

?ř: Najděte exp(\mathbb{Z}_{45}^*). Kolik prvků v \mathbb{Z}_{45}^* má $r(a) = \exp(\mathbb{Z}_{45}^*)^2$?

$$\mathbb{Z}_{45}^* = \mathbb{Z}_{3^2} \times \mathbb{Z}_5^*$$

$$\lambda(45) = \text{lcm}(\lambda(5), \lambda(9)) = \text{lcm}(r(g), r(a)) = \text{lcm}(4, 6) = 12 \Rightarrow \exp(\mathbb{Z}_{45}^*) = 12.$$

Najdene generátory $\mathbb{Z}_{3^2}^* = \langle 2 \rangle$ (2, 2) \leftrightarrow 2, nejvyšší rád má 2.
problém s nejvyšším rádem $\mathbb{Z}_5^* = \langle 2 \rangle$

$$\text{Počítáme rád loko prvků } r_{45}(2) = \text{lcm}(r_5(2), r_9(2)) = \text{lcm}(4, 6) = 12 \checkmark$$

Kolik prvků stejného rádu tu bude?

$$r(a^k) = \frac{r(a)}{\text{gcd}(r(a), k)} = r(a), \text{ chci } \text{gcd}(r(a), k) = 1, \text{ tj. } k \text{ nesoudělné s } r(a)$$

$$\begin{aligned} \mathbb{Z}_5^* &\text{ má 2 generátory } (\varphi(4) = 2) & \text{lcm}(4, 6) \Rightarrow 4 \text{ prvky. } \} \text{ celkem je tu 8 takových} \\ \mathbb{Z}_9^* &\text{ má taky 2 generátory } (\varphi(6) = 2) & \text{lcm}(4, 3) \Rightarrow 4 \text{ prvky} \end{aligned}$$

?ř: Řešte $x^{15} = 1$ v \mathbb{Z}_{518}^* , $518 = 2 \cdot 7 \cdot 37$, $\mathbb{Z}_{518}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_7^* \times \mathbb{Z}_{37}^* \cong \langle 2_{14}^* \rangle \times \mathbb{Z}_{37}^*$

$$\begin{aligned} \text{v } \mathbb{Z}_{14}^*: |\mathbb{Z}_{14}^*| = 6, \text{ rády: } 1, 2, 3, 6 & \quad \text{raději uvedeme cyklickou } \mathbb{Z}_{14}^*, \text{ ale máme jen dvojice} \\ \mathbb{Z}_{14}^* = \langle 3 \rangle, \text{ normici svedutými na } \text{gcd}(15, 6) = 3, \text{ tj. } x^3 = 1 & \\ P_3 = \langle 3^2 \rangle = \dots = \{1, 9, 11\} & \end{aligned}$$

$$\text{v } \mathbb{Z}_{37}^*: |\mathbb{Z}_{37}^*| = 36, \text{ rády } 1, 2, 3, 4, 6, 9, 12, 18, 36, \text{ tj. } 15\text{-ti prvkůvou podgrupu nemáme.}$$

Rovnice redukujeme: $\text{gcd}(15, 36) = 3$, $x^3 = 1$.

Najdene generátor, určíme 2?

$$2^6 = \dots = -10$$

$$2^{12} = (2^6)^2 = (-10)^2 = \dots = -21 \quad \left. \right\} \text{ano, } 2 \text{ je generátor, } \mathbb{Z}_{37}^* = \langle 2 \rangle$$

$$2^8 = \dots = -1$$

$$\text{Určíme 3-prvkovou podgrupu: } \frac{36}{3} = 12, P_3 = \langle 2^{12} \rangle = \langle -11 \rangle = \{1, 10, 26\}$$

$$\text{Řešení v } \mathbb{Z}_{518}^*: \text{ Máme } 3 \times 3 = 9 \text{ řešení, určíme dané } q_{14} = 37 \lambda = -111 \\ q_{37} = 14 \mu = 112 \quad \left. \right\} 37\lambda + 14\mu = 1$$

$$x \in \{1, 9, 11\} \cdot q_{14} + \{1, 10, 26\} \cdot q_{37}$$

Bzn: Pokud je $|G|=n$ dělitelné malými prvočísly, pak se dlog dá
spotřebit rádově rychleji (exponenciálně s menším exponentem - Polling Hellman)

Přednáška
10.4.2019

\rightarrow proto se volí prvočíselná velikost grupy

Takto: $G = \langle a \rangle$ je cyklická grupa rádu n . Pro $b \in G$ počítáme dlog (b) , tj. $x \in \mathbb{Z}_n$, takové, že $b = a^x$. Následující algoritmus funguje ve všech cyklických grupách, pro časovou složitost určujeme počet potřebujících násobení.

Brute Force: Počítáme a^i pro $i = \{1, 2, \dots, n\}$ tak, že postupně násobíme prvekem a , dokud nevyjde b . provedeme nejvýše n násobení, složitost je $O(n) = O(2^{\text{len}(n)})$ násobení.

Baby step - giant step alg: Zvolíme approximaci $m = \lceil \sqrt{n} \rceil$, pak lze $m' = \lceil \frac{n}{m} \rceil = \lceil \sqrt{n} \rceil$ získat $x = \text{dlog}_a(b) = vm + u$, pak $0 \leq u < m$, $0 \leq v < m'$, protože $0 \leq x < n$. Jde o dané příslušná u, v :

$$b = a^x = a^{vm+u}, \text{ a loko } b \cdot (a^{-m})^v = a^{vm+u} \cdot a^{-vm} = a^u$$

1) Baby steps: spočítame a^i pro všechna $0 \leq i < m$, výsledky si uložíme ideálně do bin. vyhledávacího stromu

2) Giant steps: Počítáme $b \cdot (a^{n-m})^j$ pro $0 \leq j < m'$; a kontrolyjeme, jestli vši takovy výsledek nevyjel v baby steps.

Tam, kde výšly stejně výsledky, je $i = u$ a $j = v$, dostaneme ledy:

$$\text{dlog}_a(b) = x = v \cdot m + u = jm + i$$

Casová náročnost baby step giant step je: prováděme $2 \cdot \lceil \sqrt{n} \rceil$ násobení a $\lceil \sqrt{n} \rceil$ vyhledávání ve stromě, to ale potřebuje $O(\text{len}(n))$, což je méně než obyčejné násobení. Celkem probíháme $O(\lceil \sqrt{n} \rceil) = O(2^{\frac{1}{2}\text{len}(n)})$, což je porád exponenciální, ale dvakrát méně exponenciální.

Kontrolí je, že jsme přidali exponenciální paměť, potřebujeme ji $O(2^{\frac{1}{2}\text{len}(n)})$.

Príklad: $G = \mathbb{Z}_{37}^* = \langle 2 \rangle$ spočítejte $\text{dlog}_2(7)$ algoritmem baby step - giant step.

$$n = \varphi(37) = 36, \text{ dlog}_2(7) = x$$

$$\begin{aligned} m &= \sqrt{36} = 6 & m' &= \frac{36}{m} = \frac{36}{6} = 6 \\ 7 &= 2^x = 2^{vm+u} & m' &= 2^{6v+u} \quad \rightsquigarrow 7 \cdot 2^{6v} = 2^{6v+u} \cdot 2^{-6v} = 2^u \\ &= 2^{6v+u} & & \text{tj. } 7 \cdot (2^6)^v, \text{ kde } 2^6 = 64 = 27, \text{ a } 27^{-1} = 11 \text{ v } \mathbb{Z}_{37}^* \end{aligned}$$

Chci, aby obě strany rovnice byly shodné, tj. aby platilo $\underbrace{7 \cdot 11^v}_{\text{giant}} = \underbrace{2^u}_{\text{baby}}$.

u, v	0	1	2	3	4	5	6
baby: 2^u	1	2	4	8	16	32	64
giant: $7 \cdot 11^v$	7	3	-4	30	31	4	

Náslijdejme shodu, obě strany rovnice se rovnají pro $u=2, v=5$, kde $x = vm + u = 5 \cdot 6 + 2 = \underline{\underline{32}}$.

Je stejnou časovou náročností, ale očekávanou, pracuje Pollardova p -metoda. Její výhoda je, že má polynomiální časovou náročnost.

Pollardova - Hellmanův algoritmus: Nechť G je cyklická grupa řádu n s generátorem a , nechť $b \in G$. Známe-li faktorizaci čísla n , pak lze vypočítat $\text{dlog}_a b$ využitím:

1) $|G| = n = \prod_{i=1}^k p_i^{e_i}$, pak lze počítat diskrétní logaritmy v podgrupách řádu $p_i^{e_i}$ a použít činžkovu větu.

2) $|G| = p^e$, vypočít lze pomocí rekursivního výpočtu z logaritmu v podgrupě řádu p . Počet času je $O(e \cdot p^{\frac{1}{2}} + e \cdot \text{len}(q))$ násobení.

Je-li $a^x = b \in G$, pak $x = x_{e-1} \cdot p^{e-1} + \dots + x_1 p^1 + x_0 < p^e$. Lístice $0 \leq x_i < p$. Budeme počítat posupně od x_0 jako logaritmu v podgrupě $H = \langle a^{(p^{e-1})} \rangle$ řádu p . Umožníme rovnici $a^x = b$ na p^{e-1} , protože $x(a) = p^e$, dostaneme $(a^{(p^{e-1})})^{x_0} = b(p^{e-1})$ a spočteme x_0 . Pak umocníme rovnici na p^{e-2} a dopočteme x_1 , atd až máme p -ám rovnou pro x .

3) $|G| = p$, použijeme baby step - giant step algoritmus.

Príklad: $G = \mathbb{Z}_{37}^* = \langle 2 \rangle$ spočítejte $\text{dlog}_2(7)$ algoritmem Pollard - Hellman.

$$|\mathbb{Z}_{37}^*| = 36 = 4 \cdot 9 = 2^2 \cdot 3^2 \rightarrow \text{problem rýšíme v 4 a 9 pruhové podgrupě}$$

V podgrupě velikosti 9:

$$2^x = 7 \text{ umocním na 4 } (x(2^4) = 9)$$

$$2^{4x} = 7^4$$

$16^x = 33 \leftarrow$ tohle budeme řešit v podgrupě $H = \langle 16 \rangle$ velikosti $|H| = 9$, chci majíš $x' = x \bmod 9$ a to udělám přes baby step - giant step

$$\begin{aligned} m &= \sqrt{9} = 3, m' &= \frac{9}{3} = 3, x' &= 3v + u \\ 33 &= 16^{x'} = 16^{3v+u} & 16^u &= (16^{-3})^v \cdot 33 \\ 16^{-3} &= (16^3)^{-1} = (-11)^{-1} = 10 \\ x' &= 3v + u = 3 + 2 = \underline{\underline{5}} \end{aligned}$$

i	0	1	2	3
Baby	1	16	-3	26
giant	33	-3		

$u = 2$
 $v = 1$

V podgrupě velikosti 4 to rýšíme obdobně, najde $x'' = 0$

Výsledek najdu pomocí CRT:

$$\begin{cases} x \equiv 5 \pmod{9} \\ x \equiv 0 \pmod{4} \end{cases} \quad \left. \begin{array}{l} x = 5 \cdot q_9 + 0 \cdot q_4 = 5q_9 \\ x = 0 \cdot q_9 + 4 \cdot q_4 = 4q_4 \end{array} \right\}$$

$$\begin{aligned} q_9 &= 4 \cdot 1 = 1 \pmod{9} \\ \Rightarrow 1 &= 7 \end{aligned}$$

$$q_4 = 7 \cdot 4 = 28$$

$$x = 5 \cdot q_9 = 5 \cdot 28 = 140 = \underline{\underline{32}}$$

$\exists x'' = \text{dlog}_{16}(33)$ můžeme spočítat i rekurencí, nebo $H = \langle 2^n \rangle$ řádu $q = 3^2$

$$x = x_1 \cdot 3 + x_0, \quad x < q: \quad 0 \leq x_0, x_1 \leq 2$$

$$16^{3x_1 + x_0} = 33 \quad / \cdot 13$$

$$1 \cdot (16^3)^{x_0} = 33^3, \quad \text{kde } 16^3 = -11 \\ (-11)^{x_0} = 10$$

Máme podgrupu velikosti 3, a máme řešit $(-11)^{x_0} = 10$, hrubou silou najdeme $x_0 = 2$

$$\left. \begin{array}{l} 16^{3x_1 + 2} = 33 \quad / : 16^2 \\ 16^{3x_1} = 33 \cdot 16^{-2} \\ 16^{3x_1} = -11 \\ (-11)^{x_1} = -11 \end{array} \right\} \begin{array}{l} \text{omímenum počítat,} \\ \text{máme } x_1 = 1 \end{array} \rightarrow \begin{array}{l} x_1 = 1, x_0 = 2 \\ x = 3x_1 + x_0 = 3+2 = \underline{\underline{5}} \end{array}$$

Jak rychle najít podgrupu prvočíselného řádu q , kde $q/p-1$ je grupa \mathbb{Z}_p^* , když je prvočíslo.

\mathbb{Z}_p^* je cyklická, tj. má právě jednu podgrupu řádu q , $\mathbb{Z}_p^* = \langle a \rangle$, $P_q = \langle a^{\frac{p-1}{q}} \rangle$. Hledaný generátor je pomalejší, mychleji najdeme prvek c řádu q , pak $P_q = \langle c \rangle$.

do:

vyber náhodně $b \in \mathbb{Z}_p^*$

$$c = b^{\frac{p-1}{q}}$$

while $c=1$:

$$(b^{\frac{p-1}{q}})^q = b^{p-1} = 1, \quad \text{to platí z Euler-Geromata.}$$



$$(c)^q = 1$$

Algoritmem hledám $c = b^{\frac{p-1}{q}}$ tak dletoho, než najdu nějaké, které ještě nemá 1,

return c

je jednička se s něj slane až množením.

Když $c^q = 1$, tak řídí c něm dělit q , tj. $c(q) / q$. Ale q je prvočíslo, proto:

1) $c(q) = 1$, pak ale musí $c=1$, a to máme už využito.

2) $c(q) = q$, tedy c je prvek řádu q .

Eliptické křivky: Eliptická křivka nad tělesem \mathbb{R} je množina všech

bodů (x, y) na rovině \mathbb{R}^2 splňujících rovnici $y^2 = x^3 + ax + b$.

A kubický polynom $x^3 + ax + b$ má pouze jednoduché kořeny v \mathbb{C} , což nazoveme, panež když discriminant $D = 4a^3 + 27b^2 \neq 0$.

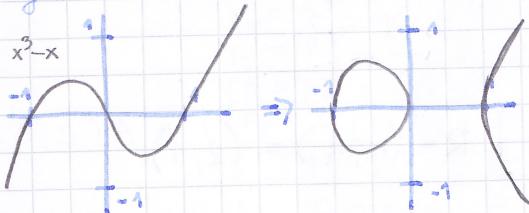
Přednáška
11.4.2019

↳ to nám zaručí, že křivka nemá osoby slom

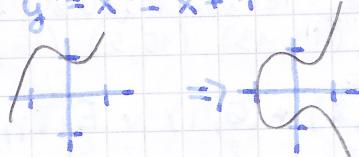
$$1) y^2 = x^3 - x = x(x^2 - 1) =$$

$$= x(x-1)(x+1)$$

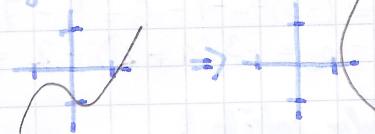
$$y = \pm \sqrt{x^3 - x}$$



$$2) y^2 = x^3 - x + 1$$



$$3) y^2 = x^3 - x - 1$$

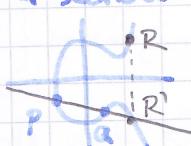


Máme množinu bodů $E = \{(x, y) \in \mathbb{R}^2, y^2 = x^3 + ax + b\}$, chci definovat operaci $+$.

P, Q jsou body na křivce. Pokud $P \neq Q$, tak proložme body přímkou. Přesněji je přímka leží na křivce v bodě Q , pak užledek je $-Q$. Jinak najdeme bod R' jehož prvek je přímka a křivka. Pak je užledek $R = -R'$. $P + (-P) = 0$, bod je nekonečný.

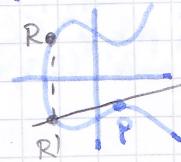
přeseky vrátí se v obou směrech, protože na křivce je inflexní bod.

$$P + P$$



$P + Q$ těžov

Tahle výkladní a toho, že když jichom se blíží, zleva (leva) ke Q , užledek bude blízko k R .



Vidíme těžnou v bodě P , najdeme přesek, užledek mezi užledek.

Tvrzení: Okružnice $E(\mathbb{R})$ množinou všech bodů eliptické křivky a bodu O. Pak $(E(\mathbb{R}), +)$ mává
Abelovu grupu, grupa se nazývá grupa bodů na eliptické křivce.
- kombinací sítu je i jiná, protože přímka PQ je stejná jako QP, asociativita se dělá hůř.

Vzorce pro aritmetický výpočet součtu $P = (p_1, p_2), Q = (q_1, q_2), R = (r_1, r_2)$

1) $P \neq \pm Q$

Přímka procházející body P, Q má rovnici $y = \lambda x + k$, kde $\lambda = \frac{q_2 - p_2}{q_1 - p_1}$, a $k = p_2 - \lambda \cdot p_1$.

$x = \frac{y - k}{\lambda}$ sčítadoucí průsečku přímky a křivky dostaneme dosazením do křivky:

$$0 = x^3 - (\lambda x + k)^2 + ax + b \approx \text{chci najít } 3\text{-li kořem, } p_1 \text{ a } q_1 \text{ jsou kořeny}$$

$$\lambda^2 = -(p_1 + q_1 + r_1) \text{ a z toho } r_1 = \lambda^2 - p_1 - q_1$$

$$\text{Výřadnice } r_2 \text{ dostaneme jako } r_2 = \lambda(p_1 - r_1) - p_2$$

pokud byla přímka sítou, výjde nám $R = -P$

2) $P = Q$, ale $p_2 \neq 0$

Yměřnicí řícty dostaneme jako derivaci, $y'(x) = \frac{3x^2 + a}{2y}$ v bodě P, třeba ji ve křivce $y = \lambda x + k$, kde $\lambda = (3p_1 + a)/2p_2$, $k = p_2 - \lambda p_1$. Výřadnice R dostaneme dosazením.

$$r_1 = \lambda^2 - 2p_1, r_2 = \lambda(p_1 - r_1) - p_2.$$

$$F(x, y) = -y^2 + x^3 + ax + b = 0 \text{ je implikativní fce, pokud nevíme } p_1 \frac{\partial F}{\partial y} = 0 \Rightarrow \text{nemá } p_2 = 0.$$

$$\text{Zdělejme podle } x: -2y(x) \cdot y'(x) + 3x^2 + a = 0 \\ y'(x) = (3x^2 + a)/-2y$$

Pro výpočet je potřeba sítání/odčítání a násobení/dělení, což máme o libovolném tělesu.
Kořítko konečné těleso je isomorfní s Galoisovým tělesem a má p^k prvků, p je prvočíslo.
G. těleso nazíváme $G(\mathbb{F}(p^k))$, p je jeho "charakteristikou". V prací se používá $G(\mathbb{F}(2^k))$ mbo \mathbb{Z}_p .

Definice: Eliptická křivka nad tělesem \mathbb{Z}_p , $p > 3$ je prvočíslo, je množina všech bodů
 $(x, y) \in \mathbb{Z}_p^2$ splňujících rovnici $y^2 = x^3 + ax + b$, kde $a, b \in \mathbb{Z}_p$ a $D = 4a^3 + 27b^2 \neq 0 \in \mathbb{Z}_p$
Okružnice $E(\mathbb{Z}_p)$ množinu všech tělesových bodů spojuje s jedním bodem O. Taky to je Abelova grupa

$13^{1/2}$, Eulerovo kvadrátum

Př: Máme $E(\mathbb{Z}_{17})$ s rovnicí $y^2 = x^3 + 7x + 13$. Jaké prvky mají na této křivce?

$$x=0 \quad y^2 = 0 + 0 \cdot 7 + 13 = 13. \text{ Platí } 13^{\frac{p-1}{2}} = 13^8 = 1 \in \mathbb{Z}_{17}, \text{ takže } 13 \text{ je čtverec. Hubou}$$

můžeme najít $y = \pm 8$, máme body: $(0, 8), (0, 9)$

$$x=1 \quad y^2 = 1 + 7 + 13 = 21 = 4. \text{ Zjistíme } y = \pm 2, \text{ máme body } (1, 2), (1, 15)$$

$$x=2 \quad y^2 = 8 + 14 + 13 = 35 = 1. \text{ Zjistíme } y = \pm 1, \text{ máme body } (2, 1), (2, 16)$$

$$x=3 \quad y^2 = 27 + 21 + 13 = 10 + 4 + 13 = 10. \text{ Platí } 10^{\frac{p-1}{2}} = 10^8 = 100^4 = (-2)^4 = 16 = -1,$$

což nazýváme odmocnit, takže $x=3$ nepřidele žádné body.

Dostali bychom body: $E(\mathbb{Z}_{17}) = \{(0, 8), (0, 9), (1, 2), (1, 15), (2, 1), (2, 16), (6, 4), (6, 13), (14, 4), (14, 13), (15, 5), (15, 12), 0\}$, má 13 prvků.

Př: Vypočítejte $(1, 2) + (6, 4) \in E(\mathbb{Z}_{17})$

$$\lambda = \frac{q_2 - p_2}{q_1 - p_1} = \frac{4 - 2}{6 - 1} = \frac{2}{5} = 2 \cdot 5^{-1} = 2 \cdot 7 = 14 = -3$$

$$r_1 = \frac{\lambda^2 - p_1 - q_1}{\lambda} = (-3)^2 - 1 - 6 = 9 - 7 = 2 \quad \left. \begin{array}{l} \\ \end{array} \right\} R = (r_1, r_2) = (2, 1)$$

Kolik operací bylo potřeba?

sčítání: $2 + 2 + 2 = 6$ krát

násobení: $1 + 1 + 1 = 3$ krát

inverze: 1 krát

nebo $4x$, když $p = 2$

$\sim O(\text{len}(p))$

$\sim O(\text{len}(p)^2)$

$\sim O(\text{len}(p)^2)$

$\left. \begin{array}{l} \\ \end{array} \right\} O(\text{len}(p)^2)$

Hasseho věta: Pro kardinál EC nad \mathbb{Z}_p platí $p+1-2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p+1+2\sqrt{p}$

$E(\mathbb{Z}_p) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, kde $n_2 / \text{gcd}(n_1, p-1)$

- když $n_2 = 1$, pak je $E(\mathbb{Z}_p)$ cyklická

- když je n_2 malá ($2, 3, 4, \dots$), tak je "dělitelná cyklická".

Jakožto těleso: Když korené těleso je izomorfní s Galoisovým tělesem a má p^k prvků, kde p je prvočíslo. Znací se $GF(p^k)$, p je charakteristikou tělesa.

Kaschho něta platí i pro elliptické křivky nad $GF(p^k)$, když v odhadu nahradíme p za p^k .

Obecný tvárovnice pro elliptickou křivku nad tělesem: $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$
 - pokud charakteristika tělesa není dve, jde rovnici upravit: $y^2 = x^3 + ax^2 + bx + c$
 - 2 am 3, 11 : $y^2 = x^3 + ax + b$
 - pro tělesa $GF(2^k)$ lze rovnici upravit: $y^2 + xy = x^3 + ax^2 + b$ nebo $y^2 + cy = x^3 + ax + b$
 - když kde má řadu diskriminant a řadu kořec na sčítání.

DIFIE-Hellmanova séména blíže na elliptických křivkách

- Alice volí skupinu bodů na elliptické křivce $E(\mathbb{Z}_p)$ a námi bude A velkého rádu n.
- Dále volí $x \in \mathbb{Z}_p$, a spočítá prvek $B = x \cdot A$ v $E(\mathbb{Z}_p)$.
- Alice posílá Bobovi prvek B a informace o grupě: $(E(\mathbb{Z}_p), n, A)$.
- Bob volí $y \in \mathbb{Z}_p$ a spočítá prvek $C = y \cdot A \in E(\mathbb{Z}_p)$
- Bob posílá Alice prvek C.
- Alice si spočítá $S_A = x \cdot C$, Bob si spočítá $S_B = y \cdot B \in E(\mathbb{Z}_p)$. Tím oba náškali stejný blíž: $S = S_A = S_B = x \cdot y \cdot A$.

Analogicky můžeme podlepravu G = $\langle A \rangle$ grupy $E(\mathbb{Z}_p)$ upravit pro El Gamala.

Př: Prověděte DH séména nad EC. Alice volí křivku $y^2 = x^3 + 7x + 13$, podgrupu $E(\mathbb{Z}_{17})$, $G = \langle A \rangle$, $A = (1, 2)$, $r(A) = 13$. Alice volí $x = 5$, Bob volí $y = 2$. $p = 17 \uparrow$
 Alice: $B = x \cdot A = 5 \cdot A$, kde 5 rozjděme binárně jako (1, 0, 1). Vektor upravíme tak, že místo 1 dáme "A" a do meren meru čísla dáme "D". Abych ADDA. Pojďme operace podobně jako u algoritmu opakovacích čtverců. Začneme v punktu O:
 - A: odd, k následku přidáme generátor (zde (1, 2)).
 - D: double, násobíme následkem dvěma

$$\begin{aligned} O(A) &= O + (1, 2) = (1, 2) \\ (1, 2)D &=? \quad \lambda = (3 \cdot p_1^2 + a)/2p_2 = (3 + a)/4 = 10/4 = 10 \cdot 4^{-1} = 10 \cdot (-4) = -40 = 11 \\ r_1 &= \lambda^2 - 2p_1 = 36 - 2 = 34 = 0 \\ r_2 &= \lambda(p_1 - r_1) - p_2 = 11 \cdot (1 - 0) - 2 = 9 \quad \rightarrow (0, 9) \\ (1, 2)D &= (0, 9) \\ (0, 9)D &=? \quad \lambda = (3 \cdot p_1^2 + a)/2p_2 = (3 \cdot 0 + 7)/18 = 7/1 = 7 \\ r_1 &= \lambda^2 - 2p_1 = 49 - 2 \cdot 0 = 49 = 15 \\ r_2 &= \lambda(p_1 - r_1) - p_2 = 7(0 - 15) - 9 = 7 \cdot 2 - 9 = 14 - 9 = 5 \quad \rightarrow (0, 5) \\ (0, 5)D &= (15, 5) \\ (15, 5)A &= (1, 2) + (15, 5) \\ \lambda &= \frac{q_2 - p_2}{q_1 - p_1} = \frac{5 - 2}{15 - 1} = \frac{3}{14} = 3 \cdot 14^{-1} = 3 \cdot 11 = 33 = 16 \\ r_1 &= \lambda^2 - p_1 - q_1 = 1 - 1 - 15 = 2 \\ r_2 &= \lambda(p_1 - r_1) - p_2 = 16(1 - 2) - 2 = -16 - 2 = -18 = 16 \\ (15, 5)A &= (2, 16) \end{aligned}$$

Alice posílá Bobovi $B = (2, 16)$

Bob: Obdobně si spočítal $C = y \cdot A = 2 \cdot (1, 2) = (0, 9)$, to posílá Alice.

$$\begin{aligned} \text{Alice } \} &\text{ spočítají si následující křivku} \quad S_A = x \cdot C = 5 \cdot (0, 9) \\ \text{Bob } \} &\text{ spočítají si následující křivku} \quad S_B = y \cdot B = 2 \cdot (2, 16) = (14, 13). \end{aligned}$$

Výhoda proti RSA je, že křivky jsou daleko menší: $1024 \text{ b RSA} \approx 160 \text{ b EC}$.

Cvičení
11.4.2019

Příklad: Domluvě společný klíč pomocí DH domluvy, náhle grupu $n \geq 30$.
 Zvolili jsme grupu $\mathbb{Z}_{37}^* = \langle 2 \rangle$, $\varphi(37) = 36$. Obě strany si volily klíč 13.
 $C = 2^{13} \mod 37 = 15$, $S = C^{13} = 20$, tedy hajný klíč je 20.

Příklad: Protokol ElGamal používá $P = \langle 9 \rangle$ v grupě \mathbb{Z}_{107}^* . 107 je prvočíslo, $\varphi(107) = 106$.
 Vyhledejte rád grupy P a vyhledejte veřejný klíč. $106 = 2 \cdot 53$
 Jaký je rád prvek 9?
 $9^2 = 81 \neq 1$
 $9^{53} = (3^2)^{53} = 3^{106} = 1$ díky EF věci. Télikož P je 53.

Zvolíme $x = 7$, spočtěme $b = a^x = 9^7 = \dots = 69$

Zároveň uvedeme: $(\mathbb{Z}_{107}^*, \langle 9 \rangle, |\langle 9 \rangle| = 53, b = 69)$

Habíček se počítá
mimochodem
naobratně
a exponenci.

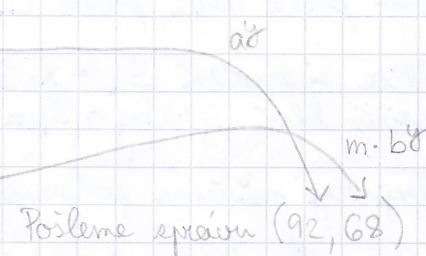
Příklad: Uživatel s ElGamalem klíčem $(107, 9, 53, 69)$ chce poslat správu $m = 21$.

Zvolíme jepíčí klíč $y = 5$.

$$c = 9^5 = \dots = 92$$

$$s = 69^5 = \dots = 44 \quad \leftarrow \text{pomocí tohoto se správa šifruje}$$

$$\bar{m} = s \cdot m = 44 \cdot 21 = 924 = 68$$



Příklad: Dešifrujte správu $(92, 68)$.

Upočítáme s : $s = (a^x)^{-1} = 92^{-1} = \dots = 44$

$$\text{Najdeme } s^{-1} = 44^{-1} = 1 \cdot 44^{-1} = \underbrace{92^{53}}_{=1} \cdot \underbrace{(92^7)^{-1}}_{=44} = 92^{53-7} = 92^{46} = \dots = 90$$

$$\text{Dešifrujeme: } m = \bar{m} \cdot s^{-1} = 68 \cdot 90 = \dots = 21$$

Příklad: Veřejný ElGamal klíč Boba je $(107, 9, 53, 10)$. Eva nacítila správu pro Boba $(c, \bar{m}) = (35, 18)$. Algoritmem Baby step-giant step najděte Bobinu hajný klíč $x = \text{dlog}_9(10)$ a dešifrujte správu.

Chceme najít $9^x = 10$ v grupě Příčku 53. $9^{-7v} = ((9^7)^{-1})^v = \dots = ((69)^{-1})^v = \dots = 76^v$

$$\lfloor \frac{9}{53} \rfloor = 7 \Rightarrow 9^{7v+u} = 10, 0 \leq u, v \leq 7$$

$$\underbrace{10 \cdot 9^{-7v}}_{\text{giant}} = \underbrace{9^u}_{\text{baby}} \quad \text{správne } 9^{-7v} = 76^v$$

i	0	1	2	3	4	5	6	7
9^i	1	9	81	87	34	92	79	69
$10 \cdot 76^i$	10	11	87	87	34	92	79	69
					$m=3$	$v=2$		

$$x = 7v + u = 7 \cdot 2 + 3 = 17, \text{ ano, 10 sedí, } 9^{17} = 10 \text{ v } \mathbb{Z}_{107}$$

Dešifrujeme správu $s = c^x = 35^{17} = \dots = 56$ ← habíček vlastně nemusí počítat, ably když máme v množině menší potřeba

$$s^{-1} = 56^{-1} = 1 \cdot 56^{-1} = 35^{106} \cdot (35^{17})^{-1} = 35^{106-17} = 35^{89} = \dots = 86$$

$$m = \bar{m} \cdot s^{-1} = 18 \cdot 86 = 1548 = 50$$

$$\varphi(47) = 46 = 2 \cdot 23 \\ |P| = 23$$

Příklad: Algoritmem baby step-giant step najděte $\text{dlog}_4(18)$ v P = $\langle 4 \rangle$ v \mathbb{Z}_{47} .

$$4^x = 18 \quad \lfloor \frac{18}{47} \rfloor = 5, \quad x = 5v + u$$

$$4^{5v+u} = 18 : 4^5v$$

$$\underbrace{4^u}_{\text{baby}} \quad \underbrace{4^{5v}}_{\text{giant}}$$

$$(4^{-5}) = (4^5)^{-1} = 37^{-1} = 14$$

i	0	1	2	3	4	5
4^i	1	4	16	17	21	37
$18 \cdot 4^v$	18	17				

$$u = 3, v = 1 \Rightarrow x = 5v + u = 5 + 3 = 8$$

$$4^8 = 65536 = 18 \text{ v } \mathbb{Z}_{47} \quad \checkmark$$