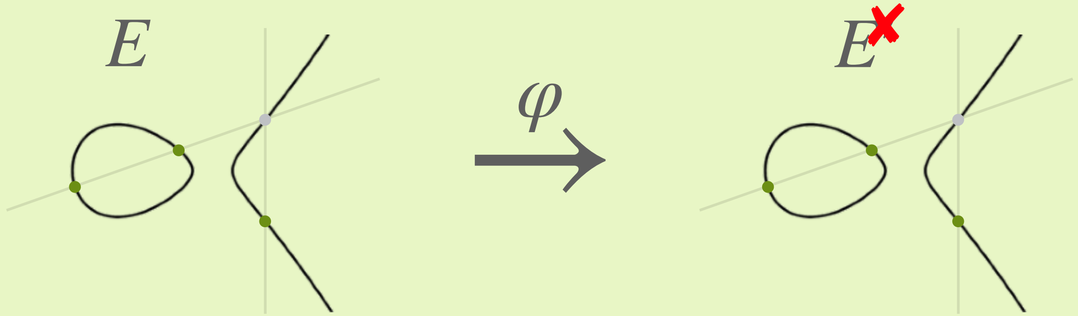
PART 1

SQIsign

endomorphism



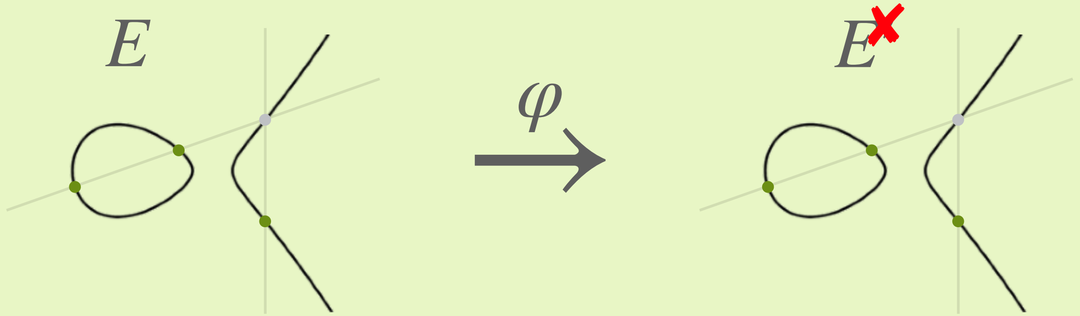
Isogeny Endomorphism

- "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!

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!

toy example

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

$$(x, y) \mapsto \left(\frac{x^4 - 2x^2 + 1}{4(x^3 + x)} : \frac{x^6 y + 5x^4 y - 5x^2 y - y}{8(x^6 + 2x^4 + x^2)} \right) \quad \text{over } \mathbb{F}_{11}$$