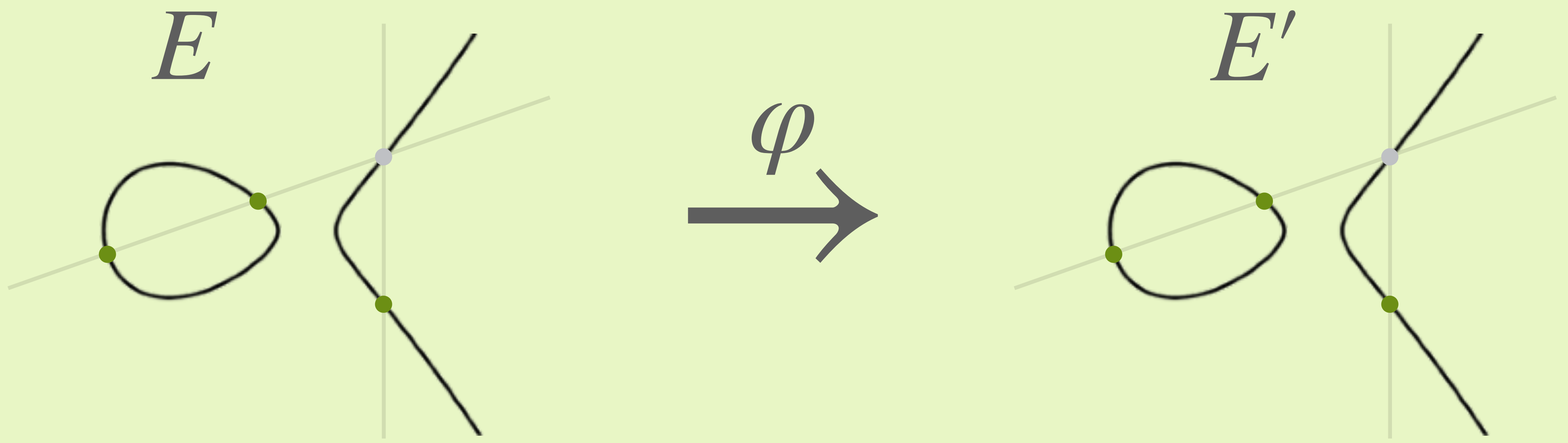
PART 1

SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk "down to earth", I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

isogenies



Isogeny

- "nice" map φ (group homomorphism) between elliptic curves $E \to E'$
- given by rational functions: a point $(x, y) \in E$ is mapped to $\left(f_1(x,y)/f_2(x,y) \ , \ g_1(x,y)/g_2(x,y) \right)$
- size of $\ker \varphi$ is same as degree of φ!

toy example

$$E : y^2 = x^3 + x \xrightarrow{\ \varphi\ } E' : y^2 = x^3 + 5$$

$$(x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, \frac{y(x^3 - 4x^2 + 2)}{(x-5)^3} \right) \qquad \text{over } \mathbb{F}_{11}$$

Can check

- this is a group homomorphism: $\varphi(\mathcal{O}) = \mathcal{O}'$ and $\varphi(P+Q) = \varphi(P) + \varphi(Q)$
- kernel: $\varphi(P) = \mathcal{O}'$ when $P = \mathcal{O}$ or $x_P = 5$, so $P = (5,3)$ and $P = (5,-3)$
- so φ is of degree 3 and we can say E and E' are 3-isogenous

Question

given E and E', can we find
an isogeny $\varphi : E \to E'$?