ISOGENIES

DEF. Let E_1, E_2 be elliptic curves. A morphism

$$\phi : E_1 \longrightarrow E_2 \quad \text{w/} \quad \phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$$ is called an isogeny.

If $\phi(E_1) \neq \{\mathcal{O}_{E_2}\}$ we say that E_1 and E_2 are isogenous.

ex $[0] : E_1 \longrightarrow E_2$

$P \longmapsto \mathcal{O}_{E_2}$

$[m] : E_1 \longrightarrow E_1$

$P \longmapsto [m]P = \underbrace{P+P+\cdots+P}_{m \text{ times}}$ for $m \geq 1$.

THM $E \times E \longrightarrow E$ is a morphism

$(P, Q) \longmapsto P+Q$

$E \longrightarrow E$ is a morphism

$P \longmapsto -P$

ex $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 2ax + \underbrace{(a^2-4b)}_{r}x$

$\phi : E_1 \longrightarrow E_2$

$(x,y) \longmapsto \left(\frac{y^2}{x^2} \right.$