

Криптосистеми на еліптичних кривих

Lecture 1: The Roots

Грубіян Євген Олександрович

Структура курсу

- Поняття еліптичної кривої, мотивація застосування еліптичних кривих в криптографії
- Форми еліптичних кривих: форми Вейєрштраса, Монтгомері та Едвардса
- Алгебраїчна структура еліптичних кривих, група точок кривої над скінченим полем та її порядок
- Задача дискретного логарифмування ECDLP в групі точок
- Базові криптосистеми, стійкість яких базується на задачі ECDLP: ECDH, ECDSA, EdDSA
- Відображення еліптичних кривих: криві кручення, ізогенії
- Вступ до теорії дівізорів та спарювання Вейля, застосування білінійних спарювань для побудови новітніх криптосистем
- Криптосистеми на основі ізогеній еліптичних кривих

Історія

- Роботи Діофанта, Фібоначчі та ін., що досліджували діофантові рівняння
- XVII-XVIIIст. - роботи Фабіані та Ферма із дослідження довжини дуги еліпса та деяких класів діофантових рівнянь
- XIXст. - роботи Якобі, Абеля та Вейєрштраса, інвертування еліптичного інтеграла, еліптичні (двoperіодичні) функції
- XXст. - роботи Марделла, Вейля, Тейта із топології та алгебри еліптичних кривих
- Ідеї Міллера та Кобліца у 80x роках дали початок застосуванню ЕК в криптографії

Чому нам потрібні еліптичні криві?

- Скінчені абелеві групи, а криптографи люблять їх, особливо циклічні великого простого порядку !
- Теорія чисел, багато результатів якої базовані на теорії ЕК, а криптографи люблять теорію чисел :)
- Довжина ключів порівняно невелика із іншими криптосистемами, а криптографи люблять невеликі ключі
- Білінійне спарювання, а криптографи дуже люблять його (всілякі блокчейни із zk-доказами не дадуть збрехати)
- Це просто красivo

Що таке еліптична крива?

Еліптична крива над полем K

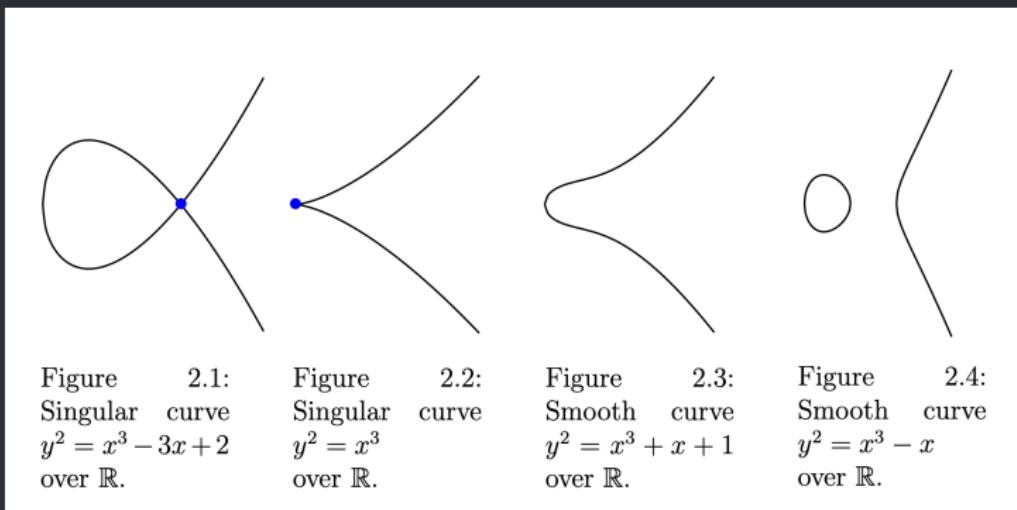
Це гладка проективна алгебраїчна крива першого роду із особливою точкою на нескінченності \mathcal{O}

Не стало краще ? :)



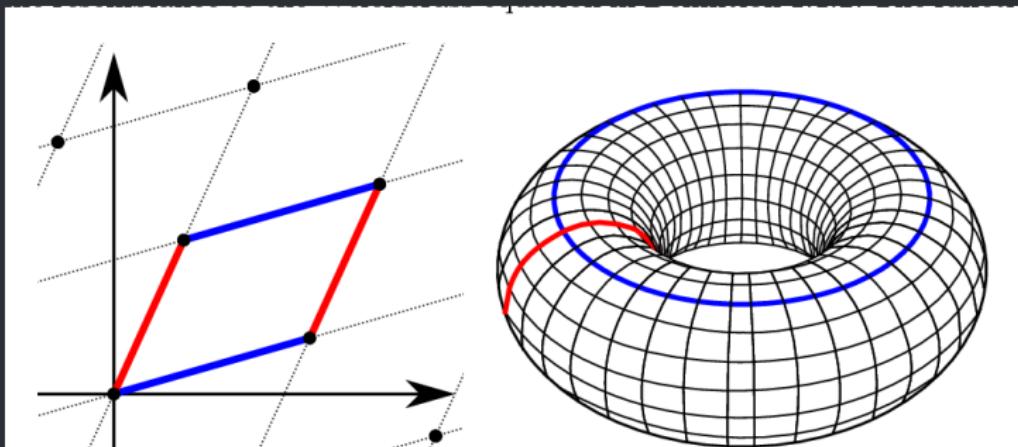
Приклади кривих

Деякі кубічні криві над полем \mathbb{R} , але еліптичними є останні дві



Еліптична крива над \mathbb{C}

Над полем комплексних чисел \mathbb{C} еліптична крива є двoperiodичною мероморфною функцією, що топологічно еквівалентна тору (сфері із 1 ручкою, звідси рід(genus) кривої - 1)



Означення еліптичної кривої

Еліптична крива над полем K

Множина точок $(x, y) \in \bar{K}^2$, що задовольняють рівнянню:

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K, \Delta \neq 0$$

плюс точка на нескінченості \mathcal{O}

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

Множина точок $(x, y) \in \bar{K}^2$, що задовольняють рівнянню
Вейєрштраса:

$$E/K : y^2 = x^3 + ax + b, \quad a, b \in K, \quad \Delta = 4a^3 + 27b^2 \neq 0.$$

плюс точка на нескінченості \mathcal{O}

Група точок

На початку ХХст. Пуанкарє (1901) висловив ідею що К-раціональні точки кривої, координати яких належать полю К утворюють групу(при цьому назвавши це не групою, а *un système des points rationnelles fondamentaux*). В 1922 Марделл довів теорему що група К-раціональних точок є скінченнопородженою абелевою групою.

Теорема Марделла-Вейля

Множина $E(K)$ К-раціональних точок еліптичної кривої E/K утворює скінченнопороджену абелеву групу за операцією додавання точок із нейтральним елементом \mathcal{O}

Додавання точок на кривій

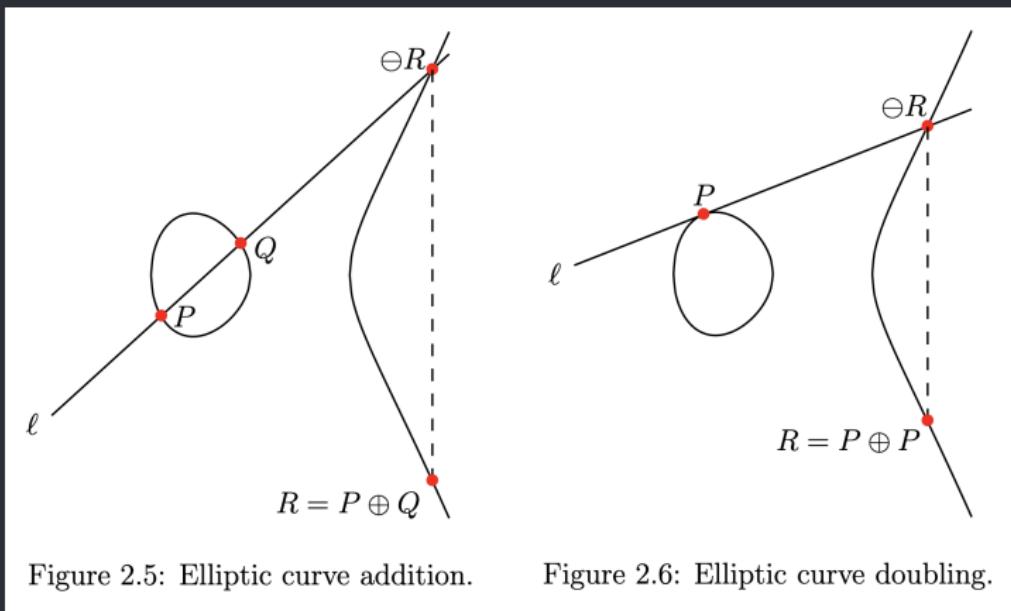


Figure 2.5: Elliptic curve addition.

Figure 2.6: Elliptic curve doubling.

Група точок еліптичної кривої

Груповий закон

1. Точка на нескінченності \mathcal{O} - нейтральний елементр.
2. Якщо $x_P \neq x_Q$, визначимо тангенс кута нахилу прямої між точками $\lambda := \frac{y_P - y_Q}{x_P - x_Q}$. Тоді точка $R = (x_R, y_R) = P \oplus Q$:

$$x_R := \lambda^2 - x_P - x_Q, \quad y_R := \lambda(x_P - x_R) - y_P.$$

3. Якщо $P = Q$, тоді тангенс кута нахилу дотичної в точці P $\lambda := \frac{3x_P^2 + a}{2y_P}$, при цьому $R = (x_R, y_R) = 2P$:

$$x_R := \lambda^2 - 2x_P, \quad y_R := \lambda(x_P - x_R) - y_P.$$

4. Якщо $x_P = x_Q, y_P = -y_Q$, тобто $P = \Theta Q$ тоді $P \oplus Q := \mathcal{O}$.