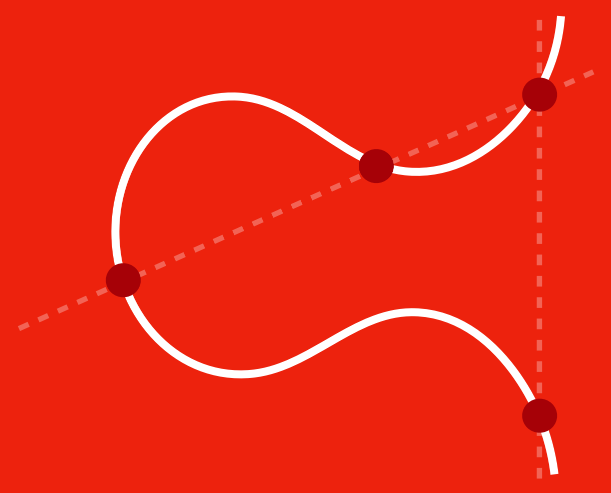
What are pairings and what are isogenies?

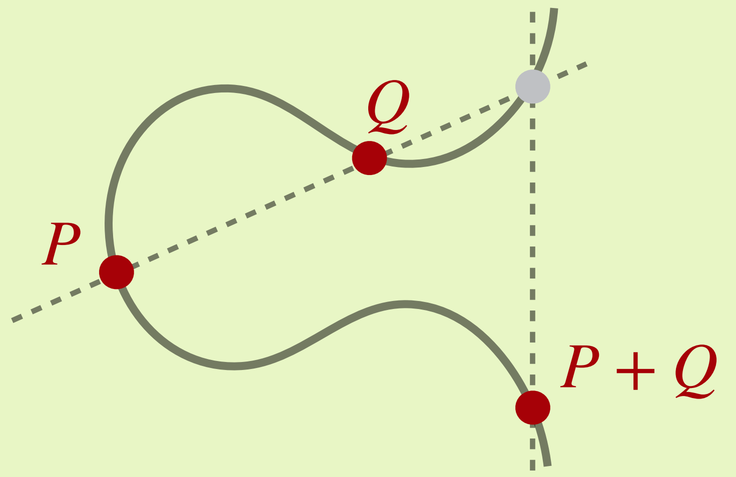


Isogenies
& Pairings

elliptic curves in CSIDH

supersingular elliptic curve

- has $p+1$ points in $E(\mathbb{F}_p)$
- choose p so that $p+1 = 4 \cdot \ell_1 \cdot \ell_2 \cdot \ldots \cdot \ell_n$
- this implies the rational points on E have orders that divide $p+1$



$E : y^2 = x^3 + Ax^2 + x, \quad A \in \mathbb{F}_p$