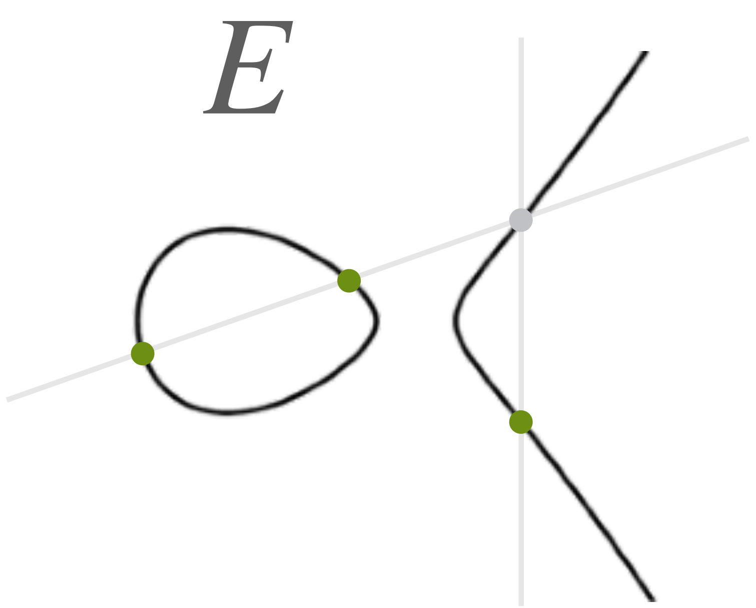
PART 1

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.

endomorphism ring

- we can "add together" different endomorphisms

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P)$$

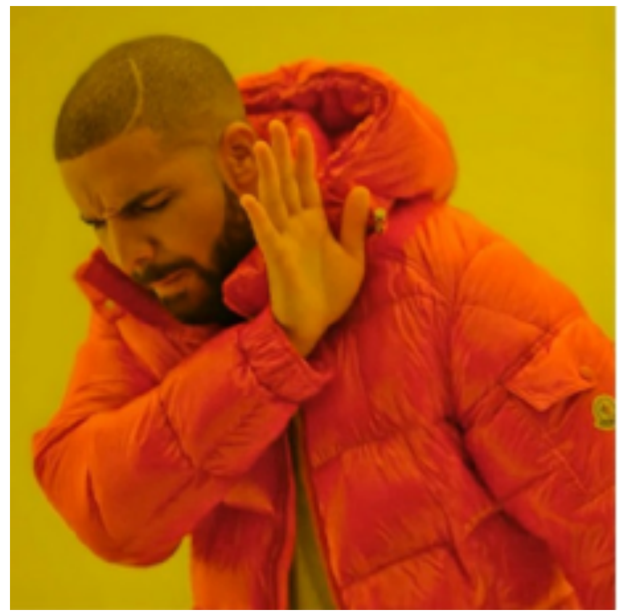
- we can "multiply" endomorphisms by composition

$$(\varphi \cdot \psi)(P) = \varphi(\psi(P))$$

- so, we get a ring structure $\mathrm{End}(E)$, by our examples dimension is at least 2

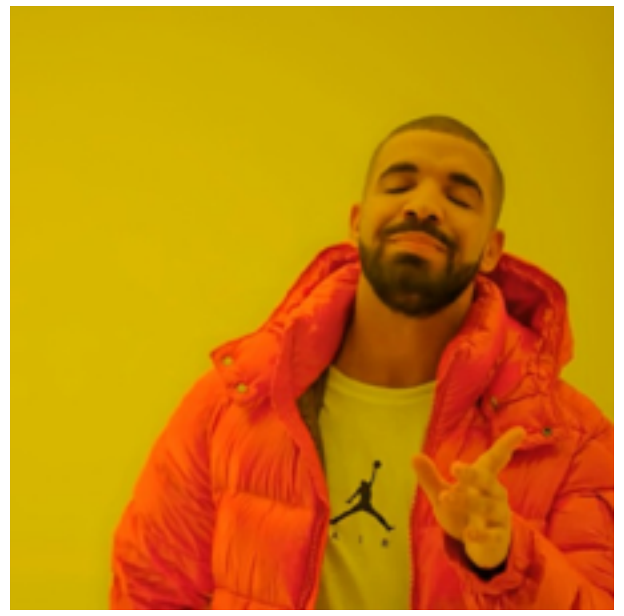
if dim 2

E is **ordinary**



if dim 4

E is
✨✨ **supersingular**✨✨
(weird funky maps!!)



Question

given supersingular E, can we find
weird, funky endomorphisms $\omega \in \mathrm{End}(E)$?