PART 1

The Tate Pairing

Corollary. Let 2^n divide $p+1$ for some prime p, and take a supersingular Montgomery curve over $\mathbb{F}_{p^2}$ given by

$$E_A : y^2 = x^3 + Ax^2 + x, \qquad \text{with } A \in \mathbb{F}_{p^2}.$$

If a point $P = (x_P, y_P) \in E(\mathbb{F}_{p^2})$ has x_P non-square, then P has order divisible by 2^n

PART 1

The Tate Pairing

Corollary. Let 2^n divide $p+1$ for some prime p, and take a supersingular Montgomery curve over $\mathbb{F}_{p^2}$ given by

$$E_A : y^2 = x^3 + Ax^2 + x, \qquad \text{with } A \in \mathbb{F}_{p^2}.$$

If a point $P = (x_P, y_P) \in E(\mathbb{F}_{p^2})$ has x_P non-square, then P has order divisible by 2^n

Tate Pairing?