

elliptic curves in CSIDH

supersingular elliptic curve

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

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

the order of \mathbf{P} is readable
from the non-zero \mathbf{P}_i 's

the torsion that P is *missing*
are precisely the zero P_i 's

full-torsion points

we call a point $P \in E(\mathbb{F}_p)$ a **full-torsion point**
if the order is $p + 1$, equivalently, all P_i are non-zero

torsion points and isogenies

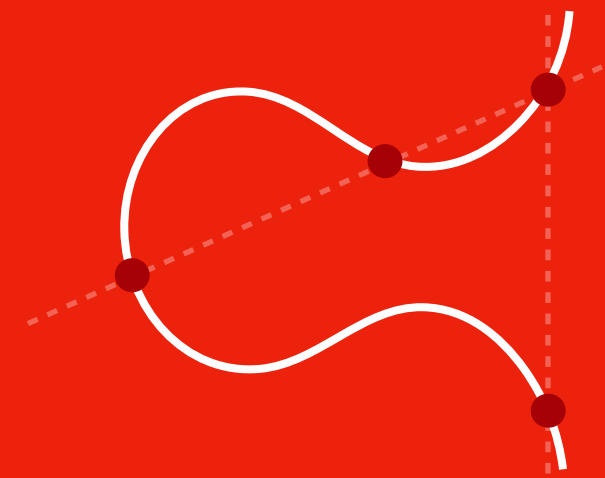
1. Any* isogeny φ of degree N
 - given by kernel of size N
 - generated by point P of order N

$$\text{Diagram} \xrightarrow[\text{deg } 3 \cdot 5 \cdot 7]{\varphi} \text{Diagram}$$

2. Any* isogeny φ of degree $N = \prod \ell_i$
 - splits into sub-isogenies of degree ℓ_i
 - each generated by point \mathbf{P} of order ℓ_i

3. Any* isogeny φ of degree $N = \prod \ell_i$
 - computed using one **full-torsion** P
 - per ℓ_i , compute $[\frac{p+1}{\ell_i}]P$ to get $\ker(\varphi_i)$

$$\begin{aligned} P &= P_3 + P_5 + P_7 \in E(\mathbb{F}_p) \\ [5 \cdot 7]P &= P'_3 + \mathcal{O} + \mathcal{O} \in E(\mathbb{F}_p) \\ \varphi_1(P) &= \mathcal{O} + P'_5 + P'_7 \in E'(\mathbb{F}_p) \end{aligned}$$



Isogenies & Pairings

the Tate pairing*

bilinear pairing from torsion groups to fields

- choose a degree r
- take point P of order r on E , that is $P \in E(\mathbb{F}_{p^2})[r]$
- take point Q on E such that $Q \in E(\mathbb{F}_{p^2})/rE(\mathbb{F}_{p^2})$
- then $e_r(P, Q) = \zeta \in \mu_r$

