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

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

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

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

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

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

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

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

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

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

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

(it preserves the group structures we have on E and E')