Kryptografia z elementami algebry, wykład 5

Maciej Grześkowiak

29 stycznia 2022

Elementy algebry

Ciało K

Definicja

Zbiór $(K, +, \cdot)$ z dwoma działaniami, który spełnia następujące warunki:

- $(K, +)$ jest grupą abelową,
- $(K \setminus \{0\}, \cdot)$ jest grupą abelową,
- $\forall a, b, c \in K$ mamy
    - $a(b + c) = ab + ac$,
    - $(b + c)a = ba + ca$

nazywamy ciałem.

Ciało p-elementowe $\mathbb{F}_p$

Przyklad Niech p będzie liczbą pierwszą.
Definiujemy z dwoma działaniami

$$(\mathbb{F}_p, +, \cdot), \qquad \mathbb{F}_p = \{0, 1, 2, \ldots, p-1\},$$

który spełnia warunki

- $(\mathbb{F}_p, +)$ jest grupą abelową,
- $(\mathbb{F}_p \setminus \{0\}, \cdot)$ jest grupą abelową
- $\forall a, b, c \in \mathbb{F}_p$ mamy
  - $a(b+c) = ab + ac$,
  - $(b+c)a = ba + ca$

Struktura $(\mathbb{F}_p, +, \cdot)$ jest ciałem skończonym.

Krzywa eliptyczna nad $\mathbb{F}_p$

Niech $p > 3$ będzie liczbą pierwszą.
Definicja: Krzywa eliptyczna nad ciałem $\mathbb{F}_p$ zdefinowanana jest przez równanie

$$E : Y^2 = X^3 + AX + B, \quad A, B \in \mathbb{F}_p,$$

gdzie wyróżnik $\Delta_E = 4A^3 + 27B^2 \not\equiv 0 \pmod{p}$.

Uwaga: Zapis $E/\mathbb{F}_p$ oznacza, że krzywa E jest zdefiniowana nad $\mathbb{F}_p$.

Krzywa eliptyczna nad $\mathbb{F}_p$

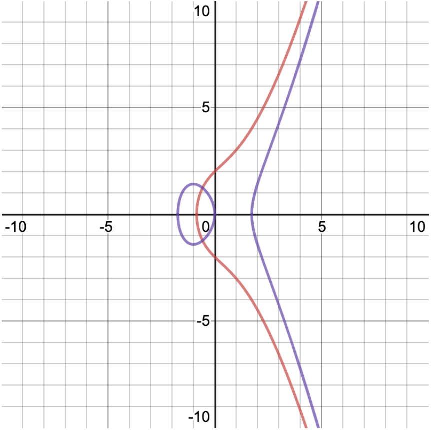
Definicja: Mówimy, że punkt $P = (x_0, y_0)$ należy do $E/\mathbb{F}_p$ jeśli spełnia równanie:

$$y_0^2 \equiv x_0^3 + Ax_0 + B \pmod{p}.$$

Definicja: Zbiór wszystkich punktów należących do $E/\mathbb{F}_p$:

$$E(\mathbb{F}_p) = \{(x, y) : y^2 \equiv x^3 + Ax + B \pmod{p}\} \cup \mathcal{O}$$

Krzywe $Y^2 = X^3 + 4X + 4$ oraz $Y^2 = X^3 - 3X$ nad $\mathbb{R}$



Przykład:

Niech $p = 11$. Zbadaj czy równanie defniuje krzywą eliptyczną nad F_{11}:

1. $E_1 : Y^2 = X^3 + 1$
2. $E_2 : Y^2 = X^3$

Rozwiązanie: Mamy,

$$\Delta_{E_1} = 4A^3 + 27B^2 \equiv 27 \equiv 5 \pmod{11},$$
$$\Delta_{E_2} = 4A^3 + 27B^2 \equiv 0 \pmod{11}.$$

Przykład: Niech E/F_7 będzie postaci

$$E : Y^2 = X^3 + 1.$$

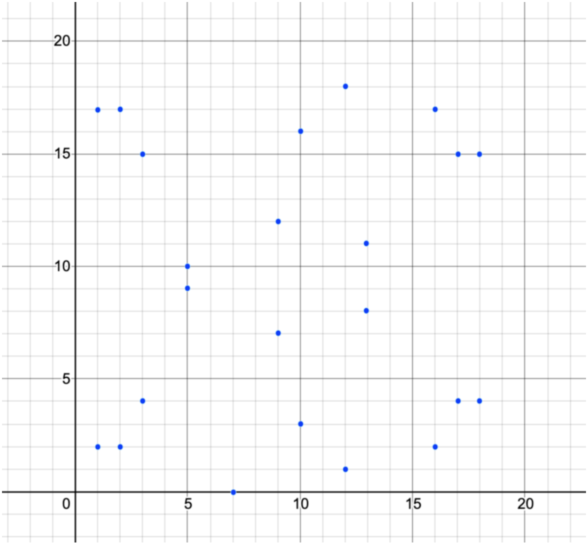
Wyznacz zbiór $E(\mathbb{F}_7)$.

Rozwiązanie: Mamy, $\Delta_E = 4A^3 + 27B^2 \equiv 27 \equiv 6 \pmod 7$. Zatem

x	x^3+1	y	(x,y)
0	1	±1	$(0,\pm1)$
1	2	±3	$(1,\pm3)$
2	2	±3	$(2,\pm3)$
3	0	0	$(3,0)$
-3	2	±3	$(-3,\pm3)$
-2	0	0	$(-2,0)$
-1	0	0	$(-1,0)$

Stąd
$E(\mathbb{F}_7) = \{(0,\pm1),(1,\pm3),(2,\pm3),(3,0),(4,\pm3),(-2,0),(-1,0)\} \cup \{\mathcal{O}\}$

Krzywa eliptyczna $E : Y^2 = X^3 - 7X + 10$ nad $\mathbb{F}_{19}$

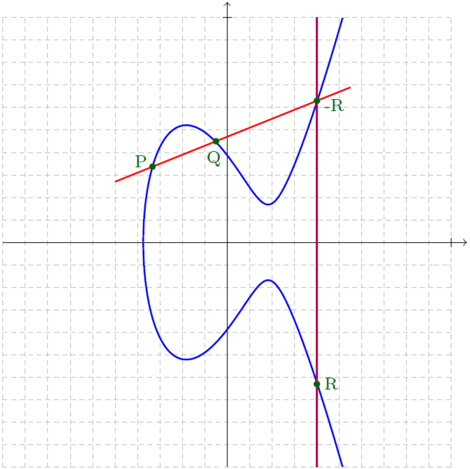


Rząd $E(F_p)$ i rząd punktu na E

Twierdzenie:(Hasse)

$$\sharp E(F_p) = p + 1 - t, \quad |t| \leq 2\sqrt{p}$$

Definiujemy działanie $\oplus$, $P \oplus Q = R$



Definiujemy działanie $\oplus$, $P \oplus Q = R$

Niech

$$E/\mathbb{F}_p : Y^2 = X^3 + AX + B.$$

Niech

$$P, Q \in E(\mathbb{F}_p), \quad P = (x_1, y_1), \quad Q = (x_2, y_2), \quad x_1 \neq x_2$$

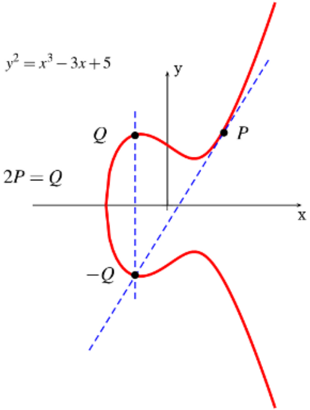
Wtedy,

$$P \oplus Q = R, \quad R = (x_3, y_3),$$

gdzie

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \pmod{p}, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \pmod{p}, \\ \lambda &= (y_2 - y_1)(x_2 - x_1)^{-1} \pmod{p}, \end{aligned}$$

Definiujemy działanie $\oplus$, $P \oplus P = 2P = Q$



Definiujemy działanie $\oplus$, $P \oplus P = 2P = Q$

Niech

$$E/\mathbb{F}_p : Y^2 = X^3 + AX + B.$$

Niech

$$P \in E(\mathbb{F}_p), \quad P = (x_1, y_1).$$

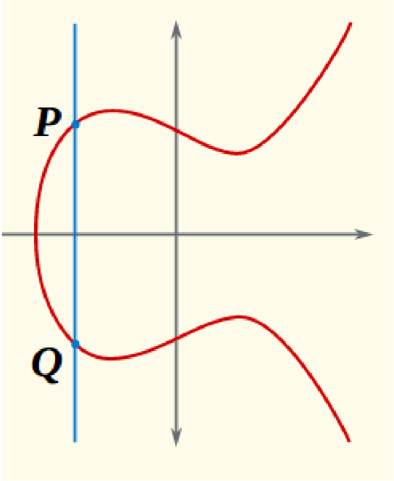
Wtedy,

$$P \oplus P = Q, \quad Q = (x_3, y_3),$$

gdzie

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \pmod p, \\ y_3 &= \lambda(x_1 - x_3) - y_1 \pmod p, \\ \lambda &= (3x_1^2 + A)(2y_1)^{-1} \pmod p, \end{aligned}$$

Definiujemy działanie $\oplus$, $P \oplus Q$, gdy $Q = -P$



Definiujemy działanie $\oplus$, $P \oplus Q$, gdy $Q = -P$

Niech

$$E/\mathbb{F}_p : Y^2 = X^3 + AX + B.$$

Niech

$$P, Q \in E(\mathbb{F}_p), \quad P = (x_1, y_1), \quad Q = (x_2, y_2), \quad x_1 = x_2, \quad y_1 = -y_2$$

Wtedy,

$$P \oplus Q = \mathcal{O}$$

Ponadto,

$$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P.$$

Twierdzenie

1. działanie $\oplus$ jest wewnetrzne w $E(\mathbb{F}_p)$, tzn. dla dowolnych $P, Q \in E(\mathbb{F}_p)$ mamy $P \oplus Q \in E(\mathbb{F}_p)$,
2. dla dowolnych $P, Q, R \in E(\mathbb{F}_p)$ mamy $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$,
3. dla każdego $P \in E(\mathbb{F}_p)$ istnieje Q takie, że $P \oplus Q = \mathcal{O}$,
4. dla każdego $P, Q \in E(\mathbb{F}_p)$ mamy $P \oplus Q = Q \oplus P$,

Uwaga:
Przyjmujemy, że jeśli $P = (x, y)$, to $-P = (x, -y)$.
Przyjmujemy $P \oplus (-Q) = P \ominus Q$.

Wniosek Zbiór $(E(\mathbb{F}_p), \oplus)$ jest grupą abelową.

Generowanie E nad $\mathbb{F}_p$

Dane k - liczba bitów
Wynik $E : Y^2 = X^3 + AX + B$ nad $\mathbb{F}_p$

1. Losuj k- bitową liczbę pierwszą p,
2. Losuj A oraz B z ciała $\mathbb{F}_p$,
3. Oblicz $\Delta_E = 4A^3 + 27B^2 \pmod{p}$,
4. **if** $\Delta_E = 0 \pmod{p}$ **then**
5. skok do 2
6. return (A, B, p)

Generowanie $P \in E(\mathbb{F}_p)$

Dane $E : Y^2 = X^3 + AX + B$ nad $\mathbb{F}_p$
Wynik $P = (x, y) \in E(\mathbb{F}_p)$

1. Losuj x z ciała $\mathbb{F}_p$,
2. Oblicz $f(x) = x^3 + Ax + B \pmod p$
3. **if** $\left(\frac{f(x)}{p}\right) = -1$ **then**
4. skok do 1,
5. Oblicz $y \in \mathbb{F}_p$ takie, że $y^2 = f(x) \pmod p$
6. return $P = (x, y)$

Krzywa eliptyczna nad $\mathbb{F}_p$, przykład

Przykład:
Niech E/F_{11} będzie postaci $E : Y^2 = X^3 + 2X - 2$. Znajdź punkt należący do $E(\mathbb{F}_{11})$.

Rozwiązanie: Mamy,

$$\Delta_E = 4A^3 + 27B^2 \equiv 4 \cdot 2^3 - 5 \cdot 4 \equiv 1 \pmod{11}.$$

Szukam x, y takiego, że $P = (x, y) \in E(\mathbb{F}_{11})$. W tym celu losujemy $x = 1$ i obliczam

$$x^3 + 2x - 2 \equiv 1 \pmod{11}$$

Rozwiązuję kongruencję

$$Y^2 \equiv 1 \pmod{11},$$

Stąd $y \equiv \pm \pmod{11}$. Zatem

$$P = (1, 1) \in E(\mathbb{F}_{11}).$$

Zadanie:

Niech E/F_7 będzie postaci

$$E : Y^2 = X^3 + 1.$$

Niech $P = (1, 3)$, $Q = (2, 4)$, $R = (6, 0)$. Oblicz

1. $-Q$
2. $R \oplus \mathcal{O}$
3. $P \oplus Q$,
4. $2R$

Rozwiązanie:

$$-Q = -(2, 4) = (2, -4),$$
$$R \oplus \mathcal{O} = R = (6, 0).$$

$E: Y^2 = X^3 + 1$ nad $\mathbb{F}_7$, przykład

Rozwiązanie cd:

$$P \oplus Q = (1,3) \oplus (2,4) = (x_3, y_3),$$

gdzie

$$\begin{aligned}
\lambda &= (y_2 - y_1)(x_2 - x_1)^{-1} \equiv (4-3)(2-1)^{-1} \equiv 1 \pmod 7,\\
x_3 &= \lambda^2 - x_1 - x_2 \equiv 1^2 - 1 - 2 \equiv -2 \equiv 5 \pmod 7,\\
y_3 &= \lambda(x_1 - x_3) - y_1 \equiv 1(1-5) - 3 \equiv -7 \equiv 0 \pmod 7.
\end{aligned}$$

Stąd,

$$P \oplus Q = (1,3) \oplus (2,4) = (5,0),$$

Rozwiązanie cd:

$$2P = P \oplus P = (1,3) \oplus (1,3) = (x_3, y_3),$$

gdzie

$$\begin{aligned}
\lambda &= (3x_1^2 + A)(2y_1)^{-1} \equiv (3 \cdot 1^2 + 0)6^{-1} \equiv 3 \cdot 6 \equiv 4 \pmod 7,\\
x_3 &= \lambda^2 - 2x_1 \equiv 4^2 - 2 \equiv 0 \pmod 7,\\
y_3 &= \lambda(x_1 - x_3) - y_1 \equiv 4(1-0) - 3 \equiv 1 \pmod 7.
\end{aligned}$$

$$P \oplus P = (1,3) \oplus (1,3) = (0,1).$$

Funkcja jednokierunkowa, przykład

Niech $p > 3$ będzie liczbą pierwszą oraz $E/\mathbb{F}_p : Y^2 = X^3 + AX + B$.
$P \in E(\mathbb{F}_p)$, $P \neq \mathcal{O}$, $1 < n < \sharp E(\mathbb{F}_p)$, $n \in \mathbb{N}$

Definicja:

$$F(P, E, n, p) = nP$$

oraz

$$F^{-1}(P, Q, E, p) = n, \quad \text{takie, że } Q = nP, \quad Q \in E(\mathbb{F}_p)$$

Czy funkcja F może być jednokierunkowa?

Niech E/F_7 będzie postaci

$$E : Y^2 = X^3 + 1.$$

Problem (ECDLP):

Dane $P = (6, 0), Q = (1, 3) \in E(\mathbb{F}_p)$
Wynik: znajdź, o ile istnieje, $n \in \mathbb{N}$ takie, że $P = nQ$.

Mamy,

$$\begin{array}{lll} 1Q = (1,3), & 2Q = (0,1), & 3Q = (3,0), \\ 4Q = (0,6), & 5Q = (1,4), & 6Q = \mathcal{O}, \end{array}$$

Zatem, nie istnieje $n \in \mathbb{N}$ takie, że $P = nQ$.

Problem (ECDLP):

Dane $P = (1,4), Q = (1,3) \in E(\mathbb{F}_p)$
Wynik: znajdź, o ile istnieje, $n \in \mathbb{N}$ takie, że $P = nQ$.

Mamy,

$$\begin{aligned} 1Q &= (1,3), & 2Q &= (0,1), & 3Q &= (3,0), \\ 4Q &= (0,6), & 5Q &= (1,4), & 6Q &= \mathcal{O}, \end{aligned}$$

Zatem, istnieje $n = 5$ takie, że $P = 5Q$.

Mamy,

x	x^3+1	y	(x,y)
0	1	±1	$(0,\pm1)$
1	2	±3	$(1,\pm3)$
2	2	±3	$(2,\pm3)$
3	0	0	$(3,0)$
-3	2	±3	$(-3,\pm3)$
-2	0	0	$(-2,0)$
-1	0	0	$(-1,0)$

Stąd

$$E(\mathbb{F}_7) = \{(0,1),(0,6),(1,3),(1,4),(2,3),(2,4),\\ (3,0),(4,3),(4,4),(5,0),(1,0)\} \cup \{\mathcal{O}\}$$

Problem logarytmu dyskretnego, wnioski

$$E(\mathbb{F}_7) = \{(0,1),(0,6),(1,3),(1,4),(2,3),(2,4),\\ (3,0),(4,3),(4,4),(5,0),(1,0)\} \cup \{\mathcal{O}\}$$

Widzimy, że $\mathrm{ord}_E(Q) = 6$ i $\sharp E(F_p) = 12$ oraz, że

$$\mathrm{ord}_E(P) \mid \sharp E(F_p).$$

Wniosek: Ze względu bezpieczeństwa:

- $\sharp E(F_p)$ powinnien mieć duży dzielnik pierwszy lub być dużą liczbą pierwszą,
- $\mathrm{ord}_E(P)$ powinien być duży, najlepiej liczbą pierwszą,

Algorytm (metoda binarna):
Dane: $n \in \mathbb{N}$, $P \in E(\mathbb{F}_p)$, gdzie $n \in \mathbb{N}$
Wynik: $R \in E(\mathbb{F}_p)$, takie, że $R = nP$.

1. $Q = P$
2. $R = \mathcal{O}$
3. **while** $n > 0$ **do**
4.   **if** $n = 1 \pmod 2$ **then**
5. $R = R \oplus Q$
6. $n = n - 1$
7. $Q = Q \oplus Q$
8. $n = n/2$
9. Return R

Kryptosystem ElGamala na krzywej eliptycznej $E/\mathbb{F}_p$

Alice (Algorytm generowania kluczy)

1. Losuje liczbę pierwszą p i ustala $\mathbb{F}_p$,
2. Losuje krzywą E nad $\mathbb{F}_p$,
3. Losuje $P \in E(\mathbb{F}_p)$, $P \neq \mathcal{O}$,
4. Losuje $x \in \mathbb{N}$, $x < \sharp E(\mathbb{F}_p)$,
5. Oblicza $Q = xP$,
6. Przyjmuje $K_A = [E, p, P, Q]$ za klucz publiczny i go publikuje
7. Przyjmuje $k_A = [E, p, P, Q, x]$ za klucz tajny.

Kryptosystem ElGamala na krzywej eliptycznej $E/\mathbb{F}_p$

Bob (Algorytm szyfrowania)
$K_A = [E, p, P, Q]$

1. Ustala wiadomość M,
2. Pobiera K_A klucz publiczny Alice,
3. Koduje M na P_M punkt krzywej E,
4. Losuje $y \in \mathbb{N}$, $y < \sharp E(\mathbb{F}_p)$,
5. Oblicza $C_1 = yP$,
6. Oblicza $C_2 = P_M \oplus yQ$,
7. Wysyła $C = [C_1, C_2]$ do Alice.

Alice (Algorytm deszyfrowania)
$C = [C_1, C_2]$, $k_A = [E, p, P, Q, x]$

1. Oblicza $P_M = C_2 \ominus (xC_1)$,
2. Dekoduje P_M na M,

Poprawność:
Mamy,

$$C_2 \ominus (xC_1) = P_M \oplus yQ \ominus xyP = P_M \oplus yxP \ominus xyP = P_M \oplus \mathcal{O} = P_M.$$

Kodowanie M na $P_M \in E(\mathbb{F}_p)$, $E : Y^2 = X^3 + AX + B$

Algorytm kodowania

Wybieramy N, μ, takie, że $0 \leq M < N$ oraz $p > N\mu$, gdzie $\mu \in \mathbb{N}$
Dane: M, N, μ

1. Dla $j = 1, 2, \ldots$ do μ wykonuj:
2. $\quad x \equiv M\mu + j \pmod{p}$,
3. $\quad f \equiv x^3 + Ax + B \pmod{p}$,
4. $\quad$ jeśli $\left(\frac{f}{p}\right) == 1$, to
5. $\quad\quad$ oblicz y taki, że $y^2 \equiv f \pmod{p}$,
6. Return $P_M = (x, y)$.

Uwaga:
wybór N związany jest z liczbą bitów M,
algorytm zakoduje M z prawdopodobieństwem co najmniej $\frac{1}{2^\mu}$, warto wybrać $\mu \in \{30, \ldots, 50\}$.

Algorytm dekodowania

Dane: $P_M = (x, y), \mu$

1. Oblicz $\lfloor M = (x-1)/\mu \rfloor$
2. Return M.

Poprawność:

$$M + \frac{1-1}{\mu} \leq \frac{x-1}{\mu} = \frac{M\mu + j - 1}{\mu} = M + \frac{j-1}{\mu} \leq M + \frac{\mu - 1}{\mu}$$

Stąd,

$$\lfloor \frac{x-1}{\mu} \rfloor = M.$$