

ВИЗУАЛИЗАЦИЯ ОПЕРАЦИЙ  
НАД ЭЛЛИПТИЧЕСКИМИ  
КРИВЫМИ НАД КОНЕЧНЫМИ  
ПОЛЯМИ

# что такое эллиптическая кривая?

- 

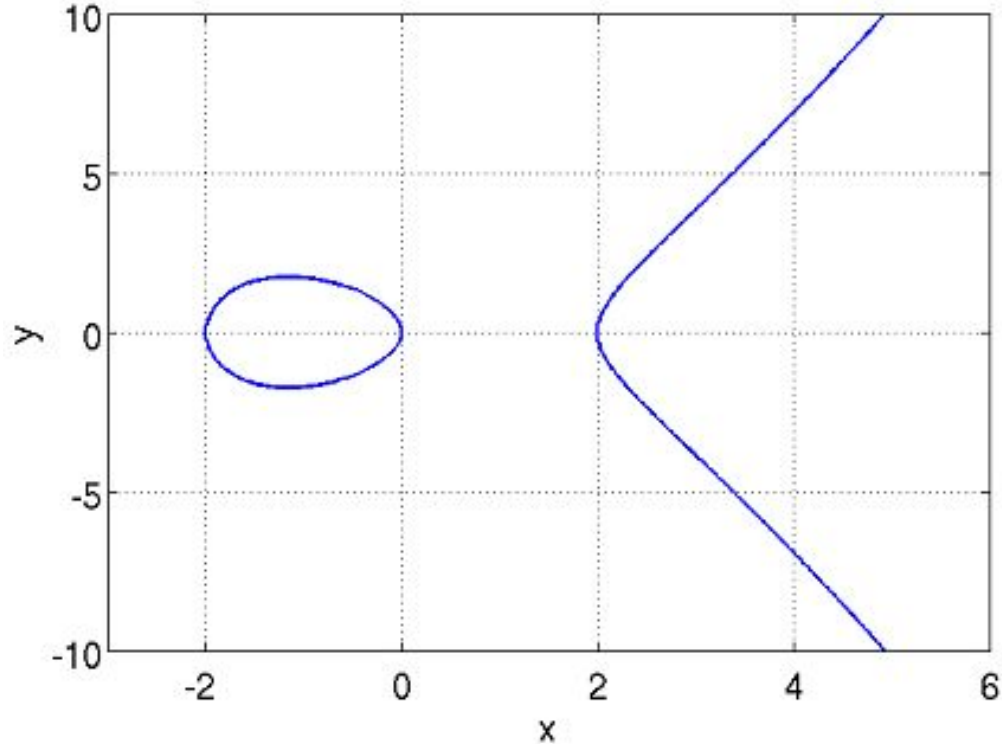
$$y^2 = x^3 + ax + b$$

$4a^3 + 27b^2 = 0 \Rightarrow$  кривая **сингулярная**,  
иначе **гладкая**

# эллиптические кривые над рациональными числами

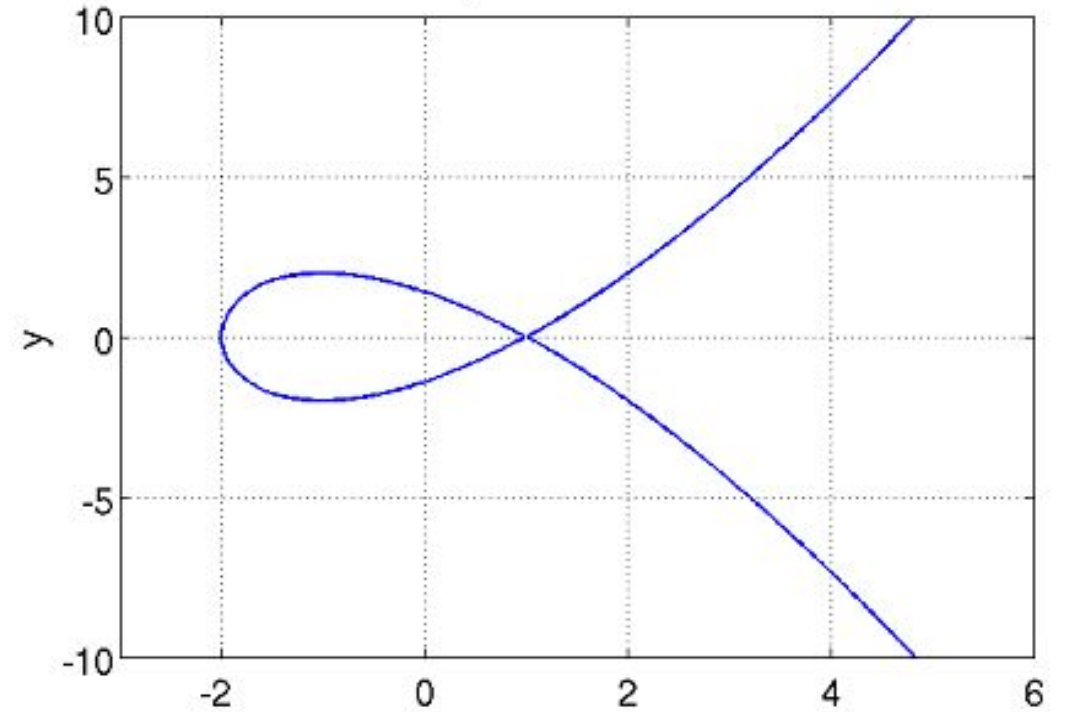
гладкая кривая

$$y^2 = x^3 - 4x + 0$$



сингулярная кривая

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



# операция сложения двух точек

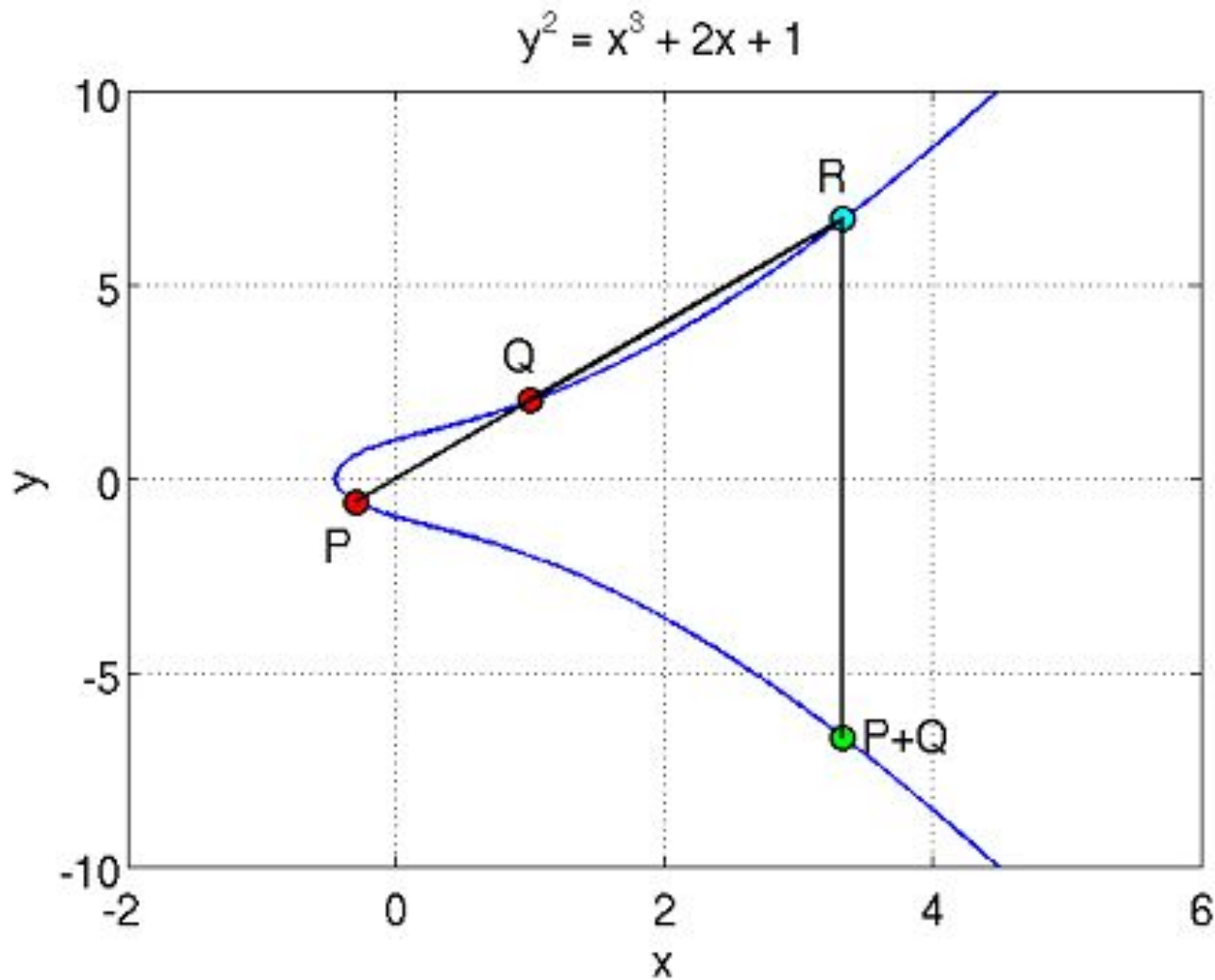
$$P(x_P, y_P), Q(x_Q, y_Q)$$

$$P + Q = -R$$

$$\alpha = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_{P+Q} = \alpha^2 - x_P - x_Q$$

$$y_{P+Q} = \alpha^2 - y_P - y_Q$$



# ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД КОНЕЧНЫМИ ПОЛЯМИ

под эллиптической кривой понимается набор точек, чьи координаты принадлежат конечному полю

 $Z_p$ 

кольцо вычетов, операции в котором производятся по модулю простого числа  $p$

или

 $GF(2^m)$ 

поле Галуа, или бинарное конечное поле

$$y^2 + xy = x^3 + ax^2 + b, \quad b \neq 0$$

# эллиптическая криптография

Операция умножения точки  $G$  на число  $k$ :

$$\underbrace{G + G + \dots + G}_{k \text{ слагаемых}}, \text{ где } k \in \mathbb{Z}$$

Пусть  $M$  – сообщение,  $M \in \mathbb{Z}$ , тогда

$$C = M * V$$

это зашифрованное с помощью точки  $V$  сообщение

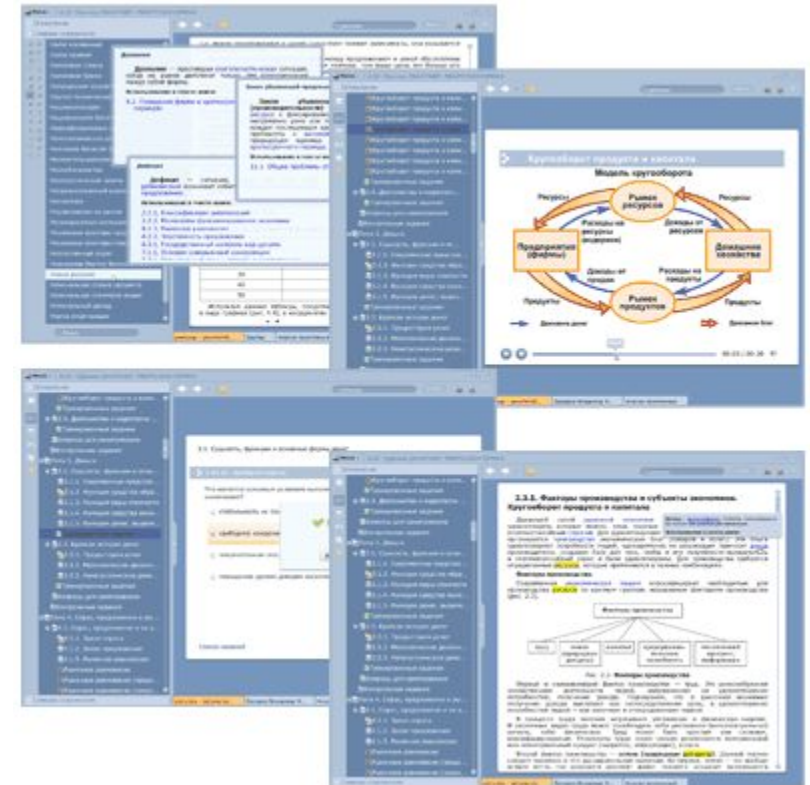
# приложения

- ECDSA
- ECDH
- ECMQV
- Dual EC DRBG
- факторизация с помощью эллиптических кривых

# цель курсовой работы

Интерактивный учебник на **СиШарпе**:

- теоретический минимум
- графики и изображения
- вопросы на понимание материала





спасибо за  
внимание

СПАСИБО ЗА ВНИМАНИЕ!