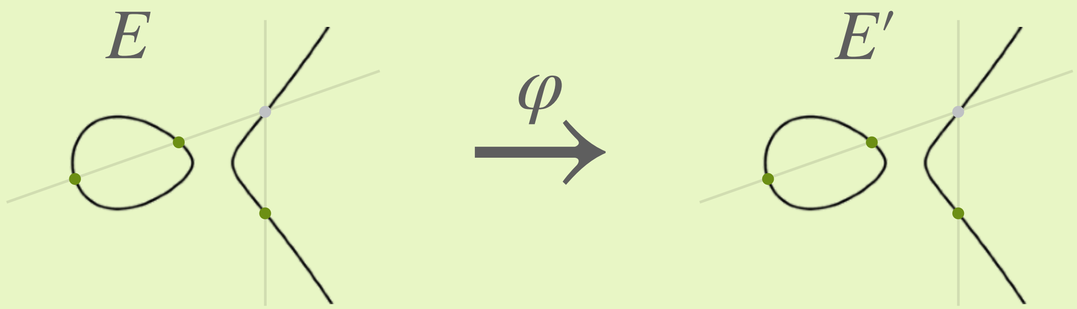
PART 1

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

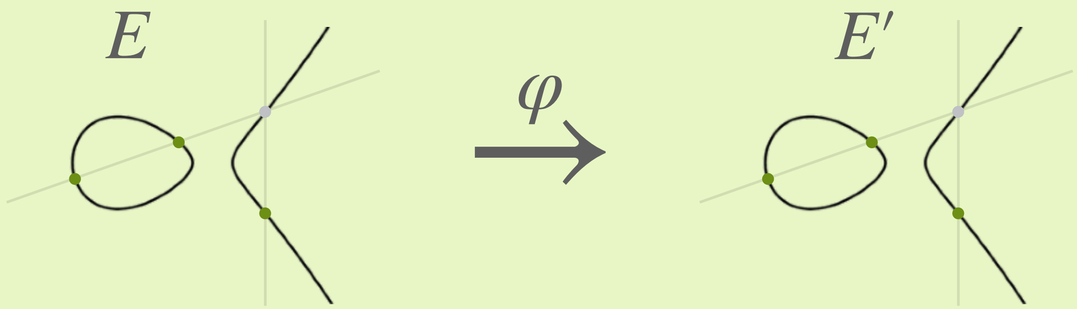
- "nice" map φ (group homomorphism) between elliptic curves $E \to E'$
- given by rational functions: a point $(x, y) \in E$ is mapped to $(f_1(x,y)/f_2(x,y) \ , \ g_1(x,y)/g_2(x,y))$
- size of $\ker \varphi$ is same as degree of φ!

PART 1
SQIsign

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

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

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