Question

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

easy

easy to verify that *some isogeny* exists, e.g. that E and E' are **isogenous**

intermediate

what if we additionally know some points $P, Q \in E$ and their images $\varphi(P), \varphi(Q) \in E'$

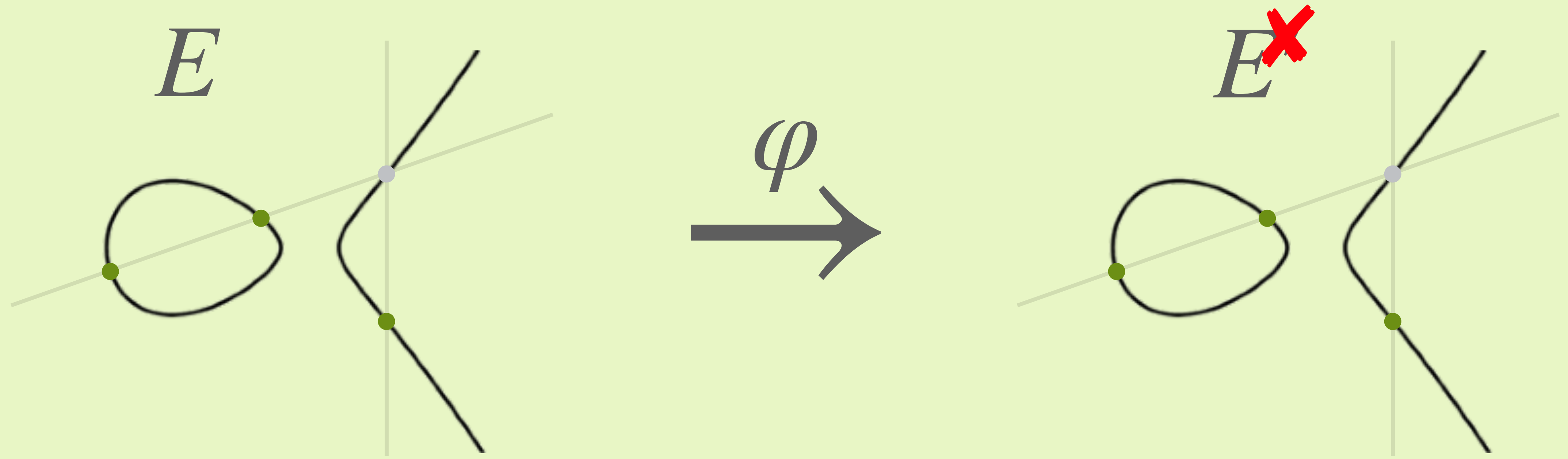
hard

actually giving an isogeny $\varphi : E \to E'$ or some way to compute this

PART 1

SQIsign

endomorphism



~~Isogeny~~ Endomorphism

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