Лекція 19. Еліптичні криві над скінченними полями.

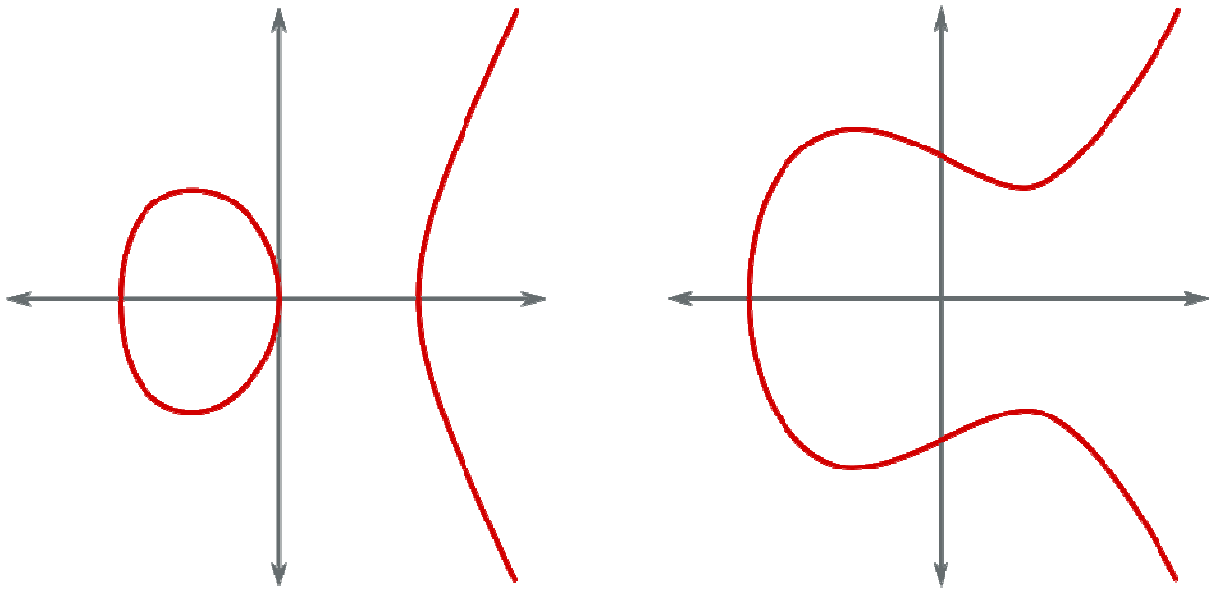
У 1985 р. Н. Кобліц і Х. Міллер незалежно один від одного запропонували використовувати для побудови криптографічних систем алгебраїчні структури, які називають еліптичними кривими над скінченними полями.

З огляду на традицію у випадку еліптичних кривих говорять не про множення елементів, а про їхнє додавання. У цьому разі використовують знак "+" (додавання) замість знака "·" (множення). Замість того, щоб говорити про піднесення до k-го степеня, у випадку еліптичних кривих говорять про k-те кратне.

Еліптична крива над множиною (полем) дійсних чисел – це множина точок (x, y) (пар дійсних чисел), що задовольняють рівняння

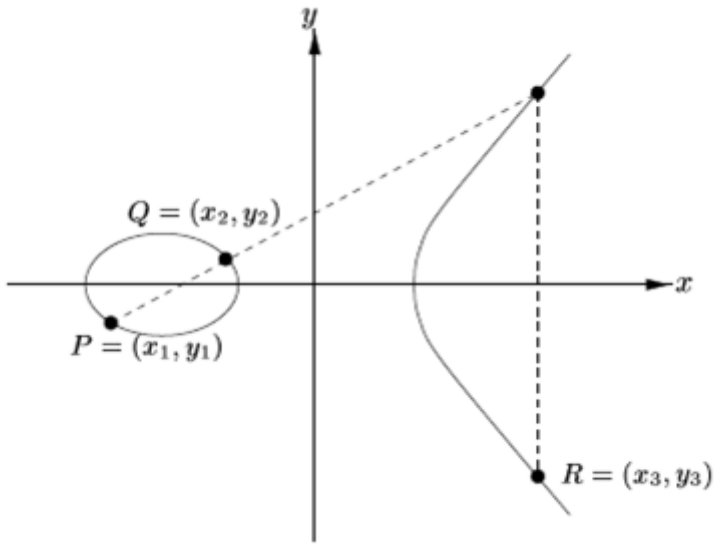
$$y^2 = x^3 + ax + b,$$

де $4a^3 + 27b^2$ відмінне від нуля. Крім того уводять у розгляд додаткову точку **O**, що лежить у нескінченності. Наведене вище рівняння описує криву на площині, вигляд якої залежить від значень параметрів a та b. Умова $4a^3 + 27b^2 \neq 0$ гарантує, що рівняння кривої не має кратних нулів, вилучаючи з розгляду певні специфічні ситуації. Далі наведено приклади еліптичних кривих над полем дійсних чисел.

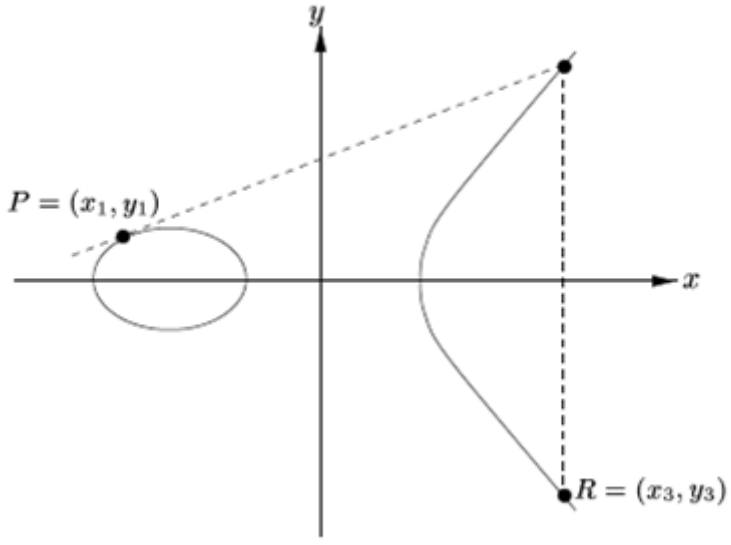


На множині описаних точок задають операцію додавання, що має просту геометричну інтерпретацію. Для отримання суми двох точок необхідно

провести через них пряму. Ця пряма перетинає еліптичну криву в додатковій третій точці. Третя точка, симетрично відбита відносно осі *x*, і є результатом додавання перших двох. Геометрична ілюстрація додавання двох різних точок на еліптичній кривій наведена далі.



Геометрична ілюстрація додавання точки до самої себе (подвоєння) наведена далі.



Описана операція додавання робить множину точок еліптичної кривої абелевою групою, нейтральним елементом якої є точка **O**.

Дійсні числа, які є координатами точок еліптичної кривої, можна замінити на елементи з інших алгебраїчних структур, наприклад на елементи

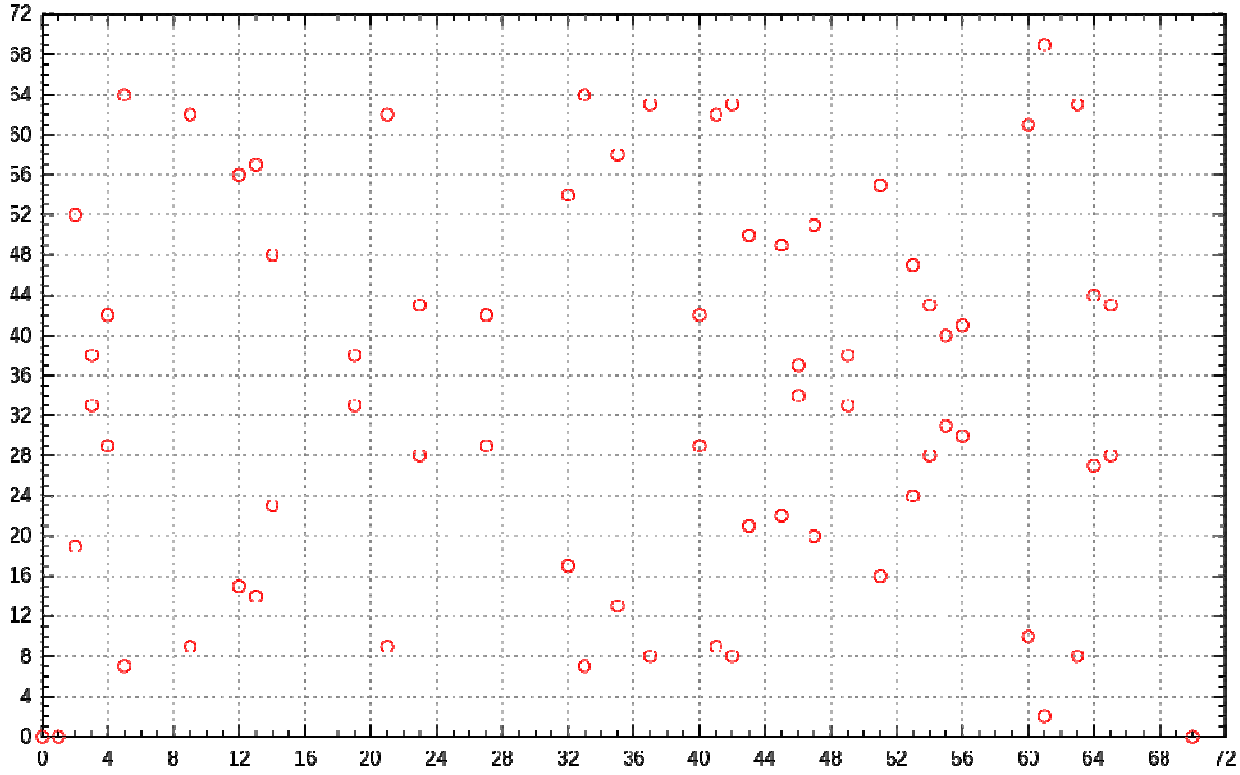
скінченного поля $\mathbf{Z}_p$. У цьому разі всі операції, які розглядаємо далі під час означення еліптичної кривої над скінченним полем $\mathbf{Z}_p$, виконують у $\mathbf{Z}_p$.

Нехай $p > 3$ – просте число, і нехай a та b - такі елементи поля $\mathbf{Z}_p$, що $4a^3 + 27b^2 \neq 0$. Еліптичною кривою E над скінченним полем $\mathbf{Z}_p$ називають множину розв'язків (x, y) рівняння

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

разом з додатковою точкою в нескінченності $\mathbf{O}$.

Множина точок еліптичної кривої $y^2 = x^3 - x$ над скінченним полем $\mathbf{Z}_{71}$ наведена далі.



Задамо бінарну операцію на множині E з використанням адитивного запису так:

$$\mathbf{O} + \mathbf{O} = \mathbf{O};$$

для довільних елементів x, y з множини E:

$$(x, y) + \mathbf{O} = (x, y);$$

для довільних елементів x_1, y_1 з множини E ($y_1 \neq 0$):

$$(x_1, y_1) + (x_1, y_1) = \left(\lambda^2 - 2x_1, \lambda(x_1 - x_2) - y_1\right), \ \lambda \equiv \left(3x_1^2 + a\right)(2y_1)^{-1};$$

для довільних елементів x_1, y_1, x_2, y_2 з множини $E(x_1 \neq x_2)$:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3),\ x_3 \equiv \lambda^2 - x_1 - x_2,\ y_3 \equiv \lambda\,(x_1 - x_3) - y_1,\ \lambda \equiv (y_2 - y_1)(x_2 - x_1)^{-1}.$$

Множина точок еліптичної кривої E із заданою таким способом операцією утворює скінченну абелеву групу.