

a) SEDL: 1. fáze

Nechť p_1, \dots, p_k jsou všechna prvočísla do y , ježich sedly k . Na hledanou nulovou
součinnou $(k+1)$ y -bladkých čísel se \mathbb{Z}_p^* nazvou $a_i^{\pm} \cdot b_i^{\pm} \cdot h_i$, kde $a_i^{\pm} \cdot b_i^{\pm} = g_i$,

$g_i \in G$. Pro každé i od 1 do $k+1$ ho provedeme faktor:

- svůj na hledané $s_i \cdot t_i \in \mathbb{Z}_p$, a $h_i' \in \mathbb{Z}_p^*$, správně $h_i = h_i'^{-1} \cdot h_i$, $h_i \in H$
- správně $z_i = a_i^{\pm} \cdot b_i^{\pm} \cdot h_i$; a ovět., když z_i je y -bladké
- pokud ano, pak $z_i = p_1^{e_1} \cdots p_k^{e_k}$, jinak zkus rozlit jiná čísla.

Teoreticky by to šlo bez h_i , ale neměl bychom mít casovou složitost

SEDL: 2. fáze

Přime, ře $q=|G|$ je prvočíslo, proto \mathbb{Z}_q je těleso. Budeme pracovat s $k+1$ vektorům exponencií (délky k),
 $\bar{v}_i = (e_{i1}, \dots, e_{ik})$. Množina všech k -lic nad \mathbb{Z}_q má q^k lin. prostor, když naších $k+1$ vektorů
 musí být lineárně závislých a dokážeme s nimi nakombinovat nulový vektor.

Budeme řešit soustavu $c_1 \cdot \bar{v}_1 + c_2 \cdot \bar{v}_2 + \cdots + c_{k+1} \cdot \bar{v}_{k+1} = \bar{0}$

Každou i lici rozmístíme na příslušné c_i a všechny rozmístíme podle výpočtu, různého
 rozmístí $a_i^{\pm} \cdot b_i^{\pm} \cdot h_i = p_1^{e_1} \cdots p_k^{e_k} \in \mathbb{Z}_p^*$, kde $s = \sum c_i \cdot s_i$, $\lambda = \sum c_i \cdot t_i$, $h = \prod h_i^{c_i} \in \mathbb{Z}_p^*$.
 Všechna c_i jsou nulová, takže musíme $s \neq 0$, $\lambda \neq 0$. Namísto q/e_i pro t_i užíváme $p_i^{e_i} \in H$.

Nyní máme rozmístí $a_i^{\pm} b_i^{\pm} = h_i^{-1} \cdot p_1^{e_1} \cdots p_k^{e_k} \in \mathbb{Z}_p^*$, kde prvek na levé straně je $\in G$, a na
 pravé straně je $\in H$. Jenž $G \cap H = \{\pm 1\}$, proto $a_i^{\pm} b_i^{\pm} = 1 \Rightarrow G \subseteq \mathbb{Z}_p^*$. Pokud $\lambda = 0$, ohlášme neúspěch,
 jinak spočítáme dloga(b) = $-s \cdot \lambda^{-1} \in \mathbb{Z}_q$.

Příklad: $G = \langle 4 \rangle$ je podgrupa řídnu 11 v grupě \mathbb{Z}_{23}^* , $|\mathbb{Z}_{23}^*| = 22 = 2 \cdot 11$, tedy $H = \{\pm 1\}$.
 Spočítejte dlogu(12) v \mathbb{Z}_{23}^* , svoluje parních bladkosti $y=4$.

1. fáze: $\bar{p} = \{2, 3\}$, l_i k $i = 2$. Najdu $k+1$ y -bladkých čísel (nulovu $a_i^{\pm} \cdot b_i^{\pm} \cdot h_i$):

- můžu volit $h_i \in \mathbb{Z}_{23}^*$ a to pak možnost 11, nebo můžu rovnou vybrat a $H = \{\pm 1\}$

$a=4$, $b=12$, můžu $h_1 \cdot 12^1 \cdot \pm 1$

$$i=1: s_1 = 5, \lambda_1 = 7, h_1 = 1 \Rightarrow 45 \cdot 12^7 \cdot 1 = 8 = 2^3 \cdot 3^0 \quad \checkmark \quad v_1 = (3, 0)$$

$$i=2: 4^{10} \cdot 12^5 \cdot (-1) = 7 \text{ není } 4\text{-bladké} \times$$

$$4^3 \cdot 12^9 \cdot 1 = 21 \times$$

$$4^4 \cdot 12^9 \cdot 1 = 12 = 2^2 \cdot 3^1 \quad \checkmark$$

$$i=3: 4^6 \cdot 12^7 \cdot 1 = 9 = 2^0 \cdot 3^2 \quad \checkmark \quad v_3 = (0, 2)$$

$$R_1: 45 \cdot 12^7 \cdot 1 = 2^3 \cdot 3^0$$

$$R_2: 4^4 \cdot 12^9 \cdot 1 = 2^3 \cdot 3$$

$$R_3: 4^6 \cdot 12^7 \cdot 1 = 2^0 \cdot 3^2$$

2. fáze: Hledám nehomogenní kombinaci rovnou nula

$$c_1 \cdot (3, 0) + c_2 \cdot (2, 1) + c_3 \cdot (0, 2) = \bar{0}$$

$$\begin{pmatrix} 3 & 2 & 0 & | & 0 \\ 0 & 1 & 2 & | & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 8 & 0 & | & 0 \\ 0 & 1 & 2 & | & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -5 & | & 0 \\ 0 & 1 & 2 & | & 0 \end{pmatrix}$$

Volím $c_3 = 1$. Pak $c_1 = 5$, $c_2 = -2$, tedy $\bar{c} = (5, -2, 1)$

$$s = \sum s_i \cdot c_i = 5 \cdot 5 - 2 \cdot 4 + 1 \cdot 6 = 25 - 8 + 6 = 23$$

$$\lambda = \sum t_i \cdot c_i = 5 \cdot 7 - 2 \cdot 9 + 1 \cdot 7 = 24$$

$$h = \prod h_i^{c_i} = 15 \cdot 4^{-2} \cdot 1^1 = 1$$

$$e_1 = 5 \cdot 3 - 2 \cdot 2 + 1 \cdot 0 = 15 - 4 = 11$$

$$e_2 = 5 \cdot 0 - 2 \cdot 1 + 1 \cdot 2 = 0 - 2 + 2 = 0$$

$$\left. \begin{array}{l} 4^{23} \cdot 12^{24} \cdot 1 = 2^{11} \cdot 3^0 \\ 4^1 \cdot 12^2 = 1 \end{array} \right\}$$

Exponentech počítáme mod $|G| = 11$, po úpravě máme $4^1 \cdot 12^2 \cdot 1 = 2^0 \cdot 3^0 = 1$

Získali jsme nehomogenní reprezentaci jedničky v \mathbb{Z}_{23}^* , $4^1 \cdot 12^2 = 1$

2. reprezentace $4^1 \cdot 12^2 = 1$ spočítáme dlogn(12) = x $\approx 4^x = 12$

$$1 = 4^1 \cdot 12^2$$

$$4^0 = 4^1 \cdot (4x)^2$$

$$0 = 1 + 2x \quad \text{v } Z_4$$

$$x = -1 \cdot 2^{-1} = -1 \cdot 6 = -6 = 5$$

$$\text{dlog}_4(12) = 5$$

Zobecnění algoritmu SEDL: Pokud jsme v podgruppe řádu q^e grupy \mathbb{Z}_p^* , kde p je součin prvočísel, $|\mathbb{Z}_p^*| = q^e \cdot m$, $q \nmid m$, můžeme SEDL řešit obdobně. Pozejmé množinu sloupců v Gaußově eliminaci, kde na jednom místě může být nula.

Časová náročnost SEDL-n:

- každou reprezentaci (s, t) vytvářejí se stejnou pravděpodobnost.

$$(s_0, 0) \quad \leftarrow 1 \times \text{nepřes}$$

$$(s_1, 0) \quad \leftarrow q-1 \times \text{nepřes}$$

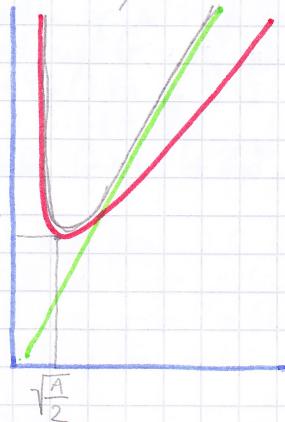
$$\text{Proto } P[\text{nepřes}] = \frac{1}{q}$$

- 1. fáze: Vyhodnocení pravděpodobnosti, že náhodný prvek ze \mathbb{Z}_p^* je y -hladký (pro výpočet q^e se používá σ). Počet cyklů do následení jednoho y -hladkého prveku je $\frac{1}{\sigma}$. V každém kroku dělíme počet cyklů od 2 do y , celkem $k+1$ krát. První fáze má náročnost $\Theta(\frac{k^2}{\sigma} \cdot \text{len}(p)^2)$.
- 2. fáze: Gaußova eliminace na matici typu $(k, (k+1))$ vyžaduje k^3 operací, tj. $\Theta(k^3 \cdot \text{len}(p)^2)$.
- Celkový čas SEDL-n je $\Theta((\frac{k^2}{\sigma} + k^3) \cdot \text{len}(p)^2)$

Vyhodnocení volby parametru y :

$$\begin{aligned} & \text{Pokud dáme } y(z) = e^{\ln(p)^{\frac{z}{A} + o(1)}}, \text{ je zde předpoklad a určíme, že } \psi(y, x) = x \cdot e^{-(1+o(1)) \cdot \frac{\ln(x)}{\ln(y)} \cdot \ln(\ln(x))} \\ & (\frac{k^2}{\sigma} + k^3) \cdot \text{len}(p)^2 = \underbrace{\left((1+o(1)) \cdot \frac{\ln(p)}{\ln(y)} \cdot \text{len}(\ln(p)) \right)}_{\frac{1}{\sigma}} \cdot \underbrace{(2+o(1)) \cdot \ln(y)}_{k^2} + \underbrace{(3+o(1)) \cdot \ln(y)}_{k^3} \cdot \underbrace{o(1) \cdot \ln(y)}_{\text{len}(p)^2} \\ & = (1+o(1)) \cdot \max \left\{ \left[\frac{\ln(p)}{\ln(y)} \cdot \ln(\ln(p)) + 2 \cdot \ln(y) \right], [3 \cdot \ln(y)] \right\} \end{aligned}$$

Deníme $\mu = \ln(y)$, $A = \ln(p) \cdot \ln(\ln(p))$. Chceme majit minimum fce $f(\mu) = \max \left\{ \frac{A}{\mu} + 2\mu, 3\mu \right\}$



$$f_1(\mu) = \frac{A}{\mu} + 2\mu \quad \text{Rádiové reprezentaci}$$

$$f_2(\mu) = 3\mu \quad \text{Gaußova eliminace}$$

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

Minimum najdeme přes první derivaci, minimum je v bodě $\mu = \sqrt{\frac{A}{2}}$

SEDL počítá nejlípe pro parametr hladkosti $y = e^{-\frac{\sqrt{A}}{2}}$, a složitost $\Theta((2\sqrt{A} + o(1)) \cdot \sqrt{\ln(p) \cdot \ln(\ln(p))})$

Př: Podívejte se na rozložení 4-hladkých čísel v \mathbb{Z}^* nad \mathbb{Z}_{23} .

(1)	(6)	(13)	(9)	(8)	(2)	(12)	(3)	(18)	(16)	(4)	(5)
-1	-6	-13	-9	-8	-2	-12	-3	-18	-16	-4	
22	17	10	14	15	21	11	20	5	7	19	

Zakroužkovaná čísla jsou 4-hladká
 \Rightarrow jsou jen v \mathbb{G} proto nám
 předmět s $b_1 = -1$ nìc nezulo.

Př: Mzd. $\mathbb{Z}_{27} = \mathbb{Z}_3$ najdete a spor. jedno řešení (nekvadratické).

$$\begin{pmatrix} 18 & 9 & 12 & 14 & | & 0 \\ 12 & 12 & 4 & 9 & | & 0 \\ 15 & 24 & 23 & 0 & | & 0 \end{pmatrix} \text{ chceme } \begin{pmatrix} 1 & 0 & 0 & b_1 & | & 0 \\ 0 & 1 & 0 & b_2 & | & 0 \\ 0 & 0 & 1 & b_3 & | & 0 \end{pmatrix}$$

Chceme smazat invertibilní kusy pivoňky a pak
 počít rádelek s nejménší mocninou když k
 zrybolování pivoňko sloupce.

$$\begin{array}{ll} 18 = 3^2 \cdot 2 & 2^{-1} = 14 \\ 12 = 3^1 \cdot 4 & 4^{-1} = 7 \\ 15 = 3^1 \cdot 5 & 5^{-1} = 11 \end{array}$$

$$22^{-1} = 16 \quad (\text{to je potřeba napsat dolů})$$

Pořadí řady lude -9, podílej se zrovna jinak a dostaneš $c = (1, 6, 6, 9)$

$$\begin{array}{l} R_1/2 \\ \sim R_1/4 \\ \sim R_1/11 \end{array} \left(\begin{array}{ccccc|c} 9 & 126 & 18 & 168 & 6 & 196 & 7 & | & 0 \\ 3 & 84 & 3 & 28 & 1 & 63 & 9 & | & 0 \\ 3 & 264 & 21 & 253 & 10 & 0 & 0 & | & 0 \end{array} \right) \sim \left(\begin{array}{ccccc|c} 9 & 18 & 6 & 7 & | & 0 \\ 3 & 3 & 1 & 9 & | & 0 \\ 3 & 21 & 10 & 0 & | & 0 \end{array} \right) \begin{array}{l} R_2 \\ \sim R_1 - 3R_2 \\ R_3 - R_2 \end{array} \left(\begin{array}{ccccc|c} 3 & 3 & 1 & 9 & | & 0 \\ 0 & 9 & 3 & 7 & | & 0 \\ 0 & 0 & 12 & 25 & | & 0 \end{array} \right)$$

$$\begin{array}{l} R_1 \\ \sim R_2 \\ R_3 + R_2 \end{array} \left(\begin{array}{ccccc|c} 3 & 3 & 1 & 9 & | & 0 \\ 0 & 9 & 3 & 7 & | & 0 \\ 0 & 0 & 12 & 25 & | & 0 \end{array} \right) \sim \begin{array}{l} R_1 \\ R_2 \\ R_3/2 \end{array} \left(\begin{array}{ccccc|c} 3 & 3 & 1 & 9 & | & 0 \\ 0 & 9 & 3 & 7 & | & 0 \\ 0 & 0 & 6 & 25 & | & 0 \end{array} \right)$$

Máme nuly pod diagonálou, ale na diagonále jsou minverzibilní čísla. Dovolime přehazovat sloupce, budem pracovat s C_4 .

$$\begin{array}{l} R_1 \\ \sim R_2 \\ -R_3 \end{array} \left(\begin{array}{ccccc|c} 3 & 3 & 9 & 1 & | & 0 \\ 0 & 9 & 7 & 3 & | & 0 \\ 0 & 0 & 1 & -6 & | & 0 \end{array} \right) \sim \begin{array}{l} R_1 - 9R_3 \\ R_2 - 7R_3 \\ R_3 \end{array} \left(\begin{array}{ccccc|c} 3 & 3 & 0 & 1 & | & 0 \\ 0 & 9 & 0 & 18 & | & 0 \\ 0 & 0 & 1 & 21 & | & 0 \end{array} \right)$$

Ted' už si můžeme víc dělat, proto
 si dovolím vybratit obvyklý rádelek 9. Jiné
 získáme nijaká řešení.

$$\begin{array}{l} R_1 \\ \sim R_2/9 \\ R_3 \end{array} \left(\begin{array}{ccccc|c} 3 & 3 & 0 & 1 & | & 0 \\ 0 & 1 & 0 & 2 & | & 0 \\ 0 & 0 & 1 & 21 & | & 0 \end{array} \right) \sim \begin{array}{l} R_1 - 3R_2 \\ R_2 \\ R_3 \end{array} \left(\begin{array}{ccccc|c} 3 & 0 & 0 & 22 & | & 0 \\ 0 & 1 & 0 & 2 & | & 0 \\ 0 & 0 & 1 & 21 & | & 0 \end{array} \right)$$

$$\begin{array}{l} c_3 \\ 16 \cdot R_1 \\ R_2 \\ R_3 \end{array} \left(\begin{array}{ccccc|c} 22 & 0 & 0 & 3 & | & 0 \\ 2 & 1 & 0 & 0 & | & 0 \\ 21 & 0 & 1 & 0 & | & 0 \end{array} \right)$$

$$\begin{array}{l} R_1 \\ \sim R_2 - 2R_1 \\ R_3 - 2R_1 \end{array} \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 21 & | & 0 \\ 0 & 1 & 0 & 3 & | & 0 \\ 0 & 0 & 1 & 18 & | & 0 \end{array} \right)$$

Nejdoume $c_1 = 1$, pakže: $c_2 = -3 = 24$

$$\begin{array}{l} c_3 \\ c_4 \end{array} \left(\begin{array}{ccccc|c} 0 & 0 & 1 & 6 & | & 0 \\ 0 & 0 & 1 & 9 & | & 0 \end{array} \right)$$

$$c = (1, 24, 6, 9)$$

Subexponentiální faktorizace - SEF

- bere písací číslo, které nemá pravocísla ani jeho mocnina, a parametr hladkosti y
- výsledek je nekvadratický faktor, neb hlaška neúspěch.

SEF: 1. fáze

Nechť p_1, \dots, p_k jsou všechna pravocísla do y , je jich k . Nejdoume volbou následne $k+1$ y -hladkých čísel se \mathbb{Z}_n^* , a to tak, že:

- vybereme náhodně $a_i \in \mathbb{Z}_n^*$

- pro každý delením očekávme, sda $m_i = a_i^2$ je y -hladké, tj. $m_i = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$

SEF: 2. fáze

Pro každé i od 1 do $k+1$ vypočítejme vektor exponencií $\bar{v}_i = (e_{i1}, \dots, e_{ik})$ jako vektor nad \mathbb{Z}_2 .
 Najdeme vektor koeficientů $c = (c_1, \dots, c_{k+1})$, aby $c_1\bar{v}_1 + \dots + c_{k+1}\bar{v}_{k+1} = \bar{0}$. Počíváme-li se na tuto kombinaci v \mathbb{Z}_2 , tak všechny složky jsou sudé (e_1, \dots, e_k jsou sudé).

Pro každou remort mocniny na příslušné c_i a normu vypočítejme výpočetní hodnotu $a_i^{c_i} = p_1^{e_{i1}} \cdot \dots \cdot p_k^{e_{ik}}$, kde $c_i \in \{0, 1\}$. Počíváme $b = p_1^{\frac{e_1}{2}} \cdot \dots \cdot p_k^{\frac{e_k}{2}}$, kde $e_i/2 \in \mathbb{N}$.

$a^2 = b^2 \in \mathbb{Z}_n^*$ upravíme na $(ab^{-1})^2 = 1 \in \mathbb{Z}_n^*$. Našli jsme $c = ab^{-1}$, druhou odmocninu z jeho.

- pokud $c = \pm 1$, ohlasime neúspěch

- jinak $\gcd(c \pm 1, n)$ je faktor.

Příklad: faktorizejte $n=77$ pomocí SEFu s parametry $y=5$.

MR sedem většinou, že to není možné, algoritmem perfektní mohou všechny, ale nemůže.

Najdeme 5-hladká písma: $P = \{2, 3, 5\}$. Záleží k nich nedělí 77, můžeme použít SEF:

1. fáze: $|P| = k = 3$. Najdeme 4 y-hladké čtverce.

$$\begin{array}{ll} i=1: 5^2 = 25 = 2^4 \cdot 3^0 \cdot 5^0 & v_1 = (4, 0, 0) \\ i=2: 3^2 = 9 = 2^0 \cdot 3^2 \cdot 5^0 & v_2 = (0, 2, 0) \\ i=3: 25^2 = 625 = 2^2 \cdot 3^1 \cdot 5^1 & v_3 = (2, 1, 1) \\ i=4: 10^2 = 100 & X \\ 13^2 = 169 = 2^0 \cdot 3^1 \cdot 5^1 & v_4 = (0, 1, 1) \end{array}$$

2. fáze: Nacházíme reprezentaci $c_1 \cdot v_1 + \dots + c_4 \cdot v_4 = \bar{c}$

$$c_1 \cdot (0, 0, 0) + c_2 \cdot (0, 0, 0) + c_3 \cdot (0, 1, 1) + c_4 \cdot (0, 1, 1) = \bar{c}$$

Gaußova výnecháme, neboť všechny řešení najdeme zde. Třeba $\bar{c} = (0, 1, 0, 0)$

$$a_1^0 \cdot a_2^0 \cdot a_3^0 \cdot a_4^0 = a_2 = 2^0 \cdot 3^2 \cdot 5^0$$

$$(3 \cdot (3^{-1}))^2 = 1^2$$

$$1^2 = 1^2$$

Výpočet nám vliváhu řešení

Zkoušíme $\bar{c} = (0, 0, 1, 1)$

$$a_2 \cdot a_4 = 37^2 \cdot 13^2 = (37 \cdot 13)^2 = 19^2 = 2^2 \cdot 3^2 \cdot 5^2 = 30^2$$

$$19^2 = 30^2$$

$$(19 \cdot 30^{-1})^2 = 1$$

$$(19 \cdot 18)^2 = 1$$

$$34^2 = 1$$

Náspech, máme $c \neq 1$.

$\gcd(35, 77) = 7$, mělo $\gcd(33, 77) = 11$. Faktory n jsou 7 a 11.

Cílem: Příklad $\mathbb{Z}_9^* = \langle 2 \rangle$ našeného významu reprezentace jednotky včetně generátorem a průběhu $b = 7$.

$$|\mathbb{Z}_9^*| = 6, \text{ když } s, t \in \mathbb{Z}_6, \text{ chceme } a^{st} = 1, \text{ kde } 2^s 7^t = 1$$

Budeme zkoušet různá s a doporučujeme k nim t :

$$t=0 \quad 2^s \cdot 1 = 1 \Rightarrow s=0. \quad 1^{-1} \text{ neexistuje, je to triviální.}$$

$$t=1 \quad 2^s \cdot 7 = 1 \Rightarrow 7^{-1}=4, \quad 2^s=4, \quad \text{proto } s=2$$

$$t=2 \quad 2^s \cdot 49 = 2^s \cdot 4 = 1 \Rightarrow 4^{-1}=7, \quad 2^s=7 \Rightarrow s=4$$

$$t=3 \quad 2^s \cdot 1 = 1, \quad s=0$$

- pro $t=4, 5$ by to dopadlo stejně jako pro $t=1, 2$. Máme 3 vliváhu dvojice $(t, s) = 3$.

s	t	a^{st}
0	0	1
2	1	4
4	2	7
0	3	1

Příklad: \mathbb{Z}_{15}^* našu 18 spočítat dlog₂(b), analýza reprezentace jednotky.

$$a) \text{dlog}_2(15) = x, \text{ když } (s, t) = (17, 5)$$

$$2^{17} \cdot 15^5 = 1$$

$$2^{17} \cdot (2^5)^5 = 2^0$$

$$17 + 5x = 0$$

$$x = -17 \cdot 5^{-1} = -17(-7) = 1 \cdot (-7) = -7 = 11$$

$$2^{11} = 15 \sim \mathbb{Z}_9^* \quad \checkmark$$

$$b) \text{dlog}_2(14) = x, \text{ když } (s, t) = (4, 2) \leftarrow \text{tahle reprezentace je triviální, SEDL by ji zařadil.}$$

$$2^4 \cdot 14^2 = 1$$

$$2^4 \cdot 2^{2x} = 2^0$$

$$4 + 2x = 0 \leftarrow \text{počítáme exponenty, když jsou v } \mathbb{Z}_{18}, \text{ a tam platí } 2^{-1}!$$

$$\sim \mathbb{Z}_{18}: 2x = -4$$

$$(-11, 1) + k \cdot (-9, 1), \sim \mathbb{Z}_{18} \text{ jsou } x=7, x=16$$

$$\sim \mathbb{Z}: 2x + 18y = -4$$

$$\text{Máme dvě řešení, protože } \gcd(4(n), 1) = \gcd(18, 2) = 2$$

$$x + 9y \equiv -2$$

$$\text{Které z nich je správné? } 2^7 = 14 \quad \checkmark$$

$$2^{16} = 5 \quad X$$

$$\text{dlog}_2(14) = 7.$$

Příklad: Je dána podgrupa $G = \langle 9 \rangle$ řádu $q = 23$ v grupě \mathbb{Z}_{47}^* . Algoritmem SEDL spočítejte dlog₉(8) v r. G, následek $y = 5$.

$$|\mathbb{Z}_{47}^*| = 46 = 2 \cdot 23 \rightarrow \mathbb{Z}_{47}^* \cong G \times H, \text{ kde } H = \{\pm 1\}$$

$$P = \{2, 3, 5\}, k = 3.$$

1. fáze:

$$a^s \cdot b^t \cdot h_i = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} = 9^s \cdot 8^t \cdot h_i$$

$$\begin{aligned} i=1: & 9^s \cdot 8^t \cdot 1 = 24 \cdot 7 \cdot 1 = 27 = 2^0 \cdot 3^3 \cdot 5^0 \\ i=2: & 9^5 \cdot 8^5 \cdot 1 = 17 \cdot 9 \cdot 1 = 12 = 2^2 \cdot 3^1 \cdot 5^0 \\ i=3: & 9^2 \cdot 8^6 \cdot 1 = 34 \cdot 25 \cdot 1 = 4 = 2^2 \cdot 3^0 \cdot 5^0 \\ i=4: & 9^9 \cdot 8^8 \cdot (-1) = 6 \cdot 2 \cdot (-1) = 35 \quad \times \\ & 9^7 \cdot 8^5 \cdot 1 = 14 \cdot 9 \cdot 1 = 32 = 2^5 \cdot 3^0 \cdot 5^0 \end{aligned}$$

lady jsou v \mathbb{Z}_{47}^*

$$\begin{aligned} v_1 &= (0, 3, 0) \\ v_2 &= (2, 1, 0) \\ v_3 &= (2, 0, 0) \\ v_4 &= (5, 0, 0) \end{aligned}$$

2. fáze: hledám rekurzivní kombinaci pomocí rule.

$$c_1 v_1 + c_2 v_2 + c_3 v_3 + c_4 v_4 = \bar{a} \rightarrow 3^{-1} = 8 \text{ v } \mathbb{Z}_{23} \leftarrow \text{když počítáme v exponencích}$$

$$\left(\begin{array}{cccc|c} 0 & 2 & 2 & 5 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \xrightarrow{R_1} \left(\begin{array}{cccc|c} 3 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \xrightarrow{R_2} \left(\begin{array}{cccc|c} 1 & 8 & 0 & 0 & 0 \\ 0 & 2 & 2 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$\text{Kvůli tomu } c_4 = 0, c_3 = -1, c_2 = -1, c_1 = 8 \rightarrow c = (8, -1, 1, 0)$$

$$S = \sum s_i \cdot c_i = 8 \cdot 3 - 1 \cdot 5 + 1 \cdot 2 = 24 = 5 + 2 = 21 \text{ v } \mathbb{Z}_{23}$$

$$A = \sum t_i \cdot c_i = 8 \cdot 4 - 1 \cdot 5 + 1 \cdot 6 = 32 + 1 = 33 = 10$$

$$h = \prod h_i^{c_i} = \prod 1^{c_i} = 1$$

$$a^s \cdot b^t \cdot h = 9^{21} \cdot 8^{10} \cdot 1 = 18 \cdot 34 \cdot 1 = 1 \text{ v } \mathbb{Z}_{47}^*$$

kompletnace nýpledku

$$9^{21} \cdot 8^{10} = 1 \quad x = -21 \cdot 10^{-1} = -21 \cdot 7 = -148 = 14 \text{ v } \mathbb{Z}_{23}$$

$$9^{21} \cdot (9x)^{10} = 9^0$$

$$21 + 10x = 0$$

$$9^{14} = 8 \text{ v } \mathbb{Z}_{47}^*$$

$$x = -21 \cdot 10^{-1}$$

Příklad: V grupě \mathbb{Z}_{509}^* , 509 je prvočíslo, máme podgrupu $G = \langle 16 \rangle$ řádu $q = 127$.

ypočítejte dlog₁₆(54) v \mathbb{Z}_{509}^* , $y = 8$.

$$|\mathbb{Z}_{509}^*| = 508 = 4 \cdot 127 \rightarrow \mathbb{Z}_{509}^* \cong G \times H, \text{ kde } |H| = 4$$

$$P = \{2, 3, 5, 7\}, k = 4.$$

Jak majdu H? Termín cokoliv a množinu ho má q: $\{H = \{\pm 1, \pm 301\}\}$
Krába 3: $3 \xrightarrow{127} 301$ v \mathbb{Z}_{509}^*

1. fáze:

$$a^s \cdot b^t \cdot h = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot 7^{e_4}$$

$$i=1: 16^3 \cdot 54^5 \cdot 208 = 227 \quad \times$$

$$16^2 \cdot 54^4 \cdot 301 = 18 = 2 \cdot 3^2$$

$$i=2: 16^5 \cdot 54^7 \cdot (-1) = 4 = 2^2$$

$$i=3: 16^5 \cdot 54^17 \cdot 208 = 348 = 2^2 \cdot 3 \cdot 29 \quad \times$$

$$16^8 \cdot 54^2 \cdot 103 = 256 \quad \times \text{ když jde o chybku, 103} \notin H!$$

$$16^{22} \cdot 54^{66} \cdot 301 = 432 = 2^4 \cdot 3^3$$

$$i=4: 16^{23} \cdot 54^9 \cdot 1 = 504 = 2^3 \cdot 3^2 \cdot 7$$

$$i=5: 16^{70} \cdot 54^4 \cdot 301 = 12 = 2^2 \cdot 3$$

$$v_1 = (1, 2, 0, 0)$$

$$v_2 = (2, 0, 0, 0)$$

$$v_3 = (4, 3, 0, 0)$$

$$v_4 = (2, 2, 0, 1)$$

$$v_5 = (2, 1, 0, 0)$$

$$\sim \mathbb{Z}_{127}$$

2. fáze:

Jsme v \mathbb{Z}_{127} , pomocí
služebnice C:

$$\begin{array}{ccccc|c} c_1 & c_2 & c_3 & c_4 & c_5 & 0 \\ \hline 1 & 2 & 4 & 2 & 2 & 0 \\ 2 & 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{array}$$

$$\bar{C} = (-64, 31, 0, 0, 1)$$

$$S = -64 \cdot 2 + 31 \cdot 15 + 1 \cdot 70 = 407 = 23$$

$$A = -64 \cdot 14 + 31 \cdot 7 + 1 \cdot 4 = -675 = 87$$

$$h = \prod h_i^{c_i} = 301^{-64} \cdot (-1)^{31} \cdot 301^1 = 208$$

$$\sim \mathbb{Z}_{509}$$

komplexe: $16^{26} \cdot 54^{87} \cdot 208 = 480 \cdot 351 \cdot 208 = 208$

$$16^{26} \cdot 54^{87} = 1$$
$$16^{26} \cdot (16^x)^{87} = 16^0$$
$$26 + 87x = 0$$
$$x = -26 \cdot 87^{-1} = -26 \cdot 73 = -1898 = 7 \quad \text{mod } 127$$
$$16^7 = 54 \quad \checkmark \quad \text{dlog}_{16}(54) = 7$$