PART 1

SQIsign

Question

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

easy

easy to verify that
such endoms exists,
e.g. that E
is **supersingular**

hard

actually giving an
endom. $\omega \in \mathrm{End}(E)$
or some way to
compute this

PART 1

SQIsign

Question

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

easy

easy to verify that
such endoms exists,
e.g. that E
is **supersingular**

surprisingly easy

we know $\mathrm{End}(E_0)$ for the
specific curve $E_0 : y^2 = x^3 + x$
and for any $E_0 \to E_A$,
we can then compute $\mathrm{End}(E_A)$
(knowledge of endom. ring is contagious)

hard

actually giving an
endom. $\omega \in \mathrm{End}(E)$
or some way to
compute this