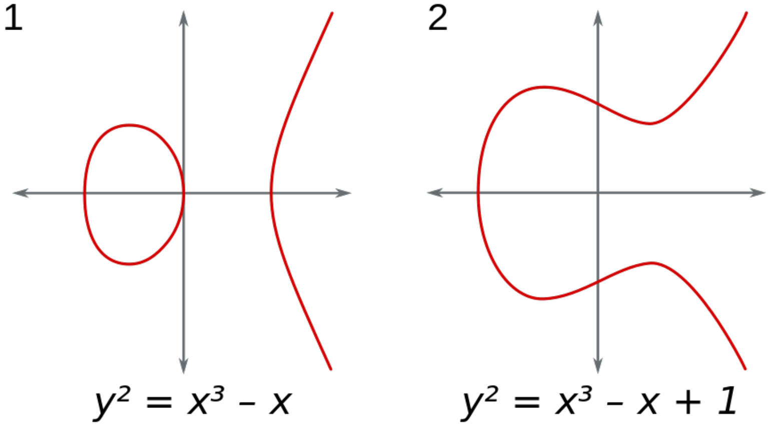
What is...elliptic addition?

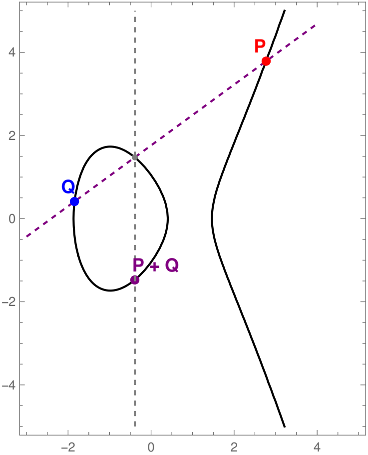
Or: Torus games

Zeros of cubic curves



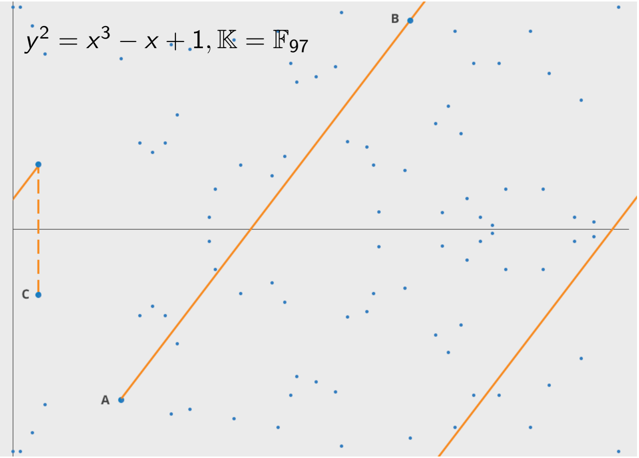
- **Elliptic curve** The solutions of $y^2 = x^3 + ax + b$ and a "point at infinity" O
- With a bit more care, these can be defined over **any field $\mathbb{K}$**

Elliptic addition

$P + Q \leftrightsquigarrow$ 

- Elliptic curves are abelian varieties Addition and geometry
- In particular, they give rise to an abelian group $E(\mathbb{K})$

Elliptic addition modulo a prime

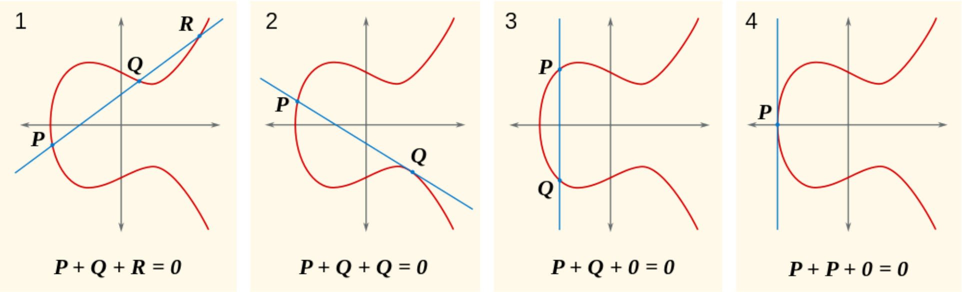


- The set of points $E(\mathbb{F}_q)$ is a finite abelian group (q is some prime power)
- Example $y^2 = x^3 - x$ gives $E(\mathbb{F}_{71}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$

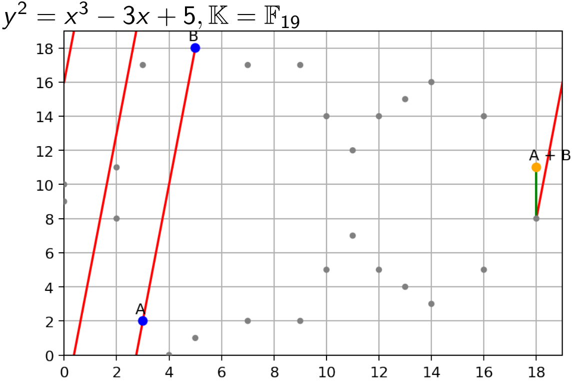
Enter, the theorem

Every elliptic curve E gives rise to an abelian group by:

- The identity is O $\infty = 0$
- If P, Q, R are points of line $\cap$ E, then $A + B + C = 0$ 1
- If line $\cap$ E consists of P and Q, is tangent to E at Q, then $P + Q + Q = 0$ 2
- If line $\cap$ E consists consists of P and Q and O, then $P + Q + 0 = 0$ 3
- If line $\cap$ E consists of P, is tangent to E at P, then $P + P + 0 = 0$ 4



Elliptic curves are in geometry and number theory, but in cryptography?



An elliptic curve cryptosystem (for fixed E over $\mathbb{F}_p$) can be defined by:

A public point $P \in E$; a private key $k \in \mathbb{N}$; a public key is $P + \ldots + P$ k-times

Breaking a 228bit RSA $\equiv$ less energy to than it takes to boil a teaspoon of water

Breaking a 228bit elliptic curve $\equiv$ energy to boil all the water on earth

Thank you for your attention!

I hope that was of some help.