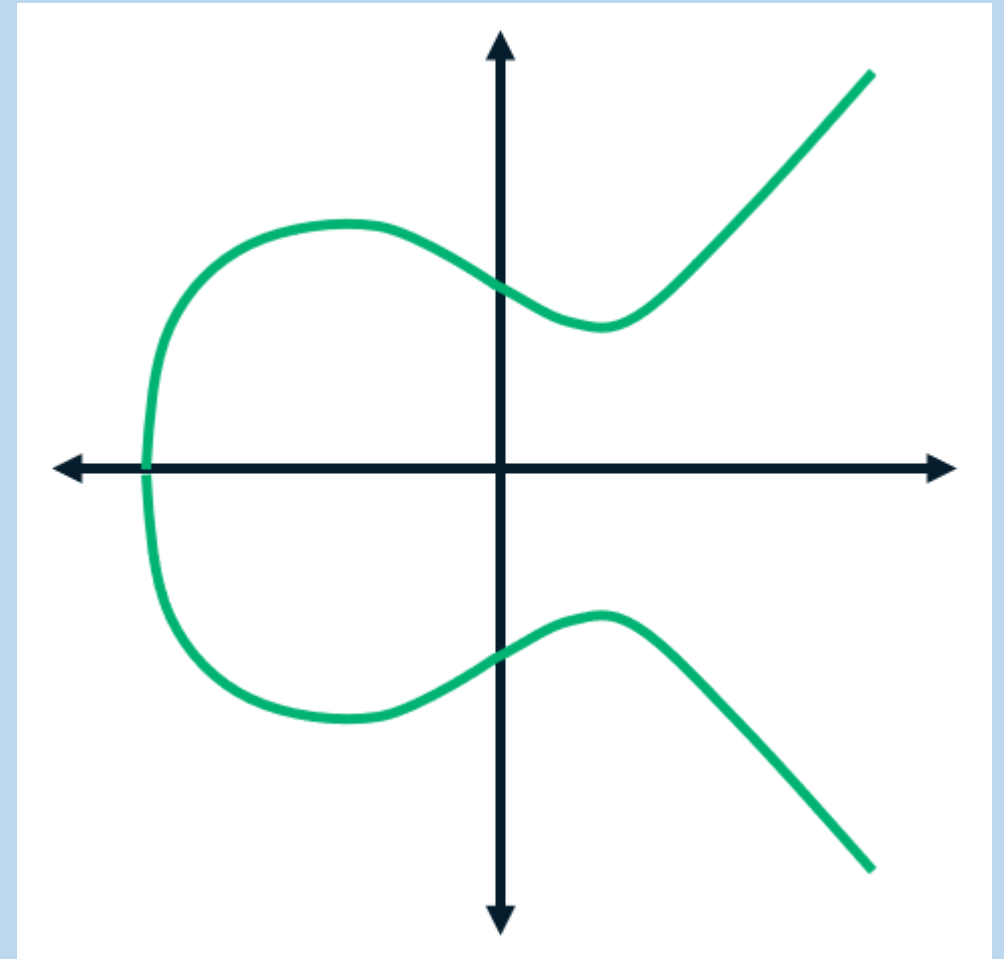


# ЛЕКЦІЯ 8

## ОСНОВИ КРИПТОГРАФІЇ НА ЕЛІПТИЧНИХ КРИВИХ



# План

1. Загальні поняття

2. Операції над точками еліптичних кривих

3. Алгоритм обміну ключами ECDH

4. Стандарт цифрового підпису ECDSA

# 1. Загальні поняття

Використання еліптичних кривих у криптографії було незалежно запропоновано **Нілом Кобліцом** (Neal Koblitz) та **Віктором Міллером** (Victor Miller) у 1985 році

**Криптографія на еліптичних кривих** (Elliptic curve cryptography, **ECC**) вивчає асиметричні криптосистеми, засновані на **еліптичних кривих** над скінченими полями



Ніл  
Кобліц

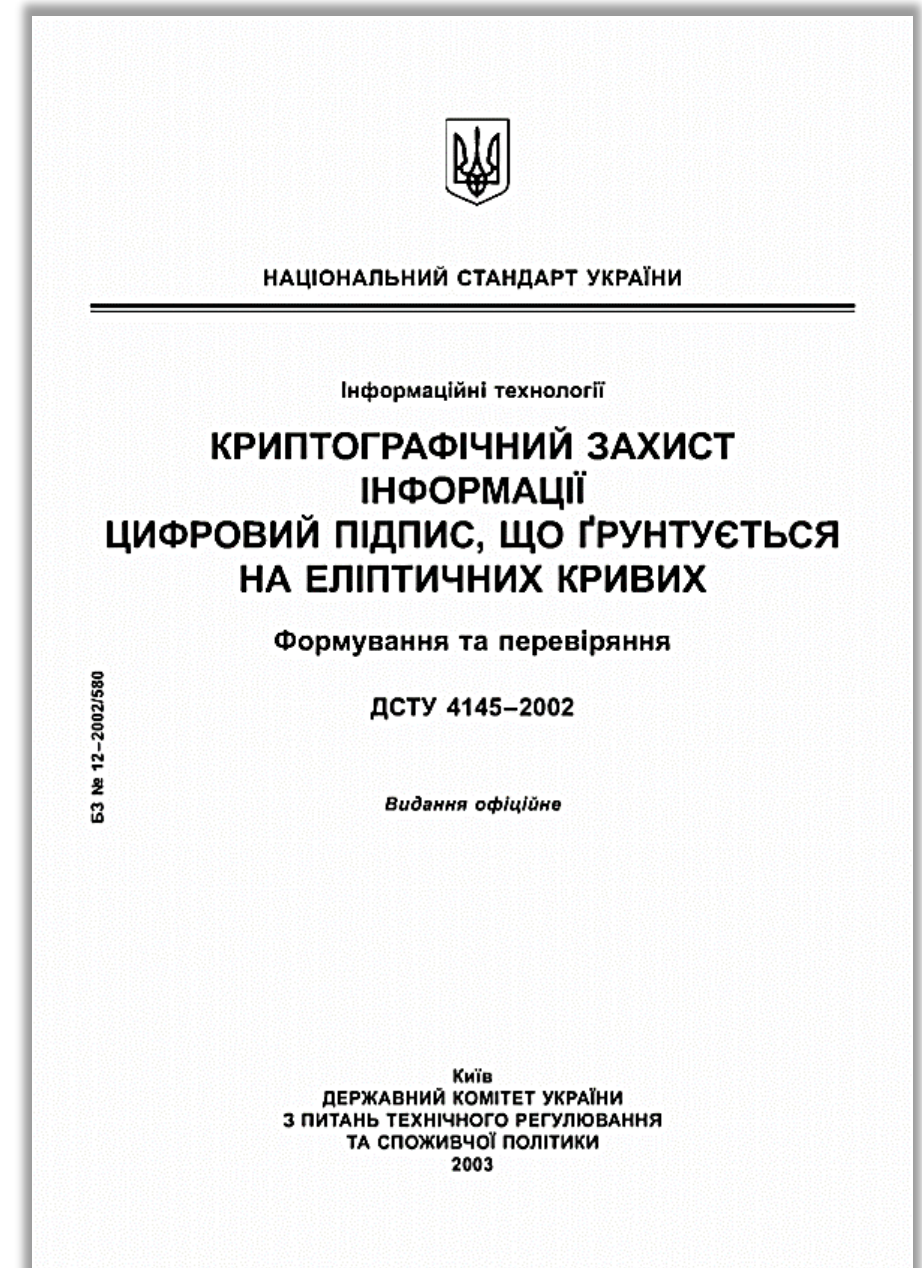


Віктор  
Міллер

# 1. Загальні поняття

З 1998 року використання еліптичних кривих для вирішення криптографічних завдань було закріплено в стандартах США **ANSI X9.62 і FIPS 186-2 (FIPS 186-3 з 2009 року)**

У 2002 році в Україні був прийнятий **ДСТУ 4145-2002** «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка»



# 1. Загальні поняття

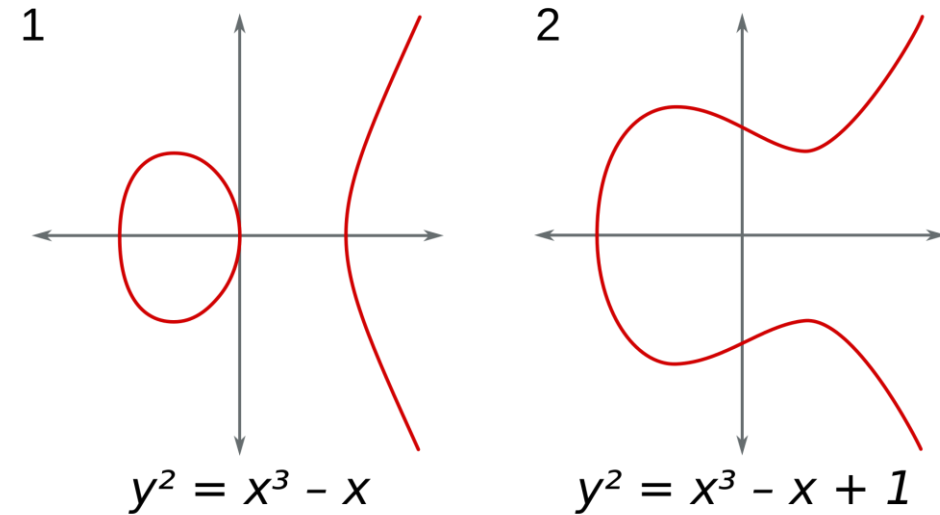
Криптосистеми на еліптичних кривих **забезпечують еквівалентний захист за меншої довжини ключа**

<i>Ступінь захисту (на кожен біт ключа)</i>	<i>Мінімальна довжина ключа (в бітах)</i>	
	<b>RSA/DSA/DH</b>	<b>ECC</b>
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

# 1. Загальні поняття

Рівняння еліптичної кривої у спрощеному вигляді (рівняння Вейєрштрасса):

$$y^2 = x^3 + ax + b \quad (1.1)$$



Так як  $y = \pm\sqrt{x^3 + ax + b}$ , то графік кривої симетричний відносно  $Ox$ .

Дискримінант рівняння:  $D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$ .

- $D < 0$  – три різних дійсних корені (графік 1);
- $D = 0$  – три дійсних корені, два з яких однакові (сингулярна крива);
- $D > 0$  – один дійсний корінь та два комплексних (графік 2).

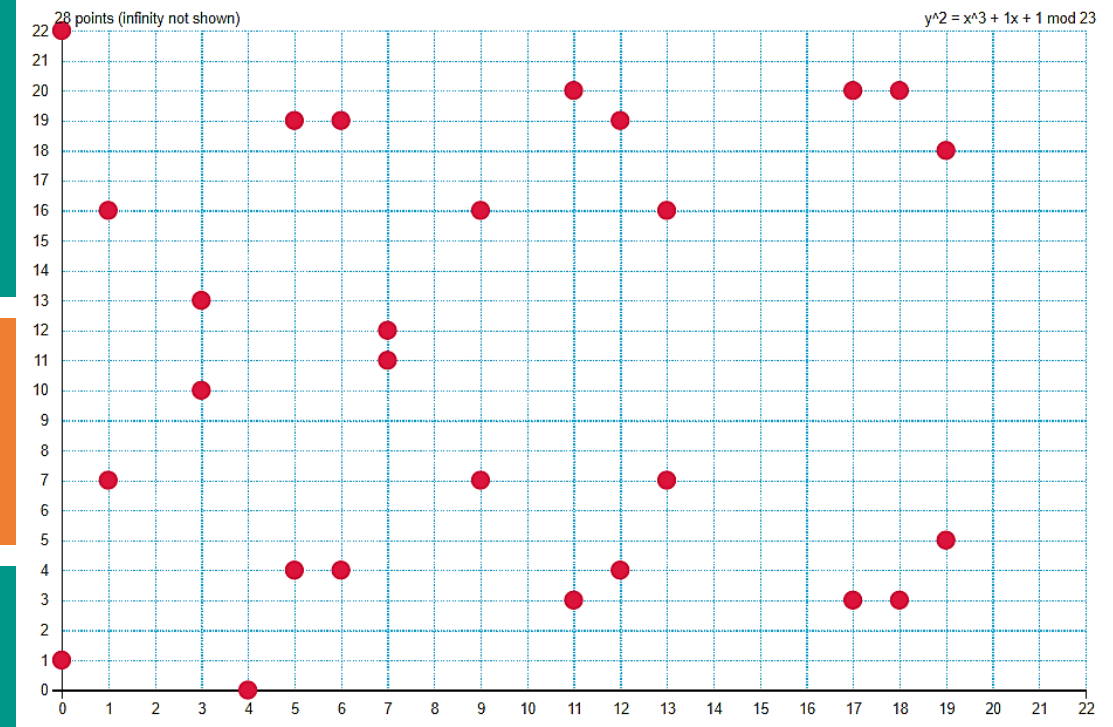
# 1. Загальні поняття

Еліптична крива над скінченним полем  $p$  описується рівнянням:

$$y^2 \equiv x^3 + ax + b \pmod{p} \quad (1.2)$$

$(x, y)$  – точки еліптичної кривої,  
 $a, b$  – параметри кривої,  
 $p$  – просте число ( $p \neq 2, p \neq 3$ ).

При цьому параметри кривої  $a$  та  $b$  мають задовольняти умову

$$4a^3 + 27b^2 \not\equiv 0 \pmod{p}$$




# 1. Загальні поняття

Позначимо через  $E_p(a, b)$  **множину точок** еліптичної кривої. Точка **належить** еліптичній кривій, якщо пара чисел  $(x, y)$  задовольняє рівнянню (1.2).

Кількість точок кривої називається **порядком кривої**.

## Приклад 1.1:

$E_5(2, 1)$  складається з 6 точок, а також точки  $O$ .  
Порядок кривої – 7.

У множину точок еліптичної кривої також включається нескінченно віддалена точка  $O$ .

solve  $y^2 \equiv x^3 + 2x + 1 \pmod{5}$

Solutions in the least residue system:

---

$$x \equiv 0, y \equiv 1 \pmod{5}$$

---

$$x \equiv 0, y \equiv 4 \pmod{5}$$

---

$$x \equiv 1, y \equiv 2 \pmod{5}$$

---

$$x \equiv 1, y \equiv 3 \pmod{5}$$

---

$$x \equiv 3, y \equiv 2 \pmod{5}$$

---

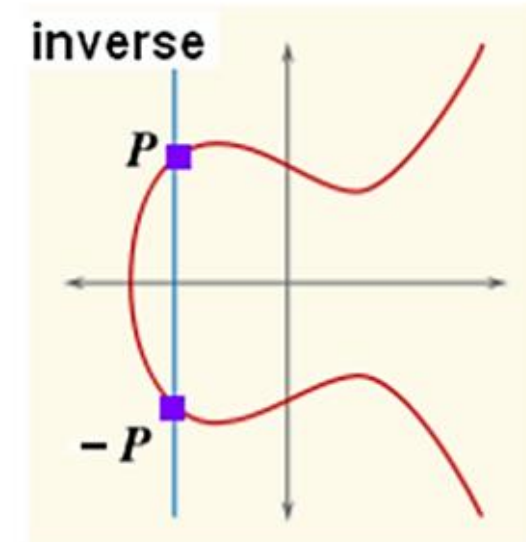
$$x \equiv 3, y \equiv 3 \pmod{5}$$



# 2. Операції над точками еліптичних кривих

## Обернена точка

Оберненою точкою до  $P(x, y)$  називають точку еліптичної кривої  $-P(x, -y)$ .



### Приклад 2.1:

Якщо  $P(3, 2)$  – точка еліптичної кривої  $y^2 \equiv x^3 + 2x + 1 \pmod{5}$ , то точка  $-P(3, -2)$ . Проте  $-2 \pmod{5} = 3$ , тому  $-P(3, 3)$ .

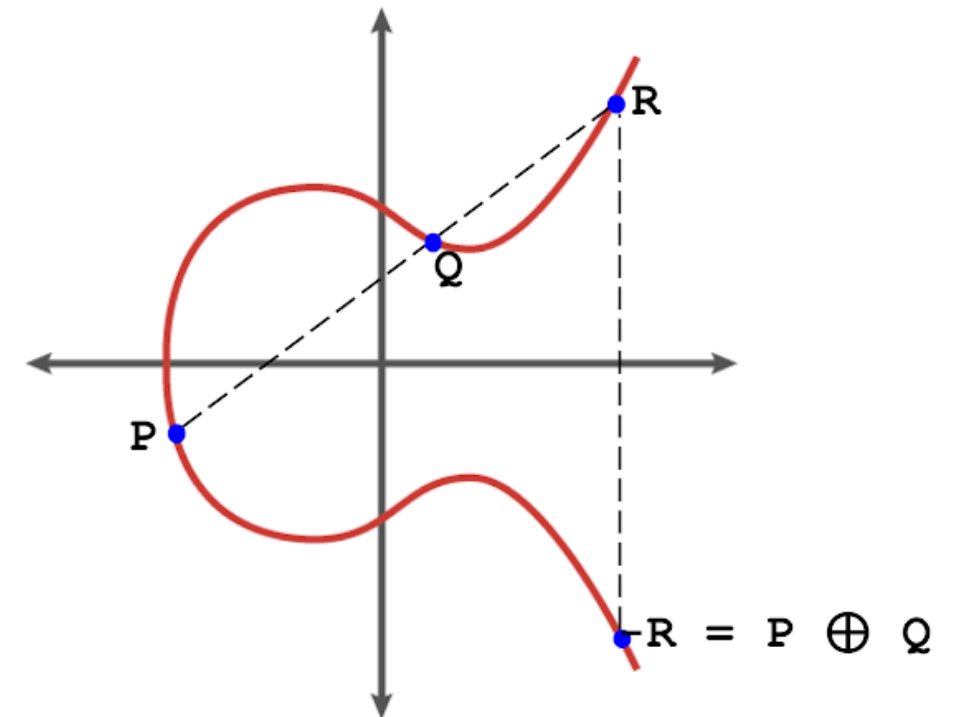
# 2. Операції над точками еліптичних кривих

## Додавання точок

Візьмемо дві різні точки  $P(x_1, y_1)$  та  $Q(x_2, y_2)$ , які належать  $E_p$  і проведемо через них пряму.

Ця пряма обов'язково перетне криву в третій точці  $R$ .

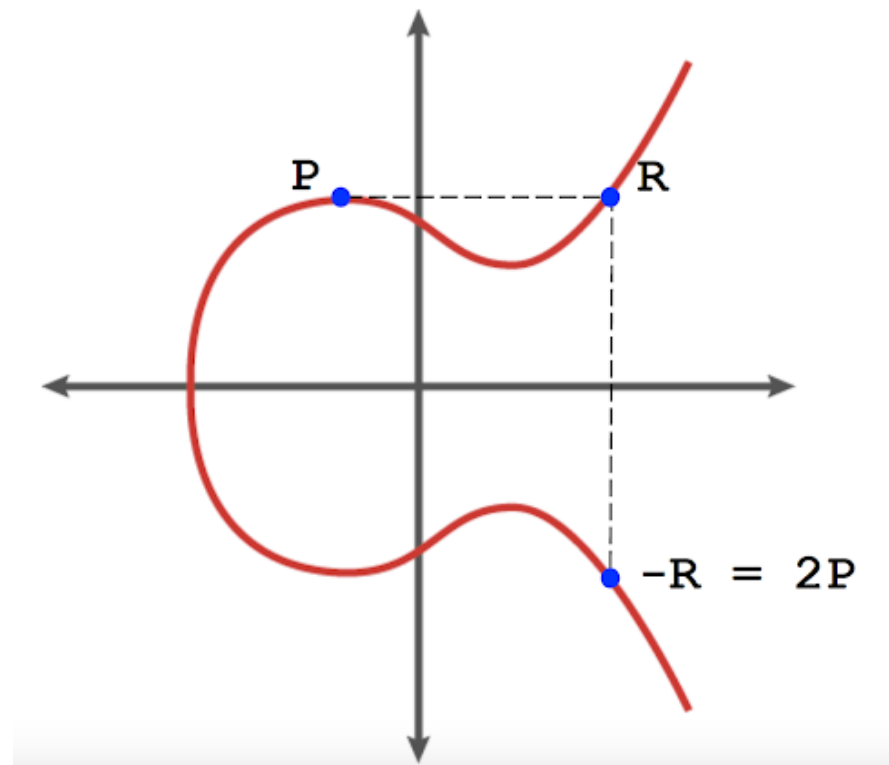
Проведемо через точку  $R$  вертикальну пряму до перетину з кривою у точці  $-R = P \oplus Q$ .



# 2. Операції над точками еліптичних кривих

## Подвоєння точки

Якщо дві точки  $P(x_1, y_1)$  та  $Q(x_2, y_2)$  співпадають, то  $P + Q = P + P$ , що рівнозначно подвоєнню точки  $2P = -R$ .  
При  $P = Q$  січна перетворюється на дотичну, тому точка  $2P$  є оберненою до точки  $R$ .



## 2. Операції над точками еліптичних кривих

Координати  $-R(x_3, y_3)$  визначаються за формулами:

*Додавання точок  
(якщо  $P \neq Q$ )*

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

*Подвоєння точки  
(якщо  $P = Q$ )*

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

$\lambda$  – кутовий коефіцієнт січної, що проведена через точки  $P(x_1, y_1)$  та  $Q(x_2, y_2)$

## 2. Операції над точками еліптичних кривих

### Приклад 2.2:

Рівняння еліптичної кривої має вигляд:

$$y^2 \equiv x^3 + x + 1 \pmod{23} \quad (2.1)$$

Потрібно перевірити чи точки  $P(3, 10)$  та  $Q(9, 7)$  належать кривій та знайти  $P + Q$ .

Підставимо значення  $P(3, 10)$  та  $Q(9, 7)$  у рівняння еліптичної кривої та переконаємося, що точки **належать** кривій:

$$10^2 \equiv 3^3 + 3 + 1 \pmod{23} \rightarrow 100 \pmod{23} \equiv 31 \pmod{23};$$

$$7^2 \equiv 9^3 + 9 + 1 \pmod{23} \rightarrow 49 \pmod{23} \equiv 739 \pmod{23}.$$

## 2. Операції над точками еліптичних кривих

### Приклад 2.2 (продовження):

Виконаємо додавання точок  $P(3, 10)$  та  $Q(9, 7)$ :

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} = \frac{7 - 10}{9 - 3} \pmod{23} = -\frac{3}{6} \pmod{23} = -\frac{1}{2} \pmod{23} = \frac{22}{2} \pmod{23} = 11.$$

Знаходимо:

$$x_3 = \lambda^2 - x_1 - x_2 \pmod{p} = 121 - 3 - 9 \pmod{23} = 109 \pmod{23} = 17$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p} = 11(3 - 17) - 10 \pmod{23} = -164 \pmod{23} = 20.$$

$$\text{Отже } P + Q = (3, 10) + (9, 7) = (17, 20).$$

## 2. Операції над точками еліптичних кривих

### Приклад 2.3:

Додати точки  $P(12, 19)$  та  $Q(5, 4)$  еліптичної кривої 2.1.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} = \frac{4 - 19}{5 - 12} \pmod{23} = \frac{-15}{-7} \pmod{23} = \frac{15}{7} \pmod{23}.$$

Потрібно знайти обернений елемент, розв'язавши рівняння:

$$7 \cdot Z \equiv 1 \pmod{23} \rightarrow Z = 10.$$

$$\lambda = 15 \cdot 10 \pmod{23} = 12.$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod{p} = 144 - 12 - 5 \pmod{23} = 127 \pmod{23} = 12.$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p} = 12(12 - 12) - 19 \pmod{23} = 4 \pmod{23} = 4.$$



## 2. Операції над точками еліптичних кривих

### Приклад 2.4:

Дано точку  $P(5, 4)$  еліптичної кривої 2.1. Знайти  $2P$  та  $3P$ .

$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p} = \frac{3 \cdot 25 + 1}{2 \cdot 4} \pmod{23} = \frac{76}{8} \pmod{23} = \frac{19}{2} \pmod{23}.$$

Знайдемо обернений елемент, розв'язавши рівняння:

$$2 \cdot Z \equiv 1 \pmod{23} \rightarrow Z = 12.$$

$$\lambda = 19 \cdot 12 \pmod{23} = 21.$$

$$x_3 = \lambda^2 - 2x_1 \pmod{p} = 441 - 10 \pmod{23} = 431 \pmod{23} = 17.$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p} = 21(5 - 17) - 4 \pmod{23} = -256 \pmod{23} = 20.$$

Отже  $2P = (17, 20)$ .

## 2. Операції над точками еліптичних кривих

### Приклад 2.4 (продовження):

Далі знайдемо суму точок  $P + 2P = (5, 4) + (17, 20)$ .

$$\lambda = \frac{20-4}{17-5} \pmod{23} = \frac{16}{12} \pmod{23} = \frac{4}{3} \pmod{23}.$$

Знайдемо обернений елемент, розв'язавши рівняння:

$$3 \cdot Z \equiv 1 \pmod{23} \rightarrow Z = 8.$$

$$\lambda = 4 \cdot 8 \pmod{23} = 9.$$

$$x_3 = 9^2 - 5 - 17 \pmod{23} = 81 - 22 \pmod{23} = 13.$$

$$y_3 = 9(5 - 13) - 4 \pmod{23} = 9 \cdot (-8) - 4 \pmod{23} = -76 \pmod{23} = 16.$$

Отже  $3P = (13, 16)$ .

## 2. Операції над точками еліптичних кривих

Множина точок еліптичної кривої  $E_p(a, b)$  разом із введеною точкою на нескінченності  $O$  утворює **комутативну групу** щодо операції додавання точок. Для цього виконуються усі необхідні властивості:

Якщо  $P$  і  $Q \in E_p(a, b)$ , то  $P + Q \in E_p(a, b)$  – замкнутість;

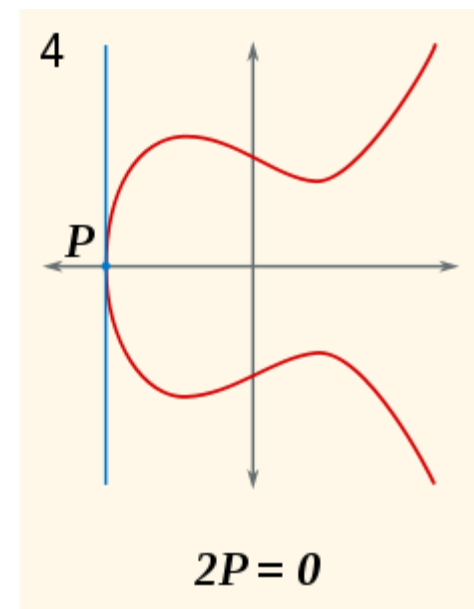
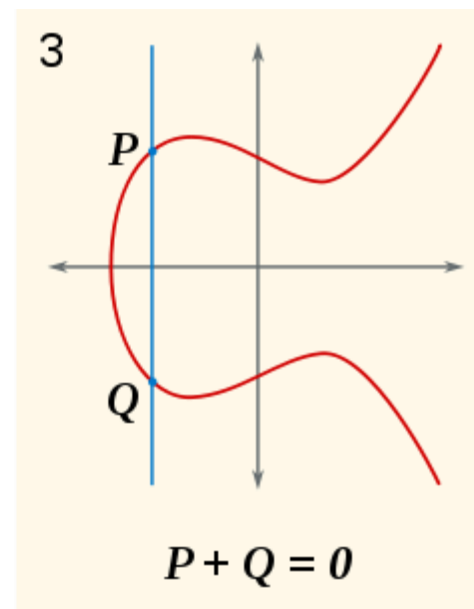
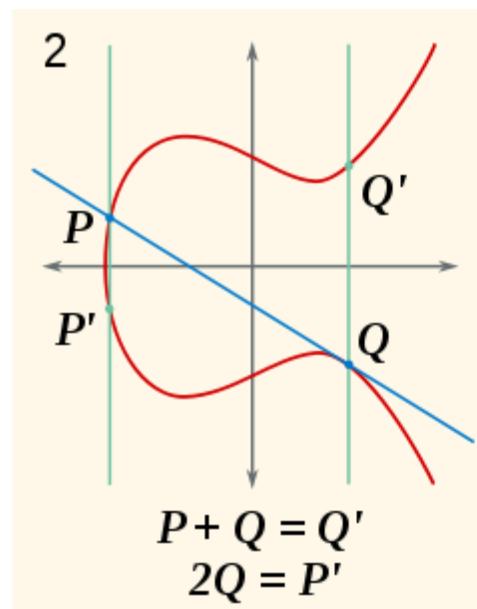
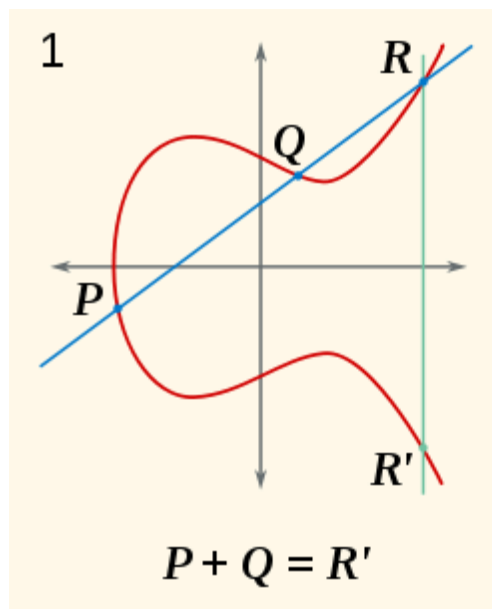
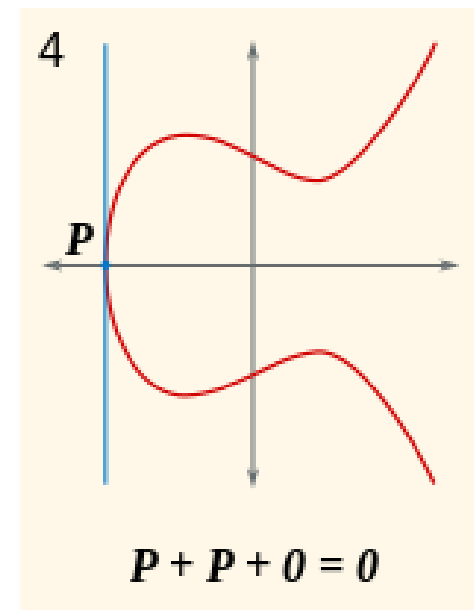
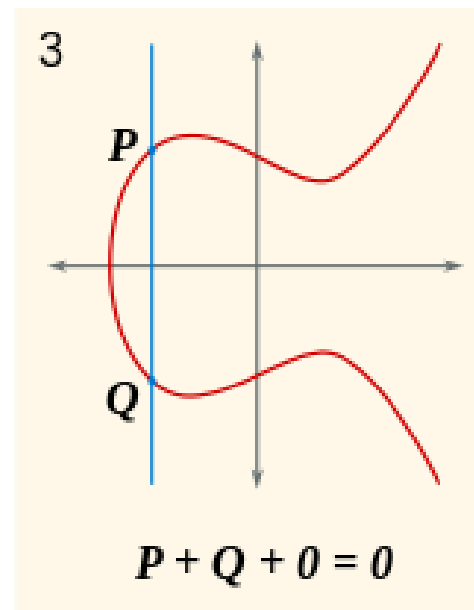
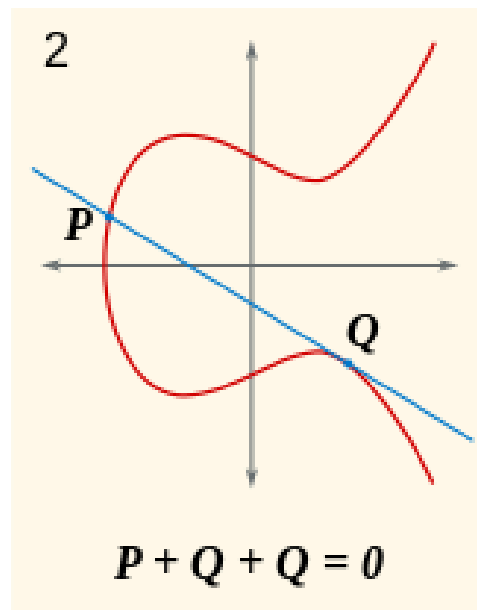
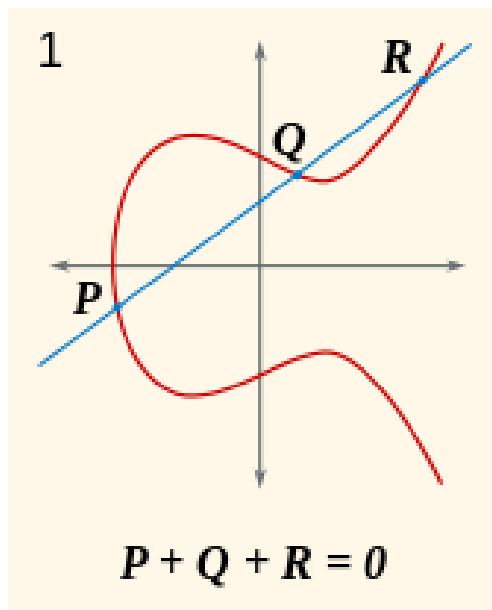
$P + Q = Q + P$  – комутативність;

$(P + Q) + R = P + (Q + R)$  – асоціативність;

$P + (-P) = O$  – обернений елемент;

$P + O = O + P = P$  – нейтральний елемент.

# 2. Операції над точками еліптичних кривих



# 2. Операції над точками еліптичних кривих

## Скалярне множення точки на число

Із попередніх операцій додавання точок та подвоєння точки впливає операція скалярного множення точки на число.

$$2P = P + P$$

$$3P = P + P + P$$

...

$$mP = \underbrace{P + P + P + \dots + P}_{m \text{ разів}}$$

$m$  разів

### Приклад 2.5:

Щоб знайти  $13P$  потрібно  $13_{10} = 1101_2 \rightarrow 13P = 8P + 4P + P$ .

## 2. Операції над точками еліптичних кривих

### Порядок точки

**Порядком точки** еліптичної кривої називають найменше натуральне число  $n$ , при якому  $nP = O$ .

### Приклад 2.6:

Рівняння еліптичної кривої має вигляд:

$$y^2 \equiv x^3 + x + 1 \pmod{5} \quad (2.3)$$

Потрібно знайти порядок точки  $P(2, 4)$ .

## 2. Операції над точками еліптичних кривих

**Приклад 2.6 (продовження):**

**$2P$ :**

$$\lambda = \frac{3 \cdot 2 + 1}{2 \cdot 4} \pmod{5} = \frac{7}{8} \pmod{5} = 14 \pmod{5} = 4.$$

$$x_3 = 16 - 4 \pmod{5} = 2.$$

$$y_3 = 4(2 - 2) - 4 \pmod{5} = 4 \pmod{23} = 1.$$

Виконаємо:  $P(2, 1) + P(2, 4)$ .

**$3P = 2P + P = O$ :**

$$\lambda = \frac{4 - 1}{2 - 2} \pmod{5} = \infty.$$

Таким чином порядок точки  $P(2, 4)$ , що належить еліптичній кривій (2.3) дорівнює 3.



## 2. Операції над точками еліптичних кривих

Стійкість криптосистем, побудованих на еліптичних кривих визначається складністю виконання **завдання дискретного логарифмування у групі точок еліптичної кривої**

**Пряма задача:**  $tP = Q$  (скалярне множення – аналог піднесення до степеню в звичайних асиметричних шифрах)

**Зворотна задача:** знаючи точки  $P$  та  $Q$  знайти  $t$  важко (дискретне логарифмування у групі точок еліптичної кривої)

## 2. Операції над точками еліптичних кривих

Точка  $G \in E_p(a, b)$  називається **базовою точкою** підгрупи точок еліптичної кривої  $E_p(a, b)$ , якщо будь-яка точка  $P$  цієї підгрупи може бути подана у вигляді  $P = tG$ , де  $t = 1, 2, \dots, n$ , де  $n$  – порядок підгрупи.

Для базової точки  $G$  має місце рівність  $nG = O$ .

### Приклад 2.7:

Точка  $G = (0, 1)$  є базовою точкою для групи точок еліптичної кривої  $y^2 \equiv x^3 + x + 1 \pmod{5}$ . Вона генерує усі інші точки підгрупи:

$$G = (0, 1) \rightarrow 2G = (4, 2) \rightarrow 3G = (2, 1) \rightarrow 4G = (3, 4) \rightarrow 5G = (3, 1) \rightarrow 6G = (2, 4) \rightarrow 7G = (4, 3) \rightarrow 8G = (0, 4) \rightarrow 9G = O$$

# 3. Алгоритм обміну ключами ECDH

## Алгоритм Діффі-Хелмана на еліптичних кривих

1. Абоненти  $A$  і  $B$  спільно обирають просте число  $p$  та параметри еліптичної кривої  $a$  та  $b$ .
2. У групі точок еліптичної кривої  $E_p(a, b)$  також обирається спільна базова точка  $G = (x, y)$ , що має дуже великий порядок  $n$ .
3. Абонент  $A$  обирає  $x < n$ , обчислює  $X_A = xG$  та відправляє його  $B$ .
4. Абонент  $B$  обирає  $y < n$ , обчислює  $Y_B = yG$  та відправляє його  $A$ .
5. Абонент  $A$  обчислює закритий ключ за формулою  $K_A = xY_B$ .
6. Користувач  $B$  обчислює закритий ключ за формулою  $K_B = yX_A$ .

# 3. Алгоритм обміну ключами ECDH

## Приклад 3.1:

1.  $p = 23, a = -2, b = 15$ , тобто  $y^2 \equiv x^3 - 2x + 15 \pmod{23}$ .

2.  $G = (4, 5)$ .

3.  $x = 3$ , обчислимо  $X_A = 3G = 2G + G = (13, 22)$ .

4.  $y = 7$ , обчислимо  $Y_B = 7G = 2G + 4G + G = (17, 8)$ .

5.  $K_A = 3Y_B = 2Y_B + Y_B = (15, 5)$ .

6.  $K_B = 7X_A = 2X_A + 4X_A + X_A = (15, 5)$ .

**Секретний ключ**, обчислений обома сторонами –  $(15, 5)$ .

# 4. Стандарт цифрового підпису ECDSS

Алгоритм ЕЦП DSS, який заснований на застосуванні еліптичної кривої називається **ECDSS** (Elliptic Curve Digital Signature Scheme).

Для створення цифрового підпису використовується алгоритм **ECDSA** (Elliptic Curve Digital Signature Algorithm)



# 4. Стандарт цифрового підпису ECDSS

## Генерація ключів

1. Обираються просте число  $p$  та параметри еліптичної кривої  $a$  та  $b$ .
2. Обираються базова точка  $G = (x, y)$  та  $n$  (просте число), таке що  $nG = O$ .
3. Закритий ключ  $d$  – випадкове ціле число, таке що  $0 < d \leq n - 1$
4. Обчислюється відкритий ключ  $Q = dG$ .

# 4. Стандарт цифрового підпису ECDSS

## Підпис повідомлення

Якщо розмірність  $n$  в бітах менше розмірності в бітах хеш-значення  $h(M)$ , то використовуються тільки ліві біти хеш-значення –  $z$

1. Вибирається випадкове ціле число  $k$  – разовий секретний ключ, де  $0 < k \leq n - 1$

2. Обчислюється  $(x_1, y_1) = kG$

3. Обчислюється  $r = x_1 \bmod n$ . Якщо  $r = 0$ , то повертаємося до п. 1.

4. Обчислюється  $s = k^{-1}(z + dr) \bmod n$ . Якщо  $s = 0$ , то повертаємося до п. 1.

5. Підписом для повідомлення  $M$  є пара  $(r, s)$ .



# 4. Стандарт цифрового підпису ECDSS

## Перевірка підпису

1. Отримується  $(r, s)$  та підтверджене значення відкритого ключа  $Q$ .
2. Обчислюється  $w = s^{-1} \bmod n$
3. Обчислюється  $u_1 = z \cdot w \bmod n$
4. Обчислюється  $u_2 = r \cdot w \bmod n$
5. Обчислюється  $(x_1, y_1) = u_1G + u_2Q$
6. Якщо  $(x_1, y_1) = O$  – підпис недійсний.
7. Якщо  $r \equiv x_1 \bmod n$  – підпис дійсний.

# 4. Стандарт цифрового підпису ECDSS

**Приклад 4.1:** Підписати та перевірити підпис повідомлення  $M$  хеш-значення, якого  $z = 10$ .

## Генерація ключів

1.  $p = 23, a = -2, b = 15$ , тобто  $y^2 \equiv x^3 - 2x + 15 \pmod{23}$ ;
2.  $G = (4, 5); n = 23$ ;
3.  $d = 3$  – **закритий ключ**;
4.  $Q = dG = 3G = 2G + G = (13, 22)$  – **відкритий ключ**.

# 4. Стандарт цифрового підпису ECDSA

**Приклад 4.1:** Підписати та перевірити підпис повідомлення  $M$  хеш-значення, якого  $z = 10$ .

## Підписування

Сесійний ключ:  $k = 19$

$$kG = 19G = (9, 17)$$

$$r = 9 \bmod 23 = 9.$$

$$\begin{aligned} s &= 19^{-1}(10 + 3 \cdot 9) \bmod 23 \\ &= 629 \bmod 23 = 8 \end{aligned}$$

$$19^{-1} \bmod 23 = 17$$

(за розширеним алгоритмом Евкліда)

## Перевірка підпису

Відомо  $M$ ,  $(9, 8)$  та  $Q = (13, 22)$

$$w = 8^{-1} \bmod 23 = 3$$

$$u_1 = 10 \cdot 3 \bmod 23 = 7$$

$$u_2 = 9 \cdot 3 \bmod 23 = 4$$

$$\begin{aligned} 7G + 4Q &= (17, 8) + (10, 2) \\ &= (9, 17) \end{aligned}$$

$9 \equiv 9 \bmod 23$  – підпис дійсний