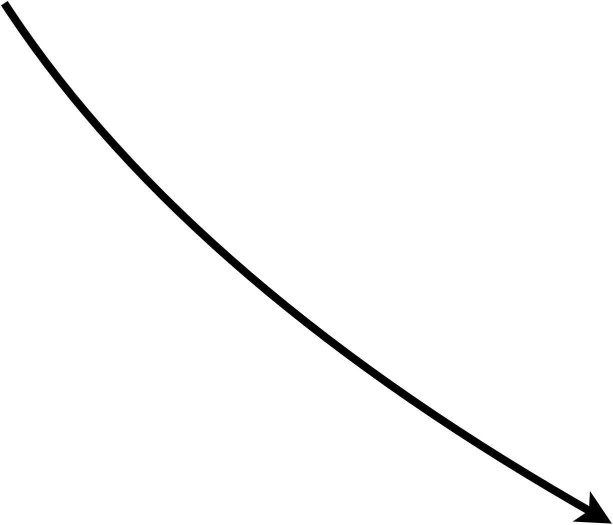
KU LEUVEN

$$\varphi : E \to E'$$

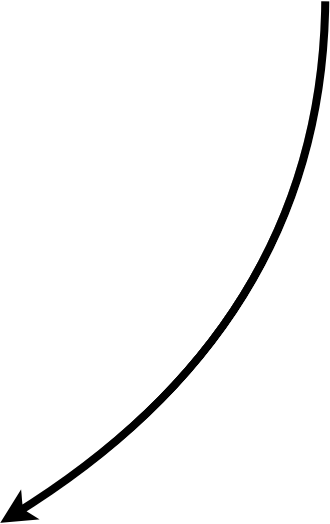


$$E : y^2 = x^3 + ax + b$$

$$a, b \in \mathbb{F}_q$$

$$E' : y^2 = x^3 + a'x + b'$$

$$a', b' \in \mathbb{F}_q$$



)

and

It has a *degree*

, which measures its complexity.

(it preserves the group structures we have on

Definition 1 (sketch). An *isogeny* is a “nice” map between elliptic curves.

E

E'

$\deg \varphi$

$$\varphi : E \to E'$$