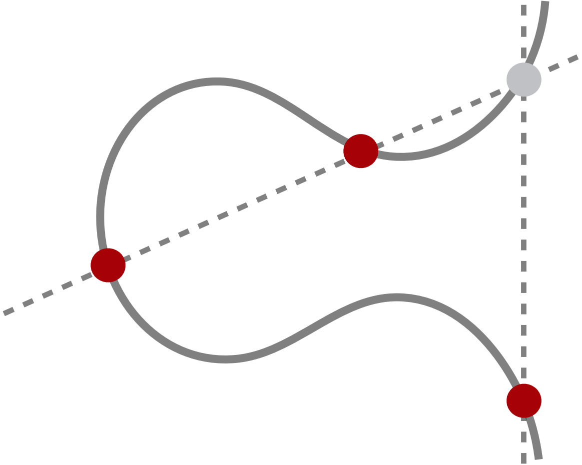
1

Isogenies & Pairings

Radboud University

IN DEI NOMINE FELICITER



elliptic curves in CSIDH

P

Q

$$P + Q$$

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

orders that divide

supersingular elliptic curve

- this implies the rational points on

points in

so that

have

- choose

- has

$$p + 1$$

$$E(\mathbb{F}_p)$$

p

$$p + 1 = 4 \cdot \ell_1 \cdot \ell_2 \cdot \ldots \cdot \ell_n$$

E

$p + 1$

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

of order

as a sum of points

$$P \in E(\mathbb{F}_p)$$

P_i

ℓ_i

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

which shows how scalars

affect the torsion

with

[λ]

$$\lambda \in \mathbb{N}$$

$$[\ell_2]P = [\ell_2]P_0 + [\ell_2]P_1 + [\ell_2]P_2 + \ldots + [\ell_2]P_n$$

$$= [\ell_2]P_0 + [\ell_2]P_1 + \quad \mathcal{O} \quad + \ldots + [\ell_2]P_n$$

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

a **full-torsion point**

, equivalently, all

we call a point

if the order is

are non-zero

$$P \in E(\mathbb{F}_p)$$

$$p + 1$$

P_i

torsion points and isogenies

- generated by point

- given by kernel of size

1. Any* isogeny

of degree

of order

φ

N

N

P

N

$$P = P_3 + P_5 + P_7 \in E(\mathbb{F}_p)$$

$$\xrightarrow{\varphi}$$

*cyclic, separable

- splits into sub-isogenies of degree

- each generated by point

2. Any* isogeny

of degree

of order

φ

$$N = \prod \ell_i$$

ℓ_i

P

ℓ_i

deg

$3 \cdot 5 \cdot 7$

deg

3

deg

5

deg

7

3. Any* isogeny

- computed using one **full-torsion**

of degree

, compute

to get

_ per

φ

$$N = \prod \ell_i$$

P

ℓ_i

$$[\frac{p+1}{\ell_i}]P$$

$\ker(\varphi_i)$

$$[5 \cdot 7]P = P'_3 + \mathcal{O} + \mathcal{O} \in E(\mathbb{F}_p)$$

$$\varphi_1(P) = \mathcal{O} + P_5' + P_7' \in E'(\mathbb{F}_p)$$

points on such curves

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

a **full-torsion point**

, equivalently, all

we call a point

if the order is

are non-zero

torsion points and isogenies

$$P = P_3 + P_5 + P_7 \in E(\mathbb{F}_p)$$