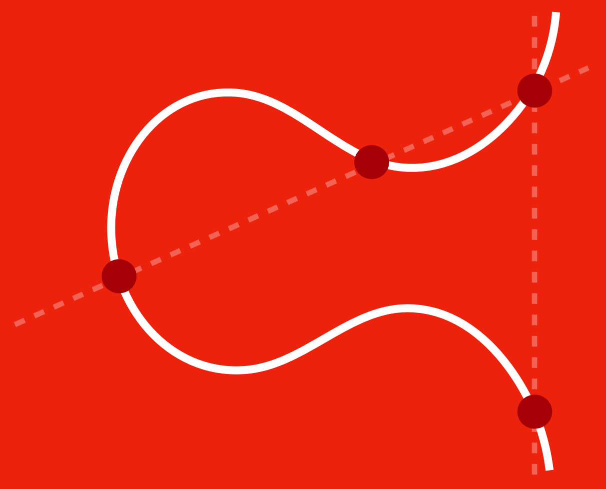
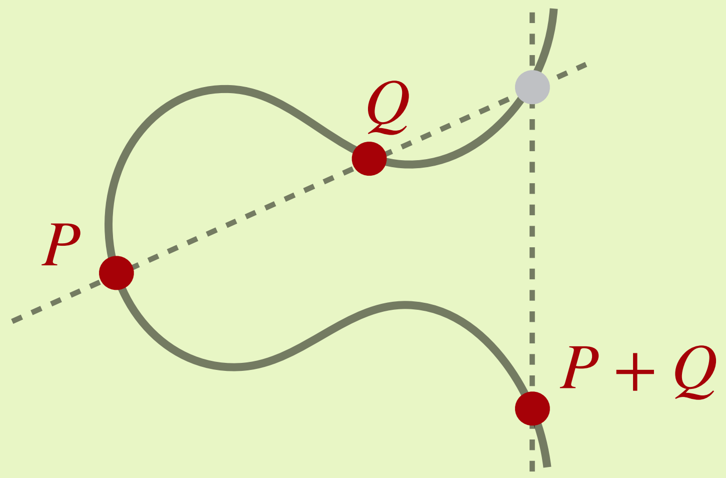


Isogenies & Pairings

elliptic curves in CSIDH

supersingular elliptic curve

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



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

points on such curves

We have that

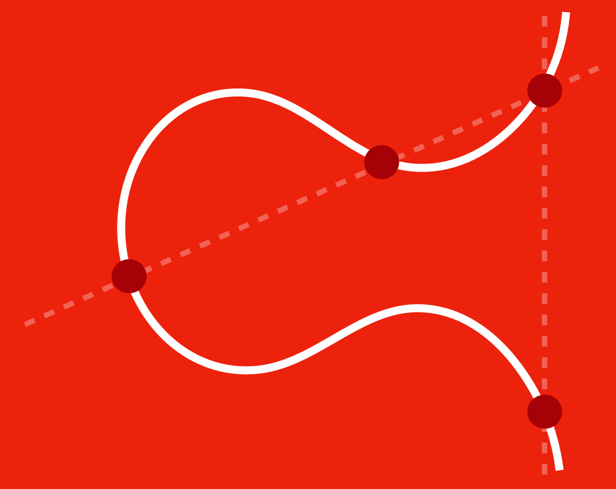
$$E(\mathbb{F}_p) \cong \mathbb{Z}_4 \times \mathbb{Z}_{\ell_1} \times \mathbb{Z}_{\ell_2} \times \ldots \times \mathbb{Z}_{\ell_n},$$

So think of a point $P \in E(\mathbb{F}_p)$ as a sum of points P_i of order ℓ_i

$$P = P_0 + P_1 + P_2 + \ldots + P_n$$

which shows how scalars $[\lambda]$ with $\lambda \in \mathbb{N}$ affect the torsion

$$\begin{aligned} [\ell_2]P &= [\ell_2]P_0 + [\ell_2]P_1 + [\ell_2]P_2 + \ldots + [\ell_2]P_n \\ &= [\ell_2]P_0 + [\ell_2]P_1 + \quad \mathcal{O} \quad + \ldots + [\ell_2]P_n \end{aligned}$$

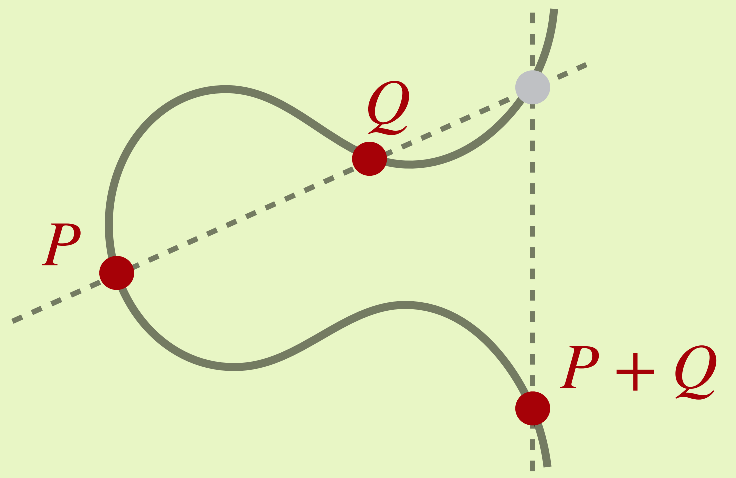


Isogenies & Pairings

elliptic curves in CSIDH

supersingular elliptic curve

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



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

points on such curves

We have that

$$E(\mathbb{F}_p) \cong \mathbb{Z}_4 \times \mathbb{Z}_{\ell_1} \times \mathbb{Z}_{\ell_2} \times \ldots \times \mathbb{Z}_{\ell_n},$$

So think of a point $P \in E(\mathbb{F}_p)$ as a sum of points P_i of order ℓ_i

$$P = P_0 + P_1 + P_2 + \ldots + P_n$$

which shows how scalars $[\lambda]$ with $\lambda \in \mathbb{N}$ affect the torsion

$$\begin{aligned}[\ell_2]P &= [\ell_2]P_0 + [\ell_2]P_1 + [\ell_2]P_2 + \ldots + [\ell_2]P_n \\ &= [\ell_2]P_0 + [\ell_2]P_1 + \quad \mathcal{O} \quad + \ldots + [\ell_2]P_n\end{aligned}$$

the order of P is readable from the non-zero 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