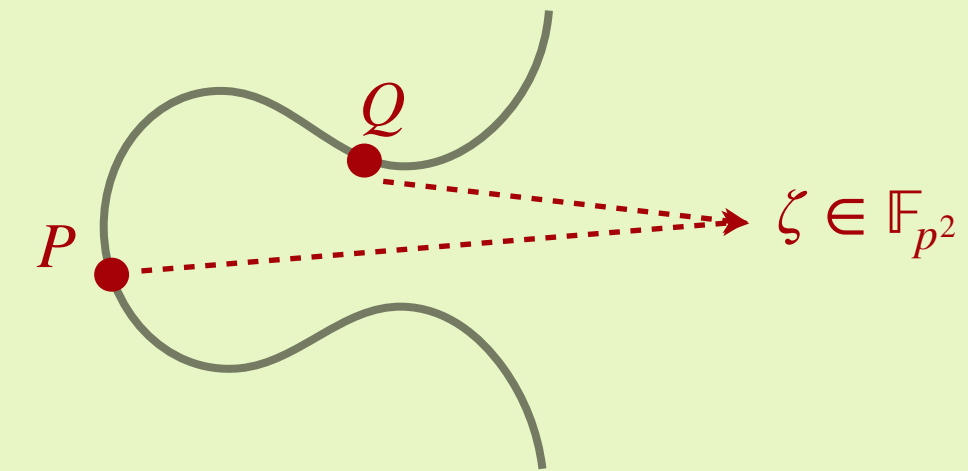


## Isogenies & Pairings

### 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,  $p+1 = 4 \cdot \ell_1 \cdot \ell_2 \cdot \dots \cdot \ell_n$  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

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

For  $Q \in E(\mathbb{F}_p)$ , we have equivalence by elements  $R$  in  $rE(\mathbb{F}_{p^2})$ . In this scenario, we can think of such elements  $R$  as  $R_0 + \mathcal{O} + \dots + \mathcal{O}$ , which implies  $Q \sim Q'$  whenever

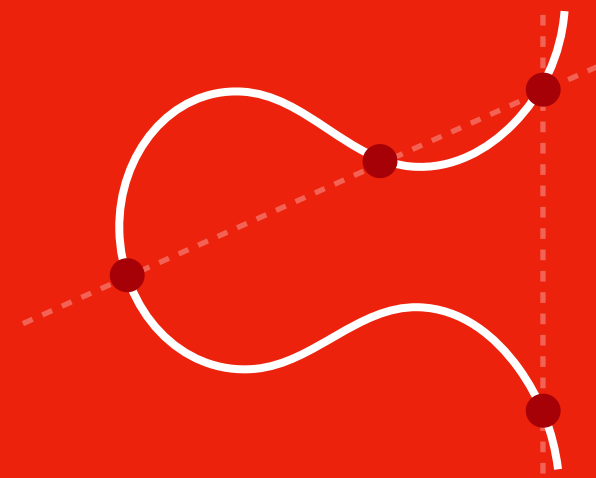
$$Q = Q_0 + Q_1 + Q_2 + \dots + Q_n \sim Q' = Q'_0 + Q_1 + Q_2 + \dots + Q_n$$

In this specific scenario, we can think of  $Q$  as the elements  $\mathcal{O} + Q_1 + \dots + Q_n$



#### problem

If we pick  $P, Q \in E(\mathbb{F}_p)$ ,  
then  $Q$  is a multiple of  $P$ .  
Then  $e_r(P, Q) = 1$

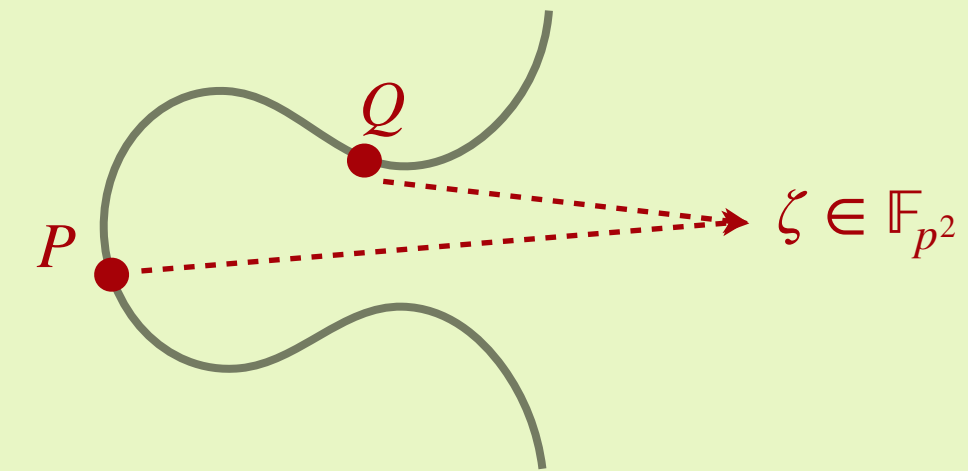


## Isogenies & Pairings

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



#### in our specific case

Formally, this pairing is abstract. Specifically in our case,  $p+1 = 4 \cdot \ell_1 \cdot \ell_2 \cdot \dots \cdot \ell_n$  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

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

For  $Q \in E(\mathbb{F}_p)$ , we have equivalence by elements  $R$  in  $rE(\mathbb{F}_{p^2})$ . In this scenario, we can think of such elements  $R$  as  $R_0 + \mathcal{O} + \dots + \mathcal{O}$ , which implies  $Q \sim Q'$  whenever

$$Q = Q_0 + Q_1 + Q_2 + \dots + Q_n \sim Q' = Q'_0 + Q_1 + Q_2 + \dots + Q_n$$

In this specific scenario, we can think of  $Q$  as the elements  $\mathcal{O} + Q_1 + \dots + Q_n$



#### problem

If we pick  $P, Q \in E(\mathbb{F}_p)$ , then  $Q$  is a multiple of  $P$ . Then  $e_r(P, Q) = 1$



#### solution

Work over  $E[r] \subseteq E(\mathbb{F}_{p^2})$ . In our specific case, just use  $Q$  on the *twist*