n^*, a^{n-1} = 1\}, \text{ kde } n > 1 \text{ je testované prvočíslo}$$

- věta: \exists -li n prvočíslo, pak $K_n = \mathbb{Z}_n^* = \mathbb{Z}_n^\pm$. \exists -li n složené číslo, pro něž $K_n \neq \mathbb{Z}_n^*$, pak $|K_n| \leq \frac{1}{2} |\mathbb{Z}_n^*| \leq \frac{1}{2} |\mathbb{Z}_n^\pm|$.

- důkaz: $n = p$ je prvočíslo, $a^{p-1} = 1 \forall a \in \mathbb{Z}_p$ pro $\mathbb{Z}_p^\pm = \mathbb{Z}_p - \{0\}$, to vychází s malým Fermatovým náletem. Přesto $K_p = \mathbb{Z}_p^*$:

$\text{Rádyc je } n \text{ složené}, \text{ pak } K_n = \{a \in \mathbb{Z}_n^*, a^{n-1} = 1\} = \text{ker } p_{n-1}, \text{ což je podgrupa.}$

$p_{n-1}: \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*: x \mapsto x^{n-1}$ je grupový homomorfismus

Víme, že velikost podgrupy dělí velikost grupy:

$$\frac{|\mathbb{Z}_n^*|}{|K_n|} = k \in \mathbb{Z} \quad \left\{ \begin{array}{l} k=1 \Rightarrow K_n = \mathbb{Z}_n^*, \text{ když } n \text{ je Carmichaelovo} \\ k \geq 2 \Rightarrow |K_n| = \frac{1}{k} |\mathbb{Z}_n^*| \leq \frac{1}{2} |\mathbb{Z}_n^*|. \end{array} \right.$$

Fermat-test (n, a):

$$b = a^{n-1} \mod \mathbb{Z}_n$$

$$\text{if } b \equiv 1:$$

return True

return False

↳ hledáme opakování pro různá k
časová náročnost je $\tilde{O}(\text{len}(n)^3)$, protož děláme jeden algoritmus provádzající čtvrtce.

Příklad: Fermatovým testem otestujte, zda 21 je prvočíslo. Zvolte $a = 8$.

$$8^{20} = \dots = 1, \text{ odpovídá je ANO, je to prvočíslo}$$

Pravděpodobnost mylného výsledku je nejvýš $\frac{1}{2}$, a to byl hruškový odhad. Jaka je skutečnost:

$$K_{21} = \{a \mid a^{20} = 1, a \in \mathbb{Z}_{21}\} \quad \text{můžeme } x^{20} = 1 \mod \mathbb{Z}_{21}^* = \mathbb{Z}_3^* \times \mathbb{Z}_7^*$$

$$\varphi(3) = 2, \text{ redukuje se k 2, } \gcd(20, 2) = 2, x^2 = 1, x \in \{\pm 1\}$$

$$\varphi(7) = 6, \text{ redukuje se k 6, } \gcd(20, 6) = 2, x^2 = 1, x \in \{\pm 1\}$$

$$\mod \mathbb{Z}_{21}^*: x \leftrightarrow (\pm 1, \pm 1) \Rightarrow x \in \{1, 8, 13, 20\}$$

Při volbě $a \in \mathbb{Z}_{21}^+$ je pravděpodobnost mylného výsledku $\frac{|K_{21}|}{|\mathbb{Z}_{21}^+|} = \frac{4}{20} = \frac{1}{5} < \frac{1}{2}$.

Zvolíme $a = 6$:

$$6^{20} = \dots = 15 \neq 1, \text{ takže 21 není prvočíslo}$$

Namísto $\gcd(21, 6) = 3$, máli jsme faktor.

Zvolíme $a = 2$

$$2^{20} = 4, \text{ takže 21 není prvočíslo. Ale } \gcd(21, 2) = 1, \text{ takže faktor jsme nenešli.}$$

Definice: Carmichaelovo číslo je lichové složené číslo n , ře pro které $a \in \mathbb{Z}_n^*$ platí $a^{n-1} = 1 \mod \mathbb{Z}_n$

Tvrdění: Lichové Carmichaelovo číslo n je tvaru $n = p_1 \cdot \dots \cdot p_r$, kde p_i jsou různá lichá prvočísla, $r \geq 3$, $(p_i-1)/(n-1)$ pro každé $1 \leq i \leq r$.

Carmichaelova čísla jsou řidka, ale je jich nekonečně mnoho. Nejméně C. číslo je 561.

Miller-Rabinův test

- svedkové pravděslovnosti pro MR test: Budu $n > 1$ liché číslo, $n-1 = t \cdot 2^k$ pro liché t .
 $L_n = \{a \in \mathbb{Z}_n^*, a^{t-1} = 1, \text{ a když } a^{2^j} = 1, \text{ pak } a^{2^{j+1}} = \pm 1 \text{ pro } 1 \leq j \leq h\}$.

- turzení: rovnice $x^2 = 1$ má v grupě \mathbb{Z}_p^* právě dve řešení, a to $x = \pm 1$, pro p prvočíslo.
 $\Rightarrow n \in \mathbb{Z}_p^*$ majou nekonečnou skupinu řešení. To platí pro libovolnou cyklickou grupu
 Víta pro $n=p^e$, kde i v takých grupách bude $L_n = K_n$.

Miller-Rabin-test(n, k):

```

if n == 2:
    return True
if n % 2 == 0: // n je sudé
    return False
for i in range(0, k):
    a = RAND(2^n)
    if a not in L_n:
        return False
return True
    
```

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

a in L_n ?
 $b = a^t$
 if $b == 1$: return True
 for j in range(0, h):
 if $b == -1$: return True
 if $b == 1$: return False
 $b = b^{1/2} \vee 2^n$
 return False

Př: MR testem ověřte, zda 21 je prvočíslo. Zvolte a=8

$$n-1 = 21-1 = 20 = 2^2 \cdot 5, \text{ kde } t=5, h=2$$

$$a=8 \xrightarrow{5} 8^5=8 \xrightarrow{2} 8^2=64=1 \xrightarrow{2} 1^2=1$$

Následující jsme nekonečnou odmocinu, kterou do pravočísla:
 Navíc určíme najít faktor: $\gcd(8+1, 21) = \gcd(9, 21) = 3$
 $\gcd(8-1, 21) = \gcd(7, 21) = 7$

Př: $561 = 3 \cdot 11 \cdot 17$ je Carmichaelovo číslo

$$\begin{aligned} \mathbb{Z}_{561}^* &\cong \mathbb{Z}_3^* \times \mathbb{Z}_{11}^* \times \mathbb{Z}_{17}^* \\ \exp(\mathbb{Z}_{561}^*) &= \text{lcm}(\exp(\mathbb{Z}_3^*), \exp(\mathbb{Z}_{11}^*), \exp(\mathbb{Z}_{17}^*)) = \text{lcm}(2, 10, 16) = 5 \cdot 16 = 80 \\ \text{Tedy platí: } \forall a \in \mathbb{Z}_{561}^* : a^{80} &= 1, \text{ když } a^{560} = (a^{80})^7 = 1 \end{aligned}$$

Turzení z předchozí strany: Každé Carmichaelovo číslo je larn $n = p_1 \cdots p_r$, kde:

1) je jíson několik lichých prvočísla

2) $r \geq 3$

3) $(p_i - 1)/(n-1)$ pro každé $1 \leq i \leq r$.

Dle: 1) Když m bylo sudé, pak $n-1$ je liché, a potom $(-1)^{\text{liché prvočíslo}} = -1 \neq 1$.

2) Když $n = p_1 \cdot p_2$, pak $n-1 = p_1 \cdot p_2 + p_2 - p_2 - 1 = p_2(p_1 - 1) + p_2 - 1 = n-1$.

Přitom $(p_1 - 1)/(n-1)$ proto musí platit i $(p_1 - 1)/(p_2 - 1)$. Obdobně lichom aškali $(p_2 - 1)/(p_1 - 1)$. Z toho ale pluje $p_1 - 1 = p_2 - 1$, když $p_1 = p_2$. Pak ale $n = p_1^2$, což nesmí být (dokážeme hned led)

3) Díme, že $\exp(\mathbb{Z}_n^*) \mid n-1$. Když $n = \prod p_i^{e_i}$, $p_i > 2 \rightarrow$ skupiny $\mathbb{Z}_{p_i^{e_i}}^*$ jsou cyklické

$$\exp(\mathbb{Z}_{p_i^{e_i}}^*) = \varphi(p_i^{e_i}) = (p_i^{e_i-1}) \cdot (p_i - 1)$$

$$\exp(\mathbb{Z}_n^*) = \text{lcm}(\exp(\mathbb{Z}_{p_1^{e_1}}^*), \dots). Chceme, aby $\exp(\mathbb{Z}_n^*) \mid (n-1)$, tím pádem musí všechny $\exp(\mathbb{Z}_{p_i^{e_i}}^*) \mid (n-1)$.$$

$$\text{Proto } p_i^{e_i-1} \cdot (p_i - 1) \mid \prod_{i=1}^r p_i^{e_i-1} - 1. \text{ To méně možné, } p_i \nmid p_i^{e_i-1} - 1, \text{ musí být}$$

mbně $e_i = 1$, pak bude $(p_i - 1) \mid (n-1)$. Toto může být i ok

Příklad: Vypočítejte dlog₄(9) v \mathbb{Z}_{13}^*

$4 \in \mathbb{Z}_{13}^*$ je generátor, $4^6 = (2^2)^6 = 2^{12} = 1 \Rightarrow r(4) = 6$, tj. $r(u) \in \{2, 3, 6\}$

$2^2 = 4^2 = 16 \equiv 3 \not\equiv 1$

$3^2 = 4^3 = 3 \cdot 4 = 12 = -1 \Rightarrow$ tj. $r(u) = 6$, 4 není generátor.

Je všobec dlog_u(9) definován?

$P_6 = \langle 4 \rangle = \{1, 2, 4, 8, 3, 6\}$ se nám nejméně dělat mnoho.

Ale prostorem $9 = -4$, a protože víme, že množina $-1 \in P_6$, a $4 \in P_6$, musí být $-4 \in P_6$.

Nebo uvažujeme to, že jsme v cyklické skupině. Ne vzdáme, že následky $x \in P_6 \Rightarrow x^6 = 1$, a díky cyklické \mathbb{Z}_6^* víme, že $x^6 = 1 \Rightarrow x \in P_6$. Dostádme $x = 9$, pak $9^6 = \dots = 1$, proto $9 \in P_6$. Výsledek počtu nebudeme.

Důkaz: dlog_a(b) v cyklické \mathbb{Z}_p^* je definován, iff $b^{r(a)} = 1 \in \mathbb{Z}_p^*$.

Příklad: Vypočítejte dlog₂(21) v \mathbb{Z}_{143}^* , kde $143 = 11 \cdot 13$. $\varphi(143) = 10 \cdot 12 = 120$

\mathbb{Z}_{143}^* není cyklická, t.j. nemá ani generátor.

Najdeme podgrupu $G = \langle 2 \rangle$, $|G| = r(2) = n$.

$$\mathbb{Z}_{143}^* \cong \mathbb{Z}_{11}^* \times \mathbb{Z}_{13}^*, \quad 2 \leftrightarrow (2, 2)$$

$$\begin{cases} 2 \in \mathbb{Z}_{11}^*: \varphi(11) = 10 = 5 \cdot 2 \\ 2^5 = \dots = 10 = -1 \\ 2^2 = \dots = 4 \end{cases} \quad \begin{cases} r(2) \in \mathbb{Z}_{13}^* = 10 \\ \mathbb{Z}_{11}^* = \langle 2 \rangle \end{cases}$$

$$\begin{cases} 2 \in \mathbb{Z}_{13}^*: \varphi(13) = 12 = 2 \cdot 2 \cdot 3 \\ 2^6 = \dots = -1 \\ 2^4 = \dots = 3 \end{cases} \quad \begin{cases} r(2) \in \mathbb{Z}_{13}^* = 12 \\ \mathbb{Z}_{13}^* = \langle 2 \rangle \end{cases} \Rightarrow G = \langle 2 \rangle, |G| = 60$$

- jaký je exponent v \mathbb{Z}_{143}^* ?

$$\exp(\mathbb{Z}_{143}^*) = \text{lcm}(10, 12) = 60 \Rightarrow \forall a \in \mathbb{Z}_{143}^*: a^{60} = 1$$

- spočítáme dlog₂(21) = x residuálně

$$v \mathbb{Z}_{11}^*: 2^x = 21, \text{ spočítáme pro všechna } x \quad v \mathbb{Z}_{13}^*: 2^x = 21 = 8$$

x	2 ^x
1	2
2	4
3	8
4	16
5	10

$$21 = 10 \in \mathbb{Z}_{11}^*$$

$$2^5 = 10$$

$$x = 5 + 10k$$

x	2 ^x
1	2
2	4
3	8

$$2^3 = 8$$

$$x = 3 + 12l$$

$$x = 5 + 10k = 3 + 12l$$

$$k, l = (1, 1) + m \cdot (6, 5)$$

$$12l - 10k = 2$$

$$6l - 5k = 0$$

$$\text{Kožliv } m = 0, \text{ pak } x = 5 + 10(1 + 6m) = 5 + 10 = \underline{\underline{15}}$$

Příklad: Vypočítejte dlog₃(141) pomocí Polling-Hellmannova v \mathbb{Z}_{223}^* , $\mathbb{Z}_{223}^* = \langle 3 \rangle$, 223 je prvočíslo

Předpoklad: 3 je generátor: $|\mathbb{Z}_{223}^*| = 222 = 2 \cdot 3 \cdot 37$

$3^6 \neq 1$, $3^{5 \cdot 37} \neq 1$, $3^{2 \cdot 37} \neq 1 \Rightarrow r(3) = 222$, je to generátor.

$\sqrt{222} = 15$, tj. Baby-Step Giant-Step by měl $2 \cdot 15 = 30$ kroků.

Polling-Hellmann: Rovnici $3^x = 141$ budeme řešit v podgrupách $P_{q_i} = \langle a^{\frac{n}{q_i}} \rangle$, a k nim siškáme $x_i = x \bmod q_i$

$$\begin{aligned} P_2: 3^x &= 141 \quad / \wedge 3 \cdot 37 \\ (3^{11})^x &= 141^{11} \\ (-1)^x &= -1 \end{aligned}$$

$$x = 1 \bmod 2$$

$$\begin{aligned} P_3: 3^x &= 141 \quad / \wedge 2 \cdot 37 \\ (3^{74})^x &= 141^{74} \\ 183^x &= 1 \end{aligned}$$

$$x = 0 \bmod 3$$

$$\begin{aligned} P_{37}: 3^x &= 141 \quad / \wedge 6 \\ (3^6)^x &= 141^6 \\ 60^x &= 56 \end{aligned}$$

Dohle jen tak neúčinně, násadíme Baby-step-Giant-step.

\approx pokračování, řešme $60^x = 56 \text{ v } \mathbb{Z}_{37}$. $\sqrt[6]{56} = 6 \Rightarrow x = 6v + w$

$$60^{6v+w} = 56 \rightarrow \text{jsem pořád v } \mathbb{Z}_{223}!$$

$$60^w = 56 \cdot (60^{-6})^v = 56 \cdot 120$$

i	0	1	2	3	4	5	6
baby step	60^i	1	60	(32)	136	132	115
giant step	$56 \cdot (120)^i$	56	30	(32)			210

$$n = r = 2$$

$$x = 6 \cdot 2 + 2 = 14 \text{ mod } 37$$

Kompletační výsledek: Použijeme čínskou metodu souběžných

$$x = 0 \text{ mod } 3$$

$$q_3 X$$

$$x = 1 \text{ mod } 2$$

$$q_2 = 111 \cdot 1 \Rightarrow q_2 = 111$$

$$x = 14 \text{ mod } 37$$

$$q_{37} = 6 \cdot 1 \Rightarrow q_{37} = 187$$

$$x = 0q_3 + 1q_2 + 14q_{37} = 111 + 14 \cdot 186 = \\ = 111 + 2604 = 2715 = \underline{\underline{51}} \text{ v } \mathbb{Z}_{223}^*$$

Př: 15. skupina $\mathbb{Z}_{25}^* = \langle 6 \rangle$ spočtejte dlogu (135). Použijte Polling-Hellman alg.

Ověřme, že 6 je generátor:

$$\varphi(25) = 250 = 5 \cdot 5 \cdot 2$$

$$6^{125} = \dots = -1 \neq 1$$

$$6^{50} = \dots = 219 \neq 1$$

} je to generátor, $\varphi(6) = 250$

$$P_2: 6^x = 135 / \wedge^{125}$$

$$(6^{125})^x = 135^{125}$$

$$(-1)^x = 1$$

$$\text{tedy } x = 0 \text{ mod } 2$$

$$P_{125}: 6^x = 135 / \wedge^2$$

$$36^x = 153$$

Baby step - Giant step by mál

$$2 \cdot \frac{1}{6^{125}} = 2 \cdot 11 = 22 \text{ kroků.}$$

Raději ho vypočítejte Polling-Hellmanovým převodem do P_5 .

$$P_5: \langle 6^{50} \rangle = \langle 219 \rangle, x \in \mathbb{Z}_{125} \text{ mapujeme na druhou } x' = x_2 \cdot 25 + x_1 \cdot 5 + x_0, \text{ pro } x_i \leq 4.$$

$$36^{25x_2 + 5x_1 + x_0} = 153$$

Umožníme to na 25 a využijeme toho, že $36^{125} = 1$, několik $\varphi(36) = 125$.

$$36^{25x_0} = 153^{25}$$

$$219^{x_0} = 113 \text{ hrubou silou:}$$

i	0	1	2	3
219 ⁱ	1	219	20	(113)

$$\Rightarrow x_0 = 3$$

$$36^{25x_2 + 5x_1 + 3} = 153$$

$$36^{25x_2} \cdot 36^3 = 153$$

$$219^{x_2} = 153 \cdot 7^3 = \dots = 20$$

} hodnoty hrubou silou vřechné, $x_2 = 2$

$$x' = 25x_2 + 5x_1 + x_0 = 50 + 0 + 3 = 53 \text{ mod } 125$$

Kompletační výsledek:

$$x = 0 \text{ mod } 2$$

$$x = 53 \text{ mod } 125$$

$$q_2 = 125 \cdot 1 = 125$$

$$q_{125} = 21 = 126$$

$$x = 0 \cdot 125 + 53 \cdot 126 = 6678 = \underline{\underline{178}}$$