Криптосистеми на еліптичних кривих

Lecture 2: Arithmetics

Грубіян Євген Олександрович

Додавання двох точок на еліптичній кривій

$P = (x_1, y_1), Q = (x_2, y_2), x_1 \neq x_2$ — точки на еліптичній кривій:

$$E/K: \; y^2 = x^3 + ax + b, \mathrm{char}(K) \neq 2, 3$$

Крок 1. Знаходимо нахил прямої $y = \lambda x + c$, що проходить через P та Q:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Крок 2. Ця пряма перетинає нашу криву в 3х точках, координати яких задовольняють також рівняння кривої:

$$(\lambda x + c)^2 = x^3 + ax + b, \tag{1}$$

$$x^3 - (\lambda x + c)^2 + ax + b = 0 \tag{2}$$

Оскільки x_1, x_2, x_3 координати точок є коренями одержаного поліному - коефіцієнт біля x^2 є сумою коренів зі зворотнім знаком за теоремою Вієта:

$$\lambda^2 = x_1 + x_2 + x_3$$

Додавання двох точок на еліптичній кривій

Крок 3. Оскільки сума будь яких трьох різних точок які є точками перетину довільної прямої та кривої визначається як $P + Q + R = \mathcal{O}$, тоді $P + Q$ - відображення третьої точки $R = (x_3, y_3)$ щодо осі x, звідси отримуємо:

$$R = -(P + Q) = (x_3, y_3) \tag{3}$$

$$x_3 = \lambda^2 - x_1 - x_2 \tag{4}$$

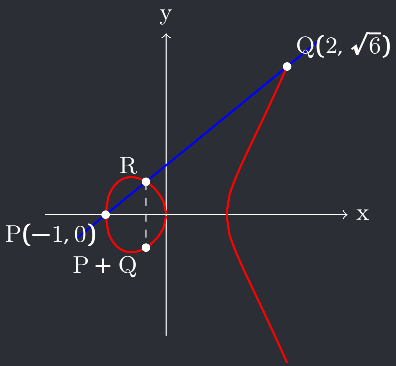
$$y_3 = \lambda(x_3 - x_1) + y_1. \tag{5}$$

Звідси:

$$P + Q = -R = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$$

Зауважимо також що операція додавання точок комутативна, що видно з симетричності формул додавання

Графічна ілюстрація додавання точок в $\mathbb{E}/\mathbb{R}$



Червоним нанесено еліптичну криву $y^2 = x^3 - x$ над полем $\mathbb{R}$. Синя пряма $y = \frac{\sqrt{6}}{3}(x + 1)$ проходить через точки $P = (-1, 0)$ та $Q = (2, \sqrt{6})$ і перетинає криву в третій точці $R = (-\frac{1}{3}, \frac{2\sqrt{6}}{9})$. Відображення R через вісь x дає точку $P + Q = (-\frac{1}{3}, -\frac{2\sqrt{6}}{9})$.

Подвоєння точки на еліптичній кривій

Нехай $P = (x_1, y_1)$ — точка на $E/K: \ y^2 = x^3 + ax + b$ з $y_1 \neq 0$.

Крок 1. Знаходимо нахил дотичної до E в точці P:

$$\lambda = \frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}.$$

Крок 2. Дотична перетинає криву ще в одній точці $R = (x_3, y_3)$, тому за аналогією:

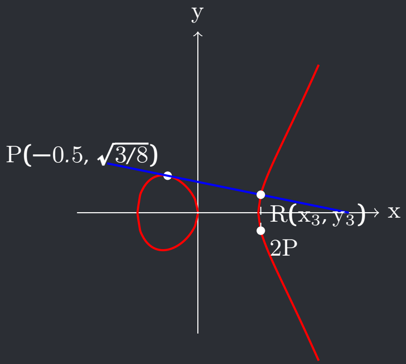
$$x_3 = \lambda^2 - 2x_1 \tag{6}$$

$$y_3 = \lambda(x_3 - x_1) + y_1. \tag{7}$$

Таким чином, подвоєння точки задається формулою:

$$2P = (x_3, -y_3) = (\lambda^2 - 2x_1, \lambda(x_1 - x_3) - y_1)$$

Графічна ілюстрація подвоєння точки в $\mathbb{E}/\mathbb{R}$



Червоним нанесено еліптичну криву $y^2 = x^3 - x$ над R. Синя дотична в точці $P(-0.5, \sqrt{3/8})$ перетинає криву в точці $R(x_3, y_3)$; відображення R через горизонтальну вісь дає $2P = (x_3, -y_3)$.

Скалярний добуток та порядок точки

Часто в криптографії використовують так звану операцію скалярного добутку:

$$Q = [k]P$$

Що означає додати точку P саму до себе k разів

Порядок точки $\mathrm{ord}(P)$

Таке мінімальне число $n \in \mathbb{N}_0$ що $[n]P = \mathcal{O}$ або 0 якщо такого натурального числа не існує.

Проективна площина

Проективна площина $\mathbb{P}^2(K)$ над полем K

$$\mathbb{P}^2(K) = \{(X : Y : Z) \in K^3 \setminus \{(0,0,0)\}\}/\sim,$$

де еквівалентність задана співвідношенням

$$\exists \lambda \in K^\times \quad (X : Y : Z) \sim (\lambda X : \lambda Y : \lambda Z)$$

Перехід між афінними та проективними координатами

$$(X : Y : Z) \xrightarrow{\text{aff}} (X/Z, Y/Z) \tag{8}$$

$$(x, y) \xrightarrow{\text{proj}} (x : y : 1) \tag{9}$$

Проективні координати

Еліптичні криві зручно задавати в проективних координатах, оскільки реалізація арифметики значно ефективніша через відсутність "дорогого"ділення в полі

Еліптична крива над полем K, $\mathrm{char}(K) \neq 2, 3$

Множина точок $P = (X : Y : Z) \in \mathbb{P}^2(\overline{K})$, що задовольняють рівнянню Вейєрштраса:

$$E_{\mathbb{P}}/K : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in K, \quad \Delta = 4a^3 + 27b^2 \neq 0.$$

Зазначимо, що точка на нескінченності перейде в $\mathcal{O} \xrightarrow{\mathrm{proj}} (0 : 1 : 0)$

Формули додавання в проективних координатах

Нехай $P = (X_1 : Y_1 : Z_1)$ та $Q = (X_2 : Y_2 : Z_2)$ — точки на еліптичній кривій, заданій рівнянням

$$Y^2 Z = X^3 + aXZ^2 + bZ^3.$$

Визначимо проміжні змінні:

$$U_1 = Y_1 Z_2, \qquad U_2 = Y_2 Z_1, \qquad V_1 = X_1 Z_2, \qquad V_2 = X_2 Z_1,$$
$$U = U_2 - U_1, \qquad V = V_2 - V_1.$$

При умові $V \neq 0$ координати суми $P + Q = (X_3 : Y_3 : Z_3)$ можна записати як:

$$X_3 = U^2 Z_1 Z_2 - V^3 - 2V^2 V_1,$$
$$Y_3 = U\left(V^3 + 2V^2 V_1 - X_3 V_1\right) - V^3 U_1,$$
$$Z_3 = V^3 Z_1 Z_2.$$

Формули додавання в проективних координатах (спеціальні випадки)

1. Подвоєння точки (коли $P = Q$):
Нехай $P = (X_1 : Y_1 : Z_1)$ — точка еліптичної кривої

$$Y^2 Z = X^3 + aXZ^2 + bZ^3.$$

Визначимо:

$$\begin{aligned} W &= 3X_1^2 + aZ_1^2, \quad S = Y_1 Z_1, \quad B = X_1 Y_1, \quad H = W^2 - 8B, \\ X_3 &= 2SH, \quad Y_3 = W(4B - H) - 8Y_1^2 X_1, \quad Z_3 = 8S^3. \end{aligned}$$

Тоді подвоєння точки записується як:

$$2P = (X_3 : Y_3 : Z_3).$$

2. Якщо $Q = -P$, тобто $Q = (X_1 : -Y_1 : Z_1)$ то $P + (-P) = \mathcal{O}$,

Ілюстрація еліптичної кривої в проективній площині