IN PRACTICE

- computing isogenies often **bottleneck** in efficiency of isogeny-based cryptography
- isogenies of degree 2^n are **most efficient**, for largest n with rational points of order 2^n
- can describe such an isogeny by a single point $K \in E[2^n](\mathbb{F}_q)$
- we **choose** our field $\mathbb{F}_q$ and curve E such that we have many of such points/isogenies

The Study of Vermeer (1964)

IN PRACTICE

- computing isogenies often **bottleneck** in efficiency of isogeny-based cryptography
- isogenies of degree 2^n are **most efficient**, for largest n with rational points of order 2^n
- can describe such an isogeny by a single point $K \in E[2^n](\mathbb{F}_q)$
- we **choose** our field $\mathbb{F}_q$ and curve E such that we have many of such points/isogenies

FINDING POINTS

Q: How do we find a point K of order 2^n?

- there is no $P \in E(\mathbb{F}_q)$ such that $[2]P = K$, otherwise, P has order 2^{n+1} (contradiction)
- so K is not a point in the subgroup $[2]E(\mathbb{F}_q)$
- for a point $P \in E(\mathbb{F}_q)$, can we quickly find out if

$$P \in E(\mathbb{F}_q) \ \setminus \ [2]E(\mathbb{F}_q)$$