Grupa na eliptični krivulji

Za kriptografijo sta jo leta 1985 prva predlagala Neal Koblitz in Victor Miller.

Eliptična krivulja E nad obsegom $\mathbb{Z}_p$ je definirana z Weierstrassovo enačbo:

$$\boldsymbol{y^2 = x^3 + ax + b} \qquad (1)$$

kjer sta $a, b \in \mathbb{Z}_p$ in $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$
($GF(2^m)$: $y^2 + xy = x^3 + ax^2 + b$).

$$E(\mathbb{Z}_p) := \{(x, y) \,|\, x, y \in \mathbb{Z}_p, \text{ ki ustrezajo } (1)\} \cup \mathcal{O}.$$

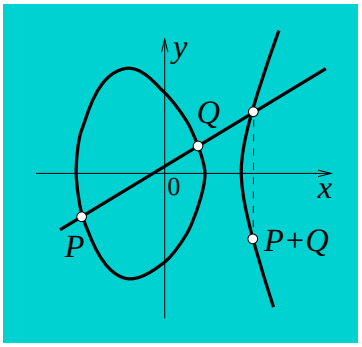
Pravilo za seštevanje

1. $P=(x_1, y_1),\ Q=(x_2, y_2) \in E(\mathbb{Z}_p)$,
   kjer $P \neq -Q := (x_2, -y_2)$.

   Potem je $P+Q=(x_3, y_3)$, kjer je

   $x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$, in

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & ; \text{za } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & ; \text{za } P = Q. \end{cases}$$



2. $P + \mathcal{O} = \mathcal{O} + P = P \quad$ in $\quad P + (-P) = \mathcal{O}$
   za vsak $P \in E(\mathbb{Z}_p)$.

Množica $E(\mathbb{Z}_p)$ je sestavljena iz točk (x, y), $x, y \in \mathbb{Z}_p$, ki ustrezajo zgornji enačbi, vključno s točko neskončno $\mathcal{O}$.

Izrek (Hasse).

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$$

Schoofov algoritem izračuna $|E|$ v $O((\log p)^8)$ bitnih operacijah.

Grupa E je izomorfna $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, kjer je $n_2 | n_1$ in $n_2 | (p-1)$, tako da lahko najdemo ciklično podgrupo $\mathbb{Z}_{n_1}$, ki jo uporabimo za ElGamalov kriptosistem.

Podeksponentno metodo **index calculus** zaenkrat ne znamo uporabiti pri DLP na eliptični grupi (razen če ni eliptična krivulja supersingularna).

Zato si lahko izberemo eliptično krivuljo s ciklično podgrupo velikosti (samo) okoli 2^{160}.

Primer: EC nad $\mathrm{GF}(2^4)$

- Naj bo $\mathrm{GF}(2^4)$ generiran s korenom $\alpha = x$ nerazcepnega polinoma $f(x) = 1 + x + x^4$.
- $E_1(\mathrm{GF}(2^4))$
  $= \{(x, y) : y^2 + xy = x^3 + \alpha^4 x^2 + 1\} \cup \{\mathcal{O}\}$.
- $E_1(\mathrm{GF}(2^4))$ tvori grupo za seštevanje z $\mathcal{O}$ kot identiteto.

Rešitve enačbe: $y^2 + xy = x^3 + \alpha^4 x^2 + 1$ nad GF(2^4)

$(0, 1)$	
$(1, \alpha^6)$	$(1, \alpha^{13})$
(α^3, α^8)	(α^3, α^{13})
(α^5, α^3)	(α^5, α^{11})
(α^6, α^8)	(α^6, α^{14})
(α^9, α^{10})	(α^9, α^{13})
(α^{10}, α^1)	(α^{10}, α^8)
$(\alpha^{12}, 0)$	$(\alpha^{12}, \alpha^{12})$

Primer seštevanja v $E_1(\mathrm{GF}(2^4))$:

Naj bo $P_1 = (\alpha^6, \alpha^8)$, $P_2 = (\alpha^3, \alpha^{13})$.

- $P_1 + P_2 = (x_3, y_3)$:

$$\begin{aligned} x_3 &= (\frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3})^2 + \frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3} + \alpha^6 + \alpha^3 + \alpha^4 \\ &= (\frac{\alpha^3}{\alpha^2})^2 + \frac{\alpha^3}{\alpha^2} + \alpha^2 + \alpha^4 = 1 \end{aligned}$$

$$\begin{aligned} y_3 &= (\frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3})(\alpha^6 + 1) + 1 + \alpha^8 \\ &= (\frac{\alpha^3}{\alpha^2})\alpha^{13} + \alpha^2 = \alpha^{13} \end{aligned}$$

- $2P_1 = (x_3, y_3)$:

$$\begin{aligned} x_3 &= (\alpha^6)^2 + \frac{1}{(\alpha^6)^2} \\ &= \alpha^{12} + \alpha^3 = \alpha^{10} \end{aligned}$$

$$\begin{aligned} y_3 &= (\alpha^6)^2 + (\alpha^6 + \frac{\alpha^8}{\alpha^6})\alpha^{10} + \alpha^{10} \\ &= \alpha^3 + (\alpha^6 + \alpha^2)\alpha^{10} = \alpha^8 \end{aligned}$$

Še en primer EC nad $\mathrm{GF}(2^4)$

- Naj bo $\mathrm{GF}(2^4)$ generiran s korenom $\alpha = x$ nerazcepnega polinoma $f(x) = 1 + x + x^4$.
- $E_2(\mathrm{GF}(2^4))$ $= \{(x, y) : y^2 + \alpha^6 y = x^3 + \alpha^3 x + 1\} \cup \{\mathcal{O}\}$.
- $E_2(\mathrm{GF}(2^4))$ tvori grupo za seštevanje z $\mathcal{O}$ kot identiteto.

Iščemo rešitve enačbe

$$y^2 + \alpha^6 y = x^3 + \alpha^3 x + 1$$

nad GF(2^4). Ta enačba ima samo 8 rešitev:

(α^2, α^8)	(α^2, α^{14})
$(\alpha^{10}, 1)$	$(\alpha^{10}, \alpha^{13})$
$(\alpha^{11}, 0)$	(α^{11}, α^6)
(α^{13}, α^5)	(α^{13}, α^9)

Primer: EC nad GF(23)

- Naj bo $p = 23$.
- $y^2 = x^3 + x + 1$, (i.e., $a = 1$, $b = 1$).
  Velja: $27a^3 + 16b^2 = 3 \cdot 1^3 + 16 \cdot 1^3 = 19 \neq 0$ v GF(23).
- $E_3(\mathrm{GF}(23)) = \{(x, y) : y^2 = x^3 + x + 1\} \cup \{\mathcal{O}\}$.
- $E_3(\mathrm{GF}(23))$ tvori grupo za seštevanje
  z $\mathcal{O}$ kot identiteto.

Rešitve enačbe $y^2 = x^3 + x + 1$ nad $\mathbb{Z}_{23}$:

(0, 1)	(6, 4)	(-11,-4)
(0,-1)	(6,-4)	(-10, 7)
(1, 7)	(7, 11)	(-10,-7)
(1,-7)	(7,-11)	(-6, 3)
(3, 10)	(9, 7)	(-6,-3)
(3,-10)	(9,-7)	(-5, 3)
(4, 0)	(11, 3)	(-5,-3)
(5, 4)	(11,-3)	(-4, 5)
(5,-4)	(-11,4)	(-4,-5)

Primera seštevanja na $E_3(\mathrm{GF}(23))$

1. $P_1 = (3, 10)$, $P_2 = (9, 7)$,
   $P_1 + P_2 = (x_3, y_3)$.

   $\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \in \mathbb{Z}_{23}$.

   $x_3 = 11^2 - 3 - 9 = 6 - 3 - 9 = -6$,
   $y_3 = 11(3 - (-6)) - 10 = 11(9) - 10$
   $= 89 = 20 = -3$.
   Sledi $P_1 + P_2 = (-6, -3)$.

2. $P_1 = (3, 10),\ \ 2P_1 = (x_3, y_3),$

$\lambda = \frac{3(3^2)+1}{20} = \frac{5}{20} = \frac{1}{4} = 6.$

$x_3 = 6^2 - 6 = 30 = 7,$
$y_3 = 6(3 - 7) - 10 = -24 - 10 = -11.$

Sledi $2P_1 = (7, -11)$.

$P = (0, 1)$ je generator:

P=(0, 1)	
$2P$=(6,-4)	$15P$=(9, 7)
$3P$=(3,-10)	$16P$=(-6,3)
$4P$=(-10,-7)	$17P$=(1,7)
$5P$=(-5,3)	$18P$=(12,-4)
$6P$=(7,11)	$19P$=(-4,5)
$7P$=(11,3)	$20P$=(5,4)
$8P$=(5,-4)	$21P$=(11,-3)
$9P$=(-4,-5)	$22P$=(7 -11)
$10P$ =(12,4)	$23P$=(-5,-3)
$11P$=(1,-7)	$24P$=(-10,7)
$12P$=(-6,-3)	$25P$=(3,10)
$13P$=(9,-7)	$26P$=(6,4)
$14P$=(4,0)	$27P$=(0,-1)

Log – antilog tabela

log	elt	log	elt
0	$\mathcal{O}$	14	(4,0)
1	(0,1)	15	(9,7)
2	(6,-4)	16	(-6,3)
3	(3,-10)	17	(1,7)
4	(-10,-7)	18	(-11,-4)
5	(-5,3)	19	(-4,5)
6	(7,11)	20	(5,4)
7	(11,3)	21	(11,-3)
8	(5,-4)	22	(7,-11)
9	(-4,-5)	23	(-5,-3)
10	(-11,4)	24	(-10,7)
11	(1,-7)	25	(3,10)
12	(-6,-3)	26	(6,4)
13	(9,-7)	27	(0,-1)

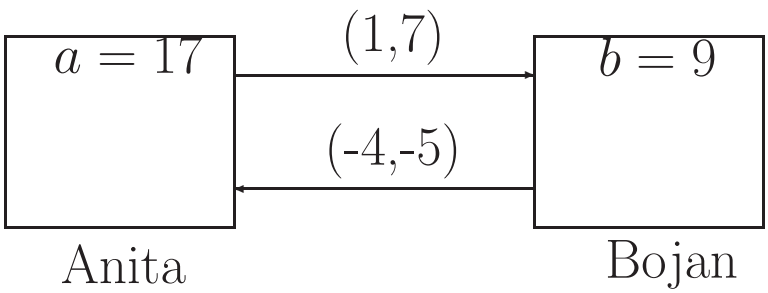
Antilog – log tabela

elt	log	elt	log
$\mathcal{O}$	0	(9,7)	15
(0,1)	1	(9,-7)	13
(0,-1)	27	(11,3)	7
(1,7)	17	(11,-3)	21
(1,-7)	11	(-11,4)	10
(3,10)	25	(-11,-4)	18
(3,-10)	3	(-10,7)	24
(4,0)	14	(-10,-7)	4
(5,4)	20	(-6,3)	16
(5,-4)	8	(-6,-3)	12
(6,4)	26	(-5,3)	5
(6,-4)	2	(-5,-3)	23
(7,11)	6	(-4,5)	19
(7,-11)	22	(-4,-5)	9

Diffie–Hellmanov protokol nad $E(\mathrm{GF}(23))$

Javni parametri:

$$y^2 = x^3 + x + 1$$
$$P = (0, 1)$$



- Anita izračuna $17P = (1, 7)$,
- Bojan izračuna $9P = (-4, -5)$,
- Anita izračuna $17(-4, -5) = (6, 4)$,
- Bojan izračuna $9(1, 7) = (6, 4)$.

Anita in Bojan imata skupno točko $(6, 4)$.

Računanje logaritmov

Izračunaj $\log_P(9,7)$**.**

Izračunaj naslednjo tabelo:

elt	(0,1)	(7,11)	(-6,-3)	(12,-4)	(-10,7)
log	1	6	12	18	24

Če je $k = \log_P(9,7)$, potem velja $kP = (9,7)$.

- Računamo
  $(9,7)+P,\ \ (9,7)+2P,\quad (9,7)+3P,\ldots,$
  vse, dokler ne dobimo element iz tabele.
- Tako dobimo: $(9,7)+3P=(12,-4)$.
- Iz tabele preberemo $(12,-4)=18P$.
- Sledi $(9,7)+3P=18P$
  oziroma $(9,7)=15P$, torej $k=15$.

- Če je $|E(\mathrm{GF}(q))| = n$, lahko posplošimo metodo za $E(\mathrm{GF}(23))$ na naslednji način:
  - naredi tabelo (i, iP) velikosti $\sqrt{n}$,
  - za iskanje logaritma elementa v tej tabeli potrebujemo največ $\sqrt{n}$ seštevanj točk.
- Če je $q \approx 10^{40}$, potem je $|E(\mathrm{GF}(q))| \approx 10^{40}$ in ima tabela 10^{20} vrstic.

  To je očitno popolnoma nedosegljivo.