

# Криптография на эллиптических кривых

---

- Математические понятия
- Аналог алгоритма Диффи-Хеллмана обмена ключами
- Алгоритм цифровой подписи на основе эллиптических кривых ECDSA
- Шифрование/расшифрование с использованием эллиптических кривых
- Варианты эллиптических кривых

# Математические понятия

---

- Преимущество подхода на основе эллиптических кривых в сравнении с задачей факторизации числа, используемой в RSA, или задачей целочисленного логарифмирования, применяемой в алгоритме Диффи-Хеллмана и в DSS, заключается в том, что в данном случае обеспечивается эквивалентная защита при меньшей длине ключа.
- В общем случае уравнение эллиптической кривой **E** имеет вид:

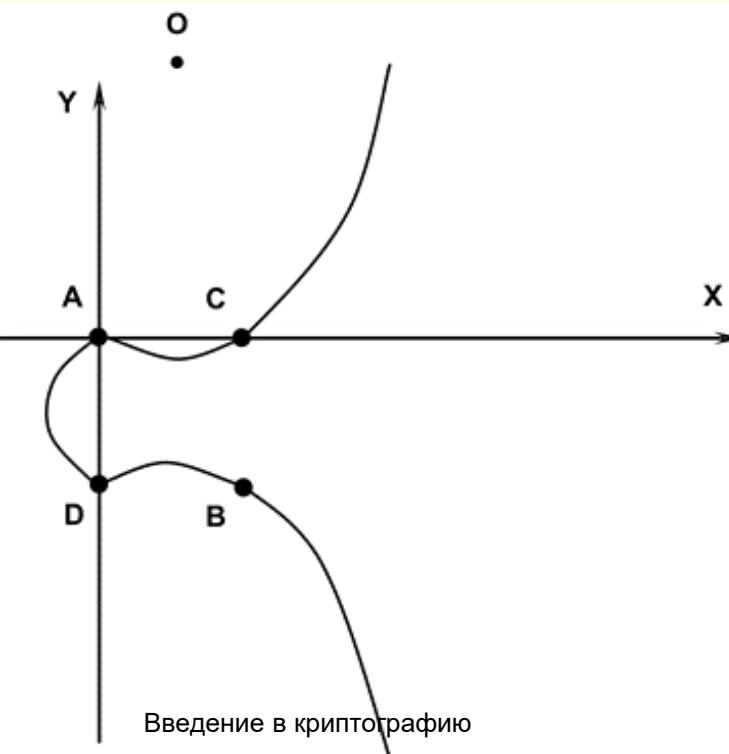
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

- В качестве примера рассмотрим эллиптическую кривую **E**, уравнение которой имеет вид:

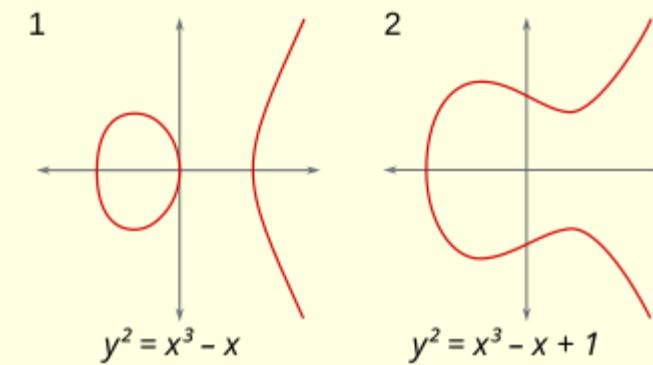
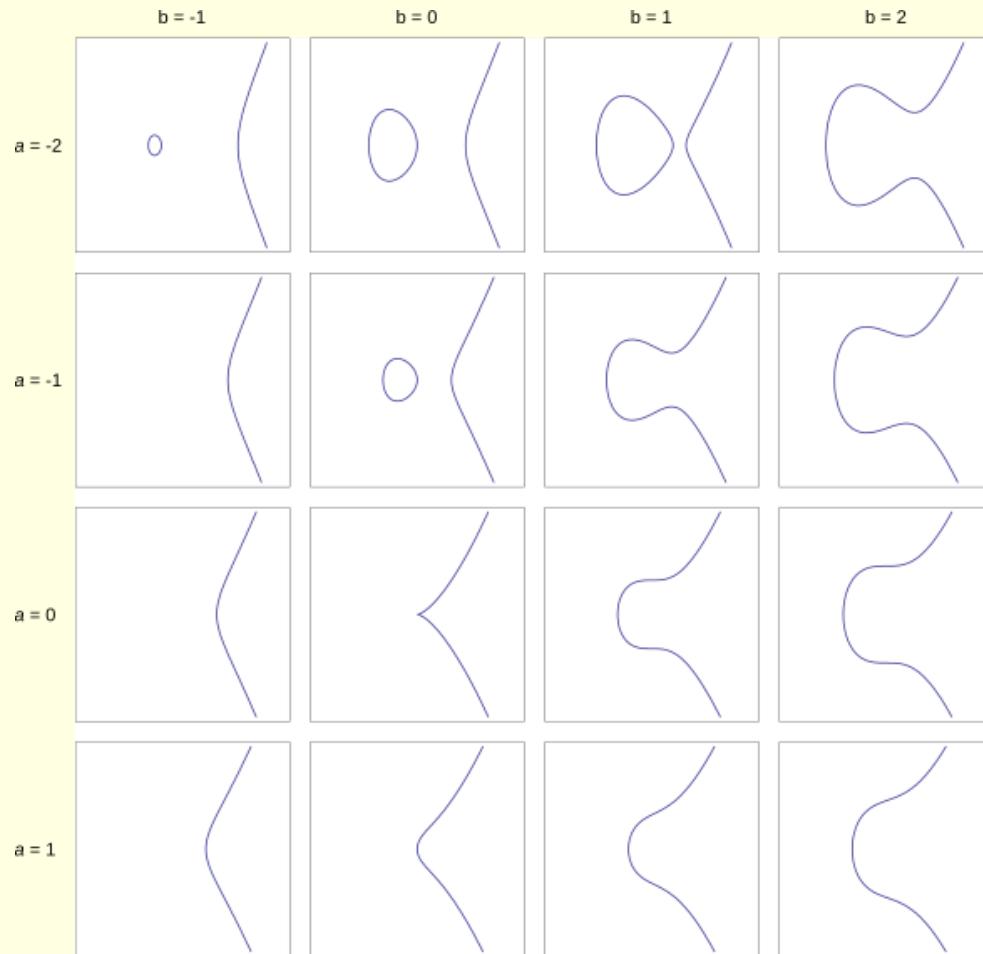
$$y^2 + y = x^3 - x^2$$

# Математические понятия

- На этой кривой лежат только четыре точки, координаты которых являются целыми числами. Это точки  
**A (0, 0), B (1, -1), C (1, 0) и D (0, -1)**



# Математические понятия



# Математические понятия

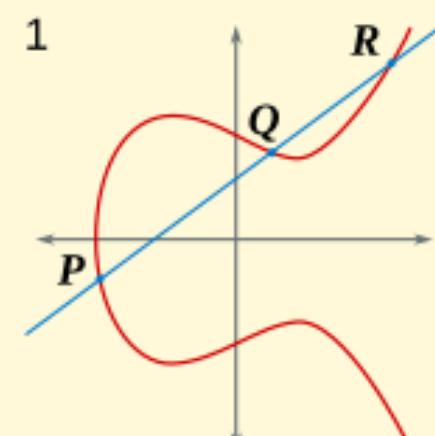
---

Для определения операции сложения двух точек на эллиптической кривой сделаем следующие предположения:

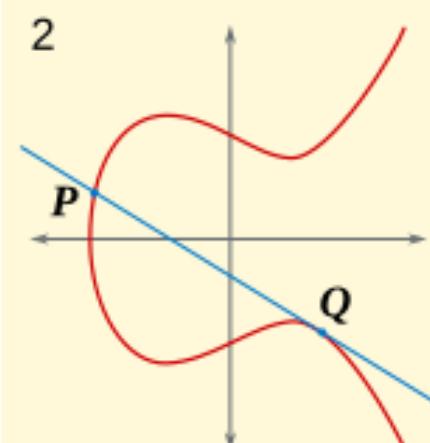
- На плоскости существует бесконечно удаленная точка  $O \in E$ , в которой сходятся все вертикальные прямые.
- Будем считать, что касательная к кривой проходит через точку касания два раза.
- Если три точки эллиптической кривой лежат на прямой линии, то их сумма есть  $O$ .

# Математические понятия

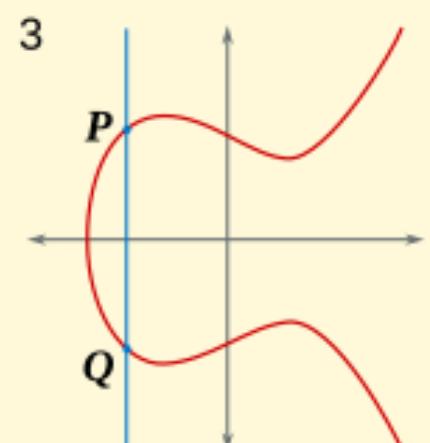
Сложение точек на эллиптической кривой



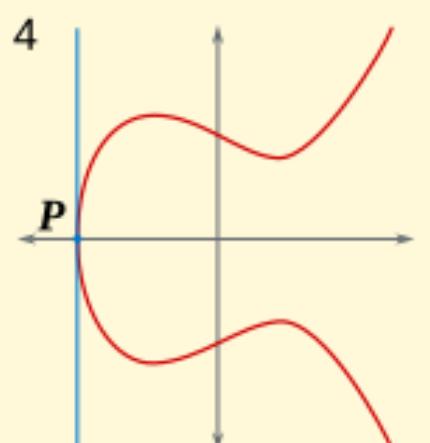
$$P + Q + R = 0$$



$$P + Q + Q = 0$$



$$P + Q + 0 = 0$$



$$P + P + 0 = 0$$

# Математические понятия

Введем следующие правила сложения точек на эллиптической кривой:

- Точка  $\mathbf{O}$  выступает в роли нулевого элемента. Так,  $\mathbf{O} = -\mathbf{O}$ , и для любой точки  $\mathbf{P}$  на эллиптической кривой  $\mathbf{P} + \mathbf{O} = \mathbf{P}$ .
- Вертикальная линия пересекает кривую в двух точках с одной и той же координатой  $\mathbf{x}$   $\mathbf{S}=(\mathbf{x}, \mathbf{y})$  и  $\mathbf{T}=(\mathbf{x}, -\mathbf{y})$ . Эта прямая пересекает кривую и в бесконечно удаленной точке. Поэтому  $\mathbf{P}_1 + \mathbf{P}_2 + \mathbf{O} = \mathbf{O}$  и  $\mathbf{P}_1 = -\mathbf{P}_2$ .
- Чтобы сложить две точки  $\mathbf{P}$  и  $\mathbf{Q}$  с разными координатами  $\mathbf{x}$ , следует провести через эти точки прямую и найти точку пересечения ее с эллиптической кривой. Если прямая не является касательной к кривой в точках  $\mathbf{P}$  или  $\mathbf{Q}$ , то существует только одна такая точка, обозначим ее  $\mathbf{S}$ . Согласно нашему предположению

$$\mathbf{P} + \mathbf{Q} + \mathbf{S} = \mathbf{O}$$

Следовательно,

# Математические понятия

Если прямая является касательной к кривой в какой-либо из точек  $P$  или  $Q$ , то в этом случае следует положить  $S=P$  или  $S=Q$  соответственно.

Чтобы удвоить точку  $Q$ , следует провести касательную в точке  $Q$  и найти другую точку пересечения  $S$  с эллиптической кривой. Тогда  $Q + Q = 2 \times Q = -S$ .

Введенная таким образом операция сложения подчиняется всем обычным правилам сложения, в частности коммутативному и ассоциативному законам. Умножение точки  $P$  эллиптической кривой на положительное число  $k$  определяется как сумма  $k$  точек  $P$ .

В криптографии с использованием эллиптических кривых все значения вычисляются по модулю  $p$ , где  $p$  является простым числом. Элементами данной эллиптической кривой являются пары неотрицательных целых чисел, которые меньше  $p$  и удовлетворяют частному виду эллиптической кривой:

$$y^2 = x^3 + ax + b \pmod{p}$$

# Математические понятия

Такую кривую будем обозначать  $E_p(a, b)$ . При этом числа  $a$  и  $b$  должны быть меньше  $p$  и должны удовлетворять условию  $4a^3 + 27b^2 \pmod{p} \neq 0$ . Множество точек на эллиптической кривой вычисляется следующим образом. Для каждого такого значения  $x$ , что  $0 \leq x \leq p$ , вычисляется

$$x^3 + ax + b \pmod{p}.$$

Для каждого из полученных таким образом значений выясняется, имеет ли это значение целочисленный квадратный корень. Если нет, то в  $E_p(a, b)$  нет точек с этим значением  $x$ . Если целочисленный корень существует, имеется два значения  $y$ , равные этим значениям квадратного корня. Исключением является случай, когда  $y$  равен нулю. Эти значения  $(x, y)$  и будут точками  $E_p(a, b)$ .

# Аналог алгоритма Диффи-Хеллмана обмена ключами

---

- Обмен ключом с использованием эллиптических кривых может быть выполнен следующим образом. Сначала выбирается простое число  $p \approx 2^{180}$  и параметры  $a$  и  $b$  для уравнения эллиптической кривой. Это задает множество точек  $E_p(a,b)$ . Затем в  $E_p(a,b)$  выбирается генерирующая точка  $G = (x_1, y_1)$ . При выборе  $G$  важно, чтобы наименьшее значение  $n$ , при котором  $n \times G = O$ , оказалось очень большим простым числом. Параметры  $E_p(a,b)$  и  $G$  криптосистемы являются параметрами, известными всем участникам.

# Аналог алгоритма Диффи-Хеллмана обмена ключами

- Обмен ключами между пользователями А и В производится по следующей схеме.
  1. Участник А выбирает целое число  $n_A$ , меньшее n. Это число является закрытым ключом участника А. Затем участник А вычисляет открытый ключ  $P_A = n_A \times G$ , который представляет собой некоторую точку на  $E_p(a,b)$ .
  2. Точно так же участник В выбирает закрытый ключ  $n_B$  и вычисляет открытый ключ  $P_B = n_B \times G$ .
  3. Участники обмениваются открытыми ключами, после чего вычисляют общий секретный ключ K

Участник А:  $K = n_A \times P_B$

Участник В:  $K = n_B \times P_A$

- Следует заметить, что общий секретный ключ представляет собой пару чисел. Если данный ключ предполагается использовать в качестве сеансового ключа для алгоритма симметричного шифрования, то из этой пары необходимо создать одно значение.

# Алгоритм цифровой подписи на основе эллиптических кривых ECDSA

---

Алгоритм ECDSA (Elliptic Curve Digest Signature Algorithm) принят в качестве стандартов ANSI X9F1 и IEEE P1363.

## Создание ключей

Выбирается эллиптическая кривая  $E_p(a, b)$ . Число точек на ней должно делиться на большое целое  $n$ .

Выбирается точка  $P \in E_p(a, b)$ .

Выбирается случайное число  $d \in [1, n-1]$ .

Вычисляется  $Q = d \times P$ .

Закрытым ключом является  $d$ , открытым ключом  $(E, P, n, Q)$ .

# Алгоритм цифровой подписи на основе эллиптических кривых ECDSA

---

## Создание подписи

Выбирается случайное число  $k \in [1, n-1]$ .

Вычисляется  $k \times P = (x_1, y_1)$  и  $r = x_1 \pmod{n}$ . Проверяется, чтобы  $r$  не было равно нулю, так как в этом случае подпись не будет зависеть от закрытого ключа. Если  $r = 0$ , то выбирается другое случайное число  $k$ .

Вычисляется

$$k^{-1} \pmod{n}$$

Вычисляется

$$s = k^{-1} \cdot (H(M) + d \cdot r) \pmod{n}$$

Проверяется, чтобы  $s$  не было равно нулю, так как в этом случае необходимого для проверки подписи числа  $s^{-1} \pmod{n}$  не существует. Если  $s=0$ , то выбирается другое случайное число  $k$ .

Подписью для сообщения  $M$  является пара чисел  $(r, s)$ .

# Алгоритм цифровой подписи на основе эллиптических кривых ECDSA

---

## Проверка подписи

Проверяется, что целые числа  $r$  и  $s$  принадлежат диапазону чисел  $[0, n-1]$ . В противном случае результат проверки отрицательный, и подпись отвергается.

Вычисляется

$$w = s^{-1} \pmod{n} \text{ и } H(M)$$

Вычисляется

$$u_1 = H(M) \cdot w \pmod{n}$$

$$u_2 = r \cdot w \pmod{n}$$

Вычисляется

$$u_1 \times P + u_2 \times Q = (x_0, y_0)$$

$$v = x_0 \pmod{n}$$

# Шифрование/расшифрование с использованием эллиптических кривых

---

- Рассмотрим самый простой подход к шифрованию/расшифрованию с использованием эллиптических кривых. Задача состоит в том, чтобы зашифровать сообщение  $\mathbf{M}$ , которое может быть представлено в виде точки на эллиптической кривой  $P_m(x, y)$ .
- Как и в случае обмена ключами, в системе шифрования/расшифрования в качестве параметров рассматривается эллиптическая кривая  $E_p(a, b)$  и точка  $G$  на ней.
- Участник **B** выбирает закрытый ключ  $n_B$  и вычисляет открытый ключ  $P_B = n_B \times G$ . Чтобы зашифровать сообщение  $P_m$  используется открытый ключ получателя **B**  $P_B$ .
- Участник **A** выбирает случайное целое положительное число  $k$  и вычисляет зашифрованное сообщение  $C_m$ , являющееся точкой на эллиптической кривой.  
$$C_m = \{k \times G, P_m + k \times P_B\}$$

# Шифрование/расшифрование с использованием эллиптических кривых

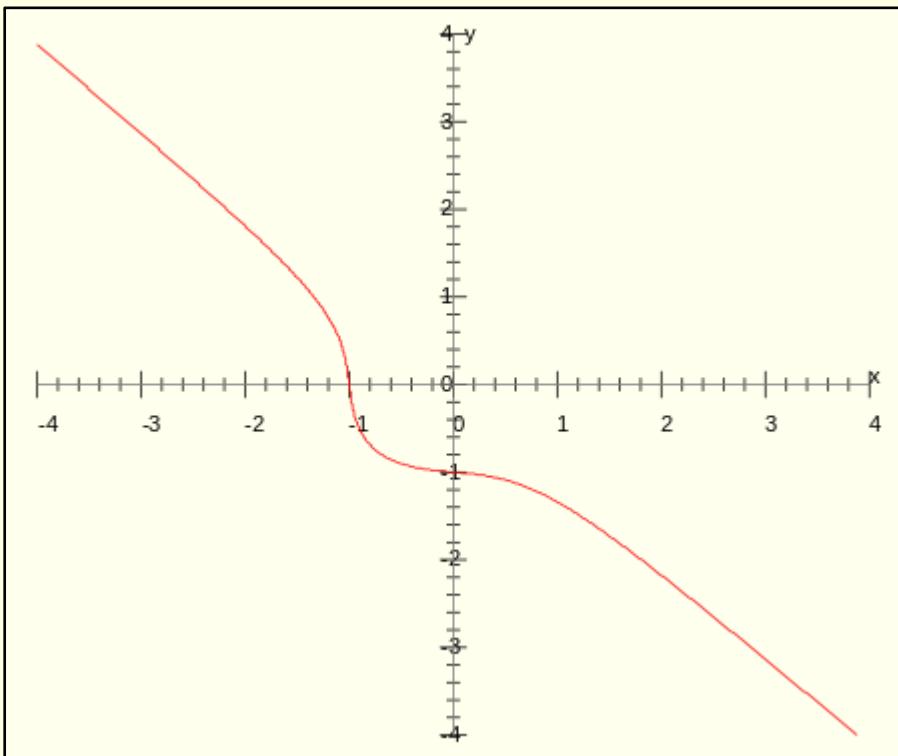
- Чтобы расшифровать сообщение, участник **B** умножает первую координату точки на свой закрытый ключ и вычитает результат из второй координаты:

$$P_m + k \times P_B - n_B \times (k \times G) = P_m + k \times (n_B \times G) - n_B \times (k \times G) = P_m$$

- Участник **A** зашифровал сообщение  $P_m$  добавлением к нему  $k \times P_B$ . Никто не знает значения  $k$ , поэтому, хотя  $P_B$  и является открытым ключом, никто не знает  $k \times P_B$ . Противнику для восстановления сообщения придется вычислить  $k$ , зная  $G$  и  $k \times G$ . Сделать это будет нелегко
- Получатель также не знает  $k$ , но ему в качестве подсказки посыпается  $k \times G$ . Умножив  $k \times G$  на свой закрытый ключ, получатель получит значение, которое было добавлено отправителем к незашифрованному сообщению. Тем самым получатель, не зная  $k$ , но имея свой закрытый ключ, может восстановить незашифрованное сообщение.

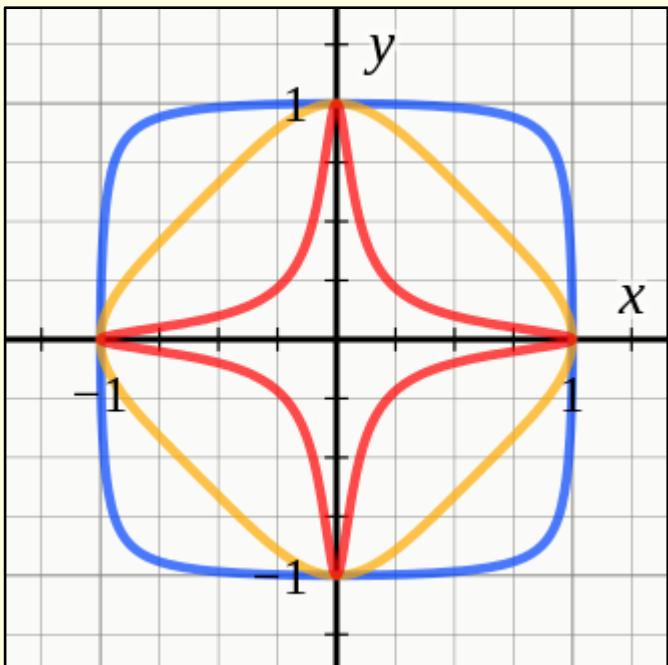
# Варианты эллиптических кривых

Hessian form of an elliptic curve



# Варианты эллиптических кривых

## Edwards curve

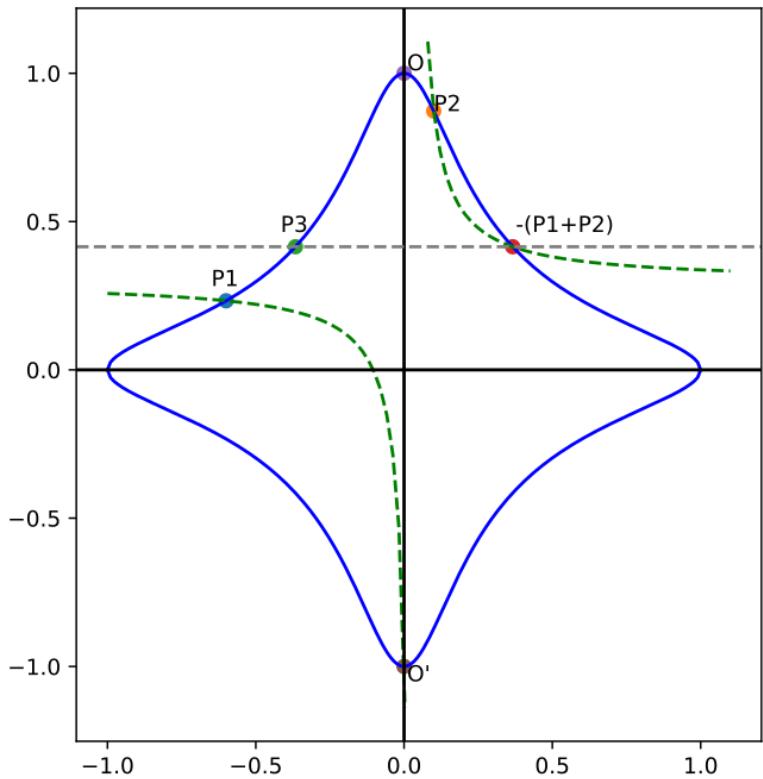


Edwards curves of equation  $x^2 + y^2 = 1 - d \cdot x^2 \cdot y^2$  over the real numbers for  $d = 300$  (red),  $d = \sqrt{8}$  (yellow) and  $d = -0.9$  (blue)

На любой эллиптической кривой сумма двух точек задается рациональным выражением координат точек, хотя в общем случае может потребоваться использовать несколько формул, чтобы охватить все возможные пары. Для кривой Эдвардса, принимая нейтральный элемент за точку  $(0, 1)$ , сумма точек  $(x_1, y_1)$  и  $(x_2, y_2)$  задается формулой

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

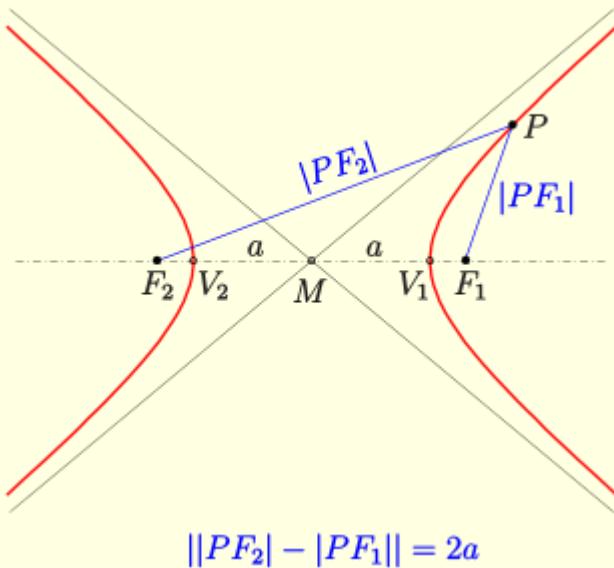
# Варианты эллиптических кривых



Сумма двух точек на кривой Edwards с  $d = -30$

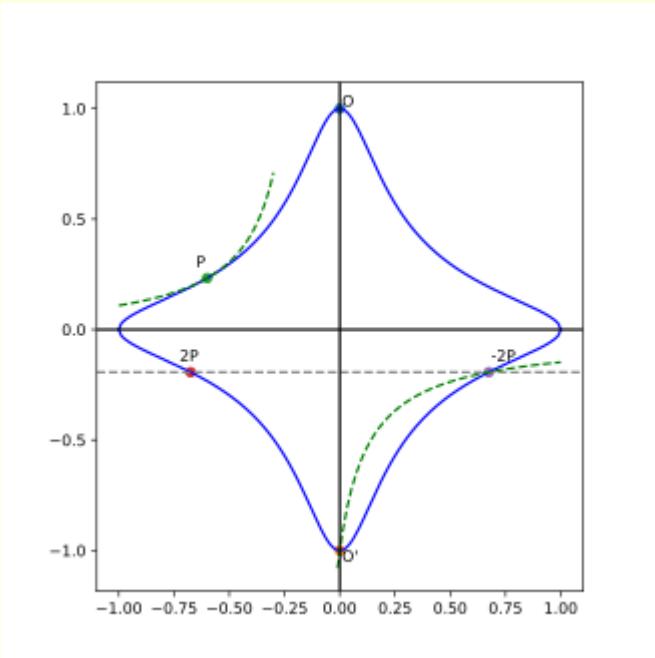
Для кривых Edwards три точки  $P_1$ ,  $P_2$  и  $-(P_1+P_2)$  лежат на гиперболе

# Варианты эллиптических кривых



Гипербола: расстояние точек до двух фиксированных точек, которые называются фокусами

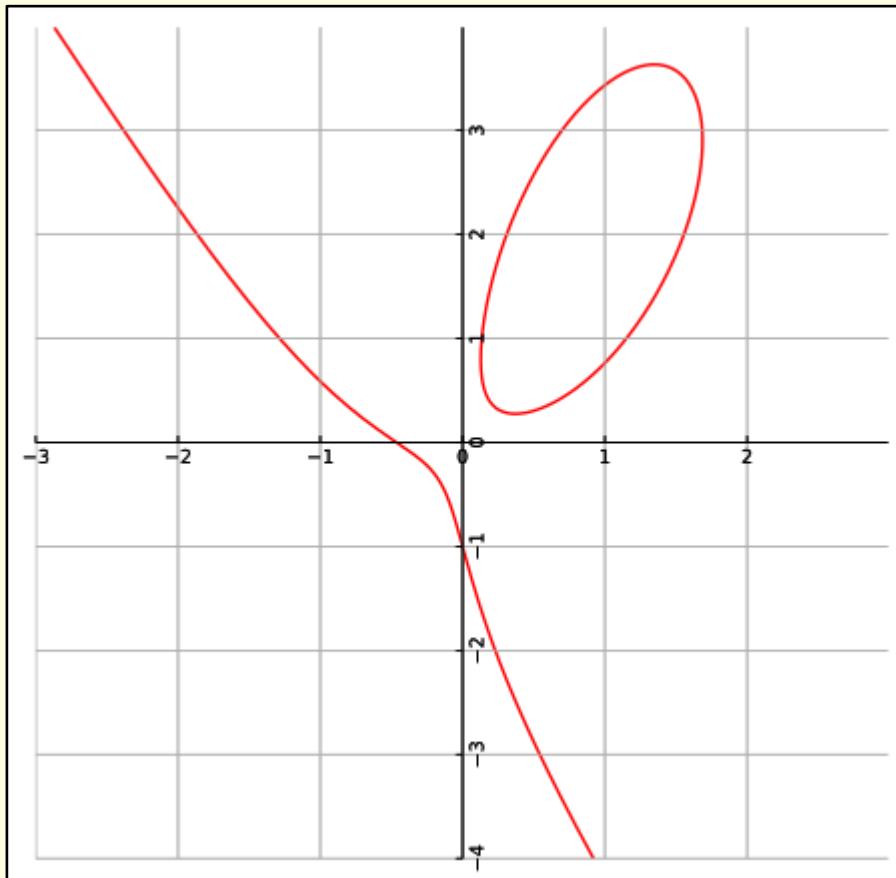
# Варианты эллиптических кривых



Удвоение точки на кривой Edwards с  $d=-30$

# Варианты эллиптических кривых

## Twisted Hessian curves



A Twisted Hessian curve of equation

$$10x^3 + y^3 + 1 = 15xy$$

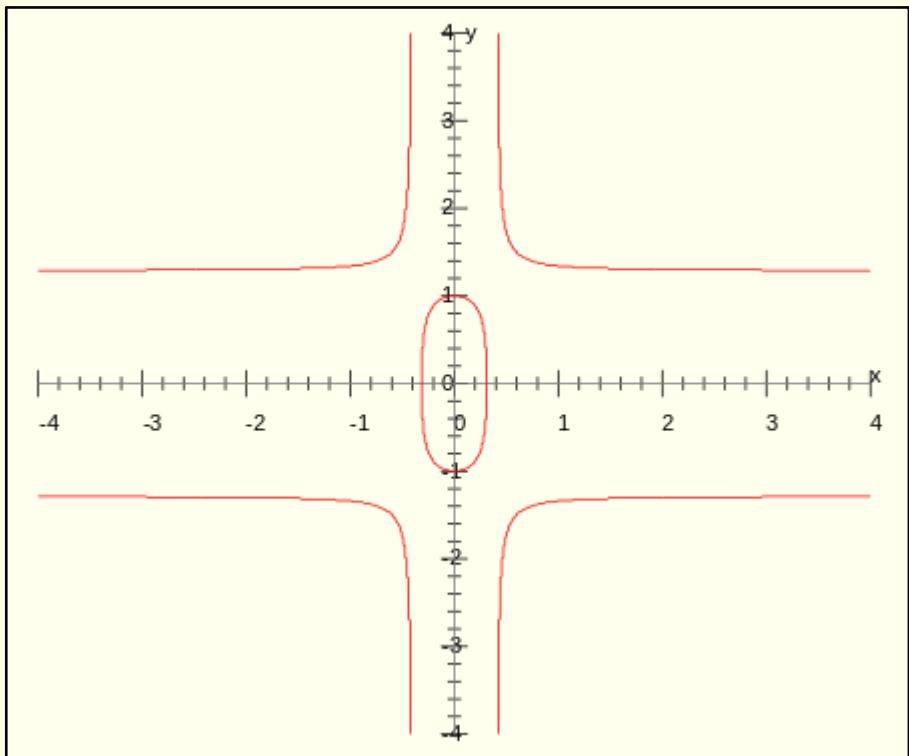
Пусть  $P=(x_1, y_1)$  и  $Q=(x_2, y_2)$ , тогда  $R = P+Q = (x_3, y_3)$

$$x_3 = \frac{x_1 - y_1^2 \cdot x_2 \cdot y_2}{a \cdot x_1 \cdot y_1 \cdot x_2^2 - y_2}$$

$$y_3 = \frac{y_1 \cdot y_2^2 - a \cdot x_1^2 \cdot x_2}{a \cdot x_1 \cdot y_1 \cdot x_2^2 - y_2}$$

# Варианты эллиптических кривых

## Twisted Edwards curve



A twisted Edwards curve of equation

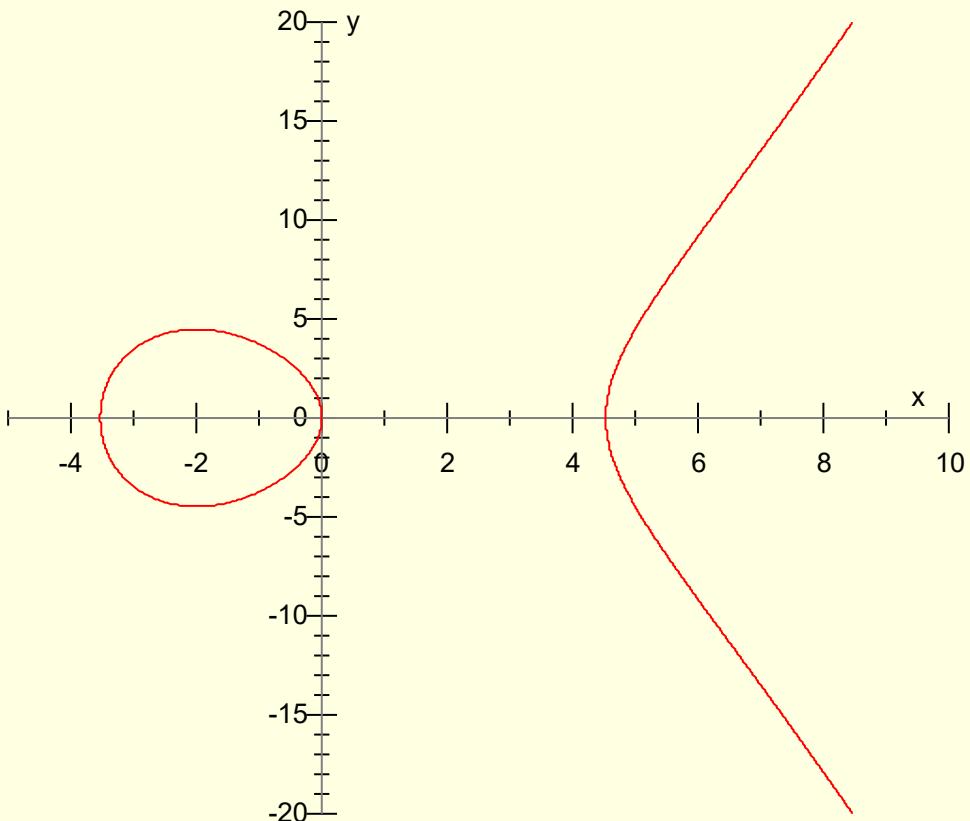
$$10x^2 + y^2 = 1 + 6x^2y^2$$

Сумма двух точек:

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

# Варианты эллиптических кривых

## Doubling-oriented Doche–Icart–Kohel curve

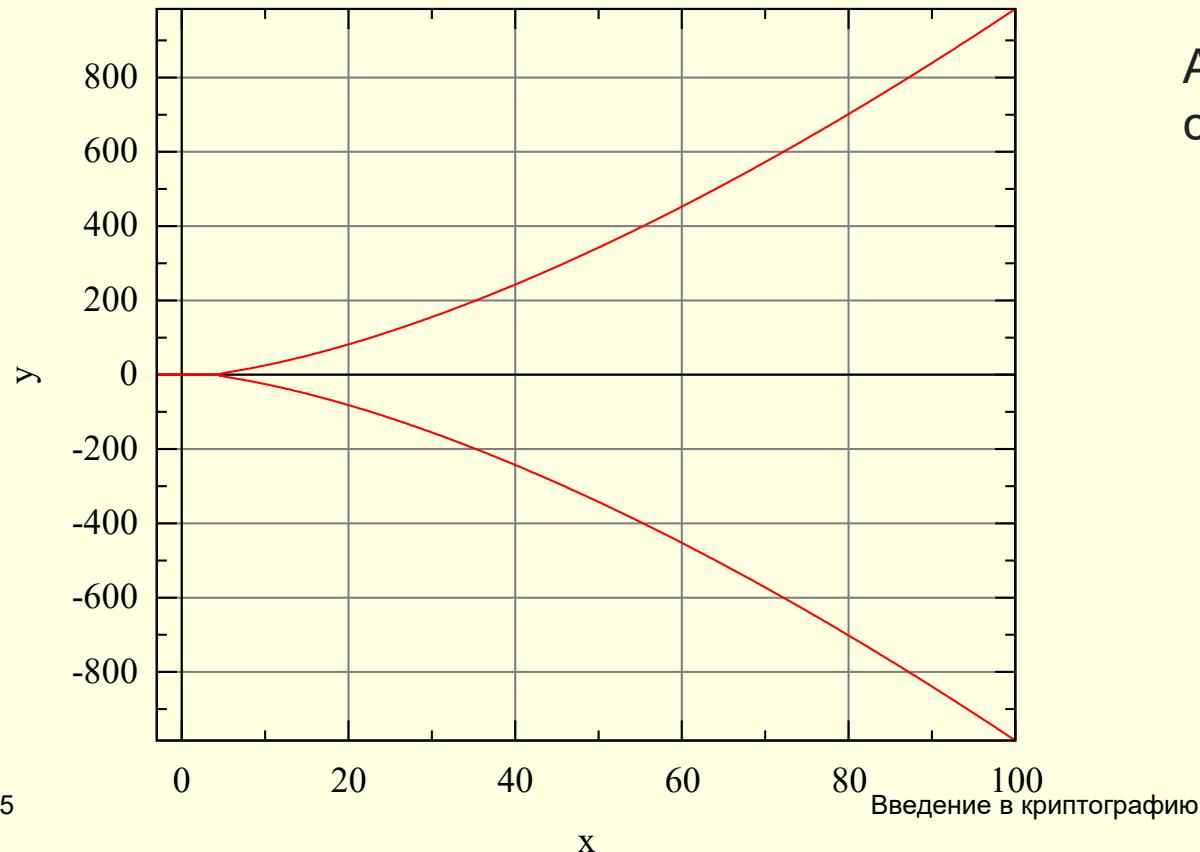


A Doubling-oriented Doche–Icart–Kohel curve  
of equation

$$y^2 = x^3 - x^2 - 16x$$

# Варианты эллиптических кривых

## Tripling-oriented Doche–Icart–Kohel curve

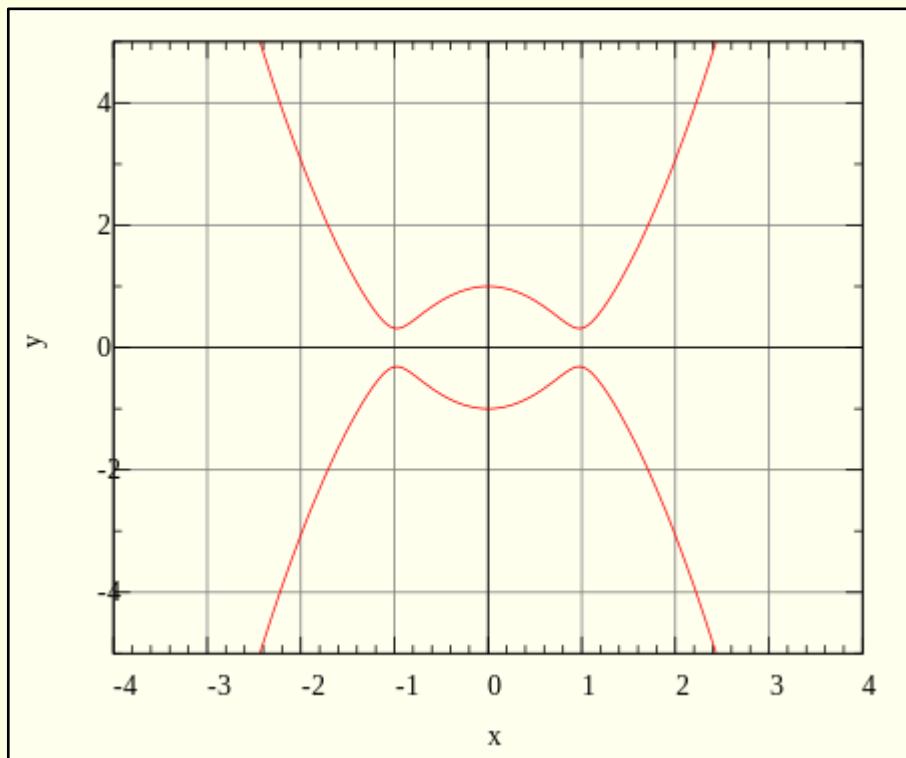


A tripling-oriented Doche–Icart–Kohel curve of equation

$$y^2 = x^3 - 3x^2 - 6x - 3$$

# Варианты эллиптических кривых

## Jacobian curve

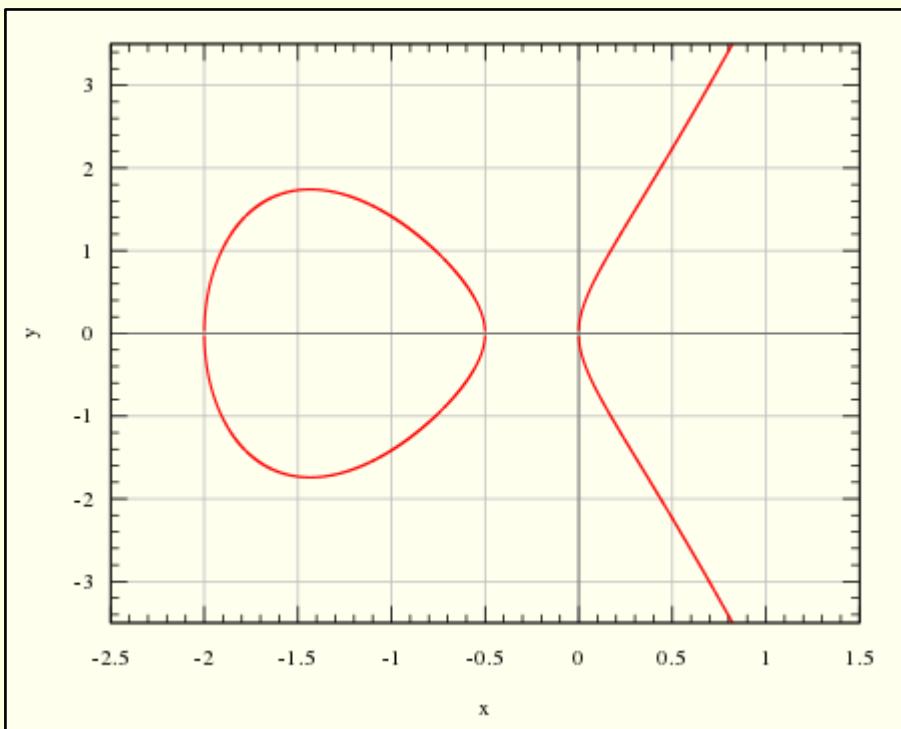


A Jacobi quartic of equation

$$y^2 = x^4 - 1.9x^2 + 1$$

# Варианты эллиптических кривых

## Montgomery curve



A Montgomery curve of equation

$$\frac{1}{4}y^2 = x^3 + \frac{5}{2}x^2 + x$$