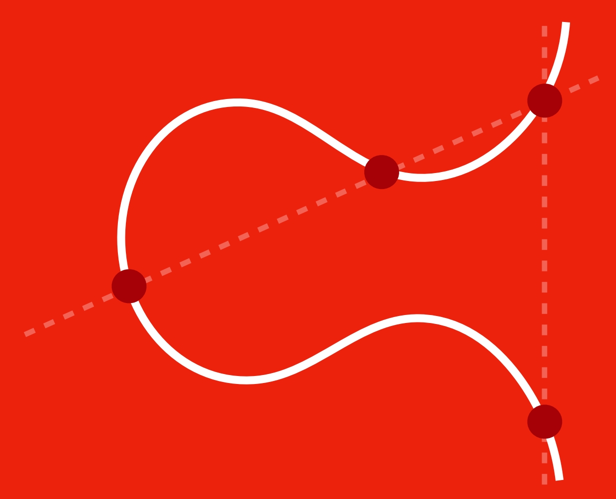
1

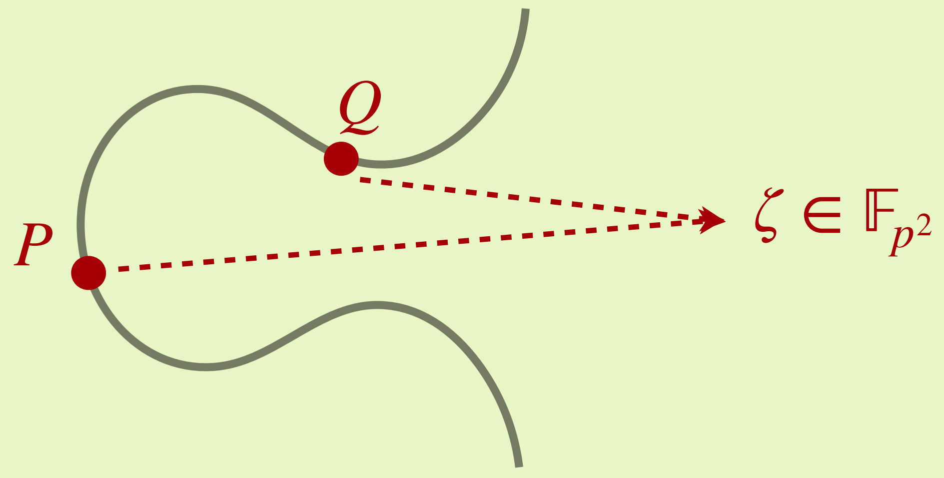


Isogenies & Pairings

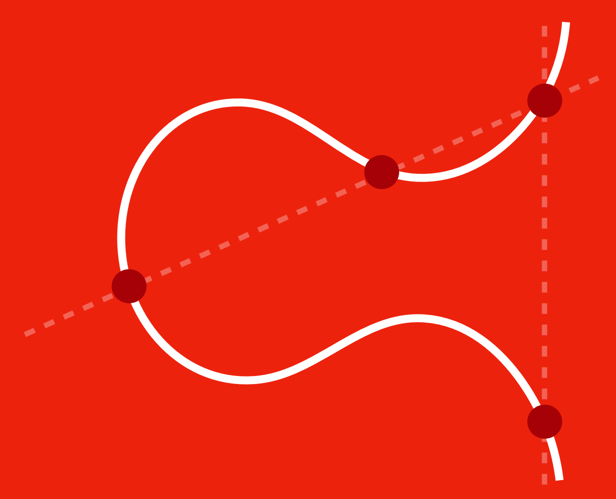
the Tate pairing*

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 $e_r(P,Q) = \zeta \in \mu_r$



*reduced

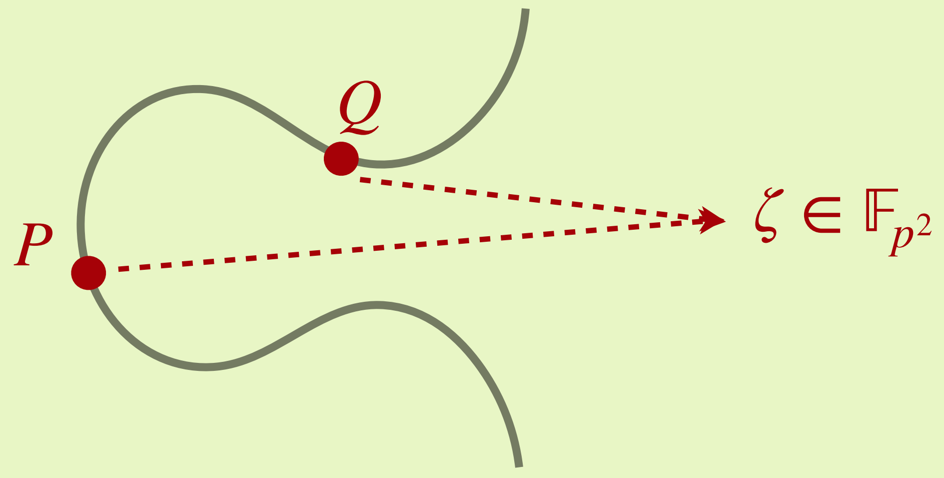


Isogenies & Pairings

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 $e_r(P, Q) = \zeta \in \mu_r$



in our specific case

Formally, this pairing is abstract. Specifically in our case, $p + 1 = 4 \cdot \ell_1 \cdot \ell_2 \cdot \ldots \cdot \ell_n$ there is a nice interpretation of this pairing.

Choose r dividing $p+1$, say $r = \prod \ell_i = \frac{p+1}{4}$ then for $P \in E(\mathbb{F}_p)$ we get

$$P = \mathcal{O} + P_1 + P_2 + \ldots + P_n.$$

*reduced