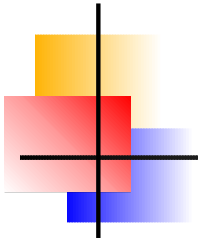
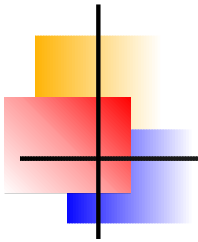


Eliptické krivky v kryptografii

Stanislav Palúch

Fakulta riadenia a informatiky, Žilinská univrzita, Department of Mathematical Methods

28. novembra 2019



Kvadratická a kubická rovnica

$$ax^2 + bx + c = 0 \tag{1}$$

Diskriminant

$$D = b^2 - 4ac \tag{2}$$

Ak $D < 0$, potom rovnica (1) nemá reálne riešenie

Ak $D = 0$, potom rovnica (1) má jedno reálne riešenie $x = \frac{-b}{2a}$

Ak $D = 0$, potom rovnica (1) má dve reálne riešenia

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{3}$$

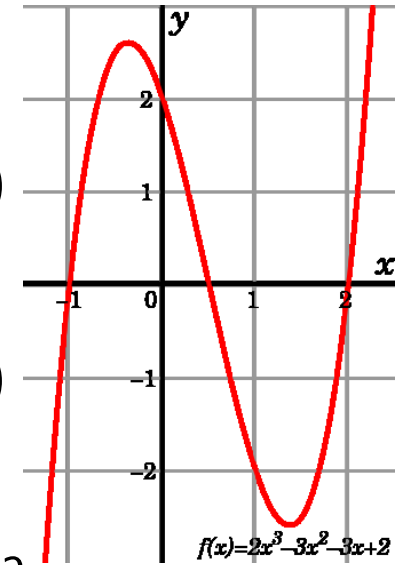
Kubická rovnica

Kubická rovnica:

$$\alpha y^3 + \beta y^2 + \gamma y + \delta = 0 \qquad (4)$$

Diskriminant

$$D = 18\alpha\beta\gamma\delta - 4\beta^3\delta + \beta^2\gamma^2 - 4\alpha\gamma^3 - 27\alpha^2\delta^2 \qquad (5)$$



Ak $D > 0$, potom rovnica (4) má tri rôzne reálne riešenia
Ak $D < 0$, potom rovnica (4) má jedno reálne riešenie
Ak $D = 0$, potom rovnica (4) má jedno trojnásobné reálne riešenie alebo jedno jednoduchá a jedno dvojnásobné reálne riešenie.

Zavedenímm novej premennej x s vlastnosťou $y = x - \frac{\beta}{3\alpha}$ t.j. dosadením za y do (4) dostaneme

kubicka rovnica

$$\alpha\left(x-\frac{\beta}{3\alpha}\right)^3+\beta\left(x-\frac{\beta}{3\alpha}\right)^2+\gamma\left(x-\frac{\beta}{3\alpha}\right)+\delta = 0$$

$$\alpha\left[x^3+3x\left(\frac{\beta}{3\alpha}\right)^2-3x^2\frac{\beta}{3\alpha}-\left(\frac{\beta}{3\alpha}\right)^3\right]+$$

$$+\beta\left[x^2-2x\frac{\beta}{3\alpha}+\left(\frac{\beta}{3\alpha}\right)^2\right]+\gamma\left(x-\frac{\beta}{3\alpha}\right)+\delta = 0$$

$$x^3\alpha+x\frac{\beta^2}{3\alpha}-x^2\beta-\frac{\beta^3}{27\alpha^2}+x^2\beta-2x\frac{\beta^2}{3\alpha}+\frac{\beta^3}{9\alpha^2}+x\gamma-\frac{\beta\gamma}{3\alpha}+\delta = 0$$

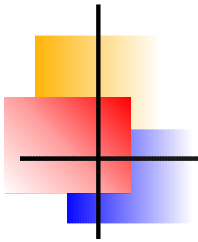
$$x^3\alpha+x\left(\gamma-\frac{\beta^2}{3\alpha}\right)-\frac{\beta^3}{27\alpha^2}+\frac{\beta^3}{9\alpha^2}-\frac{\beta\gamma}{3\alpha}+\delta = 0$$

$$x^3\alpha+x\left(\frac{3\alpha\gamma-\beta^2}{3\alpha}\right)+\frac{2\beta^3-9\alpha\beta\gamma+27\alpha^2\delta}{27\alpha^2} = 0$$

$$x^3+x\left(\frac{3\alpha\gamma-\beta^2}{3\alpha^2}\right)+\frac{2\beta^3-9\alpha\beta\gamma+27\alpha^2\delta}{27\alpha^3} = 0$$

$$x^3+ax+b=0,$$

kde $a=\dfrac{3\alpha\gamma-\beta^2}{3\alpha^2}$, $b=\dfrac{2\beta^3-9\alpha\beta\gamma+27\alpha^2\delta}{27\alpha^3}$



Kubická rovnica

Z pôvodnej rovnice

$$\alpha y^3 + \beta y^2 + \gamma y + \delta = 0$$

s diskriminantom

$$D = 18\alpha\beta\gamma\delta - 4\beta^3\delta + \beta^2\gamma^2 - 4\alpha\gamma^3 - 27\alpha^2\delta^2$$

máme rovnicu

$$x^3 + ax + b = 0, \tag{6}$$

ktorej diskriminant bude

$$D = 18.1.0.a.b - 4.0^3.b + 0^2.a^2 - 4.1.a^3 - 27.1^2.b^2 = -4a^3 - 27b^2 \tag{7}$$

Ak $4a^3 + 27b^2 = 0$ a $a = 0$, potom aj $b = 0$.
V tom prípade má rovnica (6) tvar $x^3 = 0$ a má trojnásobný koreň $x = 0$.
Ak $a \neq 0$, potom má rovnica (6)
jednoduchý koreň $x_1 = \frac{3b}{a}$ a dvojnásobný koreň $x_{2,3} = \frac{-3b}{2a}$, t.j.:

$$x^3 + ax + b = \left(x - \frac{3b}{a}\right).\left(x + \frac{3b}{2a}\right)^2 \tag{8}$$

Kubická rovnica

Z pôvodnej rovnice

$$\alpha y^3 + \beta y^2 + \gamma y + \delta = 0$$

substitúciou $y = x - \frac{\beta}{3\alpha}$ sme dostali rovnicu

$$x^3 + ax + b = 0$$

Ďalšou substitúciou

$$x = t - \frac{a}{3t} \tag{9}$$

$$\begin{aligned}
(t - \tfrac{a}{3t})^3 + a(t - \tfrac{a}{3t}) + b &= 0 \\
t^3 + 3t\left(\frac{a}{3t}\right)^2 - 3t^2\left(\frac{a}{3t}\right) - \left(\frac{a}{3t}\right)^3 + at - \frac{a^2}{3t} + b &= 0 \\
t^3 + \frac{a^2}{3t} - at - \frac{a^3}{27t^3} + at - \frac{a^2}{3t} + b &= 0 \\
t^3 - \frac{a^3}{27t^3} + b &= 0 \qquad * t^3 \\
t^6 + bt^3 - \frac{a^3}{27} &= 0
\end{aligned}$$

Kubická rovnica

Poslednú rovnicu možno prepísať v tvare

$$(t^3)^2 + b(t^3) - \frac{a^3}{27} = 0 \tag{10}$$

S koreňmi

$$(t^3)_{1,2} = \frac{-b \pm \sqrt{b^2 - 4a^3/27}}{2}$$

čo je tzv binomická rovnica pre neznámu t tvaru

$$t^3 = a \tag{11}$$

s riešeniami t_0, t_1, t_2

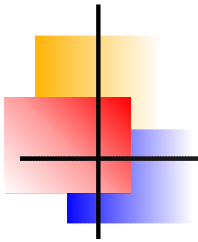
$$t_k = \sqrt[n]{|a|}\left[\cos\left(\frac{2k\pi}{3}\right) + i.\sin\left(\frac{2k\pi}{3}\right)\right] \tag{12}$$

K riešenie pôvodnej rovnice sa dostaneme substitúciami

$x = t - \frac{a}{3t}$ a $y = x - \frac{\beta}{3\alpha}$.

Inou metódou je pužitie tzv. Cardanových vzorcov.
Tieto v skutočnosti vynašiel Niccolo Fontana Targalia a pochválil sa Cardanovi s tým, že ich chce udržať v tajnosti. Cardano však vzorce publikoval síce aj s Targaliovým menom ako autorom, ale až do konca sveta sa budú volať Cardanove.

Podobne sa šifra, ktorú vynašiel Giovani Batista Belas volá Vigenerovská šifra.



Eliptická krivka v obore reálnych čísel

Eliptická krivka nad poľom reálnych čásel $\mathbb{R}$ je množina usporiadaných dvojíc reálnych čísel (x, y), t.j. prvkov z poľa $\mathbb{R}$, splňujúcich podmienku (13) spolu s nevlastným bodom $\mathcal{O}$).

$$y^2 = x^3 + ax + b, \tag{13}$$

kde koeficienty $a \in \mathbb{R}$, $b \in \mathbb{R}$ sú také prvky poľa $\mathbb{R}$, že

$$4a^3 + 27b^2 \neq 0. \tag{14}$$

$$\mathcal{E} = \{(x, y) \mid x, y \in \mathbb{R},\ y^2 = x^3 + ax + b,\ \text{kde } 4a^3 + 27b^2 \neq 0\} \cup \{\mathcal{O}\}$$

Množina bodov $\mathcal{E}$ je súmerná podľa osi x, pretože ak $y \in \mathcal{E}$ potom aj $y \in \mathcal{E}$.
Množina $\mathcal{E}$ je vlastne zjednotením grafov funkcie $y = f(x) = \sqrt{x^3 + ax + b}$ a funkcie $y = -f(x)$.

Eliptická krivka v obore reálnych čísel

Eliptická krivka je množina bodov

$$\mathcal{E} = \{(x, y) \mid x, y \in \mathbb{R},\ y^2 = x^3 + ax + b,\ \text{kde } 4a^3 + 27b^2 \neq 0\} \cup \{\mathcal{O}\}$$

kde

$$4a^3 + 27b^2 \neq 0.$$

Funkcia $y = f(x) = \sqrt{x^3 + ax + b}$ má tri nulové body, ak je diskriminant $D = -4a^3 - 27b^2$ kladný a jeden nulový bod, ak $D < 0$. Prípad $D = 0$ vylučujeme.

Derivácia funkcie $f(x)$ je

$$f'(x) = \left[(x^3 + ax + b)^{\frac{1}{2}}\right]' = \frac{1}{2}.\frac{3x^2 + a}{(x^3 + ax + b)^{\frac{1}{2}}} \qquad (15)$$

Ak je x_0 nulovým bodom funkcie $f(x)$, t.j. ak $f(x_0) = 0$, potom čitateľ zlomku v (15) je nenulový (lebo $D \neq 0$ a $x^3 + ax + b$ nemá násobný koreň) a limita menovateľa (15) pre $x \to x_0$ je 0.

Preto $\lim_{x \to x_0} f'(x) = \pm\infty$.

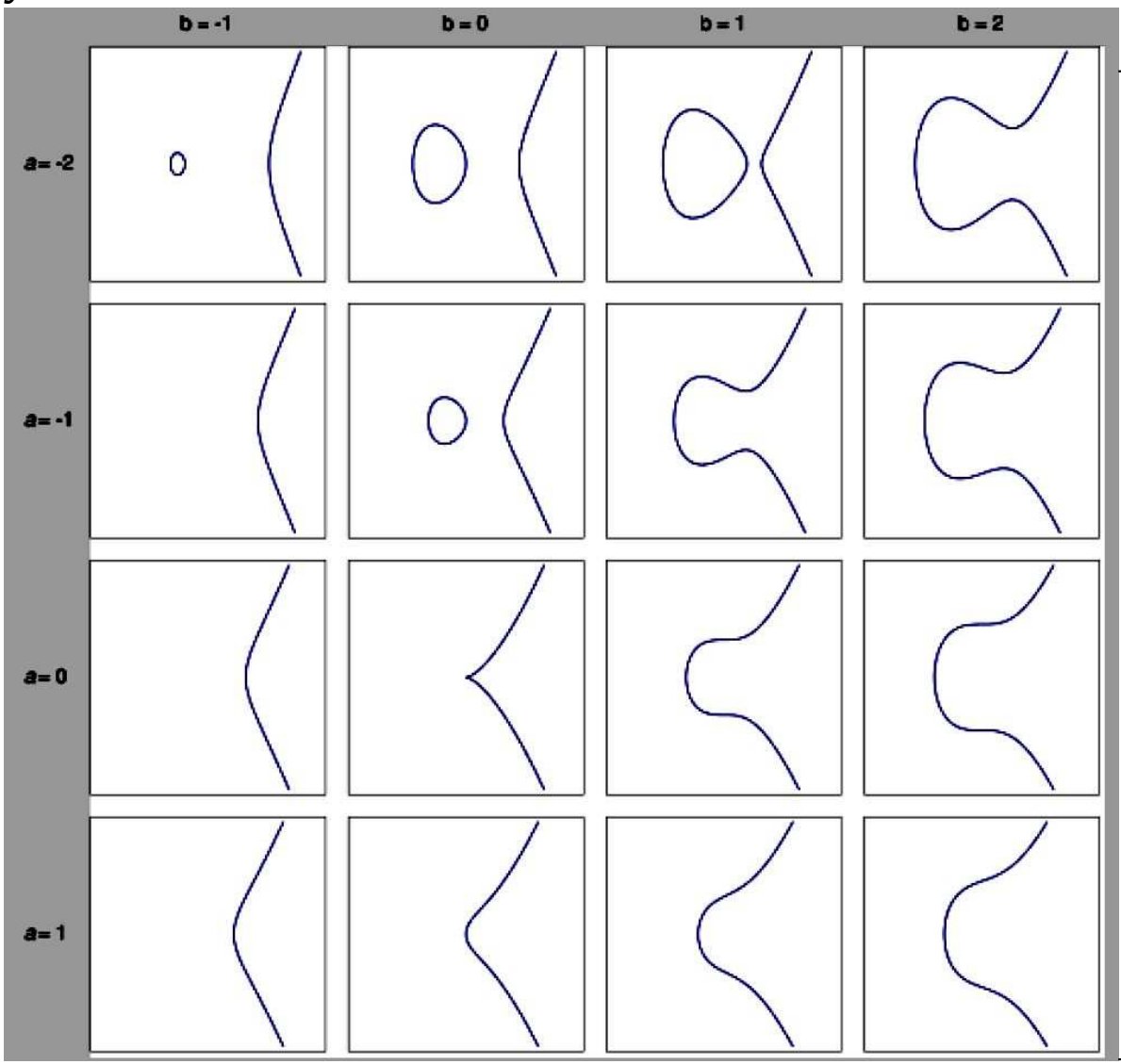
Množina $\mathcal{E}$ má teda jeden bod $(x, 0)$, ak je $4a^3 + 27b^2 < 0$ a tri body $(x_1, 0)$, $(x_2, 0)$, $(x_3, 0)$, ak je $4a^3 + 27b^2 > 0$.

Prípad $4a^3 + 27b^2 = 0$ vylučujeme.

V každom bode s nulovou ypsilonovou súradnicou má množina $\mathcal{E}$ dotyčnicu rovnobežnú s osou y.

Ukážky eliptických kriviek nad poľom reálnych čísel

$y^2 = x^3 + ax + b$

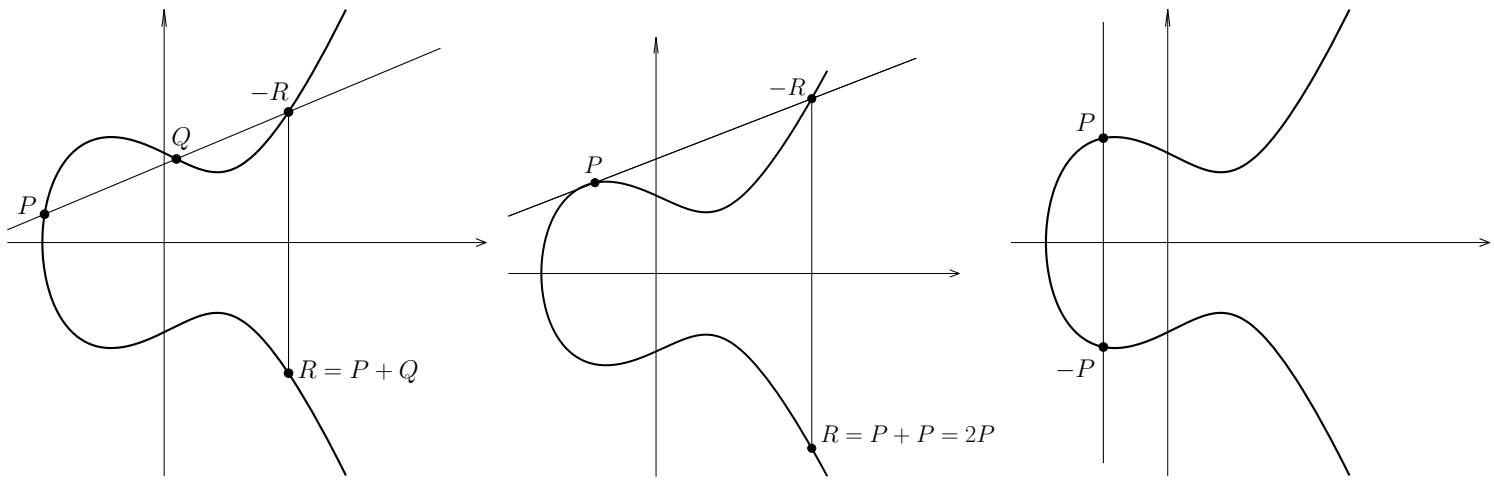


Diskriminant $D = -4a^3 - 27b^2$			
5	32	5	-76
-23	4	-23	-104
-27	0	-27	-108
-31	-4	-31	-112

Sčítanie bodov eliptickej krivky

Majme dva body eliptickej krivky $P = (x_P, y_P) \in \mathcal{E}$, $Q = (x_Q, y_Q) \in \mathcal{E}$. Na množine $\mathcal{E}$ možno definovať operáciu $R = (x_R, y_R) = P \boxplus Q$ takto:

1. Ak $x_P \neq x_Q$ a súčasne $y_P \neq y_Q$ Zostrojme v rovine s eliptickou krivkou $\mathcal{E}$ priamku určenú bodmi P a Q. Priesečník tejto priamky s krivkou $\mathcal{E}$ označme ako bod $-R$. Bod R krivky $\mathcal{E}$ ktorý je súmerný podľa osi x s bodom $-R$ prehlásime za súčet $P \boxplus Q$ bodov P a Q.



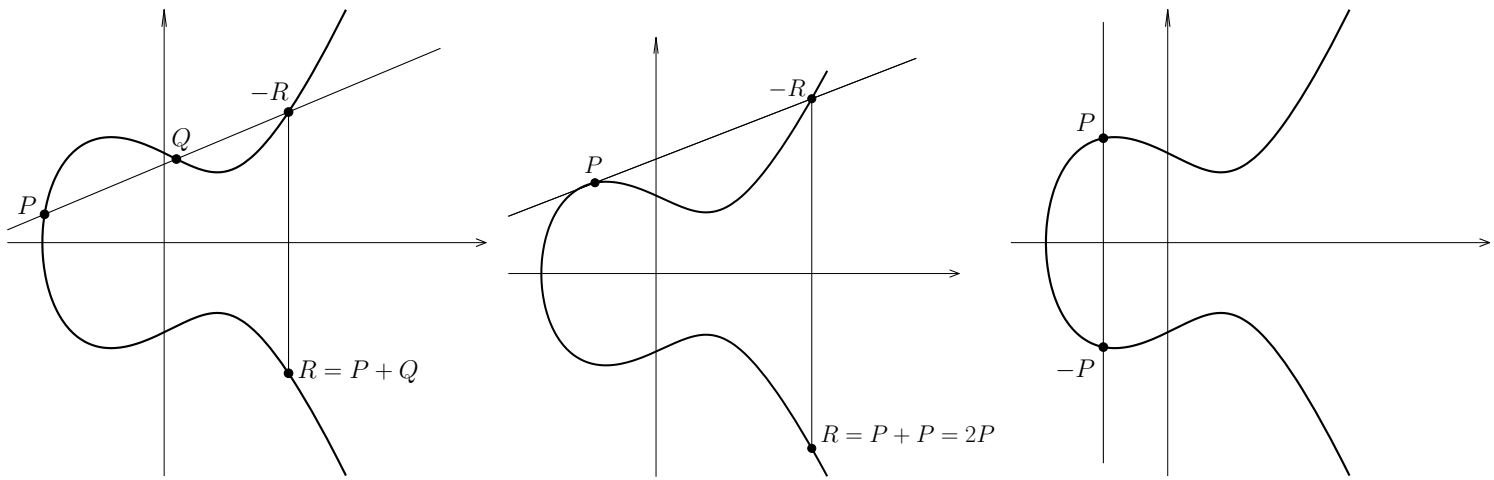
a) ak $x_p \neq x_q$ a $y_p \neq y_q$ b) ak $P = Q$ a $y_p \neq 0$ c) ak $x_p = x_q$

Obr.: Sčítanie bodov eliptickej krivky.

Sčítanie bodov eliptickej krivky

1. Ak $P = Q$ a $y_P = 0$, potom definujeme $P \boxplus P = \mathcal{O}$.

   Ak $y_P \neq 0$, vezmeme dotyčnicu ku krivke $\mathcal{E}$ v bode P, jej priesečník s krivkou $\mathcal{E}$ označme ako bod $-R$ a bod R krivky $\mathcal{E}$ ktorý je súmerný podľa osi x s bodom $-R$ prehlásime za súčet $P \boxplus Q$ bodov P a Q.

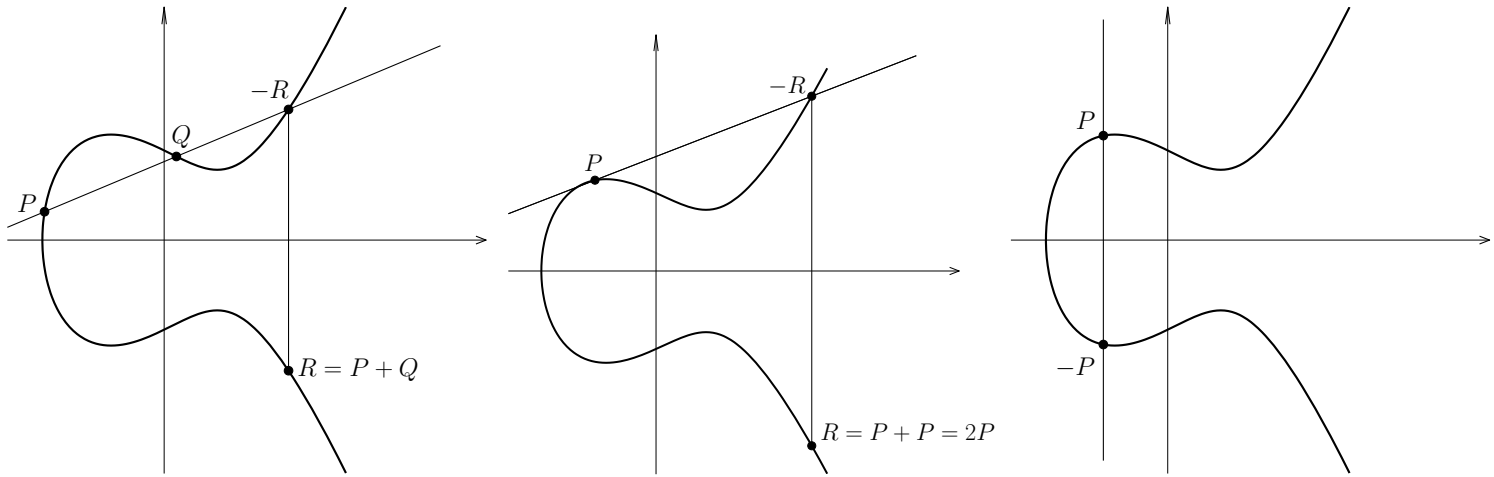


a) ak $x_p \neq x_q$ a $y_p \neq y_q$ b) ak $P = Q$ a $y_p \neq 0$ c) ak $x_p = x_q$

Obr.: Sčítanie bodov eliptickej krivky.

Sčítanie bodov eliptickej krivky

1. Ak $P \neq Q$ ale $x_P = x_Q$, potom $P \boxplus Q = \mathcal{O}$.



a) ak $x_p \neq x_q$ a $y_p \neq y_q$ b) ak $P = Q$ a $y_p \neq 0$ c) ak $x_p = x_q$

Obr.: Sčítanie bodov eliptickej krivky.

2. Ak P je ľubovoľné, potom $P \boxplus \mathcal{O} = P$.

Sčítanie bodov eliptickej krivky – vzorce

Majme dva body eliptickej krivky $P = (x_P, y_P) \in \mathcal{E}$, $Q = (x_Q, y_Q) \in \mathcal{E}$. Na množine $\mathcal{E}$ možno definovať operáciu $R = (x_R, y_R) = P \boxplus Q$ takto:

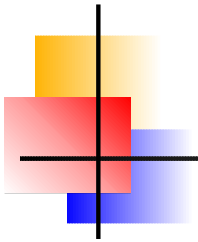
1. Ak $x_P \neq x_Q$ a súčasne $y_P \neq y_Q$

$$x_R = s^2 - (x_P + x_Q) \tag{16}$$
$$y_R = s.(x_P - x_R) - y_P, \tag{17}$$
$$\text{kde} \quad s = \frac{y_Q - y_P}{x_Q - x_P} \tag{18}$$

2. Ak $P = Q$ a $y_P = 0$, potom definujeme $P \boxplus P = \mathcal{O}$.
   Inak

$$x_R = s^2 - 2x_P \tag{19}$$
$$y_R = s(x_P - x_R) - y_P \tag{20}$$
$$\text{kde} \quad s = \frac{3{x_P}^2 + a}{2y_P} \tag{21}$$

3. Ak $P \neq Q$ ale $x_P = x_Q$, potom $P \boxplus Q = \mathcal{O}$.
4. Ak P je ľubovoľné, potom $P \boxplus \mathcal{O} = P$.



Štruktúra $(\mathcal{E}, \boxplus)$ je grupou.

Platí: Štruktúra $(\mathcal{E}, \boxplus)$ je komutatívnou aditívnou grupou s nulovým prvkom $\mathcal{O}$, t.j.

1. $\forall P, Q, R \in \mathcal{E} : P \boxplus (Q \boxplus R) = (P \boxplus Q) \boxplus R$
2. Prvok $\mathcal{O} \in \mathcal{E}$ je neutrálny prvok, t.j. $\forall P \in \mathcal{E} : P \boxplus \mathcal{O} = P = \mathcal{O} \boxplus P$
3. ku každému prvku $P \in \mathcal{E}$ existuje opačný prvok prvok $R \in \mathcal{O}$ taký, že $P \boxplus R = \mathcal{O}$.
4. $\forall P, R \in \mathcal{E} : P \boxplus R = R \boxplus P$

Eliptické krivky nad konečnými poľami

Nech $(\mathbb{K}, \oplus, \otimes)$ je konečné pole. Eliptická krivka $\mathcal{E}$ nad poľom K je množina obsahujúca nevlastný bod $\mathcal{O}$ spolu smnožinou usporiadaných dvojíc (x, y) prvkov poľa K vyhovujúcich rovnici

$$y^2 = x^3 \oplus a \otimes x \oplus b,$$

kde $a, b \in K$ také, že $4 \otimes a^3 \oplus 27 \otimes b^3 \neq 0$.
Majme dva body eliptickej krivky $P = (x_P, y_P) \in \mathcal{E}$, $Q = (x_Q, y_Q) \in \mathcal{E}$. Na množine $\mathcal{E}$ možno definovať operáciu $R = (x_R, y_R) = P \boxplus Q$ takto:

Ak $P \neq Q$ ale $x_P = x_Q$, potom

$$R = P \boxplus Q = \mathcal{O}.$$

Ak $P = Q$ a $y_P = 0$, potom

$$R = P \boxplus P = \mathcal{O}.$$

Ak $x_P \neq x_Q$ & $y_P \neq y_Q$

$$\begin{aligned} x_R &= s^2 \ominus (x_P \oplus x_Q) \\ y_R &= s \otimes (x_P \ominus x_R) \ominus y_P, \end{aligned}$$

kde $s = \dfrac{y_Q \ominus y_P}{x_Q \ominus x_P}$

Inak

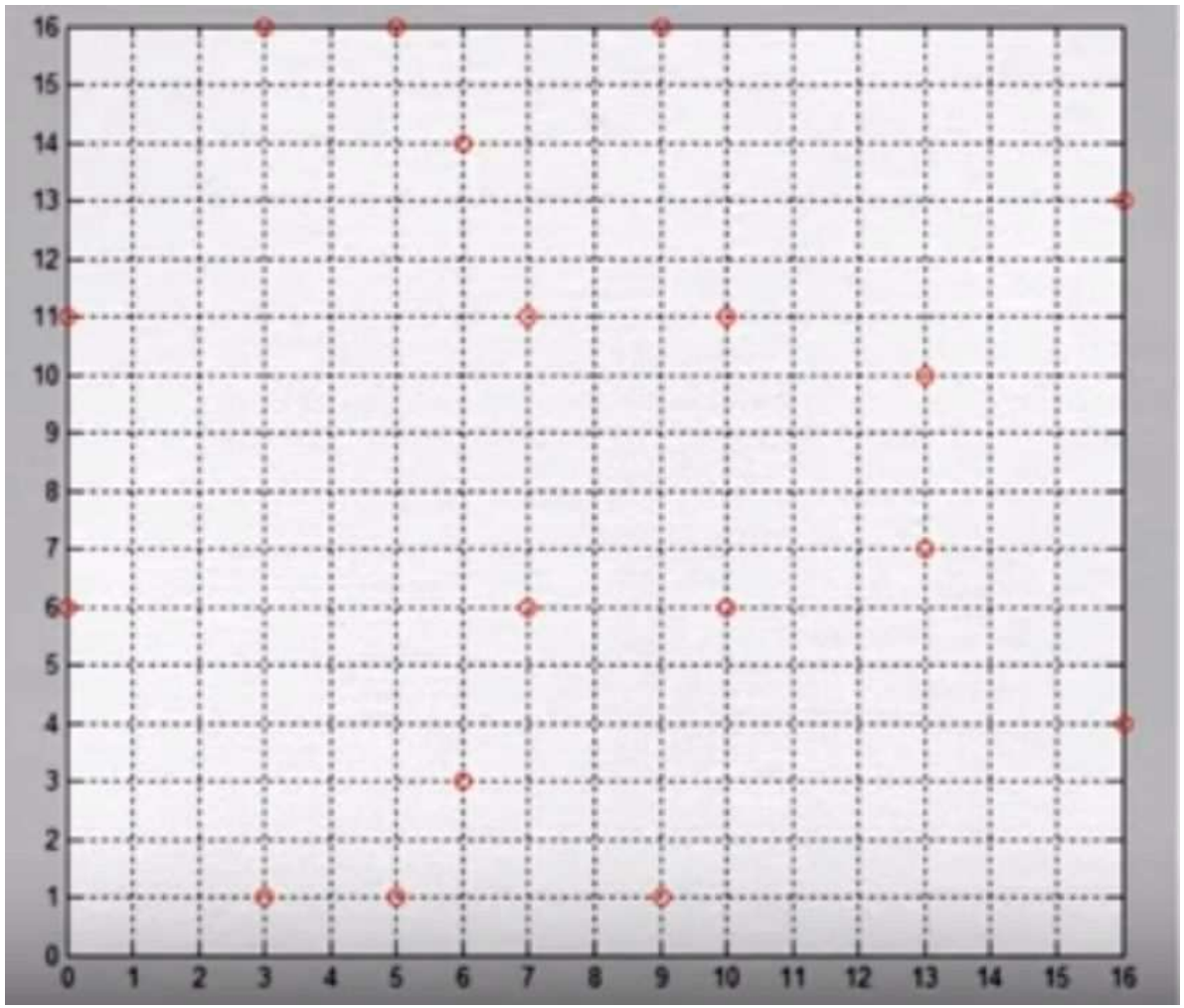
$$\begin{aligned} x_R &= s^2 \ominus 2x_P \\ y_R &= s \otimes (x_P \ominus x_R) \ominus y_P \end{aligned}$$

kde $s = \dfrac{3x_P^2 \oplus a}{2y_P}$

Pre ľubovoľné P je $P \boxplus \mathcal{O} = \mathcal{O} \boxplus P = P$.

Eliptické krivky nad konečnými poľami

Z_{17} Krivka je daná rovnicou $y^2 = x^3 + ax + b$, kde $a, b, x, y \in Z_{17}$.



Klasická Diffie - Hellmanova výmena kľúčov

Metóda je založená na tom, že vyriešiť rovnicu $s^x = a$ v konečnom poli $\mathbb{Z}_p$ (kde p je veľké prvočíslo) je veľmi ťqžký problém.
A a **B** sa dohodnú na veľkom prvočísle a čísle s, $1 < s < p$.
Čísla s, p môžu byť verejné, použiteľné opakovane aj pre viac používateľov.

A

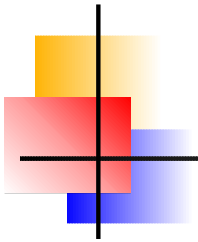
- Zvolí $a < p$ tajné.
- Vypočíta $\alpha = s^a \mod p$.
- Odošle α.
- Prijme β.
- Vypočíta kľúč $K_A = \beta^a \mod p$

B

- Zvolí $b < p$ tajné.
- Vypočíta $\beta = s^b \mod p$.
- Odošle β.
- Prijme α.
- Vypočíta kľúč $K_B = \alpha^b \mod p$

Je $K_A = K_B$?
Platí:

$$K_A = \beta^\alpha = \left(s^b\right)^a = s^{ab} = \left(s^a\right)^b = \alpha^b = K_B \mod p$$



Kryptografia s eliptickými krivkami

Majme krivku $\mathcal{E}$ nad konečným poľom Z_p danú rovnicou $y^2 = x^3 \oplus a \otimes x \oplus b$, kde $a, b, x, y \in Z_p$ a $4a^3 \oplus 27b^2 \neq 0$.
Sčítanie $\boxplus$ bodov krivky $\mathcal{E}$ je definované rovnakými vzťahmi, ako v reálnom prípade, avšak všetky operácia sa robia v poli Z_p.
Nech k je prirodzené číslo, $P \in \mathcal{E}$. Definujeme

$$k.P = \underbrace{P \boxplus P \boxplus \cdots \boxplus P}_{k\text{-krát}} \tag{22}$$

Problém diskrétneho logaritmu na eliptickej krivke:
Sú dané dva prvky eliptickej krivky $P, Q \in \mathcal{E}$ také, že $Q = k.P$.
Pre dané P, Q treba určiť k také, že $Q = k.P$
Pre eliptickú krivku $\mathcal{E}$ s veľkým počtom prvkom ide o veľmi ťaký problém.

ECC Diffie - Hellmanova výmena kľúčov

A a **B** sa dohodnú na tzv. doménových parametroch: $\{p, a, b, G, n, h\}$
- p – veľké prvočíslo definujúce pole $\mathbb{Z}_p$,
- a, b parametre eliptickej krivky $\mathcal{E}$ $(y^2 = x^3 \oplus a \otimes x \oplus b)$
- $G \in \mathcal{E}$ – generátor cyklickej podgrupy grupy $\mathcal{E}$
- n – rád (počet prvkov) cyklickej grupy generovanej prvkom G
- $h = \frac{|\mathcal{E}|}{n}$

Doménové parametre môžu byť verejné, použiteľné opakovane aj pre viac používateľov.

A

- Zvolí $1 < \alpha < n$ tajné.
- Vypočíta $A = (x_A, y_a) = \alpha.G$.
- Odošle A.
- Prijme B.
- Vypočíta kľúč $\mathcal{K}_A = \alpha.B = \alpha\beta.G$

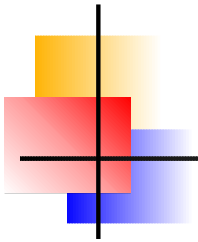
B

- Zvolí $1 < \beta < n$ tajné.
- Vypočíta $B = (B_x, B_y) = \beta.G$.
- Odošle B.
- Prijme A.
- Vypočíta kľúč $K_B = \beta.A = \beta\alpha.G = \alpha\beta.G$

A Real World Example

A Microsoft Digital Rights Management Curve

$$p = 785963102379428822376694789446897396207498568951$$
$$a = 317689081251325503476317476413827693272746955927$$
$$b = 790528966078787587181205720257185354321006519 34$$
$$G_x = 771507216262649826170648268565579889907769254176$$
$$G_y = 390157510246556628525279459266514995562533196655$$



Porovnanie veľkosti kľúčov pri rovnake bezpečnosti

Symmetric Encryption (Key Size in bits)	RSA and Diffie-Hellman (modulus size in bits)	ECC Key Size in bits	
56	512	112	0.22
80	1024	160	0.16
112	2048	224	0.11
128	3072	256	0.08
192	7680	384	0.05
256	15360	512	0.03