Laboratorium III - krzywe eliptyczne

Wstęp teoretyczny

1. Definicja krzywej eliptycznej

Krzywa eliptyczna nad ciałem K to zbiór punktów (x, y) spełniających równanie:

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

gdzie $a, b \in K$, wraz z dodatkowym punktem O (nazywanym punktem w nieskończoności).

W kryptografii najczęściej pracujemy w ciele skończonym $\mathbb{F}_p$ (gdzie p jest liczbą pierwszą), wtedy równanie przyjmuje postać:

$$y^2 \equiv x^3 + ax + b \pmod p$$

Warunkiem istnienia krzywej jest, aby jej wyróżnik był różny od zera:

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

2. Struktura grupy

Punkty krzywej eliptycznej wraz z operacją dodawania tworzą grupę abelową, co oznacza że:

- Operacja dodawania jest łączna: (P + Q) + R = P + (Q + R)
- Operacja dodawania jest przemienna: P + Q = Q + P
- Istnieje element neutralny (punkt O): P + O = P
- Dla każdego punktu P istnieje punkt przeciwny -P: P + (-P) = O

UWAGA: O nie oznacza punktu $(0, 0)$ - to jest punkt w nieskończoności.

2.1 Punkt w nieskończoności Punkt w nieskończoności (oznaczany jako O lub ∞) można rozumieć następująco: każda prosta niepionowa przecina krzywą eliptyczną w dokładnie trzech punktach (licząc z krotnościami). Dla prostej pionowej, "trzeci punkt przecięcia" jest właśnie punktem w nieskończoności

2.2 Własności algebraiczne punktu O Punkt w nieskończoności O ma następujące kluczowe własności:

Element neutralny dodawania:

$$P + O = P$$
$$O + P = P$$
$$O + O = O$$

Dla każdego punktu P:

$$P + (-P) = O$$

gdzie $-P$ to punkt przeciwny do P

Punkt w nieskończoności w implementacji numerycznej:

- reprezentowany jest zwykle jako `None` lub specjalna wartość,
- nie ma współrzędnych (x,y),
- wymaga specjalnej obsługi w funkcjach dodawania.

3. Operacje na punktach krzywej

3.1. Dodawanie różnych punktów P + Q Dla dwóch różnych punktów $P(x_1, y_1)$ i $Q(x_2, y_2)$:

1. Oblicz s:

$$s = \frac{y_2 - y_1}{x_2 - x_1} \quad mod\, p$$

2. Oblicz współrzędne punktu wynikowego $R(x_3, y_3)$:

$$x_3 = s^2 - x_1 - x_2 \mod p$$
$$y_3 = s(x_1 - x_3) - y_1 \mod p$$

3.2. Podwajanie punktu (2P) Dla punktu $P(x_1, y_1)$:

1. Oblicz s:

$$s = \frac{3{x_1}^2 + a}{2y_1} \mod p$$

2. Oblicz współrzędne punktu wynikowego $R(x_3, y_3)$:

$$x_3 = s^2 - 2x_1 \mod p$$
$$y_3 = s(x_1 - x_3) - y_1 \mod p$$

3.3. Punkt przeciwny Dla punktu $P(x, y)$, punktem przeciwnym jest: $-P = (x, -y \mod p)$

$$P + (-P) = O$$

Zadanie 1

Zaimplementuj funkcję `get_points(a, b, p)`, która jako parametry przyjmuje współczynniki a i b definiujące krzywą eliptyczną oraz liczbę pierwsza p i zwraca punkty należące do tej krzywej w postaci listy krotek.

Wykonaj rachunki dla różnych liczb p i spróbuj zobrazować wyliczone punkty ma wykresie.

Zadanie 2

1. Zaimplementuj funkcję `add_points(P, Q, a, p)`. Wykorzystaj informacje o dodawaniu punktów zawarte w części teoretycznej. Funkcja powinna zawracać krotkę zawierającą współrzędne punktu lub obiekt `None`.

   Dla punktów w nieskończoności używaj `None`.

   Pamiętaj, że w ciele $\mathbb{F}_p$ nie ma operacji dzielenia. Dzielenie przez x to mnożenie przez element odwrotny do x. Jeśli szukamy elementu odwrotnego dla x to możemy wykorzystać potęgowanie:

   ```
   y = pow(x, -1, p)
   ```

   Zastanów się dlaczego powyższe jest równoważne wyrażeniu:

   ```
   y = pow(x, p-2, p)
   ```

   W funkcji `add_points()` uwzględnij przypadki:

```
P + O -> P
O + P -> P
P + (-P) -> O
P + P -> podwajanie punktu (2P)
P + Q -> R
```

2. Przetestuj swoja funkcję dla krzywej o parametrach: `a = 2, b = 3, p = 13`. Sprawdź poprawność poniższych działań:

```
(10, 3) + (12, 0) =  (3, 6)
(3, 7) + (4, 7) =  (6, 6)
(7, 10) + (3, 6) =  (4, 6)
(0, 4) + (11, 11) =  (11, 2)
(6, 6) + (6, 6) =  (11, 11)
(6, 6) + (11, 11) =  (10, 3)
(7, 10) + (7, 3) =  None
(9, 3) + (9, 10) =  None
```

3. Wykonaj tabelkę dodawania dla punktów na krzywej `(2, 3, 7)`

Zadanie 3

Zaimplementuj funkcję `multiply_point(P, n, a, p)`, która pozwala wykonywać mnożenie punktu P na krzywej przez liczbę n.

Zadanie 4

Zaimplementuj funkcję `find_order(P, a, p)`, która znajduje rząd punktu na krzywej eliptycznej. Rząd punktu to najmniejsza liczba naturalna n taka, że $nP = O$

- Znajdź rzędy wszystkich punktów dla krzywej $y^2 = x^3 + x - 1$ w $\mathbb{F}_{11}$

Zadanie 5

Dla zbioru punktów na danej krzywej eliptycznej (a, b, p) znajdź punkt generujący grupę na krzywej. Zaimplementuj w tym celu funkcję `find_generator(a, b, p)`, która zwróci generator i jego rząd.

Dla danej grupy na krzywej rząd generatora jest równy rzędowi grupy. W tym przypadku jest to liczba punktów na krzywej powiększona o 1. Generatorem jest zatem punkt o maksymalnym rzędzie równym rzędowi grupy. Znalezienie takiego punktu może wymagać zbadania wszystkich punktów na krzywej.

- Znajdź generator dla krzywej $(2, 3, 13)$ i sprawdź czy generuje wszystkie punkty grupy.
- Sprawdź, czy dla krzywej $(1, -1, 11)$ punkt $(4, 1)$ jest generatorem.

Bibliografia

1. "Handbook of Applied Cryptography" - A. Menezes, P. van Oorschot, S. Vanstone
2. "Guide to Elliptic Curve Cryptography" - D. Hankerson, A. Menezes, S. Vanstone