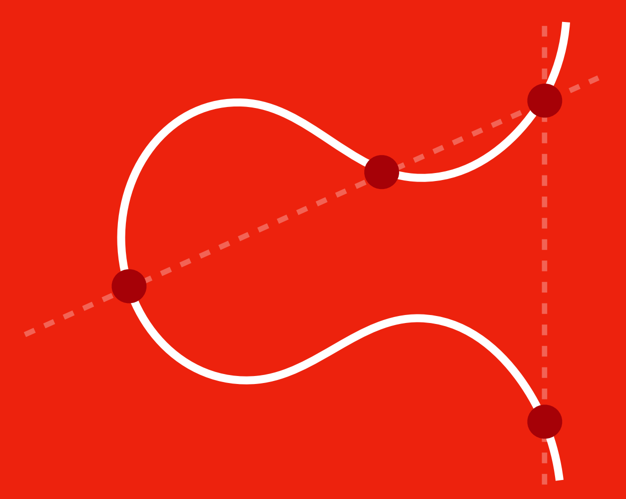
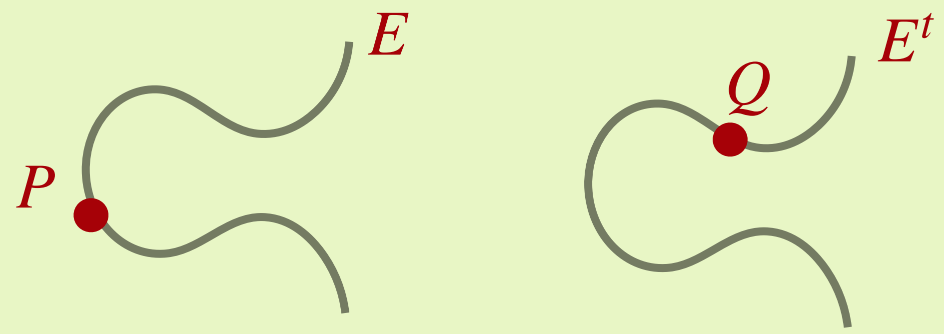


Isogenies & Pairings

the twist of E

Twist over $\mathbb{F}_p$ of supersingular curve E

- a curve E^t with $p+1$ points over $\mathbb{F}_p$
- isomorphic to a specific subset of $E(\mathbb{F}_{p^2})$
- used in CSIDH to "move backwards" in graph
- want $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$, both full order



1

consider P and Q as

$$P = P_0 + P_1 + \ldots + P_n$$
$$Q = Q_0 + Q_1 + \ldots + Q_n$$

2

let $r = p + 1$

Tate pairing $e_r(P, Q)$ captures where **both** $P_i, Q_i \neq \mathcal{O}$

crucial lemma

Let $P \in E(\mathbb{F}_p)$, $Q \in E^t(\mathbb{F}_p)$, and $r = p+1$. Let $\zeta = e_r(P, Q) \in \mathbb{F}_{p^2}$.

Then ζ is an r-th root of unity, whose order is precisely $\gcd$ of order of P, order of Q

example

If P and Q both full torsion, then ζ has order $r = p + 1$

example

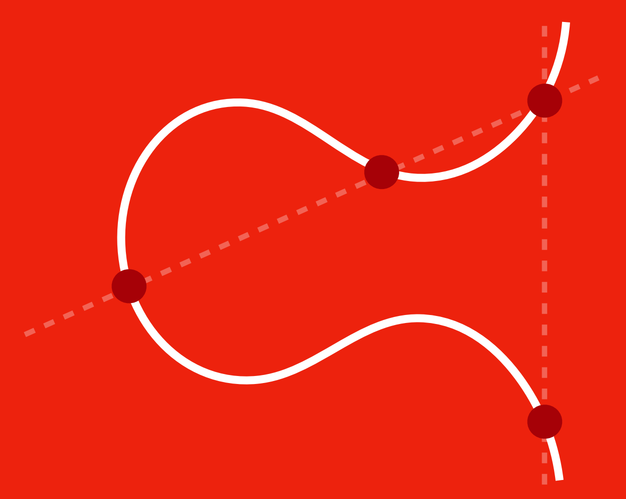
If P has order 5, and Q has order 15, then ζ has order 5

!

notice

Curve arithmetic is slow!
Field arithmetic is fast!!
(more than factor 6)

1

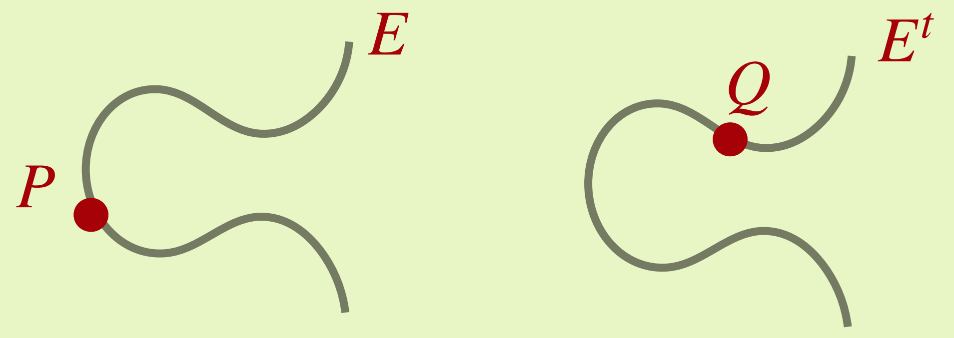


Isogenies & Pairings

the twist of E

Twist over $\mathbb{F}_p$ of supersingular curve E

- a curve E^t with $p+1$ points over $\mathbb{F}_p$
- isomorphic to a specific subset of $E(\mathbb{F}_{p^2})$
- used in CSIDH to "move backwards" in graph
- want $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$, both full order



1

consider P and Q as

$$P = P_0 + P_1 + \ldots + P_n$$
$$Q = Q_0 + Q_1 + \ldots + Q_n$$

2

let $r = p + 1$

Tate pairing $e_r(P, Q)$ captures where **both** $P_i, Q_i \neq \mathcal{O}$

crucial lemma

Let $P \in E(\mathbb{F}_p)$, $Q \in E^t(\mathbb{F}_p)$, and $r = p+1$. Let $\zeta = e_r(P,Q) \in \mathbb{F}_{p^2}$.

Then ζ is an r-th root of unity, whose order is precisely $\gcd$ of order of P, order of Q

example

If P and Q both full torsion, then ζ has order $r = p + 1$

example

If P has order 5, and Q has order 15, then ζ has order 5

!

notice

Curve arithmetic is slow!
Field arithmetic is fast!!
(more than factor 6)

✓

core idea

Pick random $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$
Instead of using curve arithmetic to compute their orders, use ζ to compute the overlap in orders!