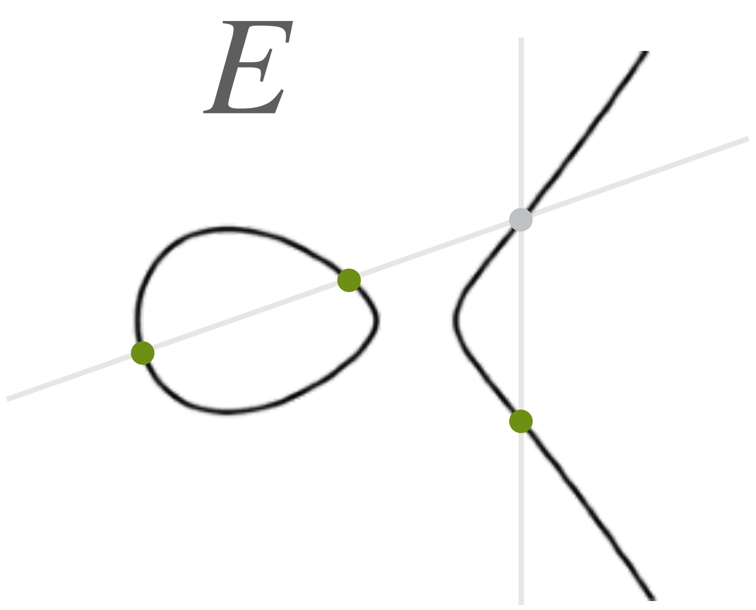
PART 1

SQIsign

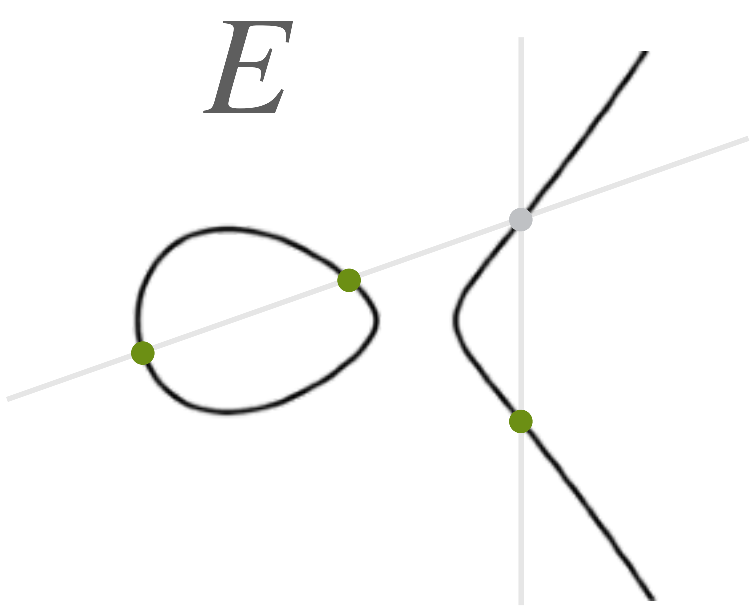


Given just any E over $\mathbb{F}_q$, we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$

PART 1

SQIsign



Given just any E over $\mathbb{F}_q$, we just saw the endomorphisms

- multiplication-by-n, so $[n] : P \mapsto P + \ldots + P$ for any $n \in \mathbb{Z}$
- Frobenius π and easily also $[n] \cdot \pi$ for any $n \in \mathbb{Z}$
- we write this as $\mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Note: applying π twice gives $\pi^2 = [-p]$, so no "new" endom.