Elliptic curves

"data structures" for crypto:

- residues mod n
- finite fields $GF(p^k)$
- elliptic curves

EG elliptic curve E given by $y^2 = x^3 - x + 9$

cubic equation

some points on E:

$(0, \pm 3)$

$(1, \pm 3)$

$(2, \pm \sqrt{15})$ irrational!

$x=0$: $y^2 = 0^3 - 0 + 9 \rightarrow y = \pm 3$

$x=1$: $y^2 = 1^3 - 1 + 9 \rightarrow y = \pm 3$

$x=2$: $y^2 = 2^3 - 2 + 9 = 15 \rightarrow y = \pm \sqrt{15}$

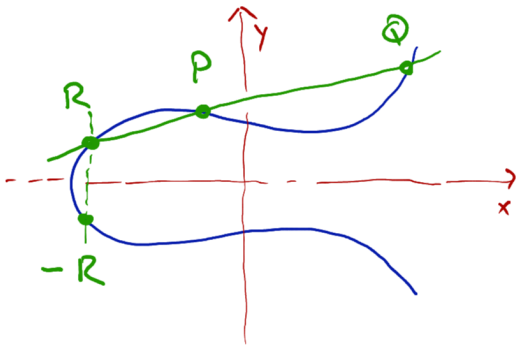
less obvious:

$(35, 207) = (0,3) \boxplus (1,-3)$

$\left(\frac{1}{36}, \frac{647}{216}\right) = (0,-3) \boxplus (0,-3) = 2\,(0,-3)$

addition on elliptic curves

$P \boxplus Q = -R$



- line through P, Q intersects E in a third point R
- $R = (r,s) \Rightarrow -R = (r,-s)$
- $P \boxplus Q := -R$

- special point $\mathcal{O}$ "at ∞"
  $P \boxplus \mathcal{O} = P$

- $R \boxplus -R = \mathcal{O}$
- $P \boxplus P$ using tangent line

- obvious: $P \boxplus Q = Q \boxplus P$
  not obvious: $P \boxplus (Q \boxplus R) = (P \boxplus Q) \boxplus R$