$\mathbb{Z}_p \rightsquigarrow (G, \cdot)$ ← grupa

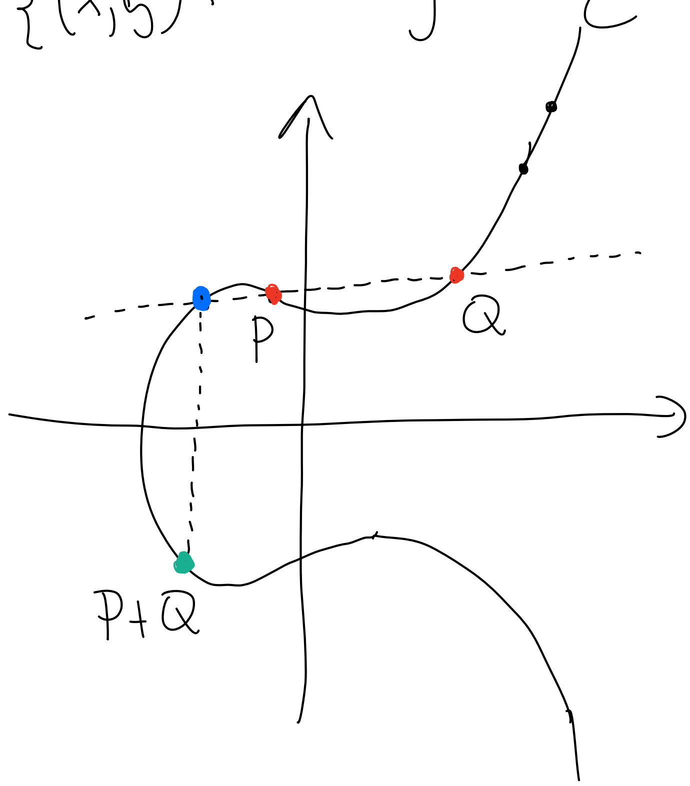
$g^x = a \longrightarrow \boxed{g^x = a}$

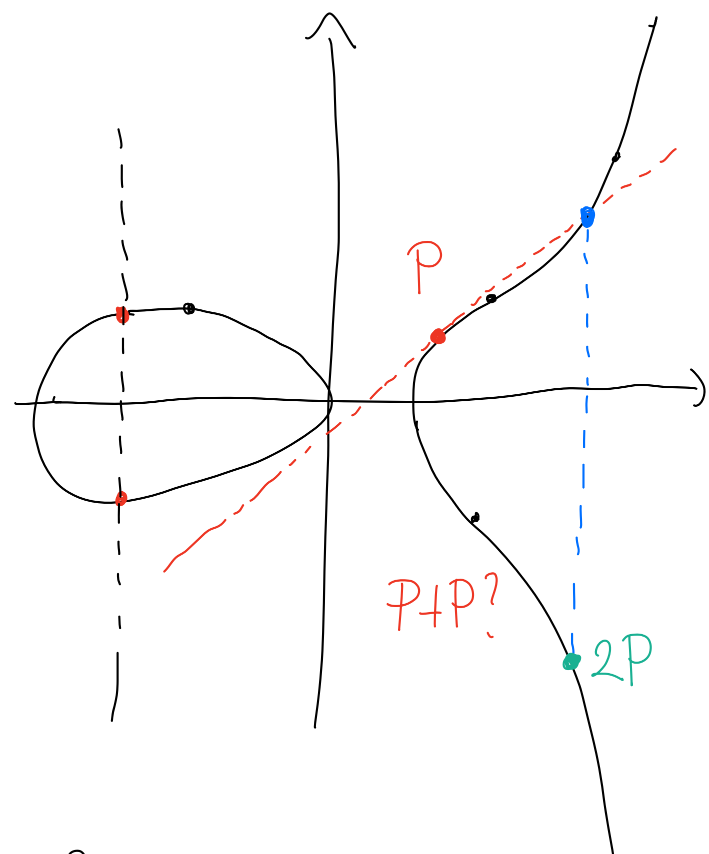
Kryptosystemy oparte o krzywe eliptyczne

(80')

$\boxed{y^2 = x^3 + ax + b, \quad a, b \in \mathbb{R}}$

$\{(x,y) : \quad \} = \mathcal{E}$





P+Q $\quad (\mathcal{E}, +)$ tworzy grupę

$y^2 = x^3 + ax + b$, $a, b \in \mathbb{R}$ { postać Weierstrassa

$\boxed{4a^3 + 27b^2 \neq 0}$

1. Krzywe algebraiczne

$\mathcal{E} = \{(x,y) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$

Jak dodać $P+Q$?

I $P \neq \mathcal{O}$, $Q = \mathcal{O}$

$P + \mathcal{O} = \mathcal{O} + P = P$

II $P = (x,y)$, $Q = (x,-y)$

$P + Q = \mathcal{O}$

{ $3 + (-3) = 0$

$-(x,y) = (x,-y)$

III $P \neq Q$ $x_1 \neq x_2$

$P = (x_1, y_1)$, $Q = (x_2, y_2)$

$P + Q = ? = (x_3, y_3)$ $x_3 = ?$ $y_3 = ?$

1 cz.

$$\boxed{\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}}$$

$P + Q = R = (x_3, y_3)$

IV $P = Q$

$$\begin{cases} \lambda = \dfrac{3x_1^2 + a}{2y_1} \\ x_3 \\ y_3 \end{cases}$$

$(G, +)$

Teoria

- $+$ jest dobrze określone
- $+$ jest przemienne $(P+Q = Q+P)$
- $+$ ma el. neutralny (O)
- istnieje el. przeciwny $P + (-P) = O$
- $+$ jest łączne $(P+Q)+R = P+(Q+R)$

technicznie skomplikowane

$(\mathcal{E}, +)$ spełnia te warunki

$(\mathcal{E}, +) \rightsquigarrow \mathbb{Z}_n$

Krzywe nad ciałami skończonymi

p - liczba pierwsza, $\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, \dots, p-1\}$

$$\mathcal{E} = \{(x,y) : y^2 = x^3 + ax + b, \ x, y \in \mathbb{Z}_p\} \cup \{O\}$$

$+$ jest zdefiniowane tak samo jak w $\mathbb{R}$!

mod p

odwrotność w $\mathbb{Z}_p$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = (y_2 - y_1) \cdot \boxed{(x_2 - x_1)^{-1}}$$

Zamiast $\mathbb{Z}_p$ można wziąć dowolne ciało skończone $\mathbb{F}_q = \mathbb{F}_{p^n}$.

Príklad $\quad p = 7 \quad\quad \mathbb{Z}_7 = \{0,1,\dots,6\}$

$$E: \quad y^2 = x^3 + x + 1 \pmod 7$$

$$4a^3 + 27b^2 = 4\cdot 1^3 + 27\cdot 1^2 = 31 \equiv 3 \neq 0 \pmod 7$$

---

y	0	1	2	3	4	5	6
$y^2 \bmod 7$	0	1	4	2	2	4	1

← rezíduá kvadratické mod 7

$\{0,1,2,4\}$

x	0	1	2	3	4	5	6
$x^3+x+1 \bmod 7$	1	3	4	3	6	5	6

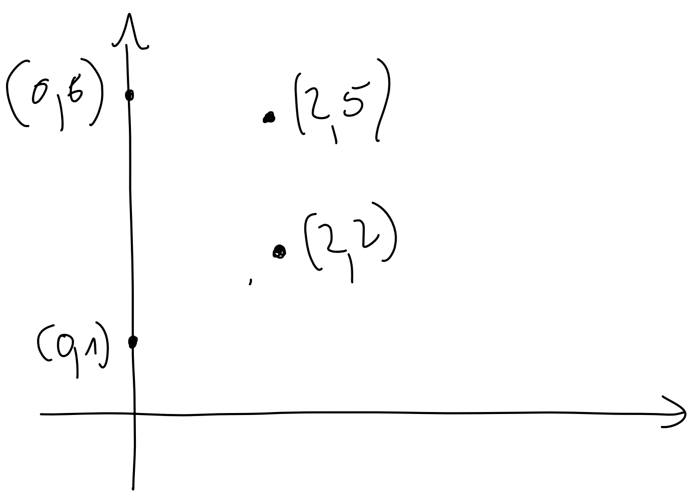
$x = 0 \quad \vee \quad x = 2$

$\hookrightarrow y^2 = 1 \qquad\qquad \hookrightarrow y^2 = 4$

$y = 1 \qquad y = 6 \qquad\qquad y = 2 \ \vee\ y = 5$

$$E = \{(0,1),(0,6),(2,2),(2,5)\} \cup \{O\}$$

$$\#E = 5$$



Test Eulera: czy a jest resztą kwadratową?

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \Rightarrow a \text{ jest resztą kwadratową } \bmod p \\ -1 & \Rightarrow a \text{ nie jest resztą kwadratową} \end{cases}$$

Jeżeli

$p \equiv 3 \pmod 4$

a jest resztą kw. mod p,

to

$$\sqrt{a} = a^{\frac{p+1}{4}}.$$

$p = 7$

$a = 4$ $\quad \sqrt{a} = 4^2 = 2$

$\sqrt{a} = 7 - 2 = 5$

$$\mathcal{E} = \{(0,1), (0,6), (2,2), (2,5)\} \cup \{O\}$$

$(0,1) + (2,2) = ?$ $\quad x_1 = 0 \quad x_2 = 2$

$y_1 = 1 \quad y_2 = 2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \lambda = (2-1)(2-0)^{-1} = 1 \cdot 2^{-1} =$$

$$= 1 \cdot 4 = 4$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad x_3 = 4^2 - 0 - 2 = 0$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad y_3 = 4(0-0) - 1 = -1 \equiv 6 \pmod 7$$

$$(0,1) + (2,2) = (0,6)$$

$P = (0,1) \qquad \underset{2P}{\overset{\shortparallel}{P+P}} = ? \qquad x_1 = 0 \quad x_2 = 0$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad y_1 = 1 \quad y_2 = 1$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \qquad \lambda = (3 \cdot 0 + 1) \cdot (2 \cdot 1)^{-1} =$$

$$= 1 \cdot 4 = 4$$

$$x_3 = 4^2 - 0 - 0 = 2$$

$$y_3 = 4(0-2) - 1 = -9 \equiv 5 \pmod 7$$

$$(0,1) + (0,1) = 2(0,1) = (2,5)$$

$$10(0,1) = 2(2(2(0,1))) + 2(0,1)$$

Ile jest punktów na krzywej eliptycznej?

$\mathbb{F}_q - \mathbb{F}_{p^n}$

$\# E \sim q + 1$

Tw. Hassego.

$$q + 1 - 2\sqrt{q} \le \# E \le q + 1 + 2\sqrt{q}$$

DH i ElGamal

Elgamal

$\mathbb{Z}_p \longrightarrow (\mathcal{E}, +)$

bezpieczeństwo	DH	RSA	ECC
112	2048	2048	224 - 255
128	3072	3072	256 - 383
192	7680	7680	384 - 511
256	15360	15360	512 +

wolne

n

metody indeksowe

sito ciała liczbowego

NIE PRZENOSZĄ SIĘ NA KRZYWĄ ELIPTYCZNĄ

DH

$(+\ p, g \longrightarrow)$

$(+\ \mathcal{E}, P \longrightarrow)$

rzędu n

$nP = 0$

A

$a \in \mathbb{Z}_p$

$a \in \mathbb{Z}_n$

$A = g^a$

$A = aP$

B

$b \in \mathbb{Z}_p$

$b \in \mathbb{Z}_n$

$B = g^b$

$B = bP$

$A \longrightarrow$

$\longleftarrow B$

$K = B^a = g^{ab}$

$K = aB = (ab)P$

$K = (ab)P$

$K = A^b = g^{ab}$

$K = bA = b(aP) = (ab)P$

$P + P + P + \dots + P$

//

Eva $\mathcal{E}$, P, $A = \cancel{P}$

$\boxed{xP = A}$? $x = ?$ $g^x \equiv a \pmod{p}$

problem log. dyskretnego
na krzywej ell.