# Сетевые технологии

## ECC (Elliptic Curve Cryptography) — криптография на эллиптических кривых [1]

Соловьев А. В.

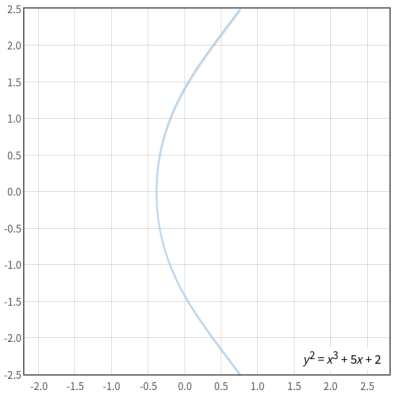
ПетрГУ

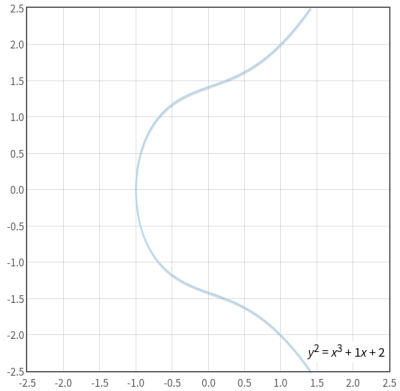
(Rev. 2024 10 25)

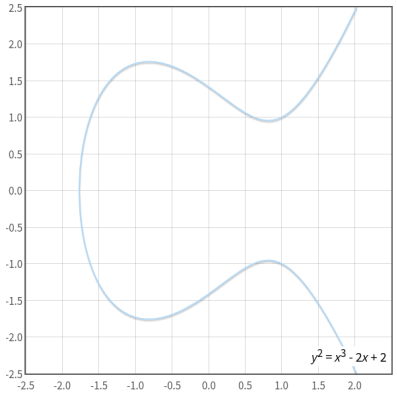
[1] По материалам *Andrea Corbellini "Elliptic Curve Cryptography: a gentle introduction"* https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

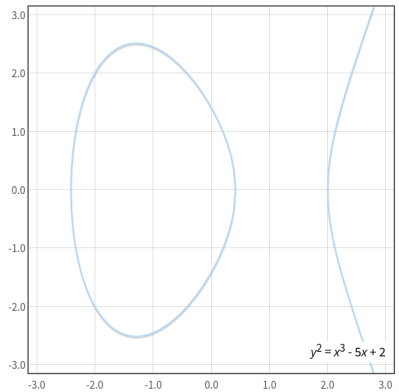
# Эллиптические кривые (ЭК)

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

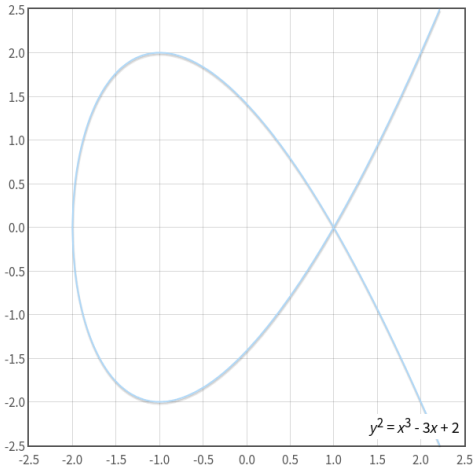


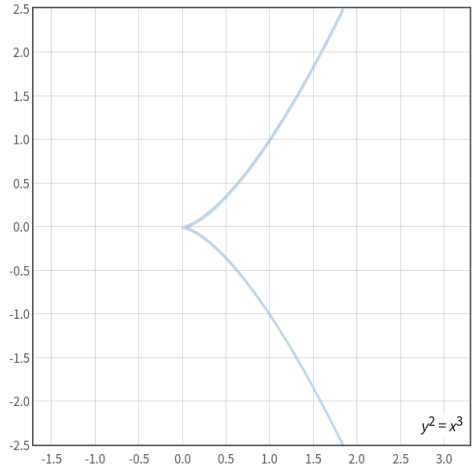







Кривые с *особенностями*: $4a^3 + 27b^2 = 0$





# Множество, группа, «сложение»

Множество: точки ЭК и бесконечно удалённая точка — $O$.

$$\mathbb{G} : \left\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\right\} \cup \{O\}$$

Групповая операция $(+)$:

- Замыкание: $\alpha \in \mathbb{G}, \beta \in \mathbb{G} \Rightarrow \alpha + \beta \in \mathbb{G}$.
- Ассоциативность: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
- Существует *нейтральный элемент* $O$: $\alpha + O = O + \alpha = \alpha$.
- Существует *обратный элемент*:
  $\forall \alpha \in \mathbb{G} \quad \exists \beta \in \mathbb{G} : \alpha + \beta = O \quad (\beta = -\alpha)$.

---

- Коммутативность: $\alpha + \beta = \beta + \alpha$.

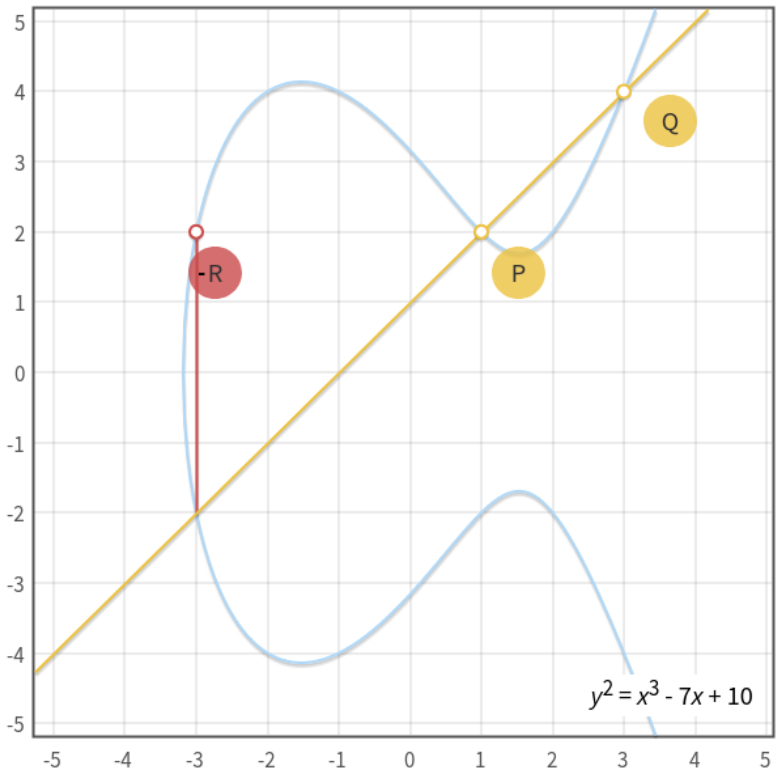
$\Rightarrow$ *абелева группа*

# «Сложение» точек ЭК

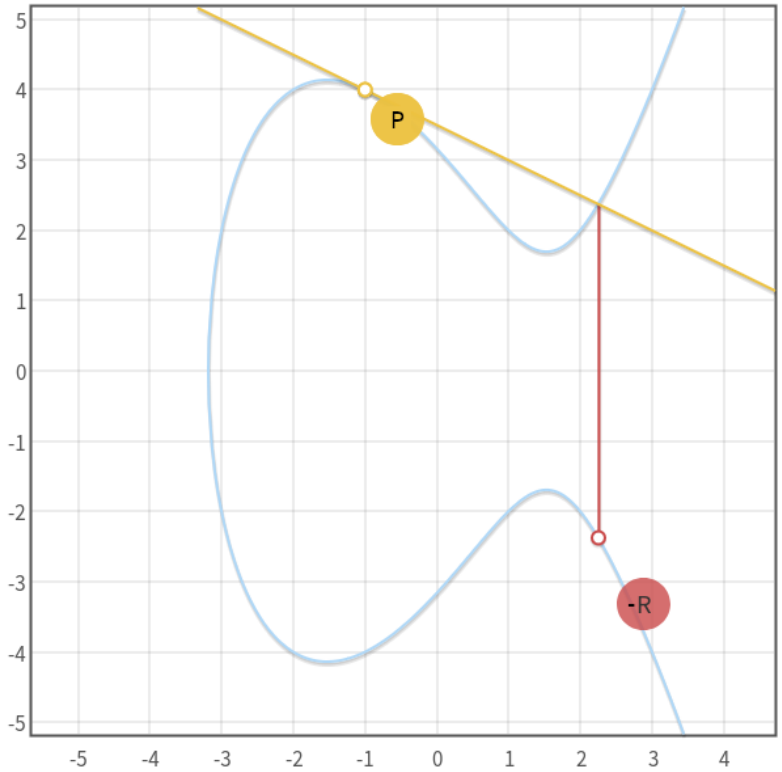
*Обратный элемент* точки $P$ — это точка, симметричная ей относительно оси OX.

Сумма трёх точек ЭК, лежащих на одной прямой, равна *нейтральному элементу*: $P + Q + R = O$.

Таким образом, $P + Q = -R$:

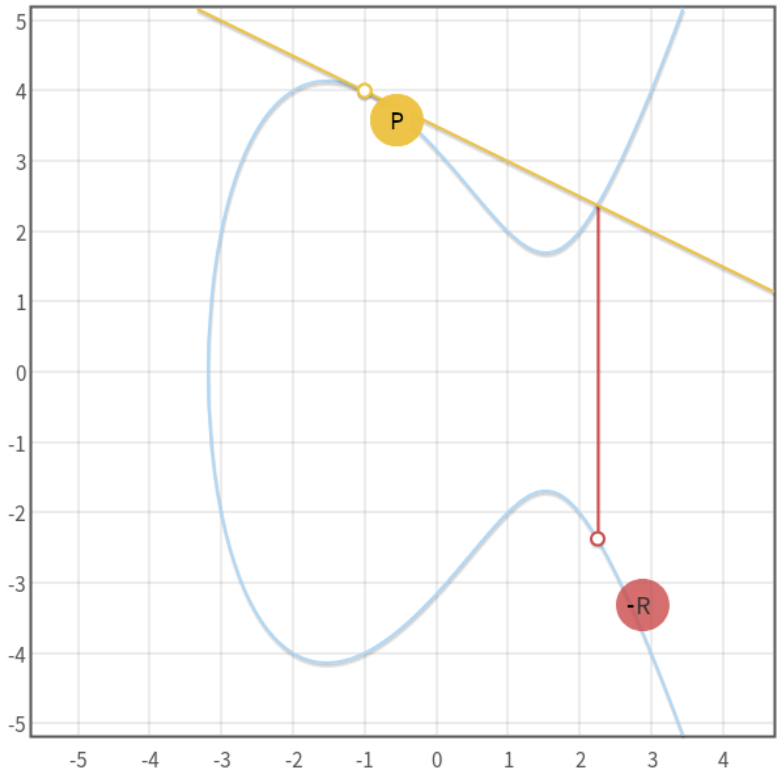



А если $P = Q$?



# Скалярное «умножение»

$$P + P = 2P = R'$$




Скалярное умножение ($n \in \mathbb{N}$):

$$R = nP = P + P + \ldots + P \quad (n \text{ раз})$$

Для реализации можно использовать алгоритм удвоения-сложения.
Например, $n = 37$:

$$37P = 32P + 4P + P$$

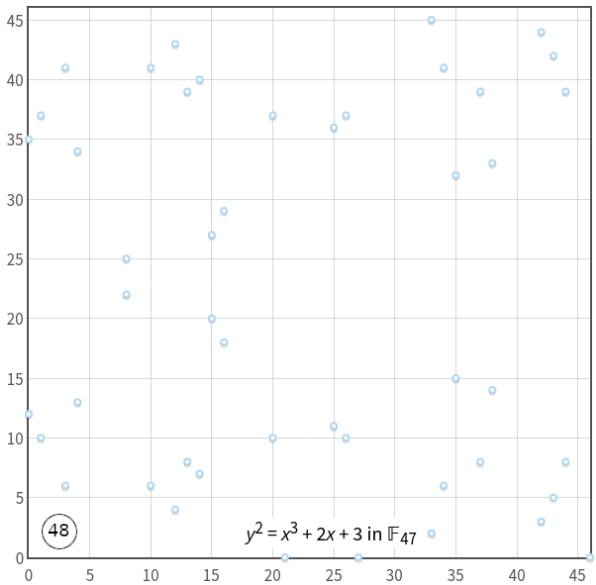
---

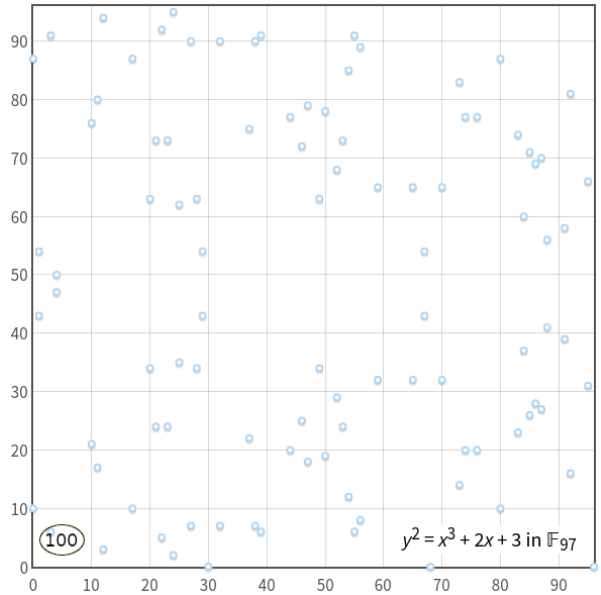
Обратная задача: при известных $P$ и $R$ найти $n$ — «*логарифмирование*».

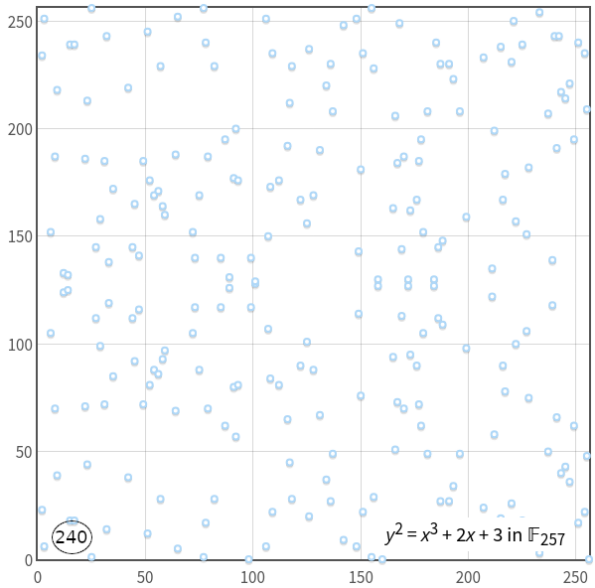
# ЭК над конечными полями

$$\left\{(x,y) \in (\mathbb{F}_p)^2 \mid y^2 = x^3 + ax + b \pmod p,\ 4a^3 + 27b^2 \neq 0 \pmod p\right\} \cup \{O\}$$

$p$ — должно быть простым!



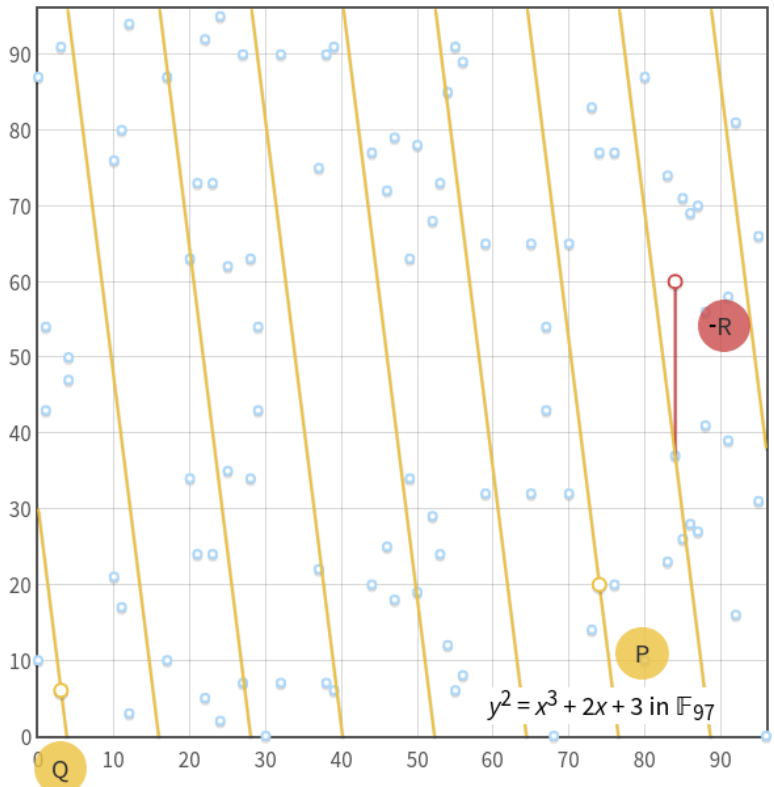

Симметрия относительно $y = p/2$

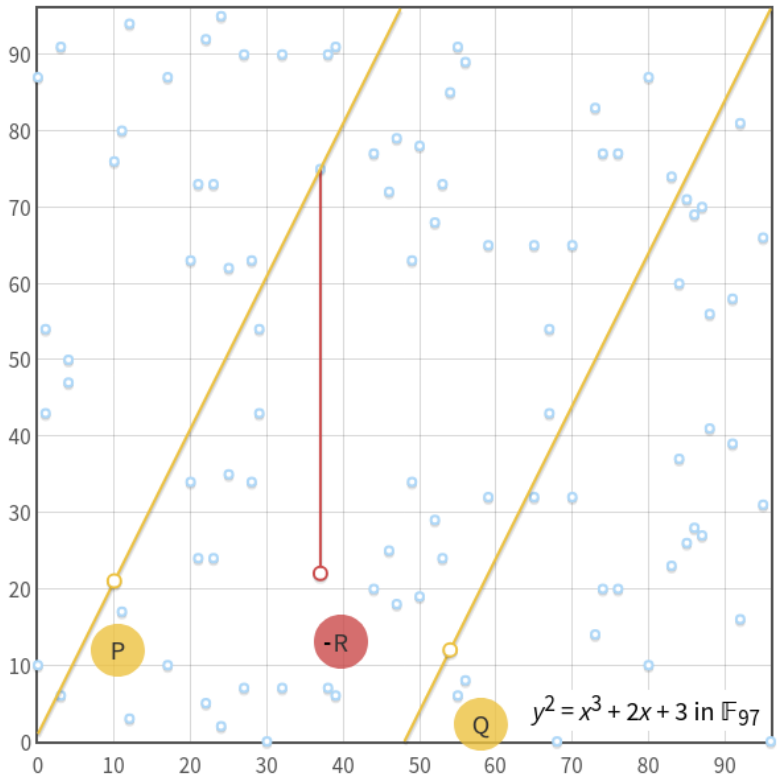
*Порядок группы* $N$ = количество точек (алгоритм Шуфа).

# «Сложение» точек

$P + Q + R = O$, где P, Q, R — точки одной «прямой».

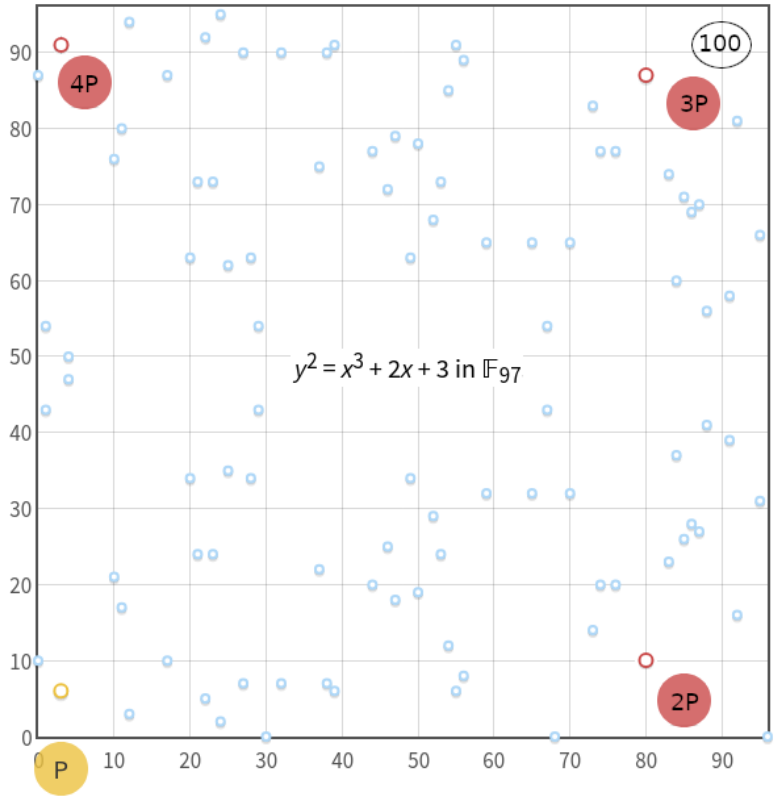
«Прямая» на $\mathbb{F}_p$ — это $\alpha x + \beta y + \gamma \equiv 0 \pmod{p}$.



# Скалярное «умножение», пример 1

Множество кратных $P$ значений — это *циклическая подгруппа группы*, образованной ЭК.




Для точки $P = (3; 6)$:

$0P = O$

$1P = (3; 6)$

$2P = (80; 10)$

$3P = (80; 87)$

$4P = (3; 91)$

$5P = O$

$6P = (3; 6)$

$7P = (80; 10)$

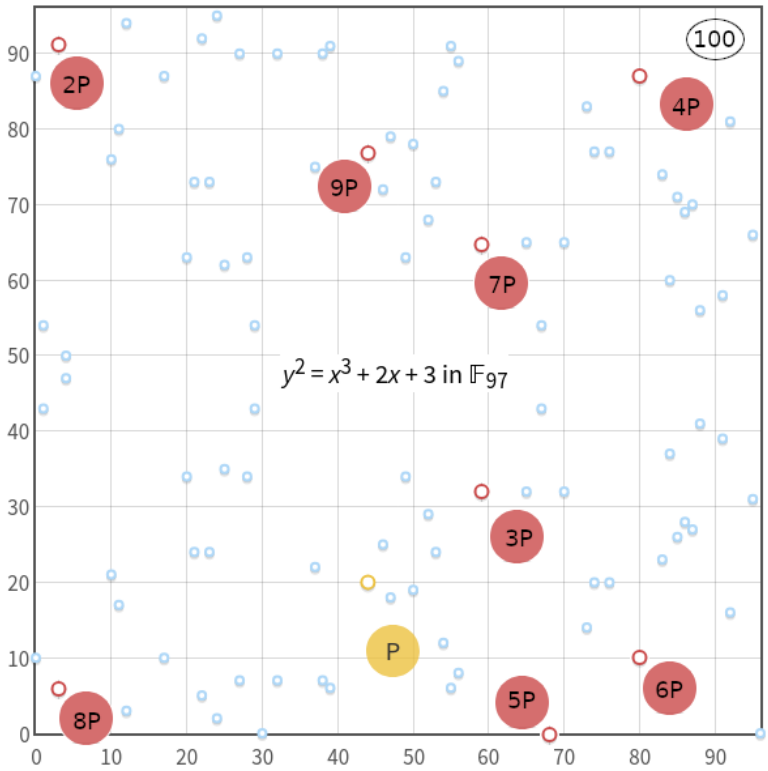
$8P = (80; 87)$

$9P = (3; 91)$

...

$P$ называется *генератором*, или *базовой точкой* циклической подгруппы.

# Скалярное «умножение», пример 2




Для точки $P = (44; 20)$:

$0P = O$

$1P = (44; 20)$

$2P = (3; 91)$

$3P = (59; 32)$

$4P = (80; 87)$

$5P = (68; 0)$

$6P = (80; 10)$

$7P = (59; 65)$

$8P = (3; 6)$

$9P = (44, 77)$

$10P = O$

...

*Порядок подгруппы* $n$ равен одному из делителей порядка исходной группы $N$.

# Выбор базовой точки

$$\forall P : NP = O,\ N = nh,\ n(hP) = O$$

Требуется подгруппа с высоким порядком $n$.

1. Вычисляется порядок ЭК $N$ (алгоритм Шуфа).
2. Выбирается порядок подгруппы $n$ (простое, делитель $N$).
3. Вычисляется *кофактор подгруппы* $h = N/n$.
4. Выбирается случайная точка $P$.
5. Вычисляется $G = hP$. Если $G = O$, то goto 4. Иначе $G$ — генератор группы с порядком $n$.

# Криптография на ЭК

Публичные параметры алгоритма: $a, b, p, G, n, h$.
Закрытый ключ: случайное $d$ из диапазона $[1, ..., n-1]$.
Открытый ключ: точка $H = dG$.

Пример Д-Х на ЭК (ECDH):

Алёна: $d_A,\ H_A = d_A G$

Алёна $\rightarrow$ Вася: $H_A$

Вася: $d_B,\ H_B = d_B G,\ S = d_B H_A$

Вася $\rightarrow$ Алёна: $H_B$

Алёна: $S = d_A H_B$

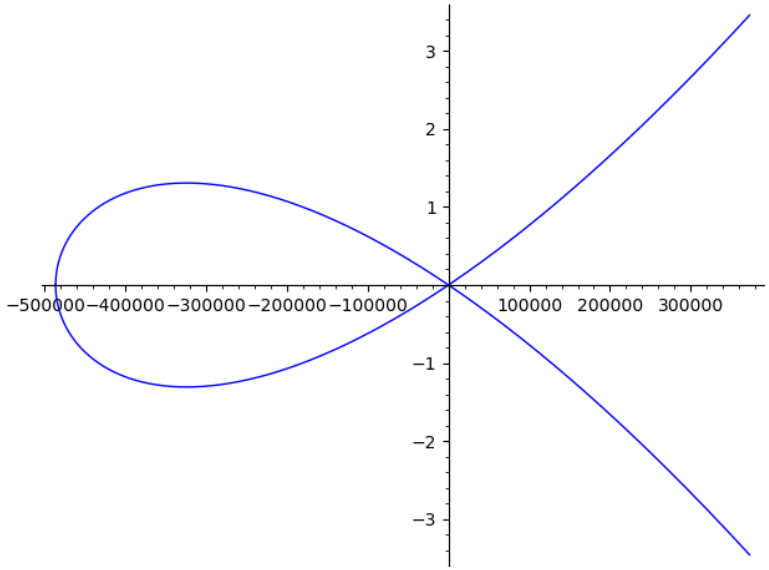
$$S = d_B H_A = d_B d_A G, \qquad S = d_A H_B = d_A d_B G$$

# Пример кривой — Curve25519

$$y^2 = x^3 + 486662x^2 + x$$

$$p = 2^{255} - 19$$

$$G = (9; \ldots)$$




$$n = 2^{252} + 27742317777372353535851937790883648493,\ h = 8$$

# Уровень криптостойкости

Криптостостойкость $n$ бит означает, что надо выполнить $2^n$ операций, чтобы сломать защиту.

Сопоставление размеров ключей для одинакового уровня защиты:

| **Криптостойкость** | **Симметричный** | **RSA/DH** | **ECC** |
|---|---|---|---|
| 80 | 2TDES | 1024 | 160 |
| 112 | 3TDES | 2048 | 224 |
| 128 | AES-128 | 3072 | 256 |
| 192 | AES-192 | 7680 | 384 |
| 256 | AES-256 | 15360 | 512 |

Критика: выбор параметров. «В рукавах ничего нет» (Nothing-up-my-sleeve).
Примеры: MD5, Blowfish, RC5.
Контр-примеры: DES, Стрибог, Dual_EC_DRBG, ЭК от NIST.
RSA не требует выбора параметров.