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 $2^n$

**Theorem 3.** For an elliptic curve $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$ with $r_i \in \mathbb{F}_{p^2}$, we have

$P \in [2]E(\mathbb{F}_{p^2})$ *if and only if* $(x_P - r_1)$, $(x_P - r_2)$, and $(x_P - r_3)$ are squares.

Consequently, $P \in E(\mathbb{F}_{p^2}) \setminus [2]E(\mathbb{F}_{p^2})$ if any $(x_P - r_i)$ is a non-square.

Tate Pairing?

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 $2^n$

---

**Theorem 3.** For an elliptic curve $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$ with $r_i \in \mathbb{F}_{p^2}$, we have

$$P \in [2]E(\mathbb{F}_{p^2}) \qquad \textit{if and only if} \qquad (x_P - r_1),\ (x_P - r_2), \text{ and } (x_P - r_3) \text{ are squares.}$$

Consequently, $P \in E(\mathbb{F}_{p^2}) \setminus [2]E(\mathbb{F}_{p^2})$ if any $(x_P - r_i)$ is a non-square.

**Tate Pairing???**